6. Übung zu algebraischen Strukturen: Gruppenhomomorphismen

Aufgabe (6.1) In der multiplikativen Gruppe $\mathbb{C}^\times$ aller komplexen Zahlen $z \neq 0$ betrachten wir die Untergruppe $\mathbb{R}^+ = (0, \infty)$ aller positiven reellen Zahlen und die Untergruppe T aller komplexen Zahlen vom Betrag 1. Gib einen Isomorphismus $f : \mathbb{C}^\times \to \mathbb{R}^+ \times T$ an! Was ist das Bild der Einschränkung von f auf $\mathbb{R}^\times$?

Aufgabe (6.2) Es sei $G = \mathrm{GL}(n, \mathbb{R})$ die Gruppe aller invertiertierbaren reellen $(n \times n)$-Matrizen. Find surjektive Homomorphismen $\alpha : G \to (\mathbb{R}\backslash\{0\}, \cdot)$, $\beta : G \to \big((0, \infty), \cdot\big)$ und $\gamma : G \to (\mathbb{R}, +)$. Was ist jeweils der Kern des gefundenen Homomorphismus?

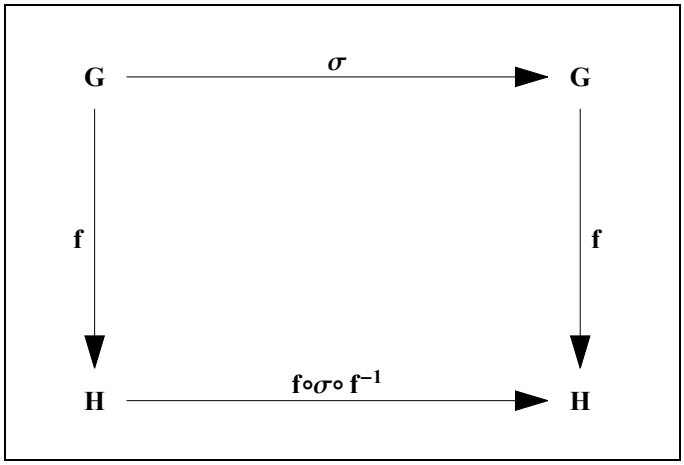
Aufgabe (6.3) Es sei K ein beliebiger Körper. Die bijektiven affinen Abbildungen $K^n \to K^n$ sind genau die Abbildungen der Form $f_{A,b}(x) := Ax + b$ mit $A \in \mathrm{GL}(n, K)$ und $b \in K^n$. Zeige, daß die Menge $\mathrm{Aff}(K^n)$ dieser Abbildungen eine Gruppe bildet (mit der Verkettung als Gruppenoperation) und daß die Abbildung

$$f_{A,b} \;\mapsto\; \begin{bmatrix} A & b \\ 0 & 1 \end{bmatrix}$$

eine Einbettung von $\mathrm{Aff}(K^n)$ in die Gruppe $\mathrm{GL}(n+1, K)$ aller invertierbaren $(n+1) \times (n+1)$-Matrizen ist.

Aufgabe (6.4) Es sei $f : G \to H$ ein Gruppenisomorphismus. Beweise die folgenden Aussagen!

(a) Das Zentrum $Z(G)$ von G wird von f auf das Zentrum $Z(H)$ von H abgebildet.
(b) Die Kommutatorgruppe G' von G wird von f auf die Kommutatorgruppe H' von H abgebildet.
(c) Für jedes Element $x \in G$ haben die Elemente $x \in G$ und $f(x) \in H$ die gleiche Ordnung.
(d) Zeige, daß durch $F(\sigma) := f \circ \sigma \circ f^{-1}$ ein Isomorphismus $F : \mathrm{Aut}(G) \to \mathrm{Aut}(H)$ gegeben ist (der als von f induzierter Isomorphismus bezeichnet wird).



Von einem Isomorphisms $f : G \to H$ induzierter Isomorphismus $F : \mathrm{Aut}(G) \to \mathrm{Aut}(H)$.

Aufgabe (6.5) Gib einige Möglichkeiten an, wie man nachweisen kann, daß zwei gegebene Gruppen *nicht* isomorph sind.

Aufgabe (6.6) Es sei G eine beliebige Gruppe. Für ein beliebiges Element $g \in G$ ist die Konjugation $\kappa_g : G \to G$ definiert durch $\kappa_g(x) := gxg^{-1}$. Zeige, daß durch

$$\varphi : \begin{array}{ccc} G & \to & \mathrm{Aut}(G) \\ g & \mapsto & \kappa_g \end{array}$$

ein Homomorphismus definiert ist, dessen Kern gerade das Zentrum von G ist. (Die Konjugationsabbildungen κ_g mit $g \in G$ werden als **innere Automorphismen** von G bezeichnet.)

Aufgabe (6.7) Es sei $G = \mathrm{GL}(n, K)$ die Gruppe aller invertierbaren $(n \times n)$-Matrizen über dem (beliebigen) Körper K. Wir definieren $\Phi : G \to G$ durch

$$\Phi(A) \;:=\; A^{T-1} \;=\; (A^T)^{-1} \;=\; (A^{-1})^T.$$

Zeige, daß Φ ein Automorphismus von G mit $\Phi^2 = \mathrm{id}_G$ ist. Zeige ferner, daß Φ genau in den folgenden Fällen ein innerer Automorphismus von G ist:

- $n = 1$, $K = \mathbb{Z}_2$;
- $n = 1$, $K = \mathbb{Z}_3$;
- $n = 2$, $K = \mathbb{Z}_2$.

Aufgabe (6.8) Bestimme alle Endomorphismen der additiven Gruppe $(\mathbb{Z}, +)$. Welche dieser Endomorphismen sind sogar Automorphismen?

Aufgabe (6.9) Zeige, daß die Endomorphismen der additiven Gruppe $(\mathbb{Z}_n, +)$ genau die Abbildungen der Form $\sigma_k : x \mapsto kx$ mit $k \in \mathbb{Z}_n$ sind und daß σ_k genau dann ein Automorphismus ist, wenn $k \in \mathbb{Z}_n^\times$ gilt. Zeige ferner, daß die Abbildung

$$\begin{array}{ccc} (\mathbb{Z}_n^\times, \cdot) & \to & \mathrm{Aut}(\mathbb{Z}_n) \\ k & \mapsto & \sigma_k \end{array}$$

ein Gruppenisomorphismus ist.

Aufgabe (6.10) Es sei G eine Gruppe. Zeige, daß die Inversionsabbildung $x \mapsto x^{-1}$ genau dann ein Automorphismus von G ist, wenn G abelsch ist.

Aufgabe (6.11) Es sei $\sigma : G \to G$ ein Automorphismus der endlichen Gruppe G. Beweise die folgenden Aussagen!

(a) Ist e der einzige Fixpunkt von σ, so gilt $G = \{x^{-1}\sigma(x) \mid x \in G\}$.
(b) Ist e der einzige Fixpunkt von G und gilt $\sigma^2 = \mathrm{id}_G$, so gilt $\sigma(a) = a^{-1}$ für alle $a \in G$.
(c) Gilt $\sigma(a) = a^{-1}$ für alle $a \in G$, so ist G abelsch.

Aufgabe (6.12) Es sei $\sigma : G \to G$ ein Automorphismus der endlichen Gruppe G, der mehr als drei Viertel der Elemente von G auf ihr jeweiliges Inverses abbildet. Zeige, daß dann σ sogar *jedes* Elemente von G auf sein Inverses abbildet. (Nach (6.10) ist dann G zwangsläufig kommutativ.)

Hinweis. Beweise für $S := \{x \in G \mid \sigma(x) = x^{-1}\}$ nacheinander die folgenden Aussagen!

(a) Für jedes Element $s_0 \in S$ gilt $|S \cap s_0^{-1}S| > |G|/2$.
(b) Für jedes Element $s_0 \in S$ gilt $S \cap s_0^{-1}S \subseteq Z_G(s_0)$, wobei $Z_G(s_0)$ den Zentralisator von s_0 in G bezeichnet.
(c) Für jedes $s_0 \in S$ gilt $Z_G(s_0) = G$.
(d) Die Gruppe G ist abelsch.
(e) Es gilt $\sigma(g) = g^{-1}$ für alle $g \in G$.

Aufgabe (6.13) Es seien G eine zyklische Gruppe der Ordnung n und $g \in G$ ein Erzeuger von G. Zeige, daß dann

$$\exp_g : \begin{array}{ccc} \mathbb{Z}_n & \mapsto & G \\ [k] & \mapsto & g^k \end{array}$$

ein Gruppenisomorphismus ist. (Bis auf Isomorphie gibt es also nur eine zyklische Gruppe der Ordnung n.) Die Umkehrabbildung $\log_g : G \to \mathbb{Z}_n$ wird als **diskreter Logarithmus** von G zur Basis g bezeichnet.

Aufgabe (6.14) Wir betrachten eine beliebige Gruppe G, ein Element $g \in G$ endlicher Ordnung $\mathrm{ord}(g) = n$ sowie ein Element $a \in \langle\langle g \rangle\rangle$. Wir wollen $\log_g a$ bestimmen, also diejenige Zahl $0 \le x \le n-1$ mit $g^x = a$. Der **Algorithmus von Shanks** (im Englischen auch als "babysteps-giantsteps algorithm" bekannt) verfährt dazu wie folgt.

(1) Setze $m := [\sqrt{n}] + 1$.
(2) Berechne $g^0, g^1, g^2, \ldots, g^{m-1}$ ("baby steps"). Ist eines dieser Elemente gleich a, so sind wir fertig.
(3) Andernfalls setze $\gamma := g^{-m}$ und berechne $a\gamma^1, a\gamma^2, a\gamma^3, a\gamma^4, \ldots$ ("giant steps").

Begründe, warum nach spätestens $m-1$ Schritten eines der in (3) erhaltenen Elemente mit einem der in (2) erhaltenen Elemente übereinstimmt, sagen wir $g^r = a\gamma^k$. Begründe weiter, warum dann $x = km + r$ der gesuchte Exponent $\log_g a$ ist.

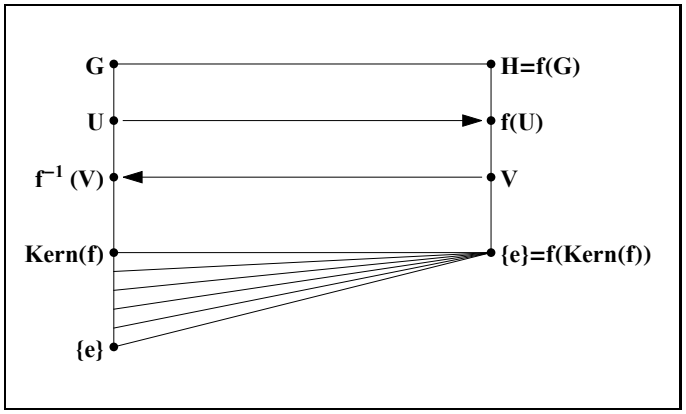
Aufgabe (6.15) Berechne mit dem Algorithmus von Shanks die folgenden diskreten Logarithmen!

(a) $\log_2 5$ in $\mathbb{Z}_{13}^\times$
(b) $\log_3 7$ in $\mathbb{Z}_{31}^\times$
(c) $\log_{11} 19$ in $\mathbb{Z}_{29}^\times$

Bemerkung. Die Aufgabenstellung ist sinnvoll, weil 5 ein Erzeuger der Gruppe $\mathbb{Z}_{13}$ ist, 3 ein Erzeuger der Gruppe $\mathbb{Z}_{31}^\times$ und 11 ein Erzeuger von $\mathbb{Z}_{29}^\times$. (Wäre dies nicht der Fall, würde man es durch Anwendung des Alogorithmus von Shanks herausfinden.)

Aufgabe (6.16) Es seien $f : G \to H$ ein Gruppenhomomorphismus und $U \le G$ eine Untergruppe. Beweise die Gleichheit $f^{-1}\big(f(U)\big) = U \cdot \mathrm{Kern}(f)$.

Aufgabe (6.17) Es sei $f : G \to H$ ein surjektiver Gruppenhomomorphismus. Zeige, daß durch $U \mapsto f(U)$ und $V \mapsto f^{-1}(V)$ zueinander inverse Bijektionen zwischen der Menge aller Untergruppen $U \le G$ mit $U \supseteq \mathrm{Kern}(f)$ und der Menge aller Untergruppen $V \le H$ gegeben sind. Zeige ferner, daß diese Korrespondenz Indices erhält, daß für alle Untergruppen $\mathrm{Kern}(f) \le U \le G$ also $[G : U] = [H : f(U)]$ gilt. (Die Struktur von G oberhalb des Kerns von f wird von f also getreu nach H transportiert.)



Aufgabe (6.18) Es seien G eine beliebige Gruppe und $\mathrm{Bij}(G)$ die Menge aller Bijektionen $G \to G$, also aller Permutationen der Elemente von G. Mit der Verkettung als Operation ist $\mathrm{Bij}(G)$ selbst eine Gruppe. Für $g \in G$ definieren wir die Linksmultiplikation $L_g : G \to G$ durch $L_g(x) := gx$. Zeige, daß die Abbildung

$$L : \begin{array}{ccc} G & \to & \mathrm{Bij}(G) \\ g & \mapsto & L_g \end{array}$$

eine Einbettung (also ein injektiver Gruppenhomomorphismus) ist.

Bemerkung: Durch Identifikation von G mit $L(G)$ können wir G als Untergruppe von $\mathrm{Bij}(G)$ auffassen. Jede beliebige Gruppe läßt sich also als Permutationsgruppe auffassen. Die Abbildung L heißt **Cayley-Einbettung**.

Aufgabe (6.19) Gib die Cayley-Einbettung von Sym_3 in Sym_6 an.