A 1.11.4 Sei G eine Untergruppe der Gruppe S_M aller Bijektionen einer Menge M auf sich. Für jedes $p \in M$ heißt $G(p) := \{\varphi \in G \mid \varphi(p) = p\}$ der Stabilisator von p in G.

(a) Zeige, dass $G(p)$ eine Untergruppe von G ist.

(b) Beweise: Falls es zu Elementen $p, q \in M$ eine Bijektion $\gamma \in G$ gibt mit $\gamma(p) = q$, so gilt $G(q) = \gamma \circ G(p) \circ \gamma^{-1}$.

(c) Bestimme in der Gruppe S_3 den Stabilisator $S_3(1)$ und mit Hilfe von (b) auch $S_3(2)$.

(d) Zeige, dass der Stabilisator $S_3(1)$ kein Normalteiler von S_3 ist.

$G(p) \subset G$

Beweis: $G(p) \neq \emptyset$, weil $G \neq \emptyset$. Seien $\alpha, \beta \in G(p)$, so gilt auch $\alpha \circ \beta^{-1} \in G(P)$, weil α, β jeweils Bijektionen sind (α^{-1}, β^{-1} existieren) und $\varphi(p) = p \Rightarrow \varphi^{-1}(\varphi(p)) = \varphi(p)$. $\square$

$\forall \gamma \in G: \gamma(p) = q \Rightarrow G(q) = \gamma \cdot G(p) \circ \gamma^{-1}$

Beweis: Sei $\gamma \in G$ beliebig. $[\gamma \circ \varepsilon \circ \gamma^{-1}](q) =$
$[\gamma \circ \varepsilon \circ \gamma^{-1}](\gamma(p)) = [\gamma \circ \varepsilon](\gamma^{-1}(\gamma(p))) =$
$[\gamma \circ \varepsilon](p) = \gamma(p) = q = \delta(q)$, wenn $\delta \in G(q)$
und $\varepsilon \in G(p)$. $\square$

$S_3(1) = \left\{\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}, \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}\right\}$; $S_3(2) = \left\{\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix},\right.$
$\left.\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}\right\}$;

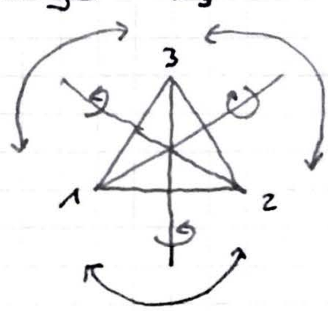
$S_3(1)$ ist kein Normalteiler von S_3

Beweis: Es müsste dazu $\forall f \in S_3: f \circ S_3(1) = S_3(1) \circ f$.
Also $f \circ S_3(1) \circ f^{-1} = S_3(1)$, was aber laut (c) nicht der Fall ist. $\square$

Anhang zu (c): Sei $\gamma(1) = 2$. Weil $G(q) = \gamma \circ G(p) \circ \gamma^{-1}$, wähle $\gamma = \{(1,2),(2,1),(3,3)\}$. Somit lässt sich $S_3(2)$ bestimmen.

Anhang zu (a): φ ist bijektiv und φ^{-1} ist bijektiv, also auch injektiv! Außerdem $\varphi \circ \varphi^{-1} = \varphi^{-1} \circ \varphi = id_M$

PS: n-gon Analogie: S_3



A 1.II.5 Sei U die Menge der komplexen Zahlen mit dem absoluten Betrag 1.

(a) Begründe, warum U, $\mathbb{R}^+$ und $\mathbb{R}^\times$ Normalteiler sind.

(b) Bestimme eine Untergruppe von $\mathbb{C}^\times$, die zu $\mathbb{C}^\times / U$ isomorph ist.

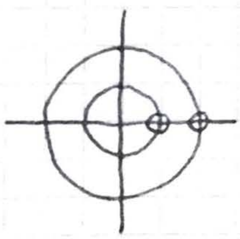
(c) —"— $\mathbb{C}^\times / \mathbb{R}^+$ —"—.

(d) —"— $\mathbb{C}^\times / \mathbb{R}^\times$ —"—.

Beweis (a): U, $\mathbb{R}^+$, $\mathbb{R}^\times$ sind Kommutativ. $\square$

$(\mathbb{R}^+, \cdot) \cong (\mathbb{C}^\times / U, \cdot)$

Beweis: Sei $f: \mathbb{R}^+ \to \mathbb{C}^\times / U : x \mapsto U \cdot x$. Dann ist f bijektiv, weil alle Elemente von $\mathbb{C}^\times / U$ (d.h. alle Ringe



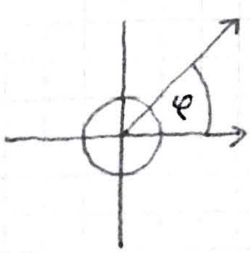
um das Zentrum $0 + 0i$) $\mathbb{R}^+$ genau einmal schneiden.

f ist ein Homomorphismus, weil

$f(x \cdot y) = U(x \cdot y) = Ux \cdot Uy = f(x) \cdot f(y)$ $\square$

$(U, \cdot) \cong (\mathbb{C}^\times / \mathbb{R}^+)$

Beweis: Sei $f: U \to \mathbb{C}^\times / \mathbb{R}^+ : x \mapsto \mathbb{R}^+ \cdot x$. Dann ist f bijektiv, weil alle Elemente von $\mathbb{C}^\times / \mathbb{R}^+$ (d.h. alle rotierten



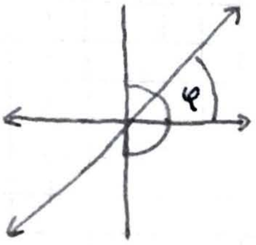
Strahlen $\mathbb{R}^+_\varphi$ von $\mathbb{R}^+$ um $\varphi \in (0, 2\pi]$) U genau einmal schneiden.

f ist ein Homomorphismus, weil

$f(x \cdot y) = \mathbb{R}^+(x \cdot y) = \mathbb{R}^+ x \cdot \mathbb{R}^+ y = f(x) \cdot f(y)$ $\square$

$U^+ := \{a + bi \in U : a > 0\} \cong \mathbb{C}^\times / \mathbb{R}^\times$

Beweis: Sei $f: U^+ \to \mathbb{C}^\times/\mathbb{R}^\times : x \mapsto \mathbb{R}^\times \cdot x$. Dann ist f bijektiv, weil alle Elemente von $\mathbb{C}^\times/\mathbb{R}^\times$ (d.h. alle rotierten „Geraden" $\mathbb{R}^\times_\varphi$ von $\mathbb{R}^\times$ um $\varphi \in (-\pi/2, \pi/2]$) U^+ genau einmal schneiden.



f ist ein Homomorphismus, weil

$f(x \cdot y) = \mathbb{R}^\times (x \cdot y) = \mathbb{R}^\times x \cdot \mathbb{R}^\times y = f(x) \cdot f(y)$ $\square$

Wenn $x \in \mathbb{R}$, dann $U^+ ;^\times \cong \mathbb{C}^\times / \mathbb{R}^\times$.

Anhang: Veranschauliche die zu den einzelnen Faktorgruppen gehörenden kanonischen Abbildungen jeweils in der Gaußschen Zahlenebene.

Anleitung zu (d): Verwende die Abbildung $z \mapsto \left(\frac{z}{|z|}\right)^2$.

A 1.11.11 Sei G eine Gruppe. Beweise, dass jede der folgenden Abbildungen ein Gruppenhomomorphismus ist, und bestimme dessen Kern.

(a) $\Psi : G \to \mathrm{Aut}(G) : a \mapsto (\Psi_{a^{-1}} : x \mapsto axa^{-1})$ (innerer Automorphismus zu a^{-1}).

(c) $\Psi : G \to S_G : a \mapsto (\rho_{a^{-1}} : x \mapsto xa^{-1})$ (Rechtstranslation mit a^{-1}).

Bemerkung: Der Kern des Homomorphismus aus (a) heißt das Zentrum der Gruppe G. Es besteht aus allen Elementen $x \in G$ mit der Eigenschaft $xy = yx$ für alle $y \in G$.

Beweis (a): $\Psi(a \cdot b) = \Psi_{(ab)^{-1}} = \Psi_{a^{-1}} \circ \Psi_{b^{-1}} = \Psi(a) \circ \Psi(b)$.
Die zweite Gleichheit gilt, weil $\Psi_{a^{-1}}(\Psi_{b^{-1}}(x)) = \Psi_{a^{-1}}(bxb^{-1}) = abxb^{-1}a^{-1} = (ab)x(ab)^{-1} = \Psi_{(ab)^{-1}}(x)$. $\square$

Sollte G kommutativ sein, so ist $\ker \Psi = G$, weil $axa^{-1} = aa^{-1}x = x$ und dadurch $\forall a \in G : \Psi_{a^{-1}} = id_G$. A priori trifft diese Eigenschaft aber nur auf $e \in G$ zu, weil $\Psi_{e^{-1}} : x \mapsto exe^{-1} = x$, also $\Psi_{e^{-1}} = id_G$; $\ker \Psi = \{e\}$.

Beweis (c): $\Psi(a \cdot b) = \rho_{(ab)^{-1}} = \rho_{a^{-1}} \circ \rho_{b^{-1}} = \Psi(a) \circ \Psi(b)$.
—″— $\rho_{b^{-1}}(\rho_{a^{-1}}(x)) = \rho_{a^{-1}}(xb^{-1}) = xb^{-1}a^{-1} = x(ab)^{-1} = \rho_{(ab)^{-1}}(x)$. $\square$

$\ker \Psi = \{e\}$, weil nur $\rho_{e^{-1}}(x) = xe^{-1} = x = id_G(x)$.

A 2.2.1 Wir erklären in $\mathbb{R}^{2\times 1}$ die Addition wie üblich, aber die Multiplikation $*: \mathbb{R} \times \mathbb{R}^{2\times 1} \to \mathbb{R}^{2\times 1}$ („Skalar mal Spalte") durch

(a) $x * (a_1, a_2)^T := (xa_1, a_2)^T$,

Ist damit $\mathbb{R}^{2\times 1}$ ein Vektorraum über $\mathbb{R}$? Überprüfe in jedem Fall alle Vektorraumaxiome, auch wenn schon klar ist, dass kein Vektorraum vorliegt.

Es liegt bei (a) kein Vektorraum vor.

Beweis: Seien $a = (a_1, a_2)$ und $b = (b_1, b_2)$.

1. $x * ((a_1, a_2) + (b_1, b_2)) = x * (a_1, a_2) + x * (b_1, b_2) =$
   $(xa_1, a_2) + (xb_1, b_2) = (xa_1 + xb_1, a_2 + b_2) =$ (Anhang)
2. $(x + y) * (a_1, a_2) = x * (a_1, a_2) + y * (a_1, a_2) =$
   $(xa_1, a_2) + (ya_1, a_2) \overset{!}{=} (xa_1, 0) + (ya_1, a_2) =$
   $(xa_1 + ya_1, 0 + a_2) = (xa_1 + ya_1, a_2) =$
   $((x+y)a_1, a_2) = (x+y) * (a_1, a_2)$, aber nicht immer $a_2 = 0$!
3. $(xy) * (a_1, a_2) = ((xy)a_1, a_2) = (x(ya_1), a_2) =$
   $x * (ya_1, a_2)$.
4. $1 * (a_1, a_2) = (1a_1, a_2) = (a_1, a_2)$.

Anhang: 1. $= (x(a_1 + b_1), a_2 + b_1) = x * (a_1 + b_1, a_2 + b_2) =$
$x * ((a_1, a_2) + (b_1, b_2))$. Lies von hinten nach vorne!

PS: Ups, Goldstern-BSP vergessen:

(c) $x * (a, b)^T = (xa, 0)^T$ (für alle reellen Zahlen x, a, b. Mit xa ist das übliche Produkt zweier reellen Zahlen x und a gemeint.

Es liegt bei (c) Kein Vektorraum vor.

Beweis: Seien —"—

1. $x * ((a_1, a_2) + (b_1, b_2)) = x * (a_1 + b_1, a_2 + b_2) =$
$(x(a_1 + b_1), 0) = (xa_1 + xb_1, 0 + 0) = (xa_1 0) + (xb_1, 0)$
$= x * (a_1, a_2) + x * (b_1, b_2).$

2. $(x + y)(a_1, a_2) = ((x+y)a_1, 0) = (xa_1 + ya_1, 0 + 0)$
$= (xa_1, 0) + (ya_1, 0) = x * (a_1, a_2) + y * (a_1, a_2).$

3. $(xy) * (a_1, a_2) = ((xy)a_1, 0) = (x(ya_1), 0) =$
$x * (ya_1, 0).$

4. $1 * (a_1, a_2) = (1a_1, 0) \overset{!}{=} (a_1, 0) \overset{!}{\Leftrightarrow} (a_1, a_2) =$
$(a_1, 0) \Rightarrow a_1 = a_1 \wedge a_2 \overset{!}{=} 0!?$

A 2.2.2 (a) Es seien $(G,+)$ eine kommutative Gruppe mit dem neutralen Element e und $\mathbb{Z}_2$ der Restklassenkörper modulo 2. Wir erklären eine Multiplikation $* : \mathbb{Z}_2 \times G \to G : \bar{0} * a := e$, $\bar{1} * a := a$. Welche notwendige und hinreichende Eigenschaft muss die Gruppe G haben, damit G ein Vektorraum über $\mathbb{Z}_2$ ist?

(c) Gib ein Beispiel einer kommutativen Gruppe an, die gemäß (a) keinen Vektorraum über $\mathbb{Z}_2$ ergibt.

Hinweis zu (a): Berechne $(\bar{1}+\bar{1}) * a$ auf zwei Arten.

Jedes Element muss sein eigenes Inverse sein.

Beweis: $a + a \overset{4.}{=} \bar{1} * a + \bar{1} * a \overset{2.}{=} (\bar{1}+\bar{1}) * a = \bar{0} * a = e.$ $\square$

$G \neq \mathbb{Z}_3$

Beweis: $\bar{1} + \bar{1} \neq \bar{0}$. $\square$

A 2.2.3 Sei K ein Unterkörper eines Körpers $(L, +, \cdot)$. Beweise, dass $(L, +)$ gemeinsam mit der auf $K \times L$ eingeschränkten Multiplikation ein Vektorraum über K ist. Gib für $K = \mathbb{Z}_2$, $K = \mathbb{Q}$, $K = \mathbb{R}$ und $K = \mathbb{C}$ je mindestens ein Beispiel für einen solchen Vektorraum L an, wobei zusätzlich $K \neq L$ erfüllt sein.

Bemerkung: Die Elemente von K spielen eine doppelte Rolle: Sie sind Skalare und zugleich Vektoren.

Beweis: Seien $x, y \in K$ und $a, b \in L$. Weil $K \subset L$, gelten Distributivität, Assoziativität und $1 \in K$, sowie $0 \in K \cap L$.

1. $x(a + b) = (xa) + (xb)$
2. $(x + y)a = (xa) + (ya)$
3. $(xy)a = x(ya)$
4. $1a = a$ $\square$

$\mathbb{Z}_2 \subsetneq GF(4)$ (siehe Beispiele 1.10.3 (2)); $\mathbb{Q} \subsetneq \mathbb{R}$; $\mathbb{R} \subsetneq \mathbb{C}$; $\mathbb{C} \subsetneq \mathbb{P}(\mathbb{C})$, wobei $\mathbb{P}(\mathbb{C})$ die Menge aller Polynome $\sum_{i=0}^{N} a_i x^i$, $N \in \mathbb{N}_0$, $a_i \in \mathbb{C}$ ist. Sie enthält $\mathbb{C}$ deswegen, weil für $N = 0$ dann $a_0 x^0 = a_0 \in \mathbb{C}$ gilt. Sollte jedoch $N > 0$, dann $\sum_{i=0}^{N} a_i x^i = \sum_{i=1}^{N} a_i x^i + a_0 \notin \mathbb{C}$. (Eigentlich gilt letzteres auch für $N = 0$, weil $\sum_{i=0}^{0} a_i x^i = \sum_{i=0}^{0} a_i x^i + a_0 x^0 = 0 + a_0 = a_0$.)

A 2.2.5 Gegeben sei der Körper $(\mathbb{R}, +, \cdot)$ mit der üblichen Addition und Multiplikation. Ferner sei $\mathbb{R}^+$ die Menge aller positiven reellen Zahlen.

(a) Wir definieren auf $\mathbb{R}^+$ eine Addition $\oplus : \mathbb{R}^+ \times \mathbb{R}^+ \to \mathbb{R}^+$ durch $a \oplus b := a \cdot b$. Zeige, dass $(\mathbb{R}^+, \oplus)$ eine kommutative Gruppe ist.

(b) Für alle $x \in \mathbb{R}$ und alle $a \in \mathbb{R}^+$ definieren wir[6] $x * a := a^x$. Zeige, dass $(\mathbb{R}^+, \oplus)$ mit dieser Multiplikation „Skalar mal Vektor" zu einem Vektorraum über $\mathbb{R}$ wird, wobei wir im Skalarkörper $\mathbb{R}$ wie üblich rechnen.

[6] Wir setzen als bekannt vorraus: Für jedes $a \in \mathbb{R}^+$ existiert die Exponentialfunktion zur Basis a, also die Funktion $\mathbb{R} \to \mathbb{R}^+ : x \mapsto a^x := e^{x \log a}$. Es gelten die aus der Schule geläufigen Rechenregeln für Potenzen wie etwa $a^{x+y} = a^x a^y$ für alle $x, y \in \mathbb{R}$.

Beweis (a): Weil $(\mathbb{R}^\times, \cdot)$ abelsch ist, können wir auch $(\mathbb{R}^+, \oplus) \subset (\mathbb{R}^\times, \cdot)$ zeigen.

Offensichtlich ist $\mathbb{R}^+ \neq \emptyset$. $\forall a, b \in \mathbb{R}^+ : a \oplus b^{-1} \in \mathbb{R}^+$, weil

$a > 0 \wedge b > 0 \Rightarrow a^{-1} > 0 \wedge b^{-1} > 0 \wedge a \oplus b > 0$. $\square$

Beweis (b): 1. $(a \oplus b)^x = a^x \oplus b^x$.

2. $a^{x+y} = a^x \oplus a^y$.

3. $a^{xy} = (a^x)^y$.

4. $a^1 = a$. $\square$