

7. Algebraische Strukturen

Allgemeine algebraische Struktur

Definition

Eine algebraische Struktur ist eine Menge X zusammen mit endlich vielen endlichstelligen Operationen f_1, \dots, f_k auf X , d. h. für $i = 1, \dots, k$ ist f_i eine Abbildung $f_i: X^{\ell_i} \rightarrow X$ mit $\ell_i \in \mathbb{N}_0$.

Bemerkungen

- oftmals sind die Operationen zweistellig/binär, d. h. $\ell_i = 2$
- formal schreibt man $\mathcal{X} = (X, f_1, \dots, f_k)$ und X heißt **unterliegende Menge**
- meistens sind die Operationen klar vom Kontext und man identifiziert die Struktur mit der unterliegenden Menge

Beispiele

- $(\mathbb{R}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, Körper im Allgemeinen
- $(\mathbb{Z}, +, \cdot)$, $(\mathbb{N}, +, \cdot)$, $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$
- BOOLSche Algebren: z. B. $(\{0, 1\}, \vee, \wedge, \neg, 0, 1)$ und $(\wp(M), \cup, \cap, \bar{}, \emptyset, M)$
- $F(A) = \{f \mid f: A \rightarrow A\}$ mit der Komposition \circ , d. h. $(f \circ g)(x) = f(g(x))$
- $(\mathcal{S}(A), \circ)$ für die Bijektionen $\mathcal{S}(A) = \{f \in F(A) : f \text{ bijektiv}\}$ auf A

Neutrale Elemente

Definition

Sei $(X, *)$ eine algebraische Struktur mit einem zweistelligen Operator $*$. Ein Element $e \in X$ heißt **neutrales Element**, falls für alle $x \in X$ gilt

$$e * x = x = x * e.$$

Proposition

Ist $*$ eine zweistellige Operation auf X , so gibt es höchstens ein neutrales Element bezüglich $*$.

Beweis:

Seien $e, e' \in X$ neutral. Dann gilt

$$e \stackrel{e' \text{ neutral}}{=} e * e' \stackrel{e \text{ neutral}}{=} e'.$$

Somit ist $e = e'$. □

Neutrale Elemente – Beispiele

- 0 ist neutral in $(\mathbb{R}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{Z}, +)$ und $(\mathbb{N}_0, +)$
- 1 ist neutral in (\mathbb{R}, \cdot) , (\mathbb{Q}, \cdot) , (\mathbb{Z}, \cdot) , (\mathbb{N}, \cdot) und (\mathbb{N}_0, \cdot)
- in jedem Körper ist die 0 neutral bezüglich $+$ und die 1 neutral bezüglich \cdot .
- 0 und 1 sind neutral bezüglich $+$ und \cdot in $(\mathbb{Z}, +, \cdot)$
- $[0]_n$ und $[1]_n$ sind neutral bezüglich $+$ und \cdot in $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$

- $(\mathbb{N}, +)$ hat **kein** neutrales Element

- Identität $\text{id}_A: A \rightarrow A$ mit $a \mapsto a$ für alle $a \in A$ ist neutral in $(F(A), \circ)$
- id_A ist eine Bijektion und so auch neutrales Element in $(S(A), \circ)$

- 0 ist neutral für \vee und 1 ist neutral für \wedge in $(\{0, 1\}, \vee, \wedge, \neg, 0, 1)$
- \emptyset ist neutral für \cup und M ist neutral für \cap in $(\mathcal{P}(M), \cup, \cap, \overline{}, \emptyset, M)$

Inverse Elemente

Definition

Sei $(X, *)$ eine algebraische Struktur mit einem zweistelligen Operator $*$ mit einem neutralen Element e . Ein Element $x \in X$ heißt **invertierbar**, falls ein Element $y \in X$ existiert, so dass

$$x * y = e = y * x.$$

In so einem Fall sagen wir **y ist invers zu x** (bezüglich $*$).

Beispiele

- $-x$ invers zu x bezüglich $+$ für $x \in \mathbb{R}, \mathbb{Q}$ oder \mathbb{Z}
- x^{-1} invers zu x bezüglich \cdot für $x \in \mathbb{R} \setminus \{0\}$ oder $\mathbb{Q} \setminus \{0\}$
- 0 hat kein Inverses bezüglich \cdot in \mathbb{R} oder \mathbb{Q}
- $[-x]_n$ invers zu $[x]_n$ in $\mathbb{Z}/n\mathbb{Z}$ bezüglich $+$
- $[2]_4$ hat kein Inverses in $\mathbb{Z}/4\mathbb{Z}$ bezüglich \cdot
- $[3]_4$ ist selbstinvers in $\mathbb{Z}/4\mathbb{Z}$ bezüglich \cdot

Gruppen

Definition (Gruppe)

Eine **Gruppe** ist eine algebraische Struktur $(G, *)$ mit einer zweistelligen Verknüpfung $*$, die folgende Eigenschaften erfüllt:

- 1 Assoziativgesetz:** $x * (y * z) = (x * y) * z$ für alle $x, y, z \in G$,
- 2 neutrales Element:** es gibt ein neutrales Element $e \in G$
- 3 inverse Elemente:** und jedes x in G ist invertierbar (bezüglich $*$).

Gilt zusätzlich das

- 4 Kommutativgesetz:** $x * y = y * x$ für alle $x, y \in G$,

dann heißt die Gruppe $(G, *)$ **abelsch/kommutativ**.

Bemerkungen

- algebraische Strukturen die **1** erfüllen, heißen **Halbgruppen**
- algebraische Strukturen die **1** und **2** erfüllen, heißen **Monoide**

Beispiele

- algebraische Strukturen (\mathbb{N}, \cdot) , $(\mathbb{R}, +)$, (\mathbb{R}, \cdot) und $(F(A), \circ)$ sind Monoide
 - $(\mathbb{N}, +)$ ist kein Monoid, da es in \mathbb{N} bezüglich $+$ kein neutrales Element gibt
 - $(\mathbb{N}, +)$ ist eine Halbgruppe.
 - für eine Menge A , die wir in diesem Zusammenhang **Alphabet** nennen, sei
 - A^* die Menge aller endlichen Folgen von Zeichen aus A
 - Elemente von A^* heißen **Wörter** über A
 - für zwei Wörter $v = a_1 \dots a_n$ und $w = b_1 \dots b_m$ definieren wir die **Verkettung** $v \frown w$ von v und w als das Wort $a_1 \dots a_n b_1 \dots b_m$
- ⇒ dann ist (A^*, \frown) ein Monoid mit dem leeren Wort als neutralem Element
- für jedes $n \geq 2$ ist $(\mathbb{Z}/n\mathbb{Z}, \cdot)$ ein Monoid

Eindeutigkeit der Inversen

Satz

Ist $(M, *)$ ein Monoid, so besitzt jedes $x \in M$ höchstens ein Inverses.

Beweis: Seien y und $y' \in M$ Inverse von $x \in M$. Dann gilt

$$y \stackrel{2}{=} y * e = y * (x * y') \stackrel{1}{=} (y * x) * y' = e * y' = y'.$$



Proposition

Ist (G, \cdot) eine Gruppe, so gilt $(xy)^{-1} = y^{-1}x^{-1}$ für alle $x, y \in G$.

Beweis: Seien $x, y \in G$. Dann gilt

$$(xy)(y^{-1}x^{-1}) \stackrel{1}{=} x(yy^{-1})x^{-1} = x \cdot e \cdot x^{-1} = xx^{-1} = e.$$

$\implies y^{-1}x^{-1}$ ist invers zu xy

\implies wegen der Eindeutigkeit der Inversen gilt $(xy)^{-1} = y^{-1}x^{-1}$



Multiplizieren und Kürzen

- für eine Gruppe G (ohne Angabe der Operation) nehmen wir standardmäßig an, dass \cdot die Operation ist, d. h. für $a, b \in G$ ist die Gruppenoperation $a \cdot b = ab$
- das neutrale Element bezeichnen wir mit e
- für $a \in G$ bezeichnet a^{-1} das Inverse von a

Lemma

Sei G eine Gruppe. Dann gilt für alle $a, b, c \in G$:

- 1 falls $ab = ac$, dann ist $b = c$. (Genauso folgt aus $ba = ca$ auch $b = c$.)
- 2 die Gleichung $ax = b$ (ebenso $xa = b$), wobei x eine Unbekannte ist, ist eindeutig lösbar.

Beweis:

- 1 multipliziere beide Seiten der Gleichung mit a^{-1} von links ✓
- 2 Multiplikation mit a^{-1} von links zeigt $x = a^{-1}b$ ist eine Lösung
Sei c auf der anderen Seite eine Lösung $\Rightarrow ac = b = aa^{-1}b$ und somit gilt wegen dem ersten Teil auch $c = a^{-1}b$. □

Gruppen – Beispiele

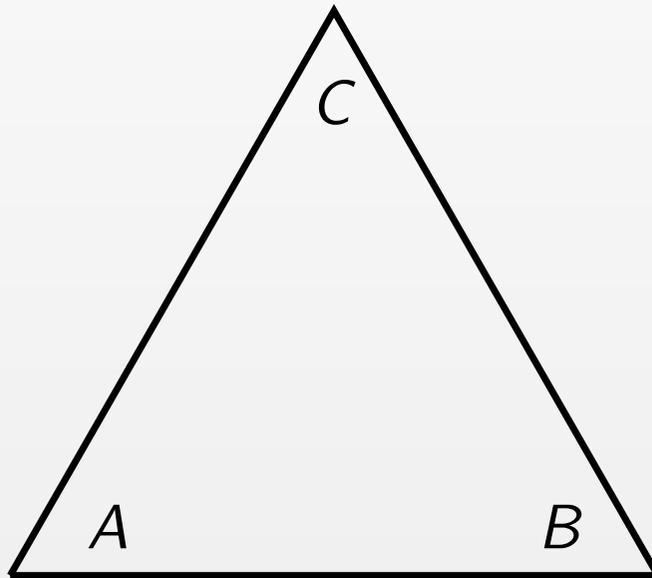
- $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$ und $(\mathbb{R}, +)$ sind abelsche Gruppen
- für jedes $n \geq 1$ ist $(\mathbb{Z}/n\mathbb{Z}, +)$ eine abelsche Gruppe
- $(\mathbb{Q} \setminus \{0\}, \cdot)$ und $(\mathbb{R} \setminus \{0\}, \cdot)$ sind abelsche Gruppen
- ist p eine Primzahl, so ist $(\mathbb{Z}/p\mathbb{Z} \setminus \{[0]_p\}, \cdot)$ eine abelsche Gruppe
- für jedes $n \geq 2$ ist die Einheitengruppe $((\mathbb{Z}/n\mathbb{Z})^\times, \cdot)$ eine abelsche Gruppe
- für eine Menge A bildet die Menge $\mathcal{S}(A)$ der Bijektionen von A nach A zusammen mit der Komposition (Hintereinanderausführung) \circ die Gruppe $(\mathcal{S}(A), \circ)$
 - für jede Bijektion $f \in \mathcal{S}(A)$ gibt es eine Umkehrfunktion f^{-1} , die das zu f inverse Element ist
 - $(\mathcal{S}(A), \circ)$ heißt die **symmetrische Gruppe** auf A
 - für $A = [n] = \{1, \dots, n\}$ mit $n \in \mathbb{N}_0$ ist $\mathcal{S}([n])$ die Menge der Permutationen auf $[n]$ und wir bezeichnen die symmetrische Gruppe mit $\mathcal{S}_n := ([n], \circ)$ bzw. bezeichnen sie auch als **Permutationsgruppe**
 - für $n \geq 3$ ist \mathcal{S}_n **nicht** abelsch:

$$(2, 3, 1) \circ (1, 3, 2) = (2, 1, 3) \neq (3, 2, 1) = (1, 3, 2) \circ (2, 3, 1).$$

Geometrisches Beispiel

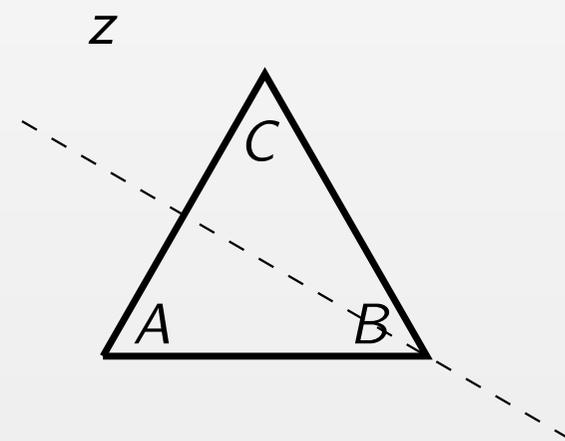
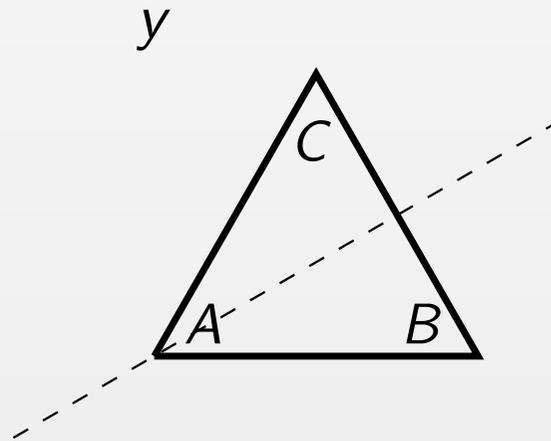
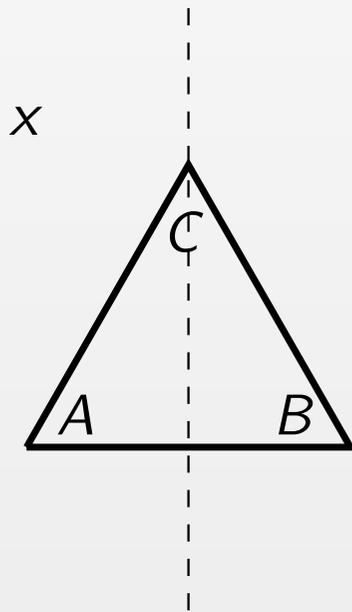
Dreiecksgruppe G_{\triangle} :

- Gruppe auf der Menge der Symmetrien eines gleichseitigen Dreiecks (Transformationen der Ebene, die das Dreieck auf das Dreieck abbilden)
- mit der zweistelligen Operation der Komposition von Abbildungen \circ



Elemente von G_{\triangle}

- **Identität i** : die jeden Punkt der Ebene auf sich selbst abbildet
- **Drehung r um 120°** : um den Mittelpunkt des Dreiecks entgegen dem Uhrzeigersinn (mathematisch positiver Drehsinn)
- **Drehung s um 240°** : um den Mittelpunkt des Dreiecks entgegen dem Uhrzeigersinn
- **Spiegelungen x , y und z** : entlang der Mittelsenkrechten des Dreiecks



G_{Δ} und S_3

Beobachtung

- alle Symmetrien i, r, s, x, y und z sind eindeutig durch die Abbildung der Ecken aufeinander bestimmt
- ⇒ jede Symmetrie entspricht einer Permutation der Menge der Ecken $\{A, B, C\}$

i	r	s
$\begin{pmatrix} A & B & C \\ A & B & C \end{pmatrix}$	$\begin{pmatrix} A & B & C \\ B & C & A \end{pmatrix}$	$\begin{pmatrix} A & B & C \\ C & A & B \end{pmatrix}$
x	y	z
$\begin{pmatrix} A & B & C \\ B & A & C \end{pmatrix}$	$\begin{pmatrix} A & B & C \\ A & C & B \end{pmatrix}$	$\begin{pmatrix} A & B & C \\ C & B & A \end{pmatrix}$

- Zwei Gruppen (G, \cdot) und (H, \odot) sind **isomorph** (geschrieben $G \cong H$), falls es eine Bijektion $\varphi: G \rightarrow H$ mit

$$\varphi(x) \odot \varphi(y) = \varphi(x \cdot y)$$

für alle $x, y \in G$ gilt und φ heißt **Gruppenisomorphismus**.

Gruppentafeln

- für (kleine) endliche Gruppen kann man alle Produkte von zwei Gruppenelementen in einer **Multiplikationstabelle/Gruppentafel** angeben
- in der Zeile für das Element a und der Spalte für das Element b steht das Produkt ab

Gruppentafel von G_{Δ} :

\circ	i	r	s	x	y	z
i	i	r	s	x	y	z
r	r	s	i	z	x	y
s	s	i	r	y	z	x
x	x	y	z	i	r	s
y	y	z	x	s	i	r
z	z	x	y	r	s	i

- Vergleich der Gruppentafeln von G_{Δ} und \mathcal{S}_3 zeigt, dass die Gruppen isomorph sind

$$\Rightarrow G_{\Delta} \cong \mathcal{S}_3$$

Gruppenisomorphismen

- $G \cong H$, falls es eine Bijektion zwischen den unterliegenden Mengen gibt, die mit den Gruppenoperationen verträglich ist

Lemma

- 1** Ist $\varphi: G \rightarrow H$ ein Gruppenisomorphismus, so auch $\varphi^{-1}: H \rightarrow G$.
- 2** Sind $\varphi: G \rightarrow H$ und $\psi: H \rightarrow I$ Gruppenisomorphismen, so auch $\psi \circ \varphi: G \rightarrow I$.
- 3** Ist $\varphi: G \rightarrow H$ ein Gruppenisomorphismus. Dann gilt
 - $\varphi(e_G) = e_H$ für die neutralen Elemente $e_G \in G$ und $e_H \in H$.
 - $\varphi(a^{-1}) = (\varphi(a))^{-1}$ für jedes $a \in G$.

Bemerkung

- Teil **1** \Rightarrow Relation \cong ist symmetrisch auf jeder Menge von Gruppen
 - Teil **2** \Rightarrow Relation \cong ist transitiv
 - Identität $\text{id}_G \Rightarrow$ Relation \cong ist reflexiv
- $\Rightarrow \cong$ definiert Äquivalenzrelation

Gruppenisomorphie ist symmetrisch

Beweis von Teil **1**:

Sei $\varphi: G \rightarrow H$ ein Gruppenisomorphismus von (G, \cdot) nach (H, \odot) .

Insbesondere φ ist bijektiv und so auch $\varphi^{-1}: H \rightarrow G$. Wir zeigen, dass φ^{-1} verträglich mit den Gruppenoperationen ist, d. h. wir zeigen

$$\varphi^{-1}(x) \cdot \varphi^{-1}(y) = \varphi^{-1}(x \odot y)$$

für alle $x, y \in H$.

Seien $x, y \in H$ beliebig und seien $a, b \in G$ die Urbilder (unter φ), d. h.

$$a = \varphi^{-1}(x) \quad \text{und} \quad b = \varphi^{-1}(y).$$

Da φ ein Gruppenisomorphismus ist, gilt insbesondere auch

$$\varphi(a \cdot b) = \varphi(a) \odot \varphi(b) = x \odot y \quad \Longrightarrow \quad a \cdot b = \varphi^{-1}(x \odot y).$$

Somit folgt die gewünschte Identität

$$\varphi^{-1}(x) \cdot \varphi^{-1}(y) = a \cdot b = \varphi^{-1}(x \odot y).$$



Gruppenisomorphie ist transitiv

Beweis von Teil 2:

Seien $\varphi: G \rightarrow H$ und $\psi: H \rightarrow I$ Gruppenisomorphismen für die Gruppen (G, \cdot) , (H, \odot) und (I, \odot) . Insbesondere sind φ und ψ bijektiv und so ist auch $\psi \circ \varphi: G \rightarrow I$ bijektiv. Wir zeigen die Verträglichkeit von $\psi \circ \varphi$ mit den Gruppenoperationen \cdot und \odot , d. h.

$$\psi(\varphi(a)) \odot \psi(\varphi(b)) = \psi(\varphi(a \cdot b))$$

für alle $a, b \in G$.

Seien $a, b \in G$ beliebig. Da ψ ein Gruppenisomorphismus ist, ist ψ verträglich mit \odot und \odot und wir haben

$$\psi(\varphi(a)) \odot \psi(\varphi(b)) = \psi(\varphi(a) \odot \varphi(b)).$$

Genauso ist der Gruppenisomorphismus verträglich mit \odot und \cdot und wir erhalten die gewünschte Identität

$$\psi(\varphi(a)) \odot \psi(\varphi(b)) = \psi(\varphi(a) \odot \varphi(b)) = \psi(\varphi(a \cdot b)).$$



Gruppenisomorphie erhält neutrale und inverse Elemente

Beweis von Teil 3:

Sei $\varphi: G \rightarrow H$ ein **Gruppenisomorphismus** zwischen den Gruppen (G, \cdot) und (H, \odot) mit neutralen Elementen e_G und e_H .

Sei $x \in H$ beliebig und sei $a \in G$ mit $\varphi(a) = x$. Dann gilt

$$x = \varphi(a) = \varphi(a \cdot e_G) = \varphi(a) \odot \varphi(e_G) = x \odot \varphi(e_G).$$

Genauso zeigt man $x = \varphi(e_G) \odot x$ für alle $x \in H$ und durch die Eindeutigkeit des neutralen Elements in H , gilt $e_H = \varphi(e_G)$. ✓

Sei nun $a \in G$ beliebig. Aufgrund des gerade Gezeigten haben wir

$$e_H = \varphi(e_G) = \varphi(a \cdot a^{-1}) = \varphi(a) \odot \varphi(a^{-1}).$$

Multiplikation mit $(\varphi(a))^{-1}$ von links auf beiden Seiten ergibt die gesuchte Identität

$$(\varphi(a))^{-1} = \varphi(a^{-1}).$$



Potenzen in Gruppen

Definition

Sei G eine Gruppe und $a \in G$. Für jedes $n \in \mathbb{N}_0$ definieren wir rekursiv

$$a^0 := e \quad \text{und} \quad a^{n+1} := a^n \cdot a$$

Für negative Exponenten definieren wir

$$a^{-n} := (a^{-1})^n$$

- wie für Potenzen reeller Zahlen rechnet man schnell für alle $a \in G$ und alle $m, n \in \mathbb{Z}$ die folgenden Rechenregeln nach:

$$a^m a^n = a^{m+n} \quad \text{und} \quad (a^m)^n = a^{mn}.$$

Ordnung von Gruppenelementen

Definition (Ordnung)

Sei G eine Gruppe und $a \in G$.

Falls ein $m \geq 1$ existiert, so dass $a^m = e$ gilt, so definiert man die **Ordnung** von a als das kleinste solche $m > 0$.

Falls kein solches m existiert, so sagen wir, dass a die Ordnung ∞ hat.

Die **Ordnung der Gruppe G** ist einfach $|G|$.

Satz

In einer endlichen Gruppe G hat jedes Element eine endliche Ordnung $\leq |G|$.

Beweis: Sei $n = |G|$ und $a \in G$. Wir betrachten die Potenzen a^1, \dots, a^n . Falls keine Potenz e ergibt und es nur $n - 1$ weitere Gruppenelemente gibt, können nicht alle diese Potenzen verschieden sein (Schubfachprinzip).

\Rightarrow es gibt $1 \leq \ell < m \leq n$, so dass $a^\ell = a^m$

$\Rightarrow a^\ell \cdot e = a^\ell a^{m-\ell}$

(Rechenregeln für Potenzen)

$\Rightarrow e = a^{m-\ell}$

(Kürzen in Gruppen)

\Rightarrow da $1 \leq m - \ell \leq n$, ist die Ordnung von a höchstens $m - \ell \leq n$ \square

Ordnung von Gruppenelementen – Beispiele

- Permutation $(2, 3, 4, 1, 5)$ hat in \mathcal{S}_5 die Ordnung 4
- in G_Δ haben r und s die Ordnung 3, x , y und z die Ordnung 2 und i ist neutral und hat Ordnung 1
- $[7]_{10}$ ist in der Einheitengruppe $((\mathbb{Z}/10\mathbb{Z})^\times, \cdot)$, da $\text{ggT}(7, 10) = 1$
Potenzen von $[7]_{10}$ sind: $[7]_{10}$, $[7]_{10}^2 = [9]_{10}$, $[7]_{10}^3 = [7 \cdot 9]_{10} = [3]_{10}$ und $[7]_{10}^4 = [7 \cdot 3]_{10} = [1]_{10} \Rightarrow$ Ordnung von $[7]_{10}$ ist 4
- **Achtung:** für die Addition in $(\mathbb{Z}, +)$ ist 0 neutral ($e = 0$) und a^n entspricht $a + \dots + a = n \cdot a$
 \Rightarrow jede ganze Zahl $x \neq 0$ hat unendliche Ordnung in $(\mathbb{Z}, +)$
- in $(\mathbb{Z}/15\mathbb{Z}, +)$ hat $[5]_{15}$ die Ordnung 3 und $[4]_{15}$ hat die Ordnung 15

Proposition

Sei G eine Gruppe, in der jedes Element $\neq e$ Ordnung 2 hat. Dann ist G abelsch.

Beweis: Seien $x, y \in G$ beliebig. Dann gilt

$$xy = (xy)e = (xy)(yx)^2 = (xy)(yx)(yx) = (x(yy)x)(yx) = (xx)(yx) = yx.$$

□

Vielfache der Ordnung

Satz

Sei G eine Gruppe und sei $a \in G$ ein Element von endlicher Ordnung m . Dann gilt für alle $n \in \mathbb{Z}$ genau dann $a^n = e$, wenn m ein Teiler von n ist.

Beweis

„ \Leftarrow “ für $n = qm$ mit $q \in \mathbb{Z}$ gilt

$$a^n = (a^m)^q = e^q = e$$

(auch für $q < 0$) ✓

„ \Rightarrow “ Sei $n = qm + r$ mit $0 \leq r < m$. Wir werden zeigen, dass $r = 0$ gelten muss. Tatsächlich gilt

$$e = a^n = a^{qm+r} = (a^m)^q \cdot a^r = e^q \cdot a^r = a^r.$$

Da m die kleinste Zahl ≥ 1 mit $a^m = e$ ist, folgt aus $r < m$ dann $r = 0$. □

Zyklische Gruppen

Definition (Zyklische Gruppe)

Ein Gruppe (G, \cdot) heißt **zyklisch**, falls sie durch Potenzen über ein Element $a \in G$ **erzeugt** wird, d. h.

$$G = \{a^z : z \in \mathbb{Z}\}.$$

Beispiele

- $(\mathbb{Z}, +)$ ist zyklisch und sowohl 1 als auch -1 erzeugen die Gruppe
Erinnerung: multiplikative Schreibweise $\Rightarrow a^z = z \cdot a$
- für alle $n \in \mathbb{N}$ ist $(\mathbb{Z}/n\mathbb{Z}, +)$ zyklisch; erzeugt von $[1]_n$
Bemerkung: für $n = 1$ ist $\mathbb{Z}/1\mathbb{Z}$ einelementig \Rightarrow zyklisch
- S_2 ist zyklisch und wird von der Permutation $(2, 1)$ erzeugt
Bemerkung: alle zweielementigen Gruppen sind isomorph
- G_Δ ist **nicht** zyklisch:
 - Potenzen (Hintereinanderausführungen) von i bleiben i
 - Drehungen r und s haben jeweils Ordnung 3 und können somit nur 3, nicht aber alle 6 Elemente, von G_Δ erzeugen
 - Spiegelungen x, y, z haben Ordnung 2 und erzeugen nur 2 Elemente

Klassifizierung zyklischer Gruppen

Satz

Eine Gruppe (G, \cdot) ist zyklisch genau dann, wenn sie isomorph zu $(\mathbb{Z}, +)$ oder isomorph zu $(\mathbb{Z}/n\mathbb{Z}, +)$ für ein $n \in \mathbb{N}$ ist.

- Rückrichtung hatten wir bereits durch die Beispiele gezeigt
- Satz \implies zyklische Gruppen sind abelsch

Beweis: Sei $G = \{a^z : z \in \mathbb{Z}\}$ durch a erzeugt mit neutralem Element e_G .

1. Fall: (a hat Ordnung ∞ in G)

Betrachte die Abbildung $\varphi: \mathbb{Z} \rightarrow G$ gegeben durch $z \mapsto a^z$.

- φ ist surjektiv, da G durch a erzeugt wird
- φ ist injektiv, da sonst aus $a^z = a^{z'}$ für $z > z'$ wegen $a^{z-z'} = e_G$ folgt, dass a endliche Ordnung $z - z' > 0$ hätte ⚡ zur Fallannahme

$\implies \varphi$ ist bijektiv

- φ ist ein Isomorphismus, da

$$\varphi(z + z') = a^{z+z'} = a^z \cdot a^{z'} = \varphi(z) \cdot \varphi(z')$$



Klassifizierung zyklischer Gruppen – endliche Ordnung

2. Fall: (a hat Ordnung n in G)

Betrachte nun die Abbildung $\psi: \mathbb{Z}/n\mathbb{Z} \rightarrow G$ gegeben durch $[z]_n \mapsto a^z$.

- ψ ist wohldefiniert: Seien $z \equiv z' \pmod{n}$

$$\Rightarrow n \mid z - z'$$

$$\Rightarrow a^{z-z'} = e_G$$

(Satz über Vielfache der Ordnung)

$$\Rightarrow a^z = a^{z'} \quad \checkmark$$

- ψ ist injektiv: falls $\psi([z]_n) = a^z = a^{z'} = \psi([z']_n)$

$$\Rightarrow a^{z-z'} = e_G$$

$$\Rightarrow n \mid z - z'$$

(Satz über Vielfache der Ordnung)

$$\Rightarrow z \equiv z' \pmod{n} \Rightarrow [z] = [z'] \quad \checkmark$$

- ψ ist surjektiv, da a die Gruppe G erzeugt

$\Rightarrow \psi$ ist bijektiv

- ψ ist ein Isomorphismus, da

$$\psi([z]_n + [z']_n) = a^{z+z'} = a^z \cdot a^{z'} = \psi([z]_n) \cdot \psi([z']_n)$$

\checkmark

Untergruppen

Definition (Untergruppe)

Sei (G, \cdot) eine Gruppe. Eine Menge $U \subseteq G$ heißt **Untergruppe** von G , falls (U, \cdot) eine Gruppe ist, wobei man die Einschränkung von \cdot auf $U \times U$ betrachtet:

- 1 für alle $u, v \in U$ gilt $u \cdot v \in U$,
- 2 es existiert $e_U \in U$ mit $u \cdot e_U = u = e_U \cdot u$ für alle $u \in U$
- 3 und für jedes $u \in U$ gibt es $u' \in U$ mit $u \cdot u' = e_U = u' \cdot u$.

Bemerkungen

- Assoziativität muss nicht extra gefordert werden, da diese sich von G auf U vererbt
- wir werden sehen (Untergruppenkriterium), dass e_U das neutrale Element von G sein muss
- ebenso entsprechen die inversen Elementen denen aus G , d. h. $u' = u^{-1}$

Beispiele

- für $m \in \mathbb{N}_0$ ist $m\mathbb{Z} := \{m \cdot z : z \in \mathbb{Z}\} \subseteq \mathbb{Z}$ die Menge aller Vielfachen von m eine Untergruppe von $(\mathbb{Z}, +)$:
 - 1 $u, v \in m\mathbb{Z} \implies m \mid u$ und $m \mid v \implies m \mid (u + v) \implies u + v \in m\mathbb{Z}$
 - 2 $0 \in m\mathbb{Z}$ und 0 ist neutral
 - 3 $u \in m\mathbb{Z} \implies m \mid -u \implies -u \in m\mathbb{Z}$ $\implies (m\mathbb{Z}, +)$ ist eine Untergruppe von $(\mathbb{Z}, +)$
- jede Gruppe G mit neutralem Element e hat triviale Untergruppen:
 - Untergruppe $\{e\}$ „kleinste Untergruppe“
 - G selbst ist eine Untergruppe von G „größte Untergruppe“
- G_Δ hat die folgenden Untergruppen:
 - triviale Untergruppen $\{i\}$ und G_Δ ,
 - $\{i, x\}, \{i, y\}, \{i, z\}$ sind Untergruppen, da Spiegelungen selbstinvers sind,
 - die Drehungen bilden mit der Identität die Untergruppe $\{i, r, s\}$ von G_Δ
 - da zwei Spiegelungen eine Drehung erzeugen und jede Drehung zusammen mit jeder beliebigen Spiegelung alle Elemente von G_Δ erzeugt, gibt es keine anderen Untergruppen in G_Δ
- $\{[0]_{15}, [5]_{15}, [10]_{15}\}$ und $\{[0]_{15}, [3]_{15}, [6]_{15}, [9]_{15}, [12]_{15}\}$ sind Untergruppen von $\mathbb{Z}/15\mathbb{Z}$
- für $a \in G$ ist $\langle a \rangle := \{a^z : z \in \mathbb{Z}\}$ die von a erzeugte Untergruppe

Untergruppenkriterien

Satz

Sei (G, \cdot) eine Gruppe mit neutralem Element e und $U \subseteq G$. Folgende Aussagen sind äquivalent:

- 1 U ist eine Untergruppe von G ,
- 2 $e, u^{-1}, uv \in U$ für alle $u, v \in U$,
- 3 $U \neq \emptyset$ und $uv^{-1} \in U$ für alle $u, v \in U$.

Beweis: („1 \Rightarrow 2“)

Sei U eine Untergruppe mit neutralem Element $e_U \in U$. Dann gilt:

$$e_U \cdot e_U \stackrel{e_U \text{ neutral in } U}{=} e_U \stackrel{e \text{ neutral in } G}{=} e_U \cdot e \implies e_U = e.$$

Seien $u \in U$ und $u' \in U$ das Inverse von u in U . Dann gilt:

$$u \cdot u' = e_U = e \quad \text{und} \quad u' \cdot u = e_U = e \implies u' = u^{-1},$$

wegen der Eindeutigkeit Inverser Elemente in G .



Beweis der Untergruppenkriterien

„**2** \Rightarrow **3**“

- $e \in U \implies U$ ist nicht leer
- $u, v \in U \implies v^{-1} \in U \implies uv^{-1} \in U$



„**3** \Rightarrow **1**“

- $U \neq \emptyset \implies$ es gibt $u \in U \implies uu^{-1} \in U \implies uu^{-1} = e \in U$
- da $e \in U$ gilt für $u \in U$ somit auch $eu^{-1} = u^{-1} \in U$
- seien nun $u, v \in U \implies v^{-1} \in U \implies u \cdot (v^{-1})^{-1} = uv \in U$



Korollar

Sei (G, \cdot) eine Gruppe und für endliches U mit $\emptyset \neq U \subseteq G$ gilt $uv \in U$ für alle $u, v \in U$. Dann ist U eine Untergruppe von G .

Beweis: Sei $U = \{u_1, \dots, u_n\}$ für ein $n \geq 1$. Für jedes $i \in [n]$ sind die n Produkte
 $u_i u_1, u_i u_2, \dots, u_i u_n$

paarweise verschieden und liegen alle in U . D.h. für jedes $u \in U$ gibt es ein $j \in [n]$ mit $u_i u_j = u$

\implies für $u = u_i$ gibt es $j \in [n]$, sodass $u_i u_j = u_i \implies e = u_j \in U$

\implies für $u = e$ gibt es $k \in [n]$, sodass $u_i u_k = e \implies u_i^{-1} = u_k \in U$

$\implies U$ ist eine Untergruppe nach Teil **2** des vorherigen Satzes.



Nebenklassen

Definition (Nebenklassen)

Sei G eine Gruppe, sei $U \subseteq G$ eine Untergruppe und $a \in G$. Wir definieren

$$aU := \{au : u \in U\} \quad \text{und} \quad Ua := \{ua : u \in U\}.$$

Wir nennen die Mengen der Form aU **Linksnebenklassen** von U und die Mengen der Form Ua **Rechtsnebenklassen**.

Beispiele:

- G abelsch $\Rightarrow aU = Ua$ für alle $a \in G$ und Untergruppen U
- für $G = (\mathbb{Z}, +)$ und $U = 6\mathbb{Z}$ ist $\{\dots, -2, 4, 10, \dots\} = [4]_6$ die Linksnebenklasse $4 + 6\mathbb{Z}$ **additive Schreibweise hier**
- für $U = \{i, x\}$ in G_Δ gilt

$$iU = \{i, x\}, \quad rU = \{r, y\}, \quad sU = \{s, z\}$$

und

$$Ui = \{i, x\}, \quad Ur = \{r, z\}, \quad Us = \{s, y\}.$$

Struktur der Nebenklassen

Satz

Sei G eine Gruppe und $U \subseteq G$ eine Untergruppe. Dann gilt:

- 1** für alle $a \in G$ ist $a \in aU$.
- 2** für alle $u \in U$ ist $uU = U$.
- 3** für $a, b \in G$ mit $b \in aU$ gilt $aU = bU$.
- 4** für $a, b \in G$ sind aU und bU entweder disjunkt oder gleich.
- 5** für alle $a \in G$ gilt $|aU| = |U|$.

Die Aussagen gelten analog für Rechtsnebenklassen.

Bemerkungen:

- Teile **1** und **4** \Rightarrow Links- bzw. Rechtsnebenklassen von U partitionieren G
 - Linksnebenklassen entsprechen Äquivalenzrelation $x \sim y :\Leftrightarrow x^{-1}y \in U$
 - Rechtsnebenklassen entsprechen Äquivalenzrelation $x \approx y :\Leftrightarrow xy^{-1} \in U$
- Beweise der Teile **1** und **2** folgen direkt aus den Gruppeneigenschaften $e \in U$ und $uv \in U$ für alle $u, v \in U$

Beweise

Teil 3: Sei $b \in aU$, d. h. $b = au_0$ für ein $u_0 \in U$.

\Rightarrow für jedes $u \in U$ gilt $bu = (au_0)u = a(u_0u) \in aU$, da $u_0, u \in U$

$\Rightarrow bu \in aU$ für alle $u \in U$

$\Rightarrow bU \subseteq aU$

Andererseits gilt für jedes $u \in U$ auch $au = (bu_0^{-1})u = b(u_0^{-1}u) \in bU$.

$\Rightarrow aU \subseteq bU$. ✓

Teil 4: Falls $aU \cap bU \neq \emptyset$, dann gibt ein $c \in G$ mit $c \in aU$ und $c \in bU$ und wegen **3** gilt

$$aU = cU \quad \text{und} \quad bU = cU \quad \Longrightarrow \quad aU = bU.$$

Teil 5: Betrachte die Abbildung $f: aU \rightarrow U$ gegeben durch $v \mapsto a^{-1}v$. ✓

■ f ist surjektiv: für $u \in U$ ist $au \in aU$ und $f(au) = u$ ✓

■ f ist injektiv: falls $f(v) = f(w)$ für $v = au_v$ und $w = au_w \in aU$, dann gilt $u_v = u_w$ und somit auch $v = au_v = au_w = w$ ✓

$\Rightarrow f$ ist eine Bijektion $\Rightarrow |aU| = |U|$ □

Satz von LAGRANGE

Korollar (Satz von LAGRANGE)

Ist G eine endliche Gruppe und U eine Untergruppe von G , so ist die Ordnung $|U|$ von U ein Teiler der Ordnung $|G|$ von G .

Wegen der erzeugten Untergruppe $\langle a \rangle$ teilt somit die Ordnung von $a \in G$ auch die Ordnung $|G|$ von G .

Beweis: Da die Linksnebenklassen von U die Menge G partitionieren (Teile **1** und **4**) und alle Nebenklassen die gleiche Größe $|U|$ haben (Teil **5**), gilt

$$|G| = |U| \cdot \text{Anzahl der Linksnebenklassen von } U.$$



Definition (Index)

Für eine Untergruppe U von G ist die Anzahl der Links- bzw. Rechtsnebenklassen der **Index von U** und wird mit $[G : U]$ bezeichnet.

Satz von LAGRANGE

$|G| = [G : U] \cdot |U|$ für jede Untergruppe U einer endlichen Gruppe G .

LAGRANGE \implies Satz von FERMAT und EULER

Satz (FERMAT und EULER)

Seien $a, m \in \mathbb{N}$ teilerfremd und sei $\varphi(m)$ die EULERSche φ -Funktion (d. h. die Anzahl der zu m teilerfremden natürlichen Zahlen kleiner m). Dann gilt

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

Beweis:

Da a und m teilerfremd sind, gilt $[a]_m \in (\mathbb{Z}/m\mathbb{Z})^\times$. Des Weiteren hat die Gruppe $((\mathbb{Z}/m\mathbb{Z})^\times, \cdot)$ die Ordnung $|(\mathbb{Z}/m\mathbb{Z})^\times| = \varphi(m)$ und nach dem Satz von LAGRANGE teilt die Ordnung k von $[a]_m$ in $(\mathbb{Z}/m\mathbb{Z})^\times$ somit $\varphi(m)$, d. h. es gibt $\ell \in \mathbb{N}$ mit $k\ell = \varphi(m)$ und es gilt

$$[a]_m^{\varphi(m)} = ([a]_m^k)^\ell = [1]_m^\ell = [1]_m \implies a^{\varphi(m)} \equiv 1 \pmod{m}.$$



Zyklizität vererbt sich auf Untergruppen

Satz

Jede Untergruppe U einer zyklischen Gruppe G ist zyklisch.

Beweis:

Sei $G = \{a^z : z \in \mathbb{Z}\} = \langle a \rangle$.

Falls $U = \{e\}$, dann ist U offensichtlich zyklisch.

Sei also $a^z \in U$ mit $a^z \neq e$.

$\Rightarrow (a^z)^{-1} = a^{-z} \in U$ und entweder $z \in \mathbb{N}$ oder $-z \in \mathbb{N}$

\Rightarrow es gibt ein **kleinstes** $n \geq 1$ mit $a^n \in U$.

Wir zeigen nun $U = \{(a^n)^z : z \in \mathbb{Z}\} = \langle a^n \rangle$.

- $\langle a^n \rangle \subseteq U$ ist klar, da U eine Gruppe ist und $a^n \in U$
- sei $a^z \in U$ und $z = qn + r$ mit $q \in \mathbb{Z}$ und $0 \leq r < n$
 - \Rightarrow da $a^{-qn} \in \langle a^n \rangle \subseteq U$, ist $a^r = a^{-qn} \cdot a^z \in U$
 - \Rightarrow wegen der **minimalen Wahl von n** und $0 \leq r < n$ folgt also $r = 0$
 - $\Rightarrow a^z = a^{qn} \in \langle a^n \rangle$

□

Gruppen mit Primzahlordnung

Satz

Jede endliche Gruppe G deren Ordnung p eine Primzahl ist, ist zyklisch und hat nur triviale Untergruppen.

Beweis: Sei $a \in G$. Da $p = |G|$ eine Primzahl ist, ist nach dem Satz von LAGRANGE die Ordnung von a entweder 1 oder p .

- Ordnung von a ist 1 $\iff a = e$
 - da $|G| \geq 2$, gibt es ein $a \in G$ mit $a \neq e$
- \implies Ordnung von a ist $p \implies a^0, a^1, \dots, a^{p-1}$ sind paarweise verschiedene Elemente von G
- $\implies G = \{a^0, a^1, \dots, a^{p-1}\} = \langle a \rangle$



Permutationen

Erinnerung:

- $\mathcal{S}(A)$ ist die Menge aller Bijektionen von A nach A
- $(\mathcal{S}(A), \circ)$ ist eine Gruppe, genannt **symmetrische Gruppe** bzw. **Permutationsgruppe** auf A mit neutralem Element id_A
- für $A = [n]$ bezeichnen wir mit \mathcal{S}_n die Permutationsgruppe $(\mathcal{S}([n]), \circ)$
- Permutationsgruppen sind „universell“ für endliche Gruppen in folgendem Sinne:

Satz (CAYLEY)

Jede endliche Gruppe G ist isomorph zu einer Untergruppe von $\mathcal{S}(G)$.

Beweis: Sei (G, \cdot) eine endliche Gruppe. Für jedes $a \in G$ ist die Abbildung $\sigma_a: G \rightarrow G$ mit $b \mapsto a \cdot b$ eine Bijektion, d. h. $\sigma_a \in \mathcal{S}(G)$. Nun betrachtet man die Abbildung $f: G \rightarrow \mathcal{S}(G)$ gegeben durch

$$a \mapsto \sigma_a .$$

Man überprüft nun, dass f ein Gruppenisomorphismus zwischen G und $\{\sigma_a: a \in G\} \subseteq \mathcal{S}(G)$ etabliert.

Gruppenisomorphismus $f: G \rightarrow \mathcal{S}(G)$ durch $a \mapsto \sigma_a$

- f ist surjektiv: per Definition auf $\{\sigma_a: a \in G\} \subseteq \mathcal{S}(G)$
- f ist injektiv: $\sigma_a = \sigma_b$ bedeutet $ac = bc$ für alle $c \in G \Rightarrow a = b$

$\Rightarrow f$ ist eine Bijektion



Seien $a, b \in G$ beliebig. Die Abbildung $\sigma_{a \cdot b} = f(a \cdot b)$ ist eine Bijektion auf G , d. h. $f(a \cdot b)$ ordnet jedem $c \in G$ ein $\sigma_{a \cdot b}(c) = (a \cdot b) \cdot c \in G$ zu. Somit gilt für jedes $c \in G$

$$f(a \cdot b)(c) = \sigma_{a \cdot b}(c) = (a \cdot b) \cdot c = a \cdot (b \cdot c) = a \cdot \sigma_b(c)$$

und somit gilt

$$f(a \cdot b)(c) = a \cdot \sigma_b(c) = \sigma_a(\sigma_b(c)) = (\sigma_a \circ \sigma_b)(c) = (f(a) \circ f(b))(c).$$

Da diese Identität für alle $c \in G$ gilt, gilt also $f(a \cdot b) = f(a) \circ f(b)$ und da $a, b \in G$ beliebig waren, ist f somit ein Gruppenisomorphismus. \square

Notation

- wir studieren Permutationsgruppen \mathcal{S}_n für $n \in \mathbb{N}_0$
- Permutationen werden oft mit kleinen griechischen Buchstaben π , σ , oder τ bezeichnet
- manchmal geben wir Permutationen explizit an, z. B.

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 1 & 4 \end{pmatrix} \in \mathcal{S}_5$$

bildet 1 auf 3, 2 auf 2, 3 auf 5, 4 auf 1 und 5 auf 4 ab,

$$\sigma(1) = 3, \quad \sigma(2) = 2, \quad \sigma(3) = 5, \quad \sigma(4) = 1 \quad \text{und} \quad \sigma(5) = 4.$$

- da die erste Zeile in der expliziten Darstellung von σ redundant ist, schreiben wir manchmal auch nur $\sigma = (3, 2, 5, 1, 4)$

ACHTUNG: nicht verwechseln mit der späteren Zykelschreibweise

- da \mathcal{S}_5 endlich ist ($|\mathcal{S}_5| = 5! = 120$), hat σ endliche Ordnung (die nach LAGRANGE ein Teiler von 120 ist), d. h. es gibt ein k mit $k \mid 120$, sodass

$$\sigma^k = \sigma \circ \dots \circ \sigma = \text{id}_{[5]}.$$

Für dieses Beispiel prüft man leicht nach, dass $k = 4$ ist.

Beispiel

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 1 & 4 \end{pmatrix} \in \mathcal{S}_5$$

- iterierte Anwendungen von σ fixiert die 2 fest ($\sigma(2) = 2$) und „zykelt“ (ausgehend von 1) durch die Elemente 3, 5, 4, 1

$$\sigma(1) = 3, \quad \sigma^2(1) = \sigma(3) = 5, \quad \sigma^3(1) = \sigma(5) = 4$$

und

$$\sigma^4(1) = \sigma^3(3) = \sigma^2(5) = \sigma(4) = 1$$

und danach wiederholt sich diese Sequenz

- σ „zerfällt“ in einen Zyklus (1 3 5 4) und einen Fixpunkt (2) (trivialer Zyklus)

Zyklen

Definition (Zyklus)

Sei $X \subseteq [n]$ mit $X = \{x_1, \dots, x_k\}$ für $k \geq 2$.

Wir bezeichnen mit $(x_1 x_2 \dots x_k)$ die Permutation $\sigma \in \mathcal{S}_n$ definiert durch

$$\sigma(x) = \begin{cases} x & \text{falls } x \notin X, \\ x_{i+1} & \text{falls } x = x_i \text{ für } \{i=1, \dots, k-1\}, \\ x_1 & \text{falls } x = x_k. \end{cases}$$

Die Permutation σ ist dann ein **Zyklus** der Länge k und Zyklen der Länge 2 (Vertauschung von zwei Elementen) heißen **Transpositionen**.

Zwei Zyklen $(x_1 x_2 \dots x_k)$ und $(y_1 y_2 \dots y_\ell)$ sind **disjunkt**, wenn die beiden Mengen $\{x_1, \dots, x_k\}$ und $\{y_1, \dots, y_\ell\}$ disjunkt sind.

Neben den Schreibweisen $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 1 & 4 \end{pmatrix}$ und $(3, 2, 5, 1, 4)$ gibt es so noch die Zykelschreibweisen

$$(1354) = (3541) = (5413) = (4135) \in \mathcal{S}_5.$$

Zyklenzerlegung

Satz

Sei $n \in \mathbb{N}_0$. Dann gilt:

- Jede Permutation $\sigma \in \mathcal{S}_n$ ist ein Produkt von paarweise disjunkten Zyklen. Eine solche Darstellung nennt man **Zyklenzerlegung** von σ und diese ist bis auf die Reihenfolge eindeutig.
 - Jeder Zyklus ist ein Produkt von Transpositionen.
- ⇒ Jede Permutation $\sigma \in \mathcal{S}_n$ ist ein Produkt von Transpositionen.

Beispiel:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 1 & 3 & 6 & 2 \end{pmatrix} \in \mathcal{S}_6$$

$$\Rightarrow \sigma = (1\ 4\ 3) \circ (2\ 5\ 6)$$

$$\Rightarrow (1\ 4\ 3) = (1\ 4) \circ (4\ 3) \text{ und } (2\ 5\ 6) = (2\ 5) \circ (5\ 6)$$

$$\Rightarrow \sigma = (1\ 4) \circ (4\ 3) \circ (2\ 5) \circ (5\ 6)$$

Beweis der Zyklenzerlegung

Beweis: Betrachte die Relation $i \sim j$ auf $[n]$ gegeben durch

$$\exists n \in \mathbb{N}_0 : \sigma^n(i) = j.$$

- man prüft direkt nach, dass \sim eine Äquivalenzrelation ist
- für jede Äquivalenzklasse $[i]$ gibt es ein $m_i \in \mathbb{N}$, sodass

$$[i] = \{\sigma^0(i), \sigma^1(i), \dots, \sigma^{m_i-1}(i)\}$$

- ist $m_i = 1$, dann ist i ein Fixpunkt von σ
 - ist $m_i > 1$, dann ist $(\sigma^0(i) \sigma^1(i) \dots \sigma^{m_i-1}(i))$ ein Zykel von σ
- ⇒ Partition durch Äquivalenzklassen codiert disjunkte Zyklen von σ ✓

Der zweite Teil folgt direkt aus der Darstellung

$$(x_1 x_2 \dots x_k) = (x_1 x_2) \circ (x_2 x_3) \circ \dots \circ (x_{k-2} x_{k-1}) \circ (x_{k-1} x_k).$$



Gerade und ungerade Permutationen

Satz

Sei $\sigma \in \mathcal{S}_n$. Die Parität (gerade/ungerade) der Anzahl der Transpositionen in jeder Darstellung von σ als Transpositionen ist gleich. Dementsprechend sagen wir eine Permutation ist **gerade** bzw. **ungerade**.

Bemerkung: Einen Beweis von diesem Satz finden Sie im Skript.

Korollar

Die Menge der geraden Permutationen $\mathcal{A}_n \subseteq \mathcal{S}_n$ bildet eine Untergruppe vom Index 2 und heißt **alternierende Gruppe**.

Beweis:

- $\text{id}_{[n]}$ wird durch 0 Transpositionen dargestellt und ist somit in \mathcal{A}_n
- da die Summe zweier gerader Zahlen gerade ist, ist die Komposition zweier gerader Permutationen wieder gerade
- da Transpositionen selbstinvers sind, gilt

$$\sigma = \tau_1 \circ \cdots \circ \tau_k \implies \sigma^{-1} = (\tau_1 \circ \cdots \circ \tau_k)^{-1} = \tau_k^{-1} \circ \cdots \circ \tau_1^{-1} = \tau_k \circ \cdots \circ \tau_1$$

\implies wenn $\sigma \in \mathcal{A}_n$, dann ist auch $\sigma^{-1} \in \mathcal{A}_n$

Somit zeigt das Untergruppenkriterium, dass \mathcal{A}_n eine Untergruppe von \mathcal{S}_n ist. \square

Körper

- mithilfe von Gruppen kann man Körper kompakter definieren

Definition (Körper)

Eine Menge K mit verschiedenen Elementen $0_K, 1_K \in K$ und binären Operationen $+: K \times K \rightarrow K$ und $\cdot: K \times K \rightarrow K$ ist ein **Körper**, falls gilt:

- 1 $(K, +)$ ist eine abelsche Gruppe mit neutralem Element 0_K ,
- 2 $(K \setminus \{0_K\}, \cdot)$ ist eine abelsche Gruppe mit neutralem Element 1_K ,
- 3 für alle $a, b, c \in K$ gelten die Distributivgesetze

$$a \cdot (b + c) = a \cdot b + a \cdot c \quad \text{und} \quad (a + b) \cdot c = a \cdot c + b \cdot c.$$

Bemerkung:

- mit den Distributivgesetzen folgt $a \cdot 0_K = 0_K \cdot a = 0_K$ für alle $a \in K$:

$$a \cdot 0_K = a \cdot (0_K + 0_K) = a \cdot 0_K + a \cdot 0_K \quad \Longrightarrow \quad 0_K = a \cdot 0_K$$

$$0_K \cdot a = (0_K + 0_K) \cdot a = 0_K \cdot a + 0_K \cdot a \quad \Longrightarrow \quad 0_K = 0_K \cdot a.$$

Ringe

- Ringe benötigen weniger multiplikative Struktur als Körper

Definition (Ring)

Eine Menge R mit binären Operationen $+: R \times R \rightarrow R$ und $\cdot: R \times R \rightarrow R$ ist ein **Ring**, falls gilt:

- 1 $(R, +)$ ist eine abelsche Gruppe,
- 2 (R, \cdot) ist eine Halbgruppe,
- 3 für alle $a, b, c \in R$ gelten die Distributivgesetze

$$a \cdot (b + c) = a \cdot b + a \cdot c \quad \text{und} \quad (a + b) \cdot c = a \cdot c + b \cdot c.$$

Das neutrale Element der Addition ist das **Nullelement** 0_R von R . Wenn die Multiplikation kommutativ ist, dann ist R ein **kommutativer Ring**. Ist (R, \cdot) sogar ein Monoid mit neutralem Element 1_R , dann ist R ein **Ring mit 1/unitärer Ring**.

- wie in Körpern folgert man $0_R \cdot a = 0_R = a \cdot 0_R$ aus den Distributivgesetzen
- wir betrachten nur Ringe mit 1 und meinen bei einem Ring immer einen mit 1
- falls $0_R = 1_R$, dann ist $R = \{0_R\}$ der Nullring mit nur einem Element, da dann für jedes $a \in R$ gilt:

$$a = a \cdot 1_R = a \cdot 0_R = 0_R.$$

Beispiele und Notation

- $(\mathbb{R}, +, \cdot)$ und $(\mathbb{Q}, +, \cdot)$ sind Körper
- jeder Körper ist ein kommutativer Ring (mit 1)
- ein Ring ist nur dann ein Körper, wenn $(R \setminus \{0_R\}, \cdot)$ eine abelsche Gruppe ist
- $(\mathbb{Z}, +, \cdot)$ ist ein kommutativer Ring (mit 1), aber kein Körper
- für jedes $n \in \mathbb{N}$ ist der Restklassenring $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ ein kommutativer Ring (mit 1)
- $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ ist nur dann ein Körper, wenn n eine Primzahl ist
- wenn die Operationen klar sind, dann identifizieren wir Körper und Ringe mit ihrer Grundmenge
- an Stelle von 0_R , 1_K etc. schreiben wir oft nur 0 und 1
- für ein Element a bezeichnen wir mit $-a$ und a^{-1} die inversen Elemente bezüglich der Addition und Multiplikation

Einheitengruppe

- in einem Monoid sind die inversen Elemente (wenn sie existieren) eindeutig

Definition (Einheiten)

Sei R ein Ring (mit 1). Die Menge der Elemente a die ein multiplikatives Inverses a^{-1} haben, heißt **Einheitengruppe** $R^\times \subseteq R$, d. h.

$$R^\times := \{a \in R : \text{es gibt } b \in R \text{ mit } a \cdot b = b \cdot a = 1\},$$

und die Elemente von R^\times heißen **Einheiten**.

Satz

Für jeden Ring (mit 1) ist die Einheitengruppe (R^\times, \cdot) eine Gruppe.

Beweis

- $a, b \in R^\times \Rightarrow (ab)^{-1} = b^{-1}a^{-1} \in R \Rightarrow ab \in R^\times$ (\cdot wohldef. auf R^\times)
- $1 \in R^\times$ und $a \in R^\times \Rightarrow a^{-1} \in R^\times$
- Assoziativität vererbt sich vom Monoid (R, \cdot) □

Beispiele

- für jeden Körper K ist $K^\times = K \setminus \{0\}$
- insbesondere

$$\mathbb{R}^\times = \mathbb{R} \setminus \{0\} \quad \text{und} \quad \mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$$

und für jede Primzahl p gilt

$$(\mathbb{Z}/p\mathbb{Z})^\times = \mathbb{Z}/p\mathbb{Z} \setminus \{[0]_p\}$$

- für die ganzen Zahlen gilt: $\mathbb{Z}^\times = \{-1, 1\}$
- $(\mathbb{Z}/8\mathbb{Z})^\times = \{[1]_8, [3]_8, [5]_8, [7]_8\}$
- $(\mathbb{Z}/15\mathbb{Z})^\times = \{[1]_{15}, [2]_{15}, [4]_{15}, [7]_{15}, [8]_{15}, [11]_{15}, [13]_{15}, [14]_{15}\}$
- allgemein wissen wir für $n \in \mathbb{N}$

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{[a]_n : \text{ggT}(a, n) = 1\}$$