P 22. Untergruppe - Nebenklasse

In der Gruppe $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ mit der Addition $(v_1, v_2) + (w_1, w_2) := (v_1 + w_1, v_2 + w_2)$ sei eine skalare Multiplikation definiert durch $\lambda \cdot (v_1, v_2) := (\lambda \cdot v_1, \lambda \cdot v_2)$ mit $\lambda \in \mathbb{R}$.

Zeigen Sie:

1. Für jedes $v \in \mathbb{R}^2 \setminus \{(0,0)\}$ ist $U_v := \{\lambda \cdot v \mid \lambda \in \mathbb{R}\}$ eine Untergruppe von $\mathbb{R}^2$.
2. Skizzieren Sie U_v und einige Nebenklassen aus $\mathbb{R}^2/U_v$ einerseits für $v = (1,0)$, anderserseits für $v = (1,-2)$.

1. Für $v = (v_1, v_2) \in \mathbb{R}^2$ ist $U_v = \{\lambda \cdot v \mid \lambda \in \mathbb{R}\} \subset \mathbb{R}^2$ eine Untergruppe von $(\mathbb{R}^2, +)$

Teilmenge klar ✓ (ist nach Vorlesung eine Gruppe)

$\Leftrightarrow$ (zu zeigen)

(i) mit $a, b \in U_v$ ist auch $a + b \in U_v$ (Abgeschlossenheit)

(ii) mit $a \in U_v$ liegt auch das Inverse a^{-1} von a in U_v

(iii) $U_v \neq \{\ \}$ (nicht leer)

bzgl. Addition in $(\mathbb{R}^2, +)$

Zu (i): $a, b \in U_v \Leftrightarrow \exists \lambda_1, \lambda_2 \in \mathbb{R}: \ a = \lambda_1 v,\ b = \lambda_2 v \Rightarrow$

$\Rightarrow a + b = \lambda_1 v + \lambda_2 v = (\lambda_1 + \lambda_2) \cdot v \Leftrightarrow a + b \in U_v$

(ausführlich: $= (\lambda_1 v_1, \lambda_1 v_2) + (\lambda_2 v_1, \lambda_2 v_2) = ((\lambda_1 + \lambda_2) v_1, (\lambda_1 + \lambda_2) v_2) =$)

Zu (ii): zu $a = \lambda \cdot v \in U_v$ wähle $a^{-1} = -\lambda \cdot v \in U_v \Rightarrow$

$\Rightarrow a + a^{-1} = \lambda \cdot v - \lambda \cdot v = (\lambda - \lambda) \cdot v = 0 \cdot v = (0,0)$ (neutrales Element von $(\mathbb{R}^2, +)$)

d.h. $a^{-1} = -\lambda \cdot v$ ist inverses Element zu $a = \lambda \cdot v$ in U_v

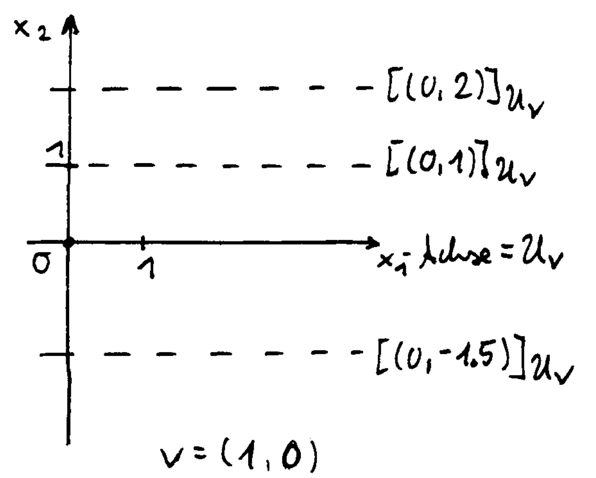
Zu (iii): $U_v \neq \{\ \}$, da $(0,0) \in U_v$ für $\lambda = 0$ ✓

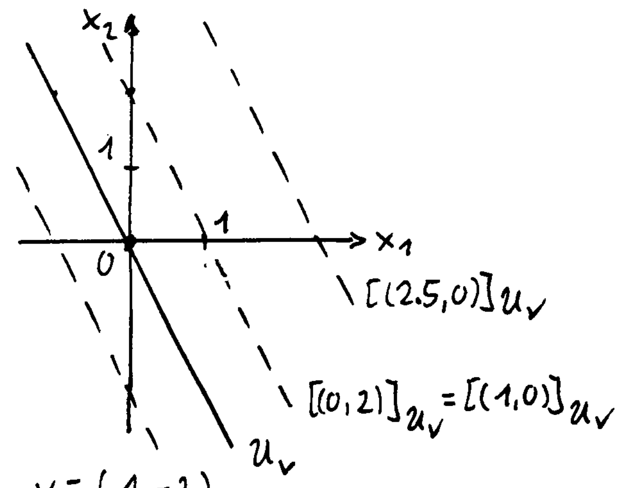
2. Nebenklasse in $\mathbb{R}^2/U_v$ zu $x \in \mathbb{R}^2$ ist $[x]_{U_v} = \{y \in \mathbb{R}^2 \mid y = x + a,\ a \in U_v\}$

kurz $[x]_{U_v} = x + U_v$ $\quad = \{y \in \mathbb{R}^2 \mid y = x + \lambda \cdot v,\ \lambda \in \mathbb{R}\}$

[$[x]_{U_v}$ ist eine Gerade durch Aufpunkt x mit Richtung v]

[$[y]_{U_v} = [x]_{U_v} \Leftrightarrow \exists \lambda \in \mathbb{R}: y = x + \lambda v \Leftrightarrow \exists \lambda \in \mathbb{R}: \ y - x = \lambda \cdot v \in U_v$]





Die Parallelenschar $\{[x]_v \mid x \in \mathbb{R}^2\}$ zur Richtung v ist jeweils eine Partition von $\mathbb{R}^2$.

Was bedeutet $y \in [x]_v$ geometrisch? Was bedeutet $[x] + [y] = [x + y]$?

M 23. Zu welchen Gruppen aus Aufgabe P 10 sind folgenden Strukturen isomorph ?

$(\mathbb{Z}_2, \oplus_2)$, $(\mathbb{Z}_3\backslash\{0\}, \odot_3)$, $(\mathbb{Z}_4\backslash\{0\}, \odot_4)$, $(\mathbb{Z}_4, \oplus_4)$, $(\mathbb{Z}_5\backslash\{0\}, \odot_5)$

Zwei Gruppen $(G, \circ)$ und $(H, \bullet)$ sind isomorph $\Leftrightarrow$
Es gibt einen bijektiven (surjektiv und injektiv) Homomorphismus $f: G \to H$
mit $f(a \circ b) = f(a) \bullet f(b)$ (strukturerhaltende Abbildung)
Dabei muss wegen $f(a) = f(e_G \circ a) = f(e_G) \bullet f(a)$ gelten $f(e_G) = e_H$.
(jeweils neutrale Elemente)

- $(\mathbb{Z}_2, \oplus_2)$ und $(\mathbb{Z}_3\backslash\{0\}, \odot_3)$ sind Gruppen mit 2 Elementen und damit isomorph zu <u>der</u> Gruppe mit 2 Elementen aus Aufgabe P10.

$\oplus_2$	0	1
0	0	1
1	1	0

isomorph

$\circ$	e	a
e	e	a
a	a	e

isomorph

$\odot_3$	1	2
1	1	2
2	2	1

$f(0) = e$, $f(1) = a$ $g(1) = e$, $g(2) = a$ (Homomorphie nachrechnen!)

- $(\mathbb{Z}_4\backslash\{0\}, \odot_4)$ ist keine Gruppe, da $2 \odot_4 2 = 0$, d.h. 2 ein Nullteiler ist.

- $(\mathbb{Z}_4, \oplus_4)$ und $(\mathbb{Z}_5\backslash\{0\}, \odot_5)$ sind Gruppen mit 4 Elementen und damit entweder zur zyklischen Gruppe oder zur Kleinschen Vierergruppe aus Aufgabe P10. Letztere besitzt nur selbstinverse Elemente, d.h. $x^2 = e \; \forall x$. Wegen $1 \oplus_4 1 = 2 \neq 0$ bzw. $2 \odot_5 2 = 4 \neq 1$ sind beide Gruppen isomorph zur zyklischen Gruppe mit 4 Elementen.

$\oplus_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

isomorph

$\circ$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

isomorph

$\odot_5$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

$f(0) = e$, $f(1) = a$, $f(2) = b$, $f(3) = c$ | $g(1) = e$, $g(2) = a$, $g(3) = c$, $g(4) = b$

Die Homomorphiebedingung stellt sicher, dass nicht nur die Elemente der beiden Gruppen bijektiv aufeinander abgebildet werden, sondern auch die Struktur der i.a. verschiedenen Verknüpfungen.

<u>Bem.</u> zu $\mathbb{Z}_5\backslash\{0\}, \odot_5$
Vertauschen von 3 und 4 liefert:

$\odot_5$	1	2	4	3
1	1	2	4	3
2	2	4	3	1
4	4	3	1	2
3	3	1	2	4

Aufgabe 24. Konjugation ist ein Automorphismus.
Es sei $(G, \circ)$ eine Gruppe. Für ein Element $a \in G$ definieren wir die Abbildung

$$f_a : \begin{cases} G & \rightarrow & G \\ x & \mapsto & a \circ x \circ a^{-1} \end{cases}.$$ Dabei bezeichne a^{-1} das inverse Element zu a in G.

Zeigen Sie, dass f_a ein Gruppenisomorphismus von G ist.

LÖSUNG:

Wir müssen nachweisen, dass f_a injektiv und surjektiv ist, und dass $f_a(x \circ y) = f_a(x) \circ f_a(y)$ für alle $x, y \in G$ erfüllt ist.
f_a ist injektiv:
Es seien $x, y \in G$ mit $f_a(x) = f_a(y)$ gegeben. Dann gilt $a \circ x \circ a^{-1} = a \circ y \circ a^{-1}$.
Multiplikation dieser Gleichung mit a^{-1} von links und mit a von rechts ergibt $x = y$.
f_a ist surjektiv:
Es sei $y \in G$ vorgegeben. Dann suchen wir ein $x \in G$ mit $f_a(x) = y$, d.h. eine Lösung von $a \circ x \circ a^{-1} = y$.
Multiplikation dieser Gleichung mit a^{-1} von links und mit a von rechts ergibt $x = a^{-1} \circ y \circ a$, und es gilt (zur Probe): $f_a(x) = f_a(a^{-1} \circ y \circ a) = a \circ (a^{-1} \circ y \circ a) \circ a^{-1} = (a \circ a^{-1}) \circ y \circ (a \circ a^{-1}) = e \circ y \circ e = y$.
f_a ist strukturerhaltend:
Es seien $x, y \in G$ und e das neutrale Element von $(G, \circ)$. Dann gilt:
$$f_a(x \circ y) = a \circ (x \circ y) \circ a^{-1} = (a \circ x) \circ (y \circ a^{-1}) = (a \circ x) \circ e \circ (y \circ a^{-1}) = (a \circ x) \circ (a^{-1} \circ a) \circ (y \circ a^{-1}) =$$
$$= (a \circ x \circ a^{-1}) \circ (a \circ y \circ a^{-1}) = f_a(x) \circ f_a(y).$$

P 25. Sei $(G, \cdot)$ eine Gruppe mit endlich vielen Elementen ($|G| < \infty$) und neutralem Element e.
Die von $A \subseteq G$ ($A \neq \{\}$) **erzeugte Menge** $\langle A \rangle$ ist definiert durch $\langle A \rangle := \{\prod_{i=1}^{n} a_i \mid n \in \mathbb{N}\backslash\{0\} \wedge a_i \in A\}$.
Zeigen Sie: $\langle A \rangle$ ist die kleinste Untergruppe von G, die A enthält ($A \subseteq \langle A \rangle$), also dass gilt:

a) $\langle A \rangle$ ist Untergruppe von G mit $A \subseteq \langle A \rangle$, (d. h. $A \subseteq \langle A \rangle \leq G$).

b) Ist H Untergruppe von G ($H \leq G$) mit $A \subseteq H \Rightarrow \langle A \rangle \subseteq H$.

$\langle A \rangle$ heißt die von $A \subseteq G$ **erzeugte Untergruppe**.

Hinweis: Betrachte zunächst die von einem Element a der endlichen Gruppe G erzeugte Menge $\langle \{a\} \rangle = \{a, a^2, a^3, ...\}$ und zeige, dass $a^{|\langle \{a\} \rangle|} = e$. $|\langle \{a\} \rangle|$ nennt man die **Ordnung** von a.

1.) Gemäß dem Hinweis betrachten wir $<\{a\}> = \{a, a^2, a^3, \ldots\}$ für $a \in G$
Da $(G, \cdot)$ als Gruppe abgeschlossen ist, folgt $<\{a\}> \subseteq G$ (Teilmenge)
Annahme: $a^i \neq a^j \;\; \forall i < j, \; i, j \in \mathbb{N}\setminus\{0\} \Rightarrow |<\{a\}>| = \infty$ im Widerspruch zu $<\{a\}> \subseteq G$, da $|G|$ endlich.
Folglich: $\exists \, i, j \in \mathbb{N}\setminus\{0\} : i < j \wedge a^i = a^j$
Somit: $\exists \, k \in \mathbb{N}\setminus\{0\} : i + k = j$ und $a^i = a^j = a^{i+k} = a^i \cdot a^k = a^k \cdot a^i$
$\Rightarrow a^k$ ist neutrales Element von G, $e = a^k$
Sei nun s die kleinste positive natürliche Zahl mit $a^s = e$
so gilt: $<\{a\}> = \{a, a^2, a^3, \ldots, a^{s-1}, a^s = e\}$ und $s = |<\{a\}>|$
<u>Wir halten fest:</u> In endlichen Gruppen hat jedes Element endliche Ordnung, d.h. $a^{|<\{a\}>|} = e$ und es gilt $a^{-1} = a^{|<\{a\}>|-1} = a^{s-1} \in <\{a\}>$.

2) Sei nun $A \subseteq G$ (Teilmenge)

a) Behauptung $\langle A\rangle := \{ \prod_{i=1}^{n} a_i \mid n \in \mathbb{N}\setminus\{0\} \wedge a_i \in A \} \leq G$ (Untergruppe)

Beweis mit Untergruppenkriterium

- nicht leer klar
- abgeschlossen $a, b \in \langle A\rangle \Rightarrow a \cdot b \in \langle A\rangle$ nach Definition von $\langle A\rangle$
- enthält Inverses zu $a \in \langle A\rangle \subseteq G$ da nach 1) $\forall a \in G: a^{-1} \in \langle\{a\}\rangle \subseteq \langle A\rangle$

alternativ: Sei $a = \prod_{i=1}^{n} a_i$ für ein $n \in \mathbb{N}\setminus\{0\}$ und $a_i \in A$

$\Rightarrow$ Nach 1) $\forall a_i \in A \subseteq G: \; a_i^{-1} \in \langle\{a_i\}\rangle \subseteq \langle A\rangle$ (nach Definition von $\langle A\rangle$)

und $a^{-1} := a_n^{-1} \circ a_{n-1}^{-1} \cdots a_2^{-1} \cdot a_1^{-1} \in \langle A\rangle$, (da $\langle A\rangle$ abgeschlossen)

ist Inverses zu a, da

$$a \cdot a^{-1} = a_1 \cdot a_2 \cdots \underbrace{a_{n-1} \cdot \underbrace{a_n \cdot a_n^{-1}}_{=e} \cdot a_{n-1}^{-1}}_{=e \text{ usw.}} \cdots a_2^{-1} \cdot a_1^{-1} = e \quad \square$$

b) $A \subseteq H \leq G \Rightarrow \langle A\rangle = \{ \prod_{i=1}^{n} a_i \mid n \in \mathbb{N}\setminus\{0\} \wedge a_i \in A \} \subseteq H$, da H als Untergruppe von G bzgl. der Gruppenoperation $\cdot$ abgeschlossen ist.

Anmerkung: $\langle A\rangle = \bigcap \{ H \mid H \leq G \wedge A \subseteq H \}$ (Durchschnitt aller Untergruppen von G, die A enthalten)

„$\subseteq$" gilt nach b)

„$\supseteq$" gilt, da $\langle A\rangle \in \{ H \mid H \leq G \wedge A \subseteq H \}$ nach a)

Anmerkung: Ist G keine endliche Gruppe und $\emptyset \neq A \subseteq G$

$\Rightarrow \langle A\rangle := \{ \prod_{i=1}^{n} a_i \mid n \in \mathbb{N}\setminus\{0\} \wedge (a_i \in A \vee a_i^{-1} \in A) \}$

Anmerkung: Bei einer endlichen Gruppe erzeugt jedes Element $a \in G$ eine zyklische Untergruppe $\langle\{a\}\rangle = \{a, a^2, a^3, \ldots, a^n = e\}$ mit $n = |\langle\{a\}\rangle| = \mathrm{ord}(a)$

Mit $a^0 := e$ gilt: $a^i \cdot a^j = a^{(i+j) \bmod n} \quad \forall i,j \in \{0, 1, \ldots, n-1\} \subseteq \mathbb{N}$

G muss deswegen noch lange nicht zyklisch sein, wie die Kleinsche Vierergruppe zeigt, vgl. P10 $\{e, a, b, c\}$ mit $a^2 = b^2 = c^2 = e$.

Frage Warum reicht nicht folgender Schluss für $|\langle\{a\}\rangle| < \infty$:

Annahme $\nexists n \in \mathbb{N}\setminus\{0\}: a^n = e \Rightarrow |\{a, a^2, \ldots\}| = \infty$ ↯ zu $|G| < \infty$?

Aufgabe 26. In welcher Klasse bin ich?
Es seien M eine Menge und R eine Teilmenge von $M \times M$. Für $(x, y) \in R$ schreiben wir kurz $x \sim y$.
R heißt **Äquivalenzrelation** auf M, wenn gilt:

(1) Für alle $x \in M$ gilt $x \sim x$, d.h. R ist **reflexiv**,
(2) Aus $x \sim y$ folgt $y \sim x$, d.h. R ist **symmetrisch**,
(3) Aus $x \sim y$ und $y \sim x$ folgt $x \sim z$, d.h. R ist **transitiv**.

Zu $x \in M$ heißt die Teilmenge $[x]_R := \{y \in M \mid y \sim x\}$ die **Äquivalenzklasse** von x bezüglich R.

Überprüfen Sie, ob nachstehende Relationen auf M Äquivalenzrelationen auf M sind. Geben Sie gegebenenfalls eine geometrische Beschreibung der Äquivalenzklassen an. In welche Partitionen wird $\mathbb{R}^2$ aufgeteilt?

1. $M := \mathbb{R}^2$, $(x_1, y_1) \sim (x_2, y_2) :\Leftrightarrow x_1^2 + y_1^2 = x_2^2 + y_2^2$
2. $M := \mathbb{R}^2$, $(x_1, y_1) \sim (x_2, y_2) :\Leftrightarrow x_1 y_2 = x_2 y_1$
3. $M := \mathbb{R}^2 \backslash \{(0, 0)\}$, $(x_1, y_1) \sim (x_2, y_2) :\Leftrightarrow x_1 y_2 = x_2 y_1$

LÖSUNG:

1.) Die angegebene Relation ist eine Äquivalenzrelation, denn sie ist
(1) reflexiv: $(x_1, y_1) \sim (x_1, y_1) :\Leftrightarrow x_1^2 + y_1^2 = x_1^2 + y_1^2$
(2) symmetrisch: $(x_1, y_1) \sim (x_2, y_2) :\Leftrightarrow x_1^2 + y_1^2 = x_2^2 + y_2^2 \Leftrightarrow (x_2, y_2) \sim (x_1, y_1)$
(3) transitiv: $(x_1, y_1) \sim (x_2, y_2) \wedge (x_2, y_2) \sim (x_3, y_3) :\Leftrightarrow x_1^2 + y_1^2 = x_2^2 + y_2^2 = x_3^2 + y_3^2 \Leftrightarrow (x_1, y_1) \sim (x_3, y_3)$

Geometrische Beschreibung der Äquivalenzklassen: Die Äquivalenzklasse $[(a, b)]$ entspricht dem Kreis mit Mittelpunkt $(0, 0) \in \mathbb{R}^2$ durch den Punkt $(a, b) \in \mathbb{R}^2$. Dies sind alle Punkte $(x, y) \in \mathbb{R}^2$, die zum Ursprung $(0, 0) \in \mathbb{R}^2$ denselben Abstand haben wie der Punkt $(a, b) \in \mathbb{R}^2$.
Die Partition von $\mathbb{R}^2$ sind konzentrische Kreise um $O = (0, 0)$.

2.) Die angegebene Relation ist keine Äquivalenzrelation, denn sie ist zwar
(1) reflexiv: $(x_1, y_1) \sim (x_1, y_1) :\Leftrightarrow x_1 y_1 = x_1 y_1$ und
(2) symmetrisch: $(x_1, y_1) \sim (x_2, y_2) :\Leftrightarrow x_1 y_2 = x_2 y_1 \Leftrightarrow (x_2, y_2) \sim (x_1, y_1)$ aber
(3) nicht transitiv: Es gilt $(1, 2) \sim (0, 0)$, denn $1 \cdot 0 = 2 \cdot 0 = 0$,
und $(0, 0) \sim (3, 4)$, denn $0 \cdot 4 = 0 \cdot 3 = 0$, aber $(1, 2) \nsim (3, 4)$, denn $1 \cdot 4 \neq 2 \cdot 3$.

3.) Die angegebene Relation ist eine Äquivalenzrelation.
Der Nachweis von Reflexivität und Symmetrie erfolgt wie in 2. Zum Nachweis der Transitivität:
Aus $(a, b) \sim (c, d) \Leftrightarrow ad = bc$ und $(c, d) \sim (e, f) \Leftrightarrow cf = de$ folgt $acdf = bcde$.
Wir müssen zeigen, dass daraus $af = be \Leftrightarrow (a, b) \sim (e, f)$ folgt.
Nach Voraussetzung ist $(a, b) \neq (0, 0)$, $(c, d) \neq (0, 0)$ und $(e, f) \neq (0, 0)$.
Fallunterscheidung für $(c, d) \neq (0, 0)$:

Fall 1: $c \neq 0$ *und* $d \neq 0$. Dann dürfen wir durch cd kürzen, und es folgt die Behauptung.

Fall 2: $c = 0$ *und* $d \neq 0$. Dann gilt $ad = 0$, und es folgt $a = 0$. Genauso folgt $de = 0$ und $e = 0$.
Mit $a = e = 0$ folgt dann $af = be = 0$.

Fall 3: $c \neq 0$ *und* $d = 0$. Mit einer ähnlichen Argumentation wie im zweiten Fall folgt $af = be = 0$.

Geometrische Beschreibung der Äquivalenzklassen: Die Äquivalenzklasse $[(a, b)]$ entspricht der Geraden durch den Ursprung und den Punkt $(a, b) \in \mathbb{R}^2$ (ohne den Punkt $(0, 0) \in \mathbb{R}^2$).
Die Partition von $\mathbb{R}^2 \backslash \{0\}$ ist das Geradenbüschel durch $O = (0, 0)$ ohne O.