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 $f: G \to G$. 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 $12\mathbb{N} + 20\mathbb{N}$.

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?

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			

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?

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

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?

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.

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?

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

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.

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?

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.