Ordnung der Gruppe G

$$\operatorname{ord}(G) := \begin{cases} |G| & \text{falls } G \text{ endlich} \\ \infty & \text{sonst} \end{cases}$$

Def: Seien G und H Gruppen.
Eine Abbildung $f: G \to H$ heißt Gruppenhomomorphismus falls gilt:

$$f(a \dot{a} b) = f(a) \dot{H} f(b)$$

Bsp.:

1) V, W $\mathbb{R}$-VR
$f: V \to W$ linear $\Rightarrow$ f Grupp. homom. zwischen $(V,+)$ und $(W,+)$

2) V: $\mathbb{R}$-VR, $\mathcal{B}$ Basis, $\dim V = n$
$M_{\mathcal{B}}^{\mathcal{B}}: \operatorname{Aut}(V) \to Gl(n, \mathbb{R})$
bijektiver Grupp. homom.
denn: $M_{\mathcal{B}}^{\mathcal{B}}(f \circ g) = M_{\mathcal{B}}^{\mathcal{B}}(f) \cdot M_{\mathcal{B}}^{\mathcal{B}}(g)$ (siehe 2.11)

3) $\operatorname{sgn}: S_n \to \{+1, -1\}$ ist Grupp. homom,
denn: $\operatorname{sgn}(b \circ \tau) = \operatorname{sgn}(b) \cdot \operatorname{sgn}(\tau)$

4) $(\mathbb{R}, +) \to (\mathbb{R} \setminus \{0\}, \cdot)$
$x \mapsto e^x$
ist Grupp. hom., denn $e^{x+y} = e^x \cdot e^y$

5) $S_n \to Gl(n, \mathbb{R})$ ist Gruppenhomom.

$$b \mapsto \left(e_{b(1)} \middle| \cdots \middle| e_{b(n)} \right)$$

Permutationsmatrix $P_b \cdot A$ vertauscht entsprechend b

$$(ij) \mapsto P_{ij}$$

$$b \mapsto \begin{pmatrix} e_{b(1)} \\ \vdots \\ e_{b(n)} \end{pmatrix}$$ ist kein Grupp. homom.

Satz 4.3 $f: G \to H$ Gruppenhomom.

Dann gilt:

a) $f(1_G) = 1_H$

b) $f(a^{-1}) = f(a)^{-1}$

c) $U \subset G$ Untergruppe $\Rightarrow f(U) \subset H$ Untergr.

Gruppennotation

additiv: $a+b$, neutrales Element 0, Inverse $-a$ (meist nur kommutativ)

multipl.: $a \cdot b = ab$, neutrales Element 1, Inverse $a^{-1} = \frac{1}{a}$

d) $V \subset H$ Untergr. $\Rightarrow f^{-1}(V) \subset G$ Untergr.

e) $g: H \to L$ Gruppenhomom.

$\Rightarrow g \circ f : G \to L$ Gruppenhomom.

f) f bijektiv

$\Rightarrow$ Umkehrabb $f^{-1} : H \to G$ ist ebenfalls Gruppenhom.

Beweis:

a) $f(1) = f(1 \cdot 1) = f(1) \cdot f(1) \quad | \cdot f(1)^{-1}$

$\Rightarrow 1 = f(1)$

b) $f(a^{-1}) \cdot f(a) = f(a^{-1} \cdot a)$

$= f(1) = 1$

c) Müssen 3 Axiome für UG nachrechnen

1) $f(U) \neq \emptyset$, da $U \neq 0$

2) $c, d \in f(U) \quad c = f(a), a \in U \quad d = f(b), b \in U$

$c \cdot d = f(a) \cdot f(b) = f(\underbrace{ab}_{\in U}) \in f(U)$

3) $c \in f(U) \quad c = f(a)$ mit $a \in U$

$\overset{b)}{\Rightarrow} c^{-1} = f(\underbrace{a^{-1}}_{\in U}) \in f(U)$

d) Übung

e) Übung f) Übung

Def: Sei $f: G \to H$ Gr. Homom.

1) f bijektiv : (Gruppen-) Isomorphismus
2) $G = H$: (Gruppen-) Endomorphismus
3) Iso + Endo : (Gruppen-) Automorphismus
4) Bild von f : $\mathrm{Im}(f) := f(G)$
5) Kern von f : $\mathrm{Ker}(f) := f^{-1}(1_H)$

Bild und Kern sind Untergruppen.
$H^{\subset}$ $^{\subset}G$

Satz 4.4

1) f surjektiv $\iff \mathrm{Im}(f) = H$
2) f injektiv $\iff \mathrm{Ker}(f) = \{1_G\}$

Beweis

1) klar
2) $f(a) = f(b) \iff f(ab^{-1}) = 1$

vgl. 2.3

Bsp:

2) $M_B^B : \mathrm{Aut}(V) \xrightarrow{\sim} GL(n, \mathbb{R})$ ist Isomorphismus

$\mathrm{Aut}(V) \cong GL(n, \mathbb{R})$

3) sgn ist surjektiv, wenn $n \geq 2$

$\mathrm{Ker}(\mathrm{sgn}) = A_n$

4) $x \longmapsto e^x$

$\mathrm{Im}(e) = \mathbb{R}_{>0}$

$(\mathbb{R}, +) \cong (\mathbb{R}_{>0}, \cdot)$

5) $P: S_n \to GL(n, \mathbb{R})$ ist injektiv, nicht surjektiv

$\sigma \in S_n \xrightarrow{P} GL(n\mathbb{R})$

$\downarrow$ sgn $\quad$ $\circlearrowleft$ $\quad$ $\downarrow$ det

$\{+1, -1\} \longrightarrow \mathbb{R}$

(B) Die zyklische Gruppe

$n \in \mathbb{Z}, n > 0 \iff n \in \mathbb{N}$

$\mathbb{Z}_n = \{0, \dots, n-1\}$

Wir definieren Verknüpfung $+_n$ auf $\mathbb{Z}_n$ durch

$$a +_n b := \begin{cases} a+b & \text{falls } a+b < n \\ a+b-n & \text{sonst} \end{cases}$$

$+_n$ assoziativ (prüfen!)

neutrales Element: 0

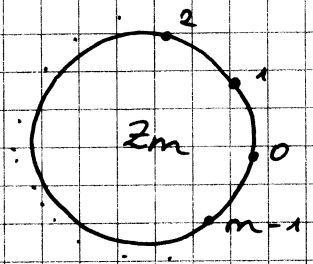
Inverse von a: $n-a$, falls $a \neq 0$

0, falls $a = 0$

$\mathbb{Z}_{24} \hat{=}$ Uhrzeit in Stunden

$\mathbb{Z}_7 \hat{=}$ Datum in Wochentage

$\mathbb{Z}_{12} \hat{=}$ Datum in Monaten



abstrakt:

$n\mathbb{Z} = \{kn \mid k \in \mathbb{Z}\}$

$\hat{=}$ alle Zahlen teilbar durch n

$a +_n \mathbb{Z} = \{a + kn \mid k \in \mathbb{Z}\}$

Idee: Teile durch n mit Rest r

$a + n\mathbb{Z} = \{$alle Zahlen mit demselben Rest wie $a\}$

$2 + 3\mathbb{Z} = \{\dots, 4, -1, 2, 5, 8 \dots\}$

$a + n\mathbb{Z}$: Restklasse von a

$\mathbb{Z} = m\mathbb{Z} \dot\cup (1+m\mathbb{Z}) \dot\cup \dots \dot\cup ((m-1)+m\mathbb{Z})$

Teilen mit Rest: Rest 0 ..... 1 ..... $m-1$

Notation: $a + m\mathbb{Z} = a' + m\mathbb{Z}$

$\Leftrightarrow a - a'$ teilbar durch m

$\Leftrightarrow : a \equiv a' \bmod m$

„a ist kongruent zu a' (modulo m)"

$\overline{a} := a + m\mathbb{Z}$

$\mathbb{Z}/m\mathbb{Z} = \{$ Restklassen von $m\mathbb{Z}\}$

$= \{ \overline{0}, \overline{1}, \dots, \overline{m-1} \}$

Addition von Restklassen:

$M + N := \{ a+b \mid a \in M, b \in N \}$

$M + N$ ist wieder Restklasse, denn $\overline{a} + \overline{b} = \overline{a+b}$

„$\subseteq$" $(a+km)+(b+\ell m) = a+b+(k+\ell)m$, $\in a+b$

„$\supseteq$" $a+b+km = (a+km)+b$, $\in \overline{a}$, $\in \overline{b}$

Satz 4.5 $(\mathbb{Z}/m\mathbb{Z}, +)$ ist abelsche Gruppe und

$\pi : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$, $a \mapsto \overline{a} = a + m\mathbb{Z}$

ist surjektiver Gruppenhomom.

Beweis:

G1) $(\overline{a}+\overline{b})+\overline{c} = \overline{a+b}+\overline{c} = \overline{a+b+c} \overset{\text{analog}}{=} \overline{a}+(\overline{b}+\overline{c})$

G2) neutrales Element:

$\overline{0} = m\mathbb{Z}$

$\overline{a} + \overline{0} = \overline{a+0} = \overline{a}$

G3) Inverse zu $\overline{a}$:

$-\overline{a} = \overline{-a}$

K4) $\bar{a} + \bar{b} = \overline{a+b} = \overline{b+a} = \bar{b} + \bar{a}$

$\Rightarrow \mathbb{Z}/m\mathbb{Z}$ Gruppe, abelsch

π surjektiv ist klar

π ist Gruppenhomom., denn $\pi(a+b) = \overline{a+b} = \bar{a} + \bar{b} = \pi(a) + \pi(b)$

Außerdem: $\ker(\pi) = m\mathbb{Z}$

$$\pi(a) = \bar{a} \overset{!}{=} \bar{0} = m\mathbb{Z}$$

$$\Leftrightarrow a \in m\mathbb{Z}$$

<u>Behauptung</u>: $(\mathbb{Z}_m, +_m) \cong (\mathbb{Z}/m\mathbb{Z}, +)$

$\mathbb{Z}/m\mathbb{Z}$ heißt zyklische Gruppe der Ordnung m.

Def: Sei $U \subset G$ Teilmenge. U heißt Untergruppe von G, falls gilt:

(U1) $U \neq \emptyset$

(U2) $a, b \in U \Rightarrow a * b \in U$

(U3) $a \in U \Rightarrow a^{-1} \in U$

Satz 4.2:

Sei U Untergruppe. Dann ist $(U, *)$ mit der eingeschränkten Verknüpfung $*: U \times U \to U$ selbst Gruppe

vgl 1.2 für VR

Beweis: Nach (U2) wird aus der Einschränkung $U \times U \to G$ tatsächlich eine Verknüpfung $U \times U \to U$.

G1) für U folgt aus G1) für G

G2) $U \neq \emptyset$. Sei $u \in U \Rightarrow$ (U3) $\Rightarrow u^{-1} \in U$

$\Rightarrow$ (U2) $u^{-1} * u = e \in U$

G3) folgt aus (U3)

Bsp: 1) $(\{+1, -1\}, \cdot) \subset (\mathbb{R} \setminus \{0\}, \cdot)$ ist UG

2) $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$ sind UG von folgt

3) $\mathbb{R}_{>0} = \{x \in \mathbb{R} \mid x > 0\}$ ist UG von $(\mathbb{R} \setminus \{0\}, \cdot)$

4) Sei $m \in \mathbb{Z}$. Dann ist $m\mathbb{Z} = \{ma \mid a \in \mathbb{Z}\}$ ist UG von $(\mathbb{Z}, +)$

11.12.2015

Ordnung einer Gruppe G

$$\operatorname{ord}(G) := \begin{cases} |G| & \text{falls endlich} \\ \infty & \text{sonst} \end{cases}$$

Def: Seien G und H Gruppen. Eine Abbildung $f: G \to H$ heißt Gruppenhomomorphismus, falls gilt:

$$f(a \underset{G}{\bullet} b) = f(a) \underset{H}{\bullet} f(b)$$

Bsp: 1) V, W $\mathbb{R}$-VR

$f: V \to W$ linear $\Rightarrow f$ Gruppenhomomorphismus zw. $(V,+)$ und $(W,+)$

2) V $\mathbb{R}$-VR, $\mathcal{B}$ Basis, $\dim V = n$

$M_{\mathcal{B}}^{\mathcal{B}}: \operatorname{Aut}(V) \longrightarrow GL(n,\mathbb{R})$

bijektiver Gruppenhomomorphismus.

denn: $M_{\mathcal{B}}^{\mathcal{B}}(f \circ g) = M_{\mathcal{B}}^{\mathcal{B}}(f) \cdot M_{\mathcal{B}}^{\mathcal{B}}(g)$

(siehe 2.11)

3) $\operatorname{sgn}: S_n \longrightarrow \{+1, -1\}$ ist Gruppenhomom.

denn: $\operatorname{sgn}(\sigma \circ \tau) = \operatorname{sgn}(\sigma) \cdot \operatorname{sgn}(\tau)$

4) $(\mathbb{R},+) \longrightarrow (\mathbb{R} \setminus \{0\}, \cdot)$

$x \longmapsto e^x$ ist Gruppenhomomorphismus

denn $e^{x+y} = e^x \cdot e^y$

5) $S_n \longrightarrow GL(n,\mathbb{R})$ ist Gruppenhom.

$$\sigma \longmapsto \left(e_{\sigma(1)} \,\middle|\, \cdots \,\middle|\, e_{\sigma(n)} \right) = P_\sigma$$

Permutationsmatrix

$P_\sigma \cdot A$ vertauscht Zeilen entsprechend σ.

$(i,j) \longmapsto P_{ij}$

$\sigma \longmapsto \begin{pmatrix} e_{\sigma(1)} \\ \vdots \\ e_{\sigma(n)} \end{pmatrix}$ ist kein Gruppenhomomorphismus

Satz 4.3 $f: G \to H$ Gruppenhomom.

Dann gilt: a) $f(1_G) = 1_H$

b) $f(a^{-1}) = f(a)^{-1}$

Gruppennotation:

additiv: $a+b$, neutrales Element 0, Inverse $-a$

multiplikativ: $a \cdot b$, " 1, " $a^{-1} = \frac{1}{a}$ (meist nur kommutativ)

c) $U \subset G$ Untergruppe $\Rightarrow f(U) \subset H$ Untergruppe

d) $V \subset H$ Untergruppe $\Rightarrow f^{-1}(V) \subset G$ Untergruppe

e) $g: H \to L$ Gruppenhomom.
$\Rightarrow g \circ f : G \to L$ Gruppenhomom.

Beweis:

a) $f(1) = f(1 \cdot 1) = f(1) \cdot f(1) \quad \| \cdot f(1)^{-1}$

$\Rightarrow 1 = f(1)$

b) $f(a^{-1}) \cdot f(a) = f(a^{-1} \cdot a)$
$= f(1) = 1$

c) Müssen 3 Axiome für Untergruppe nachrechnen

1) $f(U) \neq \emptyset$, da $U \neq \emptyset$

2) $c, d \in f(U)$. $c = f(a)$, $a \in U$
$d = f(b)$, $b \in U$

$c \cdot d = f(a) \cdot f(b) = f(a \cdot b) \in f(U)$
$\in U$

3) $c \in f(U)$ $\quad c = f(a)$ mit $a \in U$

$\overset{b)}{\Rightarrow} c^{-1} = f(a^{-1}) \in f(U)$
$\qquad\qquad\quad \in U$

d) Übung

e) "

f) "

Def: Sei $f: G \to H$ Gr. Hom.

1) f bijektiv : (Gruppen-) Isomorphismus
2) $G = H$: (Gruppen-) Endomorphismus
3) Iso- + Endo. : (Gruppen-) Automorphismus
4) Bild von f: $\operatorname{img}(f) := f(G)$
5) Kern von f: $\ker(f) := f^{-1}(1_H)$

Bild und Kern sind Untergruppen
$\quad C_H \qquad\quad C_G$

Satz 4.4

1) f surjektiv $\iff \operatorname{img}(f) = H$
2) f injektiv $\iff \ker(f) = \{1_G\}$

Beweis: 1) klar

2) $f(a) = f(b) \iff f(ab^{-1}) = 1$ $\quad$ vgl. 2.3

Bsp:

2) $M_B^B : \operatorname{Aut}(V) \xrightarrow{\sim} GL(n, \mathbb{R})$ ist Isomorphismus
$\operatorname{Aut}(V) \cong GL(n, \mathbb{R})$

3) sgn surjektiv wenn $n \geq 2$
$\ker(\operatorname{sgn}) = A_n$ (alle gerade Permutationen)

4) $e: x \longmapsto e^x$ ist injektiv

$\operatorname{img}(e) = \mathbb{R}_{>0}$

$(\mathbb{R}, +) \cong (\mathbb{R}_{>0}, \cdot)$

5) $p: S_n \longrightarrow Gl(n, \mathbb{R})$ ist injektiv, nicht surjektiv

$$\begin{array}{ccc} S_n & \xrightarrow{p} & Gl(n,\mathbb{R}) \\ \downarrow{\scriptstyle sgn} & \circlearrowright & \downarrow{\scriptstyle det} \\ \{+1,-1\} & \hookrightarrow & \mathbb{R} \end{array}$$

(B) Die zyklische Gruppe

$m \in \mathbb{Z}, m > 0 \Leftrightarrow m \in \mathbb{N}$ $\quad \mathbb{Z}_m = \{0, \dots, m-1\}$

Wir definieren die Verknüpfung $+_m$ auf $\mathbb{Z}_m$ durch

$$a +_m b := \begin{cases} a+b & \text{falls } a+b < m \\ a+b-m & \text{sonst} \end{cases}$$

$+_m$ assoziativ (prüfen)

neutrales Element: 0

Inverses von a: $m-a$ falls $a \neq 0$

0 falls $a = 0$

$\mathbb{Z}_{24} \hat{=}$ Uhrzeit in Stunden

$\mathbb{Z}_7 \hat{=}$ Daten in Wochentage

$\mathbb{Z}_{12} \hat{=}$ " in Monate

Jetzt nochmal, nur abstrakter und schöner.

$m\mathbb{Z} = \{km \mid k \in \mathbb{Z}\} \hat{=}$ alle Zahlen teilbar durch m

$a +_m \mathbb{Z} = \{a + km \mid k \in \mathbb{Z}\}$

Idee: Teile durch m mit demselben Rest wie a

$2 +_3 \mathbb{Z} = \{\dots, -4, -1, 2, 5, 8, \dots\}$

$a + m\mathbb{Z}$: Restklasse von a

$\mathbb{Z} = m\mathbb{Z} \dot\cup (1 + m\mathbb{Z}) \dot\cup \dots \dot\cup ((m-1) + m\mathbb{Z})$

Teilen mit Rest
0 1 $m-1$

Notation: $a + m\mathbb{Z} = a' + m\mathbb{Z}$
$\Leftrightarrow$ $a - a'$ teilbar durch m
$\Leftrightarrow$: $a \equiv a' \mod m$
"a ist kongruent zu a' (modulo m)"
$\bar a := a + m\mathbb{Z}$

$\mathbb{Z}/m\mathbb{Z} = \{$ Restklassen von $m\mathbb{Z}\}$
$= \{\bar 0, \bar 1, \dots, \overline{m-1}\}$

Addition von Restklassen:
$M + N := \{ \overline{a+b} \mid a \in M, b \in N\}$
$M + N$ ist wieder Restklasse, dann
$\bar a + \bar b = \overline{a+b}$
"$\subseteq$" $(a + km) + (b + \ell m) = a + b + (k-\ell)m \in \overline{a+b}$
"$\supseteq$" $a + b + km = \underbrace{(a + km)}_{\in \bar a} + \underbrace{b}_{\in \bar b}$

Satz 4.5
$(\mathbb{Z}/m\mathbb{Z}, +)$ ist abelsche Gruppe und $\pi: \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$, $a \mapsto \bar a = a + m\mathbb{Z}$ ist surjektiver Gruppenhomomorphismus.

Beweis:
G1) $(\bar a + \bar b) + \bar c = \bar a + \bar b + \bar c = \overline{a+b+c} \overset{\text{analog}}{=} \bar a + (\bar b + \bar c)$
G2) neutrales Element: $\bar 0 = m\mathbb{Z}$
$\bar a + \bar 0 = \overline{a+0} = \bar a$
G3) Inverse zu $\bar a$: $-\bar a = \overline{-a}$

K4) $\bar{a} + \bar{b} = \overline{a+b} = \overline{b+a} = \bar{b} + \bar{a}$

$\Rightarrow \mathbb{Z}/m\mathbb{Z}$ Gruppe (abelsch)

Π surjektiv ist klar.

Π ist Grp homom. (klar)

$$\Pi(a+b) = \overline{a+b} = \bar{a} + \bar{b} = \Pi(a) + \Pi(b)$$

Behauptung: $\ker(\Pi) = m\mathbb{Z}$

$$\Pi(a) = \bar{a} \overset{!}{=} \bar{0} = m\mathbb{Z} \iff a \in m\mathbb{Z}$$

Behauptung:

$$(\mathbb{Z}_m, +_m) \cong (\mathbb{Z}/m\mathbb{Z}, +)$$

$\mathbb{Z}/m\mathbb{Z}$ heißt zyklische Gruppe der Ordnung m