Übungsblatt 1: Monoide und Gruppen

Die schriftlichen Übungsaufgaben sind durch ein S gekennzeichnet und sollen in der Übung der nächsten Woche abgegeben werden. Die Votieraufgaben sind mit einem V gekennzeichnet. Nicht gekennzeichnete Aufgaben sind entweder elementar und sollen in ein Thema einführen oder weiterführend und bieten die Gelegenheit sich weitere Gedanken zu machen.
Du wolltest doch Algebra, da hast Du den Salat. — *Jules Verne*

1. Rechnen mit Mengen

Auf einer Menge G sei eine Verknüpfung $* : G \times G \to G$ gegeben, sowie Teilmengen $U, V \subset G$ und eine Abbildung $f\colon G \to G$. Wir definieren $U * V := \{u * v : u \in U, v \in V\}$ und $f(U) := \{f(u) : u \in U\}$.

V 1.1. (a) Sei $U = [1,2] \subset \mathbb{R}$. Bestimmen Sie $U+U$ und $U-U$.
Wenn $I, J \subset \mathbb{R}$ zwei Intervalle sind, ist dann $I+J$ ein Intervall?
(Zur Erinnerung: Intervalle sind die konvexen Teilmengen von $\mathbb{R}$.)
(b) Finden und beweisen Sie eine Darstellung der Menge $12\mathbb{Z}+20\mathbb{Z}$ in der Form $a\mathbb{Z}$ für ein geeignetes $a \in \mathbb{Z}$. Man vergleiche dies mit der Menge $12\mathbb{N}+20\mathbb{N}$.

Lösungshinweise: —

(a) *Zuerst Überlegen wir uns die Aussage: die Summe zweier Intervalle ist ein Intervall. Dazu seien $x = i_1 + j_1 \in I+J$ und $y = i_2 + j_2 \in I+J$. Es reicht zu zeigen, dass die Konvexkombination der beiden "Punkte" wieder in $I+J$ liegt. Aber $tx+(1-t)y = ti_1+(1-t)i_2+tj_1+(1-t)j_2 \in I+J$, da I und J selbst Intervalle (also konvex) sind. Damit ist die Aussage gezeigt.*
Um $U+U$ und $U-U$ zu bestimmen, müssen wir nur jeweils das Maximum und Minimum der Mengen bestimmen, da dies Intervalle und damit dadurch eindeutig festgelegt sind. Dies ist aber leicht gemacht und ergibt die Antwort: $U+U = [2,4]$ und $U-U = [-1,1]$.
Man beachte, dass die Differenz $U-U$ nicht die leere Menge ist!

(b) *Es gilt $12\mathbb{Z}+20\mathbb{Z} = 4\mathbb{Z}$, denn $4 = 12\cdot 2 + 20\cdot(-1) \in 12\mathbb{Z}+20\mathbb{Z}$ und damit auch $4\mathbb{Z} \subset 12\mathbb{Z}+20\mathbb{Z}$. Andererseits ist jede Zahl in $12\mathbb{Z}+20\mathbb{Z}$ durch 4 teilbar, woraus die Inklusion $12\mathbb{Z}+20\mathbb{Z} \subset 4\mathbb{Z}$ folgt.*
Im Fall $12\mathbb{N}+20\mathbb{N}$ ist das Ganze nicht ganz so einfach. In der Vorlesung wurde gezeigt, dass $3\mathbb{N}+5\mathbb{N} = \mathbb{N}\setminus\{1,2,4,7\}$, woraus durch Multiplikation mit 4 folgt, dass $12\mathbb{N}+20\mathbb{N} = 4\mathbb{N}\setminus\{4,8,16,28\}$.

—

S 1.2. (3 Punkte) Sei $(G,*)$ eine Gruppe und $U, V, W \subset G$ Teilmengen.
(a) Zeigen Sie, dass $(U*V)*W = U*(V*W)$ und $(U*V)^{-1} = V^{-1}*U^{-1}$.
(b) Ist die Potenzmenge $\mathscr{P}(G)$ mit dieser Mengenverknüpfung $*$ ein Monoid?
(c) Ist $(\mathscr{P}(G),*)$ eine Gruppe? Ist die Kürzungsregel $U*V = U*W \Rightarrow V = W$ erfüllt?

Lösungshinweise: —

(a) *Dies rechnet man direkt mit Hilfe der Definitionen nach.*

$$\begin{aligned}(U*V)*W &= \{u*v : u\in U, v\in V\}*W = \{(u*v)*w : u\in U, v\in V, w\in W\}\\ &= \{u*(v*w) : u\in U, v\in V, w\in W\} = U*\{v*w : v\in V, w\in W\} = U*(V*W)\end{aligned}$$

$$\begin{aligned}(U*V)^{-1} &= \{u*v : u\in U, v\in V\}^{-1} = \{(u*v)^{-1} : u\in U, v\in V\}\\ &= \{v^{-1}*u^{-1} : u\in U, v\in V\} = \{v^{-1} : v\in V\}*\{u^{-1} : u\in U\} = V^{-1}*U^{-1}\end{aligned}$$

(b) *In Teil (a) sieht man, dass die Verknüpfung assoziativ ist. Wir müssen also nur noch ein neutrales Element finden. Das ist gegeben durch $E = \{e\}$, wobei e das neutrale Element der Gruppe ist. Denn es gilt $E * U = \{e * u : u \in U\} = \{u * e : u \in U\} = U * E = U$.*
Bemerkung: *Man sieht auch, dass $(\mathscr{P}(G), *)$ schon zu einem Monoid wird, wenn $(G, *)$ ein Monoid war.*

(c) *Wir zeigen, dass die Kürzungsregel nicht erfüllt ist und damit keine Gruppe vorliegen kann. Es gilt zum Beispiel $G = G * E \subset G * G \subset G$ und damit $G * G = G * E$, obwohl $G \neq E$ falls $|G| > 1$.*

—

2. KLEINE GRUPPEN I: VERKNÜPFUNGSTAFELN

Ein Ziel der Algebra-Vorlesung ist es, Gruppen besser zu verstehen. Wir wollen daher versuchen, möglichst viele Gruppen so explizit wie möglich darzustellen. Hierzu werden wir nach und nach geeignete Werkzeuge kennenlernen.

Eine elementare Möglichkeit, Gruppen zu beschreiben, sind die sogenannten Verknüpfungstafeln. Für eine endliche Gruppe $(G, \cdot)$ mit Elementen $\{g_1, \dots, g_n\}$ ist dies eine $n \times n$-Matrix, deren Eintrag in der i-ten Zeile und j-ten Spalte durch das Gruppenelement $g_i \cdot g_j$ gegeben ist. Zur Vereinfachung setzt man $g_1 = e$.

2.1. Kann die folgende Tabelle zu einer Verknüpfungstafel einer Gruppe ergänzt werden? Was kann man damit über die Untergruppen einer Gruppe mit 3 Elementen aussagen?

·	e	a	b
e	e	a	
a	a	e	
b			

Lösungshinweise: — *Offenbar muss $e \cdot b = b \cdot e = b$ gesetzt werden. Damit ergibt sich aber stets ein Widerspruch, wenn man $a \cdot b$ definieren will (zum Beispiel zur Aufgabe 2.2). Damit folgt, dass eine Gruppe der Ordnung 3 keine Untergruppe der Ordnung 2 enthalten kann.* —

S 2.2. (3 Punkte) Zeigen Sie, dass in jeder Zeile und Spalte einer Verknüpfungstafel jedes Element der Gruppe genau ein Mal vorkommt. Wie kann man an der Verknüpfungstafel erkennen, ob die Gruppe kommutativ ist? Zusatzfrage: Kann man daran ebenso leicht die Assoziativität der Verknüpfung ablesen?

Lösungshinweise: — *Wir betrachten die Abbildungen $\lambda_a : G \to G : x \mapsto a \cdot x$ und $\rho_b : G \to G : x \mapsto x \cdot b$. Wenn wir zeigen können, dass die beiden Funktionen für alle $a, b \in G$ bijektiv sind, dann folgt die Aussage. Man kann entweder Injektivität und Surjektivität prüfen, oder direkt eine Umkehrfunktion angeben. Es gilt $\lambda_{a^{-1}} \circ \lambda_a(x) = a^{-1} \cdot (a \cdot x) = (a^{-1} \cdot a) \cdot x = e \cdot x = x = \mathrm{id}(x)$ für alle $x \in G$, also $\lambda_{a^{-1}} \circ \lambda_a = \mathrm{id}$. Ebenso folgt $\lambda_a \circ \lambda_{a^{-1}} = \mathrm{id}$, $\rho_{a^{-1}} \circ \rho_a = \mathrm{id}$ und $\rho_a \circ \rho_{a^{-1}} = \mathrm{id}$.*
Die Kommutativität $g_i \cdot g_j = g_j \cdot g_i$ ist offenbar äquivalent dazu, dass die Matrix symmetrisch ist.
Für die Assoziativität ist kein einfaches Kriterium bekannt. Deswegen ist es auch so nützlich eine Gruppe als Untergruppe einer größeren Gruppe zu erkennen. Dann bekommt man diese Eigenschaft "geschenkt".
—

V 2.3. Bestimmen Sie alle Gruppen mit $1, 2, 3, 4, 5, \dots$ Elementen bis auf Isomorphie. Wie weit kommen Sie?

Lösungshinweise: — *Zuerst einmal die Lösung: $\{e\}, \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/3\mathbb{Z}, (\mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}), \mathbb{Z}/5\mathbb{Z}, (\mathbb{Z}/6\mathbb{Z}, S_3)$.*
Man kann diese Gruppen als Untergruppen der symmetrischen Gruppen darstellen. Daraus erhält man die Assoziativität, ohne sie direkt prüfen zu müssen.
Um zu zeigen, dass diese Liste vollständig ist, zeigt man, dass die Verknüpfungstafeln unter Beachtung

des neutralen Elements, der Assoziativität und Aufgabe 2.2 nur auf sehr wenige Weisen ausgefüllt werden können. Einige davon gehen ineinander über, wenn man die Elemente in der Verknüpfungstafel vertauscht, so dass man sich auch schon zu Beginn einige Arbeit sparen kann, wenn man Symmetrieannahmen macht.

—

3. DAS UR-MONOID

S 3.1. (2 Punkte) Sei X eine Menge und $Abb(X) = \{f : X \to X\}$ die Menge aller Selbstabbildungen zusammen mit der Komposition von Abbildungen als Verknüpfung.
(a) Zeigen Sie, dass $Abb(X)$ mit der Komposition zu einem Monoid wird.
(b) Zeigen Sie, dass $Sym(X) = \{f : X \to X \mid f \text{ bijektiv}\}$ ein Untermonoid ist. Ist $Sym(X)$ eine Gruppe?

Lösungshinweise: —

(1) *Man muss zeigen, dass die Verknüpfung von Abbildungen assoziativ ist und ein neutrales Element existiert. Es gilt* $(f \circ (g \circ h))(x) = f((g \circ h)(x)) = f(g(h(x))) = \ldots = ((f \circ g) \circ h)(x)$ *für alle* $x \in X$ *und die Identität* id *ist das gesuchte neutrale Element, wie man ebensoleicht nachprüft.*

(2) *Die Hintereinanderausführung zweier bijektiver Abbildungen ist bijektiv. Damit ist* $Sym(X)$ *abgeschlossen unter Komposition. Die Identität ist offenbar bijektiv, ist also auch in* $Sym(X)$ *enthalten.* $Sym(X)$ *ist sogar eine Gruppe, da zu jeder bijektiven Funktion* f *eine weitere bijektive Funktion* f^{-1} *existiert, so dass* $f \circ f^{-1} = f^{-1} \circ f = \mathrm{id}$ *gilt.*

—

Die vorhergehende Konstruktion ist in folgendem Sinne universell:

V 3.2. Zeigen Sie, dass jedes Monoid $(M, \cdot)$ sich als Untermonoid von $Abb(X)$ für eine geeignete Menge X auffassen lässt. (Satz von Cayley für Monoide)
Hinweis: Für $a \in M$ ist die Linksmultiplikation $\lambda_a : M \to M : x \mapsto a \cdot x$ ein Element von $Abb(M)$ und $\varphi : M \to Abb(M) : a \mapsto \lambda_a$ ein Monoid-Homomorphismus.

Lösungshinweise: — *Dem Hinweis folgend wählen wir* $X = M$ *und die angegebene Abbildung* φ*. Diese ist ein injektiver Monoid-Homomorphismus mit* $\varphi(e) = \lambda_e = \mathrm{id}$*. Denn sei* $\varphi(a) = \varphi(b)$*, d.h.* $\lambda_a = \lambda_b$*, dann ist auch* $a = a \cdot e = \lambda_a(e) = \lambda_b(e) = b \cdot e = b$*. Die Homomorphieeigenschaft folgt aus der Assoziativität der Gruppenmultiplikation:* $\lambda_{a \cdot b}(x) = (a \cdot b) \cdot x = a \cdot (b \cdot x) = \lambda_a(\lambda_b(x))$*, also* $\lambda_{a \cdot b} = \lambda_a \circ \lambda_b$*, d.h.* $\varphi(a \cdot b) = \varphi(a) \circ \varphi(b)$
Das Bild dieses injektiven Monoid-Homomorphismus ist isomorph zu M und ist eine Teilmenge von $Abb(M)$*.*
—

Wir wollen nun sehen, ob man die obige Aussage noch weiter verallgemeinern kann.

V 3.3. Sei H eine Menge mit assoziativer Verknüpfung $\cdot$, eine sogenannte *Halbgruppe*. Wir nehmen an, dass kein neutrales Element existiert (sonst sind wir wieder im obigen Fall). Wir betrachten nun die Menge $M = H \cup \{e\}$ für ein Element $e \notin H$. Kann man die Verknüpfung auf M fortsetzen, so dass diese assoziativ bleibt und e zum neutralen Element dieser Verknüpfung wird?

Lösungshinweise: — *Ja, es geht. Da e neutral sein soll, kann die Definition nur auf eine Weise erfolgen und man prüft schnell nach, dass die Assoziativität erhalten bleibt.* —

V 3.4. Gilt der Satz von Cayley auch für jede Halbgruppe H? Reicht es, wie zuvor, von der Linksmultiplikation auf H auszugehen?

Lösungshinweise: — *Man kann zwar nicht ohne weiteres H als Unterhalbgruppe von* $Abb(H)$ *in der obigen Form konstruieren, wie das Beispiel*

$\cdot$	a	b
a	a	a
b	a	a

zeigt. Allerding folgt aus Aufgabe 3.3, dass man H als Unterhalbgruppe in $Abb(M)$ *wiederfindet. Der Beweis bleibt fast der gleiche wie im Fall eines Monoids.*
—

4. Wohlordnung und Induktion

Definition: Eine binäre Relation $\trianglelefteq$ auf einer Menge A heißt *Ordnungsrelation*, wenn sie reflexiv ist (d.h. es gilt $a \trianglelefteq a$ für alle $a \in A$), transitiv (d.h. $a \trianglelefteq b$ und $b \trianglelefteq c$ impliziert $a \trianglelefteq c$) und anti-symmetrisch (d.h. aus $a \trianglelefteq b$ und $b \trianglelefteq a$ folgt $a = b$).
Eine Ordnungsrelation heißt *total-geordnet*, wenn für $a, b \in A$ stets $a \trianglelefteq b$ oder $b \trianglelefteq a$ gilt.
Eine Menge M mit einer totalen Ordnungsrelation $\trianglelefteq$ heißt *wohlgeordnet*, wenn jede nichtleere Menge in M ein (bezüglich $\trianglelefteq$) minimales Element besitzt, d.h. ein $m_0 \in M$, so dass aus $m \trianglelefteq m_0$ folgt, dass $m = m_0$ gilt. (Ist m_0 eindeutig?)

V 4.1. (a) Zeigen Sie, dass $\mathbb{N}$ mit der kleiner-gleich Relation $\leq$ wohlgeordnet ist.
(b) Sei $K \subset \mathbb{N}$ mit $1 \in K$ und der Eigenschaft $k \in K \Rightarrow k+1 \in K$ gegeben. Zeigen Sie, dass aus der Wohlordnung von $\mathbb{N}$ folgt, dass $K = \mathbb{N}$ ist.

Lösungshinweise: —

(1) *Wir wissen aus den Grundvorlesungen, dass $\mathbb{N}$ mit $\leq$ eine geordnete Menge ist. Wir müssen noch zeigen, dass jede nichtleere Menge ein minimales Element enthält. Sei dazu $M \subset \mathbb{N}$ ohne minimales Element gegeben. Dann ist $1 \notin M$, da dieses sonst das Minimum von M wäre. Ebenso gilt, dass aus $1, \dots, k \notin M$ folgt, dass $k+1 \notin M$, denn sonst wäre $k+1$ das minimale Element von M. Damit folgt mit Induktion, dass $\mathbb{N} \backslash M = \mathbb{N}$, oder $M = \emptyset$.*

(2) *Sei $M := \mathbb{N} \backslash K$. Falls $M \neq \emptyset$, dann besitzt M ein minimales Element m_0. Nach Voraussetzung ist $m_0 \neq 1$ und $m_0 - 1 \notin M$ nach Minimalität. Das heißt aber nichts anderes, als $m_0 - 1 \in K$ und damit $m_0 \in K$. Das Widerspricht unserer Annahme. Also insgesamt $M = \emptyset$, oder $K = \mathbb{N}$.*

—

Somit kann man induktive Aussagen in $\mathbb{N}$ beweisen kann, indem man zeigt, dass es kein kleinstes Gegenbeispiel gibt. Der Vorteil dieser Methode ist, dass sie sich auch auf Mengen verallgemeinern lässt, die nicht total geordnet sind, aber noch die Eigenschaft besitzen, dass jede nichtleere Menge ein minimales Element besitzt.
Ein Spezialfall ist die Methode des *unendlichen Abstiegs*. Dabei konstruiert man aus einer angenommenen minimalen Lösung eine kleinere Lösung. Dies widerspricht der Annahme, dass man schon eine minimale Lösung vorliegen hatte. Zum Beispiel:

V 4.2. Zeigen Sie, dass es kein regelmäßiges 7-Eck mit Ecken in $\mathbb{Z}^2$ gibt.
Können Sie das ebenso für ein regelmäßiges 5-Eck zeigen?

Lösungshinweise: — *Zu einem gegebenen 7-Eck in $\mathbb{Z}^2$ mit minimalem Durchmesser und Ecken $z_1, \dots, z_7$ (zyklisch angeordnet) betrachte man die Punkte $b_i = z_{i+1} - z_i$ (dabei sei $z_8 = z_1$). Dies sind wieder sieben Punkte in $\mathbb{Z}^2$, die ein regelmäßiges 7-Eck bilden, welches einen kleineren Durchmesser hat, weil bei jedem 7-Eck die Seitenlänge echt kleiner als der halbe Durchmesser ist.*
Dieser Trick funktioniert auch für alle n-Ecke mit $n \geq 7$. Für $n = 5$ muss man sich etwas mehr Mühe geben. Dazu nutzt man die Beobachtung, dass es zu jeder Seite des Fünfecks eine parallele Diagonale gibt, die Länger als die Seite ist. Nimmt man nun also die 5 Seiten des Fünfecks und verwendet sie als Diagonalen eines neuen regelmäßigen Fünfecks, so hat dieses wieder Ecken in $\mathbb{Z}^2$ und ist kleiner als das vorhergehende. —

Eine typische Anwendung in der Gruppentheorie ist die folgende. Die Menge aller endlichen Gruppen ist durch Inklusion geordnet. Wenn eine Aussage über endliche Gruppen nicht richtig ist, so muss es eine (nicht unbedingt eindeutige) minimale Gruppe geben, die die Aussage nicht erfüllt: einen sogenannten “kleinsten Verbrecher”. Dieser müsste dann sehr spezielle Eigenschaften besitzen, was dann oft zum Widerspruch führt.