Musterlösung 8

Gruppen, Untergruppen, Ordnung

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 Neutralelement $0 \in G$.
   - 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* zwischen $(\mathbb{R} \smallsetminus \{1\}, *)$ und $(\mathbb{R} \smallsetminus \{0\}, \cdot)$.

   (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 $1 + xy \neq 0$ 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:

- Die Verknüpfung $*$ ist assoziativ: Eine Rechnung zeigt, dass für alle $x, y, z \in G$ gilt

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

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

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

für alle $x \in G$.

- Für $x \in G$ gilt zudem

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

weshalb $-x \in G$ das Inverse von x bzgl. $*$ ist.

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

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

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 wieder die Gruppenaxiome und beginnen bei der Existenz eines Neutralelements:

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

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

Damit diese Gleichungen eine von x unabhängige Lösung besitzen, erhalten wir durch Koeffizientenvergleich die notwendigen und hinreichenden Bedingungen $a = b = 1$. Zudem ist dann $e = -c$ das Neutralelement.

- Assoziativität: Unter den Bedingungen $a = b = 1$ gilt

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

für alle $x, y, z \in \mathbb{R}$.

- Ein Element $x \in \mathbb{R}$ ist genau dann invertierbar bezüglich $*$ (weiterhin unter den Bedingungen $a = b = 1$ und somit $e = -c$), 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 $(\mathbb{R}, *)$ genau dann eine Gruppe ist, wenn $a = b = 1$ (ohne Bedingungen an c) gilt.

Bemerkung: Die Abbildung $\mathbb{R} \to \mathbb{R}$, $t \mapsto t + c$ ist ein *Isomorphismus* zwischen $(\mathbb{R}, *)$ und $(\mathbb{R}, +)$.

**3. 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, die gleich mächtig ist wie X (das heisst, es existiert eine bijektive Abbildung $X \to G$). Dann "übertragen" wir die Gruppenstruktur von G mittels einer bijektiven Abbildung $f : X \to G$ auf X. (Naiv gesagt ist eine solche bijektive Abildung nur eine "Umbenennung" der Elemente. Wir können die Verknüpfung auf X definieren, indem wir Elemente von X zuerst mittels f in Elemente von G "umbenennen", dann dort die Verknüpfung von G anwenden und das Ergebnis mittels f^{-1} wieder in ein Element von X "zurück benennen".)

Falls X endlich mit n Elementen ist, so können wir für G die zyklische Gruppe Z_n mit n Elementen wählen. Nehme also an, X sei unendlich. Nach dem Hinweis ist X gleich mächtig wie $G := \Sigma(X) := \{A \subset X \mid A \text{ endlich}\}$. Auf G definieren wir die Verknüpfung $A \,\Delta\, B := (A \cup B) \smallsetminus (A \cap B)$. Diese definiert eine Gruppenstruktur auf G:

- Δ ist assoziativ: Für alle $A, B, C \in G$ gilt

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

- Die leere Menge $\varnothing \in G$ ist ein Neutralelement: Für alle $A \in G$ gilt

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

- Alle Elemente von G sind zu sich selbst invers: Für alle $A \in G$ gilt

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

Somit haben wir für jede nicht-leere Menge X eine Gruppe G gefunden, die gleich mächtig ist wie X. Es bleibt zu zeigen, wie man mittels einer bijektiven Abbildung die Gruppenstruktur übertragen kann:

Lemma: Sei $(G, *)$ eine Gruppe und sei $f : X \to G$ eine bijektive Abbildung. Dann definiert die Verknüpfung $x \star y := f^{-1}\big(f(x) * f(y)\big)$ eine Gruppenstruktur auf X.

Beweis:

- $\star$ ist assoziativ: Für alle $x, y, z \in X$ gilt

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

- Ist $e \in G$ das Neutralelement von G, so ist $f^{-1}(e) \in X$ ein Neutralelement von X: Für alle $x \in X$ gilt

$$x \star f^{-1}(e) = f^{-1}\big(f(x) * f(f^{-1}(e))\big) = f^{-1}(f(x) * e) = f^{-1}(f(x)) = x,$$

  und $f^{-1}(e) \star x = x$ genauso.

- Alle Elemente von X sind invertierbar: Für alle $x \in X$ gilt

$$x \star f^{-1}(f(x)^{-1}) = f^{-1}\big(f(x) * f(f^{-1}(f(x)^{-1}))\big) = f^{-1}\big(f(x) * f(x)^{-1}\big) = f^{-1}(e),$$

  und $f^{-1}(f(x)^{-1}) \star x = f^{-1}(e)$ genauso. □

Somit haben wir auf jeder nicht-leeren Menge eine Gruppenstruktur gefunden.

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.

4. 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?

∘	1	2	3	4	5	6
1	2					
2						
3					4	
4	5			6		
5		5				3
6			5			

∘	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:

∘	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 $C_3 \times C_3$.

5. Seien G eine Gruppe und $H_1, H_2 < G$ Untergruppen. Zeige, dass $H_1 \cup H_2$ genau dann eine Untergruppe von G ist, wenn $H_1 < H_2$ oder $H_2 < H_1$ gilt.

   Lösung: Wir nehmen zuerst an, dass $H_1 < H_2$ (beziehungsweise $H_2 < H_1$) gilt. Dann ist $H_1 \cup H_2 = H_2$ (beziehungsweise $H_1 \cup H_2 = H_1$) und somit ist $H_1 \cup H_2$ eine Untergruppe von G.

   Nun gelte umgekehrt weder $H_1 < H_2$ noch $H_2 < H_1$. Dann können wir also Elemente $h_1 \in H_1 \setminus H_2$ und $h_2 \in H_2 \setminus H_1$ wählen. Nehmen wir nun an, es wäre $h_1 h_2 \in H_1 \cup H_2$. Dann wäre $h_1 h_2$ in H_1 oder in H_2 enthalten; sei ohne Beschränkung der Allgemeinheit $h_1 h_2 \in H_1$. Wegen $h_1 \in H_1$ ist auch $h_1^{-1} \in H_1$, und somit $h_1^{-1}(h_1 h_2) = (h_1^{-1} h_1) h_2 = h_2 \in H_1$. Aber wir hatten $h_2 \in H_2 \setminus H_1$ gewählt; Widerspruch. Somit haben wir gezeigt, dass $h_1 h_2 \notin H_1 \cup H_2$. Aber es gilt $h_1, h_2 \in H_1 \cup H_2$. Also ist $H_1 \cup H_2$ keine Untergruppe von G.

6. Bestimme die Zentralisatoren aller Elemente sowie das Zentrum der Diedergruppe D_n.

   Lösung: We know that $D_n = \{1, T, \ldots, T^{n-1}, S, ST, \ldots, ST^{n-1}\}$ where T is a rotation of order n, and S is a reflection through a fixed axis of symmetry of a regular n-gon. The ST^i for all $0 < i < n$ then correspond to reflections through the remaining axes of symmetry.

   A fundamental fact about dihedral groups is the formula $S'T^j = T^{-j}S'$ for any reflection $S' = ST^i$ and any j. Geometrically this means that a reflection followed by a rotation followed by the same reflection as before is the inverse of the rotation. It may be checked by geometry or by the effect on the vertices of the dihedron.

Consider now an arbitrary rotation T^i with $0 \leqslant i < n$. If $i = 0$, then $T^i = 1$, whose centralizer is the whole group. Suppose that $i \neq 0$. Since $T^iT^j = T^{i+j} = T^jT^i$, we see that T^i commutes with all other rotations. A reflection $S' = ST^j$ commutes with T^i if and only if $T^i = T^{-i}$. This is equivalent to $T^{2i} = 1$, that is, to $n|2i$. Since $0 < i < n$, this holds if and only if n is even and $i = n/2$. It follows that

$$\mathrm{Cent}_{D_n}(T^i) = \begin{cases} D_n & \text{for } n \text{ even and } i = n/2 \\ \langle T \rangle = \{1, T \dots T^{n-1}\} & \text{otherwise.} \end{cases}$$

For an arbitrary reflection S' the equality $S'T^i = T^{-i}S'$ and the argument above show that $T^i \in \mathrm{Cent}_{D_n}(S')$ if and only if $i = 0$ or n is even with $i = n/2$. Given another reflection $S'' = ST^j$ we have

$$S'S'' = ST^iST^j = S^2T^{j-i} = T^{j-i}$$

and

$$S''S' = ST^jST^i = S^2T^{i-j} = T^{i-j}.$$

Thus $S'S'' = S''S'$ if and only if $n|2(i-j)$, which is equivalent to $S'' = S'$ or $S'' = S'T^{n/2}$ with n even. Therefore

$$\mathrm{Cent}_{D_n}(S') = \begin{cases} \langle S', T^{n/2} \rangle = \{1, T^{n/2}, S', S'T^{n/2}\} & \text{if } n \text{ is even} \\ \langle S' \rangle = \{1, S'\} & \text{if } n \text{ is odd.} \end{cases}$$

Finally, the center $Z(D_n)$ consists of exactly the elements whose centralizers are the entire group, which we determined above. If $n \leqslant 2$, any element of D_n has this property, while for $n \geqslant 3$, only the identity element and $T^{n/2}$ if $2|n$ have it. Therefore

$$Z(D_n) = \begin{cases} D_n & \text{if } n \leqslant 2, \\ \langle T^{n/2} \rangle = \{1, T^{n/2}\} & \text{if } n \geqslant 3 \text{ even}, \\ \{1\} & \text{if } n \geqslant 3 \text{ odd}. \end{cases}$$

7. Sei G eine Gruppe mit genau einer von $\{e\}$ und G verschiedenen Untergruppe. Zeige, dass G zyklisch von Ordnung p^2 für eine Primzahl p ist.

   Lösung: Es sei $H < G$ die einzige von $\{e\}$ und G verschiedene Untergruppe von G. Betrachte $x \in G \setminus H$ und die davon erzeugte Untergruppe $\langle x \rangle$. Da $x \neq e$ und $x \notin H$ ist, kann diese weder trivial noch gleich H sein. Sie ist daher gleich ganz G und G ist zyklisch.

   Wäre G unendlich zyklisch, hätte G unendlich viele Untergruppen. Daher ist G eine endliche zyklische Gruppe der Ordnung $n \geqslant 1$. Es folgt daraus, dass die Untergruppen von G in bijektiver Korrespondenz mit den Teilern von n stehen. Nach Voraussetzung hat n darum genau einen von 1 und n verschiedenen Teiler. Daher kann n nur einen Faktor p in der Primfaktorzerlegung haben und es muss $n = p^2$ gelten.