Musterlösung Serie 1

GRUPPEN, UNTERGRUPPEN

1. In welchen der folgenden Fälle ist $(G, *)$ eine Gruppe?

   (a) $G := \mathbb{R}$ mit $x * y := x + y - xy$.

   (b) $G := \mathbb{R}^3$ mit dem Kreuzprodukt $x * y := x \times y$.

   (c) G das offene Intervall $(-1, 1)$ mit $x * y := \frac{x+y}{1+xy}$.

   Lösung: Wir überprüfen in allen Fällen die Gruppenaxiome:

   (a)

   - Die Verknüpfung $*$ ist assoziativ: Für alle $x, y, z \in G$ gilt

   $$\begin{aligned}(x * y) * z &= (x + y - xy) + z - (x + y - xy)z \\ &= x + y + z - xy - xz - yz + xyz \\ &= x + (y + z - yz) - x(y + z - yz) \\ &= x * (y * z).\end{aligned}$$

   - Die Verknüpfung besitzt das neutrale Element $0 \in G$.
   - Ein Element $x \in G$ ist genau dann invertierbar, wenn ein $y \in G$ existiert mit

   $$x + y - xy = 0, \quad \text{also} \quad y(x - 1) = x.$$

   Für $x \neq 1$ hat diese Gleichung die Lösung $y = \frac{x}{x-1}$. Für $x = 1$ hat die Gleichung keine Lösung; somit ist das Element $1 \in G$ nicht invertierbar.

   Also ist G keine Gruppe.

   Bemerkung: Immerhin ist aber $\mathbb{R} \smallsetminus \{1\}$ mit der Verknüpfung $*$ eine Gruppe. Die Abbildung $\mathbb{R} \smallsetminus \{1\} \to \mathbb{R} \smallsetminus \{0\}$, $t \mapsto 1 - t$ ist ein *Isomorphismus* von $(\mathbb{R} \smallsetminus \{1\}, *, 0)$ auf $(\mathbb{R} \smallsetminus \{0\}, \cdot, 1)$.

   (b) Das Kreuzprodukt ist nicht assoziativ. Beispielsweise gilt $(x \times y) \times y \neq 0$ und $x \times (y \times y) = 0$ für je zwei $\mathbb{R}$-linear unabhängige Elemente $x, y \in \mathbb{R}^3$. Also ist G keine Gruppe.

   (c) Hier gilt es zunächst zu verifizieren, dass $G = (-1, 1)$ abgeschlossen ist unter der gegebenen Verknüpfung $*$ (also, dass diese wohl-definiert ist): Für alle $x, y \in G$ gilt $1 + xy > 0$ und

   $$x * y \;=\; \frac{x + y}{1 + xy} \;=\; \frac{(1 + x)(1 + y)}{1 + xy} - 1 \;>\; -1,$$

sowie

$$x * y \;=\; \frac{x+y}{1+xy} \;=\; 1 - \frac{(1-x)(1-y)}{1+xy} \;<\; 1.$$

Also haben wir gezeigt, dass $x * y \in (-1,1)$ ist. Nun überprüfen wir die Gruppenaxiome für alle $x, y, z \in G$:

- Die Verknüpfung $*$ ist assoziativ, denn eine direkte Rechnung zeigt:

$$(x * y) * z \;=\; \frac{x+y+z+xyz}{1+xy+xz+yz} \;=\; x * (y * z).$$

- Die Verknüpfung $*$ besitzt das linksneutrale Element $0 \in G$, denn

$$0 * x \;=\; \frac{x}{1} \;=\; x.$$

- Ausserdem hat x das Linksinverse $-x$ wegen

$$(-x) * x \;=\; \frac{-x+x}{1+(-x)\cdot x} \;=\; 0.$$

Somit ist $(G, *)$ eine Gruppe.

Bemerkung: Die Abbildung $(-1,1) \to \mathbb{R}$, $t \mapsto \frac{t}{1-t^2}$ ist ein *Isomorphismus* von $\big((-1,1), *, 0\big)$ auf $(\mathbb{R}, +, 0)$.

2. Entscheide, für welche Werte $a, b, c \in \mathbb{R}$ die Verknüpfung $x * y := ax + by + c$ eine Gruppenstruktur auf $\mathbb{R}$ definiert.

   Lösung: Wir überprüfen die Gruppenaxiome:

   - Ein Element $e \in \mathbb{R}$ ist genau dann ein beidseitiges neutrales Element bezüglich $*$, wenn für alle $x \in \mathbb{R}$ gilt

$$ax + be + c = x \quad \text{und} \quad ae + bx + c = x.$$

     Dafür, dass diese Gleichungen eine von x unabhängige Lösung besitzen, erhalten wir durch Koeffizientenvergleich die notwendigen Bedingungen $a = b = 1$. Wenn diese gelten, dann sind beide Gleichungen von $e = -c$ erfüllt.

   - Assoziativität: Unter den Bedingungen $a = b = 1$ zeigt eine direkte Rechnung, dass für alle $x, y, z \in \mathbb{R}$ gilt:

$$(x * y) * z = x + y + z + 2c = x * (y * z).$$

   - Seien weiterhin $a = b = 1$ und $e = -c$. Dann ist ein Element $x \in \mathbb{R}$ genau dann invertierbar bezüglich $*$, wenn ein $y \in \mathbb{R}$ existiert mit

$$x + y + c = -c.$$

     Diese Gleichung hat (ohne weitere Bedingungen) die Lösung $y = -x - 2c$. Also sind alle $x \in \mathbb{R}$ invertierbar.

Wir haben also gezeigt, dass $*$ genau dann eine Gruppenstruktur auf $\mathbb{R}$ definiert, wenn $a = b = 1$ gilt, unabhängig von dem Wert von c.

Bemerkung: Dann ist die Abbildung $\mathbb{R} \to \mathbb{R}$, $t \mapsto t + c$ ein *Isomorphismus* von $(\mathbb{R}, *, e)$ nach $(\mathbb{R}, +, 0)$.

3. Sudoku für Mathematiker: Vervollständige die Verknüpfungstafel auf der Menge $G := \{1, 2, 3, 4, 5, 6\}$ beziehungsweise $G := \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$, so dass $(G, \circ)$ eine Gruppe ist. Welches Element ist jeweils das Einselement? Ist die Gruppe kommutativ?

$\circ$	1	2	3	4	5	6
1	2					
2						
3					4	
4	5			6		
5		5				3
6			5			

$\circ$	1	2	3	4	5	6	7	8	9
1	9						3		
2			4						
3									
4	1								
5						4			
6			9						
7					2				5
8						3			
9	4								

Lösung: The two sudokus given here can be filled in completely with the following method.

Strategy: First identify the identity element — call it e — by a relation of the form $ea = a$ or $ae = e$. This allows one to fill in the row and column of e. Next, any entry e in the table is a relation of the form $ab = e$. This means that $a^{-1} = b$ and implies the next entry $ba = e$. One might find two relations $aa = b$ and $ab = e$, from which one deduces that $a^3 = e$ and hence two more entries $ba = e$ and $bb = a$. Next, use any known relation of the form $a^{-1} = b$ to transform any relation of the form $bc = d$ into $c = ad$. If in addition $d^{-1} = f$, deduce similarly that $cf = a$. Likewise transform $cb = d$ into $c = da$ and perhaps into $fc = a$. Keep track of which relations have been used in this way, perhaps by circling the respective

entries. When these rules yield no other entries, try applying the fact that every row and column must contain every digit precisely once. To any entry found with this rule, apply the previous rules, and repeat. One obtains:

$\circ$	1	2	3	4	5	6
1	2	1	4	3	6	5
2	1	2	3	4	5	6
3	6	3	2	5	4	1
4	5	4	1	6	3	2
5	4	5	6	1	2	3
6	3	6	5	2	1	4

From the above table, one can see that 2 is the identity element. Since the group table is not symmetric across the diagonal, the group is not abelian. It is in fact isomorphic to the dihedral group D_3.

$\circ$	1	2	3	4	5	6	7	8	9
1	9	8	5	1	7	2	3	6	4
2	8	3	4	2	1	7	9	5	6
3	5	4	2	3	8	9	6	1	7
4	1	2	3	4	5	6	7	8	9
5	7	1	8	5	6	4	2	9	3
6	2	7	9	6	4	5	1	3	8
7	3	9	6	7	2	1	8	4	5
8	6	5	1	8	9	3	4	7	2
9	4	6	7	9	3	8	5	2	1

The identity element is 4. Here the table is symmetric across the diagonal, so the group is abelian. It is in fact isomorphic to $C_3 \times C_3$.

*4. Zeige, dass auf jeder nicht-leeren Menge eine Gruppenstruktur definiert werden kann.
Hinweis: Es darf ohne Beweis benutzt werden, dass jede unendliche Menge gleich mächtig ist wie die Menge ihrer endlichen Teilmengen.

Lösung: Sei X eine beliebige nicht-leere Menge. Wir verfolgen folgende Strategie: Zunächst finden wir eine Gruppe $(G, *, e_G)$, die gleich mächtig ist wie X. Dann wählen wir eine bijektive Abbildung $f\colon X \to G$ und übertragen die Gruppenstruktur auf X mittels f. Das heisst, für alle $x, y \in X$ setzen wir $x * y := f^{-1}(f(x) * f(g))$ sowie $e_X := f^{-1}(e_G)$.

Behauptung: Dann ist $(X, *, e_X)$ eine Gruppe.

Beweis:

- Assoziativität: Für alle $x, y, z \in X$ gilt

$$\begin{aligned}(x \star y) \star z &= f^{-1}\big(f(x \star y) * f(z)\big)\\ &= f^{-1}\big(f(f^{-1}(f(x) * f(y))) * f(z)\big)\\ &= f^{-1}\big((f(x) * f(y)) * f(z)\big)\\ &= f^{-1}\big(f(x) * (f(y) * f(z))\big)\\ &= f^{-1}\big(f(x) * f(f^{-1}(f(y) * f(z)))\big)\\ &= f^{-1}\big(f(x) * f(y \star z)\big)\\ &= x \star (y \star z).\end{aligned}$$

- Linksneutrales Element: Für alle $x \in X$ gilt

$$f^{-1}(e_G) * x = f^{-1}\big(f(f^{-1}(e_G)) * f(x)\big) = f^{-1}(e_G * f(x)) = f^{-1}(f(x)) = x.$$

- Linksinverses Element: Für alle $x \in X$ gilt

$$f^{-1}(f(x)^{-1}) * x = f^{-1}\big(f(f^{-1}(f(x)^{-1})) * f(x)\big) = f^{-1}\big(f(x)^{-1} * f(x)\big) = f^{-1}(e_G).$$

□

Es bleibt, eine Gruppe G zu finden, die gleich mächtig ist wie X. Falls X endlich mit n Elementen ist, so können wir für G die zyklische Gruppe Z_n mit n Elementen wählen. Nehmen wirs also an, X sei unendlich. Nach dem Hinweis ist X dann gleich mächtig wie die Menge $G := \{A \subset X \mid A \text{ endlich}\}$. Auf G definieren wir die Verknüpfung $A \,\Delta\, B := (A \cup B) \setminus (A \cap B)$.

Behauptung: Diese definiert eine Gruppenstruktur auf G.

Beweis:

- Assoziativität: Für alle $A, B, C \in G$ gilt

$$\begin{aligned}(A \,\Delta\, B) \,\Delta\, C &= (A \cap B \cap C) \cup (A \setminus (B \cup C)) \cup (B \setminus (A \cup C)) \cup (C \setminus (A \cup B))\\ &= A \,\Delta\, (B \,\Delta\, C).\end{aligned}$$

- Neutrales Element: Für die leere Menge $\varnothing \in G$ und alle $A \in G$ gilt

$$A \,\Delta\, \varnothing = \varnothing \,\Delta\, A = (A \cup \varnothing) \setminus (A \cap \varnothing) = A \setminus \varnothing = A.$$

- Inverses Element: Jedes Element $A \in G$ ist zu sich selbst invers:

$$A \,\Delta\, A = (A \cup A) \setminus (A \cap A) = A \setminus A = \varnothing.$$ □

Aliter: Sei V der $\mathbb{F}_2$-Vektorraum aller Systeme $\underline{a} = (a_x)_{x \in X}$ mit $a_x \in \mathbb{F}_2$ für alle $x \in X$ und $a_x = 0$ für fast alle $x \in X$. Zu jedem solchen System assoziiere die Teilmenge $X_{\underline{a}} := \{x \in X \mid a_x = 1\}$. Dies liefert eine Bijektion von V auf die Menge aller endlichen Teilmengen von X. Deren Kardinalität ist also einerseits gleich der von V, und andererseits nach dem Hinweis gleich der von X. Die additive Gruppe von V ist also eine Gruppe derselben Kardinalität wie X.

**5. Sei G eine Menge mit einer assoziativen binären Operation $\circ\colon G \times G \to G$ und einem *linksneutralen* Element $e \in G$, so dass jedes Element $a \in G$ ein *Rechtsinverses* besitzt, das heisst, ein Element $a' \in G$ mit $a \circ a' = e$. Ist $(G, \circ, e)$ dann immer eine Gruppe?

Lösung: Nein, wie das folgende Beispiel zeigt: Sei X eine beliebige Menge der Kardinalität > 1 zusammen mit der Abbildung

$$X \times X \to X,\ (x, y) \mapsto x \circ y := y$$

und einem beliebigen ausgezeichneten Element e. Für alle $x, y, z \in X$ gilt dann

$$x \circ (y \circ z) \ = \ x \circ z \ = \ z \ = \ y \circ z \ = \ (x \circ y) \circ z,$$

also ist das Assoziativgesetz erfüllt. Für alle $x \in X$ gilt weiter $e \circ x = x$, also ist e ein linksneutrales Element. Für jedes $x \in X$ gilt ausserdem $x \circ e = e$, also ist e ein rechtsinverses Element zu x. Somit sind alle genannten Bedingungen erfüllt. Für jedes $x \in X \smallsetminus \{e\}$ ist aber $x \circ e = e \neq x$, somit ist e kein rechtsneutrales Element. Daher ist $(X, \circ, e)$ keine Gruppe.

Aliter: Die Menge aller Matrizen $G := \left\{ \left(\begin{smallmatrix} a & b \\ 0 & 0 \end{smallmatrix}\right) \mid a \in \mathbb{R}^\times, b \in \mathbb{R} \right\}$ zusammen mit der Einschränkung der Matrixmultiplikation und dem linksneutralen Element $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right)$.

Aliter: Die Menge $\mathbb{R} \smallsetminus \{0\}$ mit der Operation $(x, y) \mapsto |x| \cdot y$ und dem linksneutralen Element 1.

6. Sei G eine Gruppe. Zeige:

   (a) Eine Teilmenge $U \subset G$ ist eine Untergruppe genau dann, wenn sie nichtleer ist und $UU^{-1} \subset U$ gilt.

   (b) Eine endliche Teilmenge $U \subset G$ ist eine Untergruppe genau dann, wenn sie nichtleer ist und $UU \subset U$ gilt.

   (c) Für Untergruppen U und V ist UV genau dann eine Untergruppe von G, wenn $UV = VU$ gilt.

   (d) Für Untergruppen U und V ist $U \cup V$ genau dann eine Untergruppe von G, wenn $U < V$ oder $V < U$ gilt.

Lösung:

(a) Ist U eine Untergruppe, so ist sie wegen $1_G \in U$ nichtleer, und für alle $u, v \in U$ ist zuerst $v^{-1} \in U$ und dann $uv^{-1} \in U$; somit gilt $UU^{-1} \subset U$.

Sei umgekehrt $U \subset G$ nichtleer mit $UU^{-1} \subset U$. Mithilfe irgendeines Elements $u_0 \in U$ folgt dann $1_G = u_0 u_0^{-1} \in UU^{-1} \subset U$. Für jedes $u \in U$ folgt daraus weiter $u^{-1} = 1_G u^{-1} \in UU^{-1} \subset U$. Für alle $u, v \in U$ folgt aus diesem dann auch $vu = v(u^{-1})^{-1} \in UU^{-1} \subset U$. Also ist U eine Untergruppe.

(b) Wir müssen zeigen, dass für jede nichtleere endliche Teilmenge $U \subset G$ mit $UU \subset U$ auch $U^{-1} \subset U$ gilt. Betrachte dafür ein Element $u \in U$. Dann ist $u^1 = u \in U$, und wenn $u^n \in U$ ist für irgendeine ganze Zahl $n \geqslant 1$, dann ist auch $u^{n+1} = u^n u \in UU \subset U$. Durch Induktion folgt daraus $u^n \in U$ für alle $n \geqslant 1$. Da U eine endliche Menge ist, können diese Elemente nicht alle verschieden sein; daher existieren ganze Zahlen $m > n \geqslant 1$ mit $u^m = u^n$. Daraus folgt dann auch $u^{2m} = (u^m)^2 = (u^n)^2 = u^{2n}$ und daraus schliesslich

$$u^{-1} = u^{2n} u^{-2n-1} = u^{2m} u^{-2n-1} = u^{2m-2n-1}.$$

Wegen $2m - 2n - 1 \geqslant 1$ und der oben bewiesenen Induktionsaussage liegt dieses Element in U, wie zu zeigen war.

(c) Wegen $1_G \in U$ und $1_G \in V$ gilt automatisch $1_G = 1_G 1_G \in UV$. Sodann beachten wir, dass für jede Untergruppe $H < G$ gilt

$$H^{-1} \;=\; \{h^{-1} : h \in H\} \;=\; H,$$

da die Abbildung $H \to H$, $h \mapsto h^{-1}$ bijektiv ist. Daher ist stets

$$(UV)^{-1} = \{(uv)^{-1} : u \in U, v \in V\} = \{v^{-1}u^{-1} : u \in U, v \in V\} = V^{-1}U^{-1} = VU.$$

Damit UV eine Untergruppe ist, ist es also notwendig, dass $VU = UV$ gilt. Umgekehrt garantiert diese Bedingung bereits, dass UV unter Inversion abgeschlossen ist. Ausserdem impliziert $VU = UV$, dass

$$(UV)(UV) = U(VU)V = U(UV)V = (UU)(VV) \subset UV$$

ist. Daher ist UV auch unter Multiplikation abgeschlossen und somit eine Untergruppe.

(d) Ist $U < V$, so ist $U \cup V = V$ offenbar eine Untergruppe von G. Ist $V < U$, so gilt das Entsprechende mit $U \cup V = U$.

Betrachten wir nun den Fall, dass weder $U < V$ noch $V < U$ ist. Dann können wir Elemente $u \in U \smallsetminus V$ und $v \in V \smallsetminus U$ wählen. Wäre dann $uv \in U$, so wäre wegen $u^{-1} \in U$ auch $v = 1_G v = (u^{-1}u)v = u^{-1}(uv)$ in U, im Widerspruch zur Wahl von u. Wäre $uv \in V$, so erhielten wir genauso einen Widerspruch mit $u = u1_G = u(vv^{-1}) = (uv)v^{-1} \in V$. Zusammen zeigt dies, dass $uv \notin (U \cup V)$ ist. Daher ist $U \cup V$ nicht unter Multiplikation abgeschlossen und somit keine Untergruppe von G.

7. Sei G eine Gruppe und n die Anzahl ihrer Untergruppen. Zeige:

   (a) Es ist $n = 1$ genau dann, wenn $G \cong \{1\}$ ist.

   (b) Es ist $n = 2$ genau dann, wenn $G \cong C_p$ ist für eine Primzahl p.

   (c) Es ist $n = 3$ genau dann, wenn $G \cong C_{p^2}$ ist für eine Primzahl p.

   Lösung: Für jede Untergruppe H gilt $\{1\} < H < G$. Daher ist $n = 1$ genau dann, wenn $\{1\} = G$ ist, woraus (a) folgt.

   Sei also $G \neq \{1\}$. Ist $n = 2$, so besitzt G keine weitere Untergruppe. Für jedes $g \in G \setminus \{1\}$ ist dann $\langle g \rangle$ eine von $\{1\}$ verschiedene Untergruppe und daher gleich G; somit ist G zyklisch. Ist $n = 3$, so besitzt G genau eine von $\{1\}$ und G verschiedene Untergruppe H. Für jedes $g \in G \setminus H$ ist dann $\langle g \rangle$ eine von $\{1\}$ und H verschiedene Untergruppe und daher gleich G; somit ist G zyklisch.

   Da G zyklisch ist und die Zahl n unter Isomorphie invariant ist, können wir nun ohne Beschränkung der Allgemeinheit $G = \mathbb{Z}$ oder $\mathbb{Z}/m\mathbb{Z}$ für $m \geqslant 1$ annehmen. Im ersten Fall besitzt G die unendlich vielen verschiedenen Untergruppen $m'\mathbb{Z}$ für alle natürlichen Zahlen m'. Im zweiten Fall sind die Untergruppen von $\mathbb{Z}/m\mathbb{Z}$ genau die $m'\mathbb{Z}/m\mathbb{Z}$ für alle Teiler $m'|m$, und wegen $|m'\mathbb{Z}/m\mathbb{Z}| = \frac{m}{m'}$ sind diese paarweise verschieden. Die Anzahl der Untergruppen von $\mathbb{Z}/m\mathbb{Z}$ ist daher die Anzahl der Teiler von m. Somit ist $n = 2$ äquivalent dazu, dass m genau zwei Teiler besitzt, also dass m eine Primzahl ist. Schliesslich ist $n = 3$ äquivalent dazu, dass m genau drei Teiler besitzt. Dies bedeutet, dass $m = p^2$ ist für eine Primzahl p.