WS 2003/04

Diskrete Strukturen I

Ernst W. Mayr

mayr@in.tum.de
Institut für Informatik
Technische Universität München

11-04-2004

Definition

Eine Gruppe ist eine Algebra $\langle S, \circ, 1 \rangle$ mit folgenden Eigenschaften:

- Der Operator $\circ$ ist assoziativ.
- 1 ist Einselement $\in S$.
- Für jedes $b \in S$ existiert $b^{-1} \in S$ mit

$$b \circ b^{-1} = 1 = b^{-1} \circ b$$

(Existenz des Inversen).

Definition

Eine Gruppe ist eine Algebra $\langle S, \circ, 1 \rangle$ mit folgenden Eigenschaften:

- Der Operator $\circ$ ist assoziativ.
- 1 ist Einselement $\in S$.
- Für jedes $b \in S$ existiert $b^{-1} \in S$ mit

$$b \circ b^{-1} = 1 = b^{-1} \circ b$$

(Existenz des Inversen).

Definition

Eine Gruppe ist eine Algebra $\langle S, \circ, 1 \rangle$ mit folgenden Eigenschaften:

- Der Operator $\circ$ ist assoziativ.
- 1 ist Einselement $\in S$.
- Für jedes $b \in S$ existiert $b^{-1} \in S$ mit

$$b \circ b^{-1} = 1 = b^{-1} \circ b$$

(Existenz des Inversen).

Beispiel

$\langle \mathbb{Z}_n, +_{(n)}, 0 \rangle$ ist nicht Untergruppe von $\langle \mathbb{Z}, +, 0 \rangle$, da $+_{(n)}$ nicht die Restriktion (Einschränkung) von $+$ auf $\mathbb{Z}_n$ ist. Beide sind aber Gruppen.

Beispiel

$\langle \mathbb{R}, \cdot, 1 \rangle$ oder $\langle \mathbb{Q}, \cdot, 1 \rangle$ sind keine Gruppen! Zu dem Element $0 \in \mathbb{Q}$ gibt es kein inverses Element.
$\langle \mathbb{R} \setminus \{0\}, \cdot, 1 \rangle$ bzw. $\langle \mathbb{Q} \setminus \{0\}, \cdot, 1 \rangle$ sind Gruppen.

Beispiel

$\langle \mathbb{Z}_n, +_{(n)}, 0 \rangle$ ist nicht Untergruppe von $\langle \mathbb{Z}, +, 0 \rangle$, da $+_{(n)}$ nicht die Restriktion (Einschränkung) von $+$ auf $\mathbb{Z}_n$ ist. Beide sind aber Gruppen.

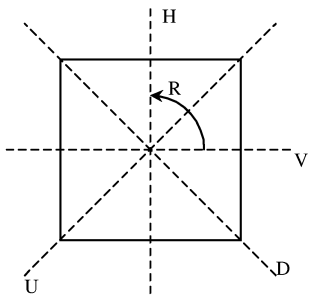
Beispiel

$\langle \mathbb{R}, \cdot, 1 \rangle$ oder $\langle \mathbb{Q}, \cdot, 1 \rangle$ sind keine Gruppen! Zu dem Element $0 \in \mathbb{Q}$ gibt es kein inverses Element.
$\langle \mathbb{R} \setminus \{0\}, \cdot, 1 \rangle$ bzw. $\langle \mathbb{Q} \setminus \{0\}, \cdot, 1 \rangle$ sind Gruppen.

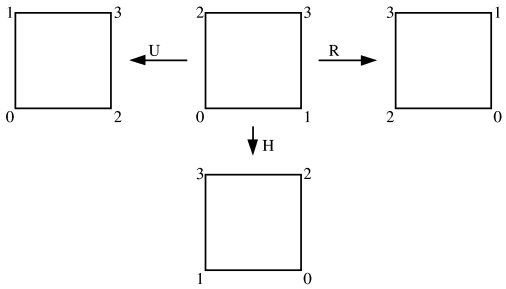
Beispiel

Automorphismengruppe des Quadrats

- ist die Komposition von Abbildungen



I identische Abbildung,
R Rotation um $90°$ gegen den Uhrzeigersinn
H horizontale Spiegelung, V vertikale Spiegelung,
D Spiegelung an der fallenden Diagonale, U Spiegelung an der steigenden.



Die Abbildungen $I, R, R^2, R^3, H, V, D, U$ bilden die Automorphismengruppe des Quadrats.

Verknüpfungstafel:

$\circ$	I	R	R^2	R^3	H	V	D	U
I	I	R	R^2	R^3	H	V	D	U
R	R	R^2	R^3	I	D	U	V	H
R^2	R^2	R^3	I	R	V	H	U	D
R^3	R^3	I	R	R^2	U	D	H	V
H	H	U	V	D	I	R^2	R^3	R
V	V	D	H	U	R^2	I	R	R^3
D	D	H	U	V	R	R^3	I	R^2
U	U	V	D	H	R^3	R	R^2	I

Satz *Sei $\langle S, \circ, 1\rangle$ eine Gruppe. Dann gilt:*

- *für alle $a \in S$:* $a = \left(a^{-1}\right)^{-1}$ *(Involutionsgesetz)*
- *für alle $a, a', b \in S$ (Kürzungsregel):*

$$a \circ b = a' \circ b \quad \Rightarrow \quad a = a'$$
$$b \circ a = b \circ a' \quad \Rightarrow \quad a = a'$$

- *für alle $a, x, b \in S$ (eindeutige Lösbarkeit linearer Gleichungen):*

$$a \circ x = b \quad \Longleftrightarrow \quad x = a^{-1} \circ b$$
$$x \circ a = b \quad \Longleftrightarrow \quad x = b \circ a^{-1}$$

- *für alle $a, b, c \in S$ (Injektivität der Operation $\circ$):*

$$a \neq b \iff a \circ c \neq b \circ c \iff c \circ a \neq c \circ b$$

- *für alle $a, b \in S$ (Surjektivität der Operation $\circ$):*

$$(\exists x)(a \circ x = b) \text{ und } (\exists y)(y \circ a = b)$$

Satz *Sei $\langle S, \circ, 1\rangle$ eine Gruppe. Dann gilt:*

- *für alle $a \in S$:* $a = \left(a^{-1}\right)^{-1}$ *(Involutionsgesetz)*
- *für alle $a, a', b \in S$ (Kürzungsregel):*

$$a \circ b = a' \circ b \quad \Rightarrow \quad a = a'$$
$$b \circ a = b \circ a' \quad \Rightarrow \quad a = a'$$

- *für alle $a, x, b \in S$ (eindeutige Lösbarkeit linearer Gleichungen):*

$$a \circ x = b \quad \Longleftrightarrow \quad x = a^{-1} \circ b$$
$$x \circ a = b \quad \Longleftrightarrow \quad x = b \circ a^{-1}$$

- *für alle $a, b, c \in S$ (Injektivität der Operation $\circ$):*

$$a \neq b \iff a \circ c \neq b \circ c \iff c \circ a \neq c \circ b$$

- *für alle $a, b \in S$ (Surjektivität der Operation $\circ$):*

$$(\exists x)(a \circ x = b) \text{ und } (\exists y)(y \circ a = b)$$

Satz *Sei $\langle S, \circ, 1\rangle$ eine Gruppe. Dann gilt:*

- *für alle $a \in S$:* $a = \left(a^{-1}\right)^{-1}$ *(Involutionsgesetz)*
- *für alle $a, a', b \in S$ (Kürzungsregel):*

$$a \circ b = a' \circ b \quad \Rightarrow \quad a = a'$$
$$b \circ a = b \circ a' \quad \Rightarrow \quad a = a'$$

- *für alle $a, x, b \in S$ (eindeutige Lösbarkeit linearer Gleichungen):*

$$a \circ x = b \quad \Longleftrightarrow \quad x = a^{-1} \circ b$$
$$x \circ a = b \quad \Longleftrightarrow \quad x = b \circ a^{-1}$$

- *für alle $a, b, c \in S$ (Injektivität der Operation $\circ$):*

$$a \neq b \iff a \circ c \neq b \circ c \iff c \circ a \neq c \circ b$$

- *für alle $a, b \in S$ (Surjektivität der Operation $\circ$):*

$$(\exists x)(a \circ x = b) \text{ und } (\exists y)(y \circ a = b)$$

Satz *Sei $\langle S, \circ, 1\rangle$ eine Gruppe. Dann gilt:*

- *für alle $a \in S$:* $a = \left(a^{-1}\right)^{-1}$ *(Involutionsgesetz)*
- *für alle $a, a', b \in S$ (Kürzungsregel):*

$$a \circ b = a' \circ b \quad \Rightarrow \quad a = a'$$
$$b \circ a = b \circ a' \quad \Rightarrow \quad a = a'$$

- *für alle $a, x, b \in S$ (eindeutige Lösbarkeit linearer Gleichungen):*

$$a \circ x = b \quad \Longleftrightarrow \quad x = a^{-1} \circ b$$
$$x \circ a = b \quad \Longleftrightarrow \quad x = b \circ a^{-1}$$

- *für alle $a, b, c \in S$ (Injektivität der Operation $\circ$):*

$$a \neq b \iff a \circ c \neq b \circ c \iff c \circ a \neq c \circ b$$

- *für alle $a, b \in S$ (Surjektivität der Operation $\circ$):*

$$(\exists x)(a \circ x = b) \text{ und } (\exists y)(y \circ a = b)$$

Satz *Sei $\langle S, \circ, 1\rangle$ eine Gruppe. Dann gilt:*

- *für alle $a \in S$:* $a = \left(a^{-1}\right)^{-1}$ *(Involutionsgesetz)*
- *für alle $a, a', b \in S$ (Kürzungsregel):*

$$a \circ b = a' \circ b \quad \Rightarrow \quad a = a'$$
$$b \circ a = b \circ a' \quad \Rightarrow \quad a = a'$$

- *für alle $a, x, b \in S$ (eindeutige Lösbarkeit linearer Gleichungen):*

$$a \circ x = b \quad \Longleftrightarrow \quad x = a^{-1} \circ b$$
$$x \circ a = b \quad \Longleftrightarrow \quad x = b \circ a^{-1}$$

- *für alle $a, b, c \in S$ (Injektivität der Operation $\circ$):*

$$a \neq b \iff a \circ c \neq b \circ c \iff c \circ a \neq c \circ b$$

- *für alle $a, b \in S$ (Surjektivität der Operation $\circ$):*

$$(\exists x)(a \circ x = b) \text{ und } (\exists y)(y \circ a = b)$$

Beweis:

Wir beweisen lediglich: $a \circ c = b \circ c \iff a = b$. Rest: Übung

$\Leftarrow$: Dass

$$a = b \Rightarrow a \circ c = b \circ c$$

gilt, ist offensichtlich.

$\Rightarrow$: Sei $a \circ c = b \circ c$.

$$\begin{aligned} b &= b \circ \left(c \circ c^{-1}\right) = (b \circ c) \circ c^{-1} \overset{\text{n.V.}}{=} (a \circ c) \circ c^{-1} \\ &= a \circ \left(c \circ c^{-1}\right) = a \end{aligned}$$

q. e. d.

Beweis:

Wir beweisen lediglich: $a \circ c = b \circ c \iff a = b$. Rest: Übung

$\Leftarrow$: Dass

$$a = b \Rightarrow a \circ c = b \circ c$$

gilt, ist offensichtlich.

$\Rightarrow$: Sei $a \circ c = b \circ c$.

$$\begin{aligned} b &= b \circ \left(c \circ c^{-1}\right) = (b \circ c) \circ c^{-1} \overset{\text{n. V.}}{=} (a \circ c) \circ c^{-1} \\ &= a \circ \left(c \circ c^{-1}\right) = a \end{aligned}$$

q. e. d.

Definition

Sei $\langle S, \circ, 1\rangle$ eine Gruppe, $a \in S$. Man definiert:

1. $a^0 := 1$
2. $a^n := a \circ a^{n-1} = a^{n-1} \circ a \quad \forall n \geq 1$
3. $a^{-n} := \left(a^{-1}\right)^n$

Satz

Sei $\langle S, \circ, 1\rangle$ eine Gruppe. Dann gilt für alle $m, n \in \mathbb{Z}$, $a \in S$:

1. $a^m \circ a^n = a^{m+n}$
2. $\left(a^n\right)^m = a^{m \cdot n}$
3. $a^m = a^n \iff a^{m-n} = 1$

Beweis.

Übung! □

Definition

Sei $\langle S, \circ, 1 \rangle$ eine Gruppe, $a \in S$. Man definiert:

1. $a^0 := 1$
2. $a^n := a \circ a^{n-1} = a^{n-1} \circ a \quad \forall n \geq 1$
3. $a^{-n} := \left(a^{-1}\right)^n$

Satz

Sei $\langle S, \circ, 1 \rangle$ eine Gruppe. Dann gilt für alle $m, n \in \mathbb{Z}$, $a \in S$:

1. $a^m \circ a^n = a^{m+n}$
2. $\left(a^n\right)^m = a^{m \cdot n}$
3. $a^m = a^n \iff a^{m-n} = 1$

Beweis.
Übung!

Definition

Sei $\langle S, \circ, 1\rangle$ eine Gruppe, $a \in S$. Man definiert:

1. $a^0 := 1$
2. $a^n := a \circ a^{n-1} = a^{n-1} \circ a \quad \forall n \geq 1$
3. $a^{-n} := \left(a^{-1}\right)^n$

Satz

Sei $\langle S, \circ, 1\rangle$ eine Gruppe. Dann gilt für alle $m, n \in \mathbb{Z}$, $a \in S$:

1. $a^m \circ a^n = a^{m+n}$
2. $\left(a^n\right)^m = a^{m \cdot n}$
3. $a^m = a^n \iff a^{m-n} = 1$

Beweis.

Übung! □

Sei $G = \langle S, \circ, 1 \rangle$ eine Gruppe mit dem Einselement 1. Sei $a \in G$ (genauer: $a \in S$) ein Gruppenelement, $a \neq 1$. Dann ist die Ordnung $\mathrm{ord}(a)$ von a das minimale $r \in \mathbb{N}$, so dass

$$a^r = 1.$$

Falls kein solches r existiert, dann ist $\mathrm{ord}(a) := \infty$. Falls gewünscht, kann man auch $\mathrm{ord}(1) = 1$ definieren.

Beispiel

$\langle \mathbb{Z}, +, 0 \rangle$: $\mathrm{ord}(1) = \infty$.

Sei $G = \langle S, \circ, 1 \rangle$ eine Gruppe mit dem Einselement 1. Sei $a \in G$ (genauer: $a \in S$) ein Gruppenelement, $a \neq 1$. Dann ist die Ordnung $\mathrm{ord}(a)$ von a das minimale $r \in \mathbb{N}$, so dass

$$a^r = 1.$$

Falls kein solches r existiert, dann ist $\mathrm{ord}(a) := \infty$. Falls gewünscht, kann man auch $\mathrm{ord}(1) = 1$ definieren.

Beispiel

$\langle \mathbb{Z}, +, 0 \rangle$: $\mathrm{ord}(1) = \infty$.

Satz *Sei G eine endliche Gruppe; dann hat auch jedes Element in G endliche Ordnung.*

Beweis. Betrachte die Abbildung

$$\mathbb{N}_0 \ni i \mapsto a^i \qquad a \in G \text{ beliebig } \neq 1$$

Also gibt es (*pigeon hole principle*) minimale k und j, $0 \leq j \leq k-1$, so dass

$$a^j = a^k.$$

Daraus folgt:

$$a^{k-j} = a^0 = 1.$$

Da k minimal gewählt wurde, folgt $j = 0$ und $\mathrm{ord}(a) = k$. □

Beispiel Betrachte $\langle \mathbb{Z}_{12}, +_{12}, 0 \rangle$:

a	0	1	2	3	4	5	6	7	8	9	10	11
$\mathrm{ord}(a)$	-	12	6	4	3	12	2	12	3	4	6	12

Satz *Sei G eine endliche Gruppe; dann hat auch jedes Element in G endliche Ordnung.*

Beweis. Betrachte die Abbildung

$$\mathbb{N}_0 \ni i \mapsto a^i \qquad a \in G \text{ beliebig } \neq 1$$

Also gibt es (*pigeon hole principle*) minimale k und j, $0 \leq j \leq k-1$, so dass

$$a^j = a^k.$$

Daraus folgt:

$$a^{k-j} = a^0 = 1.$$

Da k minimal gewählt wurde, folgt $j = 0$ und $\mathrm{ord}(a) = k$. □

Beispiel Betrachte $\langle \mathbb{Z}_{12}, +_{12}, 0 \rangle$:

a	0	1	2	3	4	5	6	7	8	9	10	11
$\mathrm{ord}(a)$	-	12	6	4	3	12	2	12	3	4	6	12

Satz *Sei G eine endliche Gruppe; dann hat auch jedes Element in G endliche Ordnung.*

Beweis. Betrachte die Abbildung

$$\mathbb{N}_0 \ni i \mapsto a^i \qquad a \in G \text{ beliebig } \neq 1$$

Also gibt es (*pigeon hole principle*) minimale k und j, $0 \leq j \leq k-1$, so dass

$$a^j = a^k.$$

Daraus folgt:

$$a^{k-j} = a^0 = 1.$$

Da k minimal gewählt wurde, folgt $j = 0$ und $\mathrm{ord}(a) = k$. □

Beispiel Betrachte $\langle \mathbb{Z}_{12}, +_{12}, 0 \rangle$:

a	0	1	2	3	4	5	6	7	8	9	10	11
$\mathrm{ord}(a)$	-	12	6	4	3	12	2	12	3	4	6	12

Satz *Sei G eine endliche Gruppe; dann hat auch jedes Element in G endliche Ordnung.*

Beweis. Betrachte die Abbildung

$$\mathbb{N}_0 \ni i \mapsto a^i \qquad a \in G \text{ beliebig } \neq 1$$

Also gibt es (*pigeon hole principle*) minimale k und j, $0 \leq j \leq k-1$, so dass

$$a^j = a^k.$$

Daraus folgt:

$$a^{k-j} = a^0 = 1.$$

Da k minimal gewählt wurde, folgt $j = 0$ und $\mathrm{ord}(a) = k$. □

Beispiel Betrachte $\langle \mathbb{Z}_{12}, +_{12}, 0 \rangle$:

a	0	1	2	3	4	5	6	7	8	9	10	11
$\mathrm{ord}(a)$	-	12	6	4	3	12	2	12	3	4	6	12

Eine Unteralgebra $\langle T, \circ, 1 \rangle$ einer Gruppe $G = \langle S, \circ, 1 \rangle$ heißt Untergruppe von G, falls $\langle T, \circ, 1 \rangle$ eine Gruppe ist.

Bemerkung: Nicht jede Unteralgebra einer Gruppe ist eine Untergruppe!

Beispiel

$\langle \mathbb{N}_0, +, 0 \rangle$ ist Unteralgebra von $\langle \mathbb{Z}, +, 0 \rangle$, aber keine Gruppe, da es im allgemeinen keine inversen Elemente gibt.

Satz

8 Eine Unteralgebra (bzgl. $\circ$) einer Gruppe ist eine Untergruppe, falls sie unter der Inversenbildung $^{-1}$ abgeschlossen ist.

Beweis.

Folgt sofort aus der Definition. □

Eine Unteralgebra $\langle T, \circ, 1\rangle$ einer Gruppe $G = \langle S, \circ, 1\rangle$ heißt Untergruppe von G, falls $\langle T, \circ, 1\rangle$ eine Gruppe ist.

Bemerkung: Nicht jede Unteralgebra einer Gruppe ist eine Untergruppe!

Beispiel

$\langle \mathbb{N}_0, +, 0\rangle$ ist Unteralgebra von $\langle \mathbb{Z}, +, 0\rangle$, aber keine Gruppe, da es im allgemeinen keine inversen Elemente gibt.

Satz

8 Eine Unteralgebra (bzgl. $\circ$) einer Gruppe ist eine Untergruppe, falls sie unter der Inversenbildung $^{-1}$ abgeschlossen ist.

Beweis.

Folgt sofort aus der Definition. □

Eine Unteralgebra $\langle T, \circ, 1\rangle$ einer Gruppe $G = \langle S, \circ, 1\rangle$ heißt Untergruppe von G, falls $\langle T, \circ, 1\rangle$ eine Gruppe ist.
Bemerkung: Nicht jede Unteralgebra einer Gruppe ist eine Untergruppe!

Beispiel

$\langle \mathbb{N}_0, +, 0\rangle$ ist Unteralgebra von $\langle \mathbb{Z}, +, 0\rangle$, aber keine Gruppe, da es im allgemeinen keine inversen Elemente gibt.

Satz

8 Eine Unteralgebra (bzgl. $\circ$) einer Gruppe ist eine Untergruppe, falls sie unter der Inversenbildung $^{-1}$ abgeschlossen ist.

Beweis.

Folgt sofort aus der Definition. □

Eine Unteralgebra $\langle T, \circ, 1\rangle$ einer Gruppe $G = \langle S, \circ, 1\rangle$ heißt Untergruppe von G, falls $\langle T, \circ, 1\rangle$ eine Gruppe ist.
Bemerkung: Nicht jede Unteralgebra einer Gruppe ist eine Untergruppe!

Beispiel

$\langle \mathbb{N}_0, +, 0\rangle$ ist Unteralgebra von $\langle \mathbb{Z}, +, 0\rangle$, aber keine Gruppe, da es im allgemeinen keine inversen Elemente gibt.

Satz

8 Eine Unteralgebra (bzgl. $\circ$) einer Gruppe ist eine Untergruppe, falls sie unter der Inversenbildung $^{-1}$ abgeschlossen ist.

Beweis.

Folgt sofort aus der Definition. □

Eine Unteralgebra $\langle T, \circ, 1\rangle$ einer Gruppe $G = \langle S, \circ, 1\rangle$ heißt Untergruppe von G, falls $\langle T, \circ, 1\rangle$ eine Gruppe ist.
Bemerkung: Nicht jede Unteralgebra einer Gruppe ist eine Untergruppe!

Beispiel

$\langle \mathbb{N}_0, +, 0\rangle$ ist Unteralgebra von $\langle \mathbb{Z}, +, 0\rangle$, aber keine Gruppe, da es im allgemeinen keine inversen Elemente gibt.

Satz

8 Eine Unteralgebra (bzgl. $\circ$) einer Gruppe ist eine Untergruppe, falls sie unter der Inversenbildung $^{-1}$ abgeschlossen ist.

Beweis.

Folgt sofort aus der Definition. □

Satz

Jede Unteralgebra (bzgl. $\circ$) einer endlichen Gruppe ist eine Untergruppe.

Beweis.

Sei $\langle T, \circ, 1\rangle$ eine Unteralgebra einer endlichen Gruppe $\langle S, \circ, 1\rangle$. Sei $b \in T$, $b \neq 1$. Dann gilt:

$$\mathrm{ord}(b) \in \mathbb{N} \setminus \{1\}$$

Sei $m := \mathrm{ord}(b)$. Dann gilt:

$$1 = b^m = b^{m-1} \circ b = b \circ b^{m-1}$$

d. h. $b^{m-1} \in T$ ist das Inverse zu b. □

Satz

Jede Unteralgebra (bzgl. $\circ$) einer endlichen Gruppe ist eine Untergruppe.

Beweis.

Sei $\langle T, \circ, 1\rangle$ eine Unteralgebra einer endlichen Gruppe $\langle S, \circ, 1\rangle$. Sei $b \in T$, $b \neq 1$. Dann gilt:

$$\mathrm{ord}(b) \in \mathbb{N} \setminus \{1\}$$

Sei $m := \mathrm{ord}(b)$. Dann gilt:

$$1 = b^m = b^{m-1} \circ b = b \circ b^{m-1}$$

d. h. $b^{m-1} \in T$ ist das Inverse zu b. □

Satz

Jede Unteralgebra (bzgl. $\circ$) einer endlichen Gruppe ist eine Untergruppe.

Beweis.

Sei $\langle T, \circ, 1\rangle$ eine Unteralgebra einer endlichen Gruppe $\langle S, \circ, 1\rangle$. Sei $b \in T$, $b \neq 1$. Dann gilt:

$$\mathrm{ord}(b) \in \mathbb{N} \setminus \{1\}$$

Sei $m := \mathrm{ord}(b)$. Dann gilt:

$$1 = b^m = b^{m-1} \circ b = b \circ b^{m-1}$$

d. h. $b^{m-1} \in T$ ist das Inverse zu b. $\square$

Satz

- *Sei* $G = \langle S, \circ, 1 \rangle$, $b \in G$ *und sei*

$$S_b := \{b^m;\ m \in \mathbb{Z}\} \subseteq S$$

die von b *erzeugte Untergruppe von* G. S_b *ist die kleinste Untergruppe, die* b *enthält.*

- *Das Bild einer Gruppe (Halbgruppe, Monoid) unter einem Homomorphismus ist wieder eine Gruppe (Halbgruppe, Monoid).*
- *Seien* $G_1 = \langle S_1, \circ, 1 \rangle$ *und* $G_2 = \langle S_2, \circ, 1 \rangle$ *Untergruppen von* $G = \langle S, \circ, 1 \rangle$. *Dann ist auch*

$$G_1 \cap G_2 = \langle S_1 \cap S_2, \circ, 1 \rangle$$

eine Untergruppe von G.

Satz

- *Sei* $G = \langle S, \circ, 1\rangle$, $b \in G$ *und sei*

$$S_b := \{b^m;\ m \in \mathbb{Z}\} \subseteq S$$

die von b *erzeugte Untergruppe von* G. S_b *ist die kleinste Untergruppe, die* b *enthält.*

- *Das Bild einer Gruppe (Halbgruppe, Monoid) unter einem Homomorphismus ist wieder eine Gruppe (Halbgruppe, Monoid).*
- *Seien* $G_1 = \langle S_1, \circ, 1\rangle$ *und* $G_2 = \langle S_2, \circ, 1\rangle$ *Untergruppen von* $G = \langle S, \circ, 1\rangle$. *Dann ist auch*

$$G_1 \cap G_2 = \langle S_1 \cap S_2, \circ, 1\rangle$$

eine Untergruppe von G.

Satz

- *Sei* $G = \langle S, \circ, 1 \rangle$, $b \in G$ *und sei*

$$S_b := \{b^m;\ m \in \mathbb{Z}\} \subseteq S$$

die von b *erzeugte Untergruppe von* G. S_b *ist die kleinste Untergruppe, die* b *enthält.*

- *Das Bild einer Gruppe (Halbgruppe, Monoid) unter einem Homomorphismus ist wieder eine Gruppe (Halbgruppe, Monoid).*
- *Seien* $G_1 = \langle S_1, \circ, 1 \rangle$ *und* $G_2 = \langle S_2, \circ, 1 \rangle$ *Untergruppen von* $G = \langle S, \circ, 1 \rangle$. *Dann ist auch*

$$G_1 \cap G_2 = \langle S_1 \cap S_2, \circ, 1 \rangle$$

eine Untergruppe von G.

Satz

- *Sei* $G = \langle S, \circ, 1 \rangle$, $b \in G$ *und sei*

$$S_b := \{b^m;\ m \in \mathbb{Z}\} \subseteq S$$

die von b *erzeugte Untergruppe von* G. S_b *ist die kleinste Untergruppe, die* b *enthält.*

- *Das Bild einer Gruppe (Halbgruppe, Monoid) unter einem Homomorphismus ist wieder eine Gruppe (Halbgruppe, Monoid).*
- *Seien* $G_1 = \langle S_1, \circ, 1 \rangle$ *und* $G_2 = \langle S_2, \circ, 1 \rangle$ *Untergruppen von* $G = \langle S, \circ, 1 \rangle$. *Dann ist auch*

$$G_1 \cap G_2 = \langle S_1 \cap S_2, \circ, 1 \rangle$$

eine Untergruppe von G.

Satz

- *Sei* $G = \langle S, \circ, 1 \rangle$, $b \in G$ *und sei*

$$S_b := \{b^m;\ m \in \mathbb{Z}\} \subseteq S$$

die von b *erzeugte Untergruppe von* G. S_b *ist die kleinste Untergruppe, die* b *enthält.*

- *Das Bild einer Gruppe (Halbgruppe, Monoid) unter einem Homomorphismus ist wieder eine Gruppe (Halbgruppe, Monoid).*
- *Seien* $G_1 = \langle S_1, \circ, 1 \rangle$ *und* $G_2 = \langle S_2, \circ, 1 \rangle$ *Untergruppen von* $G = \langle S, \circ, 1 \rangle$. *Dann ist auch*

$$G_1 \cap G_2 = \langle S_1 \cap S_2, \circ, 1 \rangle$$

eine Untergruppe von G.

Beweis.

Trivial, lediglich zur letzten Behauptung:

$$a \in S_1 \cap S_2 \;\Rightarrow\; a^{-1} \in S_1 \;\wedge\; a^{-1} \in S_2 \;\Rightarrow\; a^{-1} \in S_1 \cap S_2.$$

□

Definition

Sei $H = \langle T, \circ, 1\rangle$ eine Untergruppe von $G = \langle S, \circ, 1\rangle$ und sei $b \in G$. Dann heißt

$$T \circ b := \{c \circ b;\ c \in T\} =: H \circ b$$

eine rechte Nebenklasse von H in G und

$$b \circ T := \{b \circ c;\ c \in T\} =: b \circ H$$

eine linke Nebenklasse von H in G (*engl.: coset*).

Die Anzahl verschiedener Nebenklassen von H in G heißt der Index von H in G:

$$\mathrm{ind}(H) = \mathrm{ind}_G(H).$$

H heißt Normalteiler von G, falls

$$H \circ b = b \circ H \quad \forall b \in G$$

d. h. H ist Normalteiler genau dann, wenn $\forall b \in G : H = b \circ H \circ b^{-1}$ („konjugiert“).

Definition

Sei $H = \langle T, \circ, 1\rangle$ eine Untergruppe von $G = \langle S, \circ, 1\rangle$ und sei $b \in G$.
Dann heißt

$$T \circ b := \{c \circ b;\ c \in T\} =: H \circ b$$

eine rechte Nebenklasse von H in G und

$$b \circ T := \{b \circ c;\ c \in T\} =: b \circ H$$

eine linke Nebenklasse von H in G (*engl.: coset*).
Die Anzahl verschiedener Nebenklassen von H in G heißt der Index von H in G:

$$\mathrm{ind}(H) = \mathrm{ind}_G(H).$$

H heißt Normalteiler von G, falls

$$H \circ b = b \circ H \quad \forall b \in G$$

d. h. H ist Normalteiler genau dann, wenn $\forall b \in G : H = b \circ H \circ b^{-1}$ („konjugiert“).

Definition

Sei $H = \langle T, \circ, 1\rangle$ eine Untergruppe von $G = \langle S, \circ, 1\rangle$ und sei $b \in G$.
Dann heißt

$$T \circ b := \{c \circ b;\ c \in T\} =: H \circ b$$

eine rechte Nebenklasse von H in G und

$$b \circ T := \{b \circ c;\ c \in T\} =: b \circ H$$

eine linke Nebenklasse von H in G (*engl.: coset*).
Die Anzahl verschiedener Nebenklassen von H in G heißt der Index von H in G:

$$\mathrm{ind}(H) = \mathrm{ind}_G(H).$$

H heißt Normalteiler von G, falls

$$H \circ b = b \circ H \quad \forall b \in G$$

d. h. H ist Normalteiler genau dann, wenn $\forall b \in G : H = b \circ H \circ b^{-1}$ („konjugiert“).

Beispiel

Betrachte $\langle \mathbb{R}_{12}^*, \cdot_{12}, 1\rangle = \langle \{1,5,7,11\}, \cdot_{12}, 1\rangle$. Dann gilt: Die Untergruppe $\langle \{1,5\}, \cdot_{12}, 1\rangle$ ist Normalteiler (folgt aus Definition).

Satz

11 Sei H Untergruppe von G, $b \in G$. Dann ist die Kardinalität von $H \circ b$ gleich der Kardinalität von H (ebenso für $b \circ H$).

Beweis.

Folgt aus der Kürzungsregel: Betrachte die Abbildung

$$H \ni h \mapsto h \circ b \in H \circ b.$$

Diese Abbildung ist surjektiv und injektiv (Kürzungsregel!):

$$h_1 \circ b = h_2 \circ b \Rightarrow h_1 = h_2$$

□

Beispiel

Betrachte $\langle \mathbb{R}_{12}^*, \cdot_{12}, 1\rangle = \langle \{1,5,7,11\}, \cdot_{12}, 1\rangle$. Dann gilt: Die Untergruppe $\langle \{1,5\}, \cdot_{12}, 1\rangle$ ist Normalteiler (folgt aus Definition).

Satz

11 Sei H Untergruppe von G, $b \in G$. Dann ist die Kardinalität von $H \circ b$ gleich der Kardinalität von H (ebenso für $b \circ H$).

Beweis.

Folgt aus der Kürzungsregel: Betrachte die Abbildung

$$H \ni h \mapsto h \circ b \in H \circ b.$$

Diese Abbildung ist surjektiv und injektiv (Kürzungsregel!):

$$h_1 \circ b = h_2 \circ b \Rightarrow h_1 = h_2$$

□

Beispiel

Betrachte $\langle \mathbb{R}_{12}^*, \cdot_{12}, 1\rangle = \langle \{1,5,7,11\}, \cdot_{12}, 1\rangle$. Dann gilt: Die Untergruppe $\langle \{1,5\}, \cdot_{12}, 1\rangle$ ist Normalteiler (folgt aus Definition).

Satz

11 Sei H Untergruppe von G, $b \in G$. Dann ist die Kardinalität von $H \circ b$ gleich der Kardinalität von H (ebenso für $b \circ H$).

Beweis.

Folgt aus der Kürzungsregel: Betrachte die Abbildung

$$H \ni h \mapsto h \circ b \in H \circ b.$$

Diese Abbildung ist surjektiv und injektiv (Kürzungsregel!):

$$h_1 \circ b = h_2 \circ b \Rightarrow h_1 = h_2$$

□

Satz

12 Sei H Untergruppe von G. Dann bildet die Menge der rechten (linken) Nebenklassen von H eine Partition (Zerlegung einer Menge in disjunkte Teilmengen) von G.

Beweis.

Klar ist, dass

$$G \subseteq \bigcup_{b \in G} H \circ b$$

Seien $b, c \in G$ mit $H \circ b \cap H \circ c \neq \emptyset$, etwa $h_1 \circ b = h_2 \circ c$. Dann ist

$$H \circ c = H \circ {h_2}^{-1} \circ h_1 \circ b = H \circ b$$

□

Satz

12 Sei H Untergruppe von G. Dann bildet die Menge der rechten (linken) Nebenklassen von H eine Partition (Zerlegung einer Menge in disjunkte Teilmengen) von G.

Beweis.

Klar ist, dass

$$G \subseteq \bigcup_{b \in G} H \circ b$$

Seien $b, c \in G$ mit $H \circ b \cap H \circ c \neq \emptyset$, etwa $h_1 \circ b = h_2 \circ c$. Dann ist

$$H \circ c = H \circ {h_2}^{-1} \circ h_1 \circ b = H \circ b$$

Satz

12 Sei H Untergruppe von G. Dann bildet die Menge der rechten (linken) Nebenklassen von H eine Partition (Zerlegung einer Menge in disjunkte Teilmengen) von G.

Beweis.

Klar ist, dass

$$G \subseteq \bigcup_{b \in G} H \circ b$$

Seien $b, c \in G$ mit $H \circ b \cap H \circ c \neq \emptyset$, etwa $h_1 \circ b = h_2 \circ c$. Dann ist

$$H \circ c = H \circ {h_2}^{-1} \circ h_1 \circ b = H \circ b$$

□

Eigenschaften von Nebenklassen:

H sei Untergruppe von G, $b, c \in G$.

- Zwei Nebenklassen $H \circ b$ und $H \circ c$ sind entweder identisch oder disjunkt.
- Für alle $b \in G$ gilt $|H \circ b| = |H|$.

Eigenschaften von Nebenklassen:

H sei Untergruppe von G, $b, c \in G$.

- Zwei Nebenklassen $H \circ b$ und $H \circ c$ sind entweder identisch oder disjunkt.
- Für alle $b \in G$ gilt $|H \circ b| = |H|$.

Satz

13 (Lagrange) Sei G eine endliche Gruppe und H eine Untergruppe in G. Dann

1. *haben alle Nebenklassen von H in G gleich viele Elemente;*
2. *ist $|G| = ind_G(H) \cdot |H|$;*
3. *teilt $|H|$ die Kardinalität $|G|$ von G ganzzahlig.*

Beweis.

1. siehe oben;
2. folgt aus Satz 12;
3. folgt aus 2.

□

Satz

13 (Lagrange) Sei G eine endliche Gruppe und H eine Untergruppe in G. Dann

1. *haben alle Nebenklassen von H in G gleich viele Elemente;*
2. *ist $|G| = ind_G(H) \cdot |H|$;*
3. *teilt $|H|$ die Kardinalität $|G|$ von G ganzzahlig.*

Beweis.

1. siehe oben;
2. folgt aus Satz 12;
3. folgt aus 2.

Satz

13 (Lagrange) Sei G eine endliche Gruppe und H eine Untergruppe in G. Dann

1. *haben alle Nebenklassen von H in G gleich viele Elemente;*
2. *ist $|G| = ind_G(H) \cdot |H|$;*
3. *teilt $|H|$ die Kardinalität $|G|$ von G ganzzahlig.*

Beweis.

1. siehe oben;
2. folgt aus Satz 12;
3. folgt aus 2.

Satz

13 (Lagrange) Sei G eine endliche Gruppe und H eine Untergruppe in G. Dann

1. *haben alle Nebenklassen von H in G gleich viele Elemente;*
2. *ist $|G| = ind_G(H) \cdot |H|$;*
3. *teilt $|H|$ die Kardinalität $|G|$ von G ganzzahlig.*

Beweis.

1. siehe oben;
2. folgt aus Satz 12;
3. folgt aus 2.

Satz

13 (Lagrange) Sei G eine endliche Gruppe und H eine Untergruppe in G. Dann

1. *haben alle Nebenklassen von H in G gleich viele Elemente;*
2. *ist $|G| = ind_G(H) \cdot |H|$;*
3. *teilt $|H|$ die Kardinalität $|G|$ von G ganzzahlig.*

Beweis.

1. siehe oben;
2. folgt aus Satz 12;
3. folgt aus 2.

□