Zyklische Gruppen $(\mathbb{Z}, +)$
$(\mathbb{Z}_m, +_m)$

$G = \langle g \rangle$
$g^{\cdots} : \mathbb{Z} \to G$

Folgerung:
(aus dem Beweis) Die Ordnung von g ist die kleinste echt positive Zahl m mit $g^m = e$
Außerdem gilt $g^k = e \iff m$ teilt k
$(\iff k \in \ker(g^{\cdots}) = m\mathbb{Z})$

Satz: Sei $G = \langle g \rangle$ zyklisch und sei $x \in G$
Falls $|G| = \infty$, dann ist $\operatorname{ord}(x) = \begin{cases} 1 & \text{falls } x = e \\ \infty & \text{" } x \neq e \end{cases}$

Falls $|G| = m$, dann ist für $x = g^k$ $\operatorname{ord}(x) = \frac{m}{ggT(k,m)}$

[denn gesucht: die kleinste Zahl ℓ mit $x^\ell = (g^k)^\ell = g^{k \cdot \ell} = e$
$g^{k\ell} = e \iff m \mid k\ell$]

Insbesondere: In $\mathbb{Z}_m$: $\operatorname{ord}(k) = \frac{m}{ggT(k,m)}$

z.B. $m = 12$, $k = 8$: $\operatorname{ord}(k) = \frac{12}{ggT(8,12)} = \frac{12}{4} = 3$

Bem:
$\operatorname{ord}(e) = 1$
und e ist das einzige Element in einer Gruppe mit der Ordnung 1

euklidischer Algorithmus zur Berechnung des ggT

gegeben $a_1, a_2 \in \mathbb{Z}$: $ggT(a_1, a_2)$ wird induktiv berechnet

1. Fall $a_1 = a_2$: $ggT(a_1, a_2) = a_1$

2. Fall o.E $a_1 < a_2$: $ggT(a_1, a_2) = ggT(a_1, a_2 - a_1)$

Folgerung:

Satz: Gegeben $a_1, a_2 \in \mathbb{Z}$, dann existieren $z_1, z_2 \in \mathbb{Z}$ mit $ggT(a_1, a_2) = z_1 \cdot a_1 + z_2 \cdot a_2$

(z.B: $7, 11$: dann existieren $z_1, z_2 \in \mathbb{Z}$ mit $1 = z_1 \cdot 7 + z_2 \cdot 11$)

Beweis: Falls $a_1 = a_2$, dann z.B. $a_1 = ggT(a_1, a_2) = 1 \cdot a_1 + 0 \cdot a_2$

Falls $a_1 < a_2$, dann kann man per Induktion (über $|a_1| + |a_2|$) annehmen, dass es $z_1', z_2' \in \mathbb{Z}$ gibt mit $ggT(a_1, a_2 - a_1) = z_1' \cdot a_1 + z_2' \cdot (a_2 - a_1)$

$ggT(a_1, a_2)$ $\qquad$ $(\underbrace{z_1' - z_2'}_{=: z_1}) \cdot a_1 + \underbrace{z_2'}_{=: z_2} \cdot a_2$

Satz: Untergruppen und homomorphe Bilder zyklischer Gruppen sind zyklisch.

Beweis: Sei $G = \langle g \rangle$ zyklisch, sei $\varphi: G \to H$ ein Gruppenhomomorphismus.

$$\text{Bild}(\varphi) = \{\varphi(x) \mid x \in G\} = \{\varphi(g^k) \mid k \in \mathbb{Z}\} = \{\varphi(g)^k \mid k \in \mathbb{Z}\} = \langle \varphi(g) \rangle$$

($\varphi(g^k) = \varphi(g)^k$)

Sei $U \leq G$, $U \neq \{e\}$, und wähle k so, dass $g^k \in U$ und $|k|$ minimal.

Da mit $g^k \in U$ auch $(g^k)^{-1} = g^{-k} \in U$, ist o.E. $k > 0$.

Beh: $\langle g^k \rangle = U$.

Klar: „$\subseteq$"

Sei $g^n \in U$. Es gibt $z_1, z_2 \in \mathbb{Z}$ mit $ggT(k,n) = z_1 \cdot k + z_2 \cdot n$

Dann $g^{ggT(k,n)} = (g^k)^{z_1} \circ (g^n)^{z_2} \in U$. ($g^k \in U$, $g^n \in U$). Aus der Minimalität von k folgt: $ggT(k,n) = k$ ($\Uparrow$)

$g^n \in \langle g^k \rangle \quad \Leftarrow \quad k \mid n$ ∎

Folgerung:

Die Untergruppen von $\mathbb{Z}$ sind von der Form $\langle k \rangle = k\mathbb{Z}$

Die Untergruppen von $\mathbb{Z}_m$ sind von der Form $\{0, k, 2k, 3k, \ldots, (\frac{m}{ggT(k,m)} - 1) \cdot k\}$

$\langle k \rangle$

$\cong \mathbb{Z}_{\frac{m}{ggT(k,m)}}$

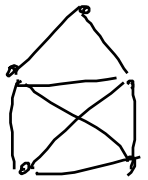
Anmerkung:

Die Erzeuger von $\mathbb{Z}$ sind 1 und -1.

Die Erzeuger von $\mathbb{Z}_m$ sind die Zahlen k mit $ggT(k,m) = 1$, also die zu m teilerfremden Zahlen

(Bsp: $m = 12$, Erzeuger sind: $1, 5, 7, 11$)

Ein Automorphismus einer Gruppe G ist ein Isomorphismus $\varphi: G \to G$.
(„Automorphismen von Strukturen beschreiben Symmetrien")



Bem:
Falls $G = \langle g \rangle$ zyklisch, H beliebige Gruppe, $h \in H$,

dann existiert ein (eindeutiger) Homomorphismus $\varphi: G \to H$, $g \mapsto h$

φ ist genau dann surjektiv, wenn $\langle h \rangle = H$.

Spezialfall $H = G$: φ ist genau dann ein Automorphismus, wenn $\varphi(g)$ ein Erzeuger von G ist.

Beweis: „$\Rightarrow$" ang. $\varphi: G \to G$ ist Automorphismus.

Dann φ surjektiv, d.h. $\text{Bild}(\varphi) = \{\varphi(x) \mid x \in G\} = \{\varphi(g)^k \mid k \in \mathbb{Z}\} \overset{!}{=} G$

also $\langle \varphi(g) \rangle = G$.

„$\Leftarrow$" ang. $\langle \varphi(g) \rangle = G$ Dann ist φ surjektiv.

Noch zu zeigen: φ ist injektiv. 1. Fall: $|G| < \infty$

Dann: eine surjektive Abbildung zwischen endlichen Mengen gleicher Größe ist auch injektiv.

2. Fall: $|G| = \infty$, dann $G \cong \mathbb{Z}$

Also entweder $g = 1$ oder $g = -1$, ebenso $\varphi(g)$

Falls $g = \varphi(g)$, dann $\varphi = id$,

Falls $g = -\varphi(g)$, dann $\varphi: x \mapsto -x$

} beide injektiv! ☐

Bsp: $\mathbb{Z}_{12}$: 4 Automorphismen:

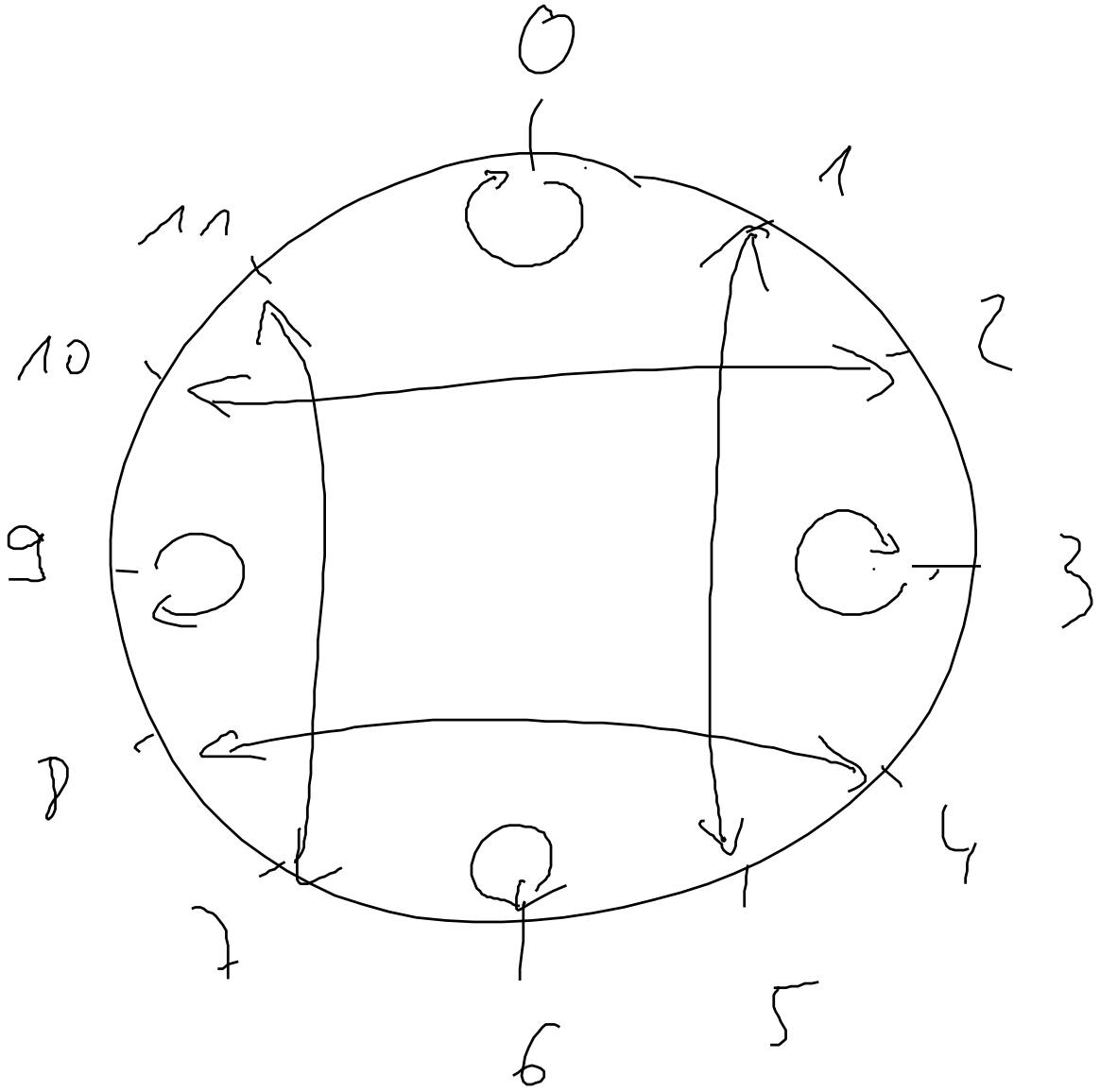
$1 \mapsto 1$ id

$1 \mapsto 11 = -1$ „Spiegelung an der senkrechten Mittelachse"

$1 \mapsto 5$

$1 \mapsto 7$

Automorphismus $1 \mapsto 5$



$4 + 7 = 11$

$8 + 11 = 7$

§ 3 Nebenklassenzerlegung und Faktorgruppen

Notation: $(G, \cdot)$ multiplikative Schreibweise

$X, Y \subseteq G$ Dann schreibt man $X \cdot Y$ oder auch XY

für $\{x \cdot y \mid x \in X, y \in Y\}$

Falls z.B. $X = \{x_0\}$, dann auch $x_0 \cdot Y = x_0 Y = \{x_0\} \cdot Y = \{x_0 \cdot y \mid y \in Y\}$

analog $Y \cdot x_0$

etc.

Sei G Gruppe, $U \subseteq G$. Definiere binäre Relation $\sim_l$ auf G durch

$$g \sim_l h \iff g^{-1} \cdot h \in U$$ l wie links

Bem: $\sim_l$ ist Äquivalenzrelation $\iff$ U ist Untergruppe

Beweis:

- reflexiv: $g \sim_l g \iff g^{-1} \cdot g = e \in U$
- symmetrisch: $g \sim_l h \iff g^{-1} \cdot h \in U$ $\quad h^{-1} \cdot g = (g^{-1} \cdot h)^{-1}$

  $h \sim_l g \iff h^{-1} \cdot g \in U$

  es folgt: $\sim_l$ symmetrisch $\iff$ U unter Inversenbildung abgeschlossen
- transitiv: $g \sim_l h \iff g^{-1} \cdot h \in U$
  $h \sim_l i \iff h^{-1} \cdot i \in U$

  } falls U unter Produkten abg. $\Rightarrow$ $g^{-1} \cdot h \cdot h^{-1} \cdot i \in U$

  $g^{-1} \cdot i$, d.h. $g \sim_l i$

Umgekehrt: falls $u_1, u_2 \in U$, dann $e \sim_e u_1$, denn $e^{-1} \cdot u_1 \in U$
$u_2^{-1} \sim_e e$ denn $(u_2^{-1})^{-1} \cdot e \in U$
u_2

Falls $\sim_e$ transitiv, dann $u_2^{-1} \sim_e u_1$, d.h. $(u_2^{-1})^{-1} \cdot u_1 = u_2 \cdot u_1 \in U$ ∎

$g \sim_e h$
$\Leftrightarrow$
$g^{-1} \cdot h \in U$

Sei $U \leq G$.

Die Äquivalenzklassen von $\sim_e$ heißen Linksnebenklassen und sind von der Form $gU = \{gu \mid u \in U\}$ ← die Äquivalenzklasse von g!

$(g \sim_e h \Leftrightarrow g^{-1} \cdot h = u \in U \Leftrightarrow h = g \cdot u$ für ein $u \in U)$

- Die Nebenklasse von e ist gerade U.
- $gU = hU \Leftrightarrow g \sim_e h \Leftrightarrow g^{-1} \cdot h \in U$

Notation: Die Menge der Linksnebenklassen wird mit G/U bezeichnet.

Analog: Definiere $g \sim_r h :\Leftrightarrow h \cdot g^{-1} \in U$

$\sim_e$ ist Äquivalenzrelation $\Leftrightarrow$ U Untergruppe

Die Äquivalenzklassen heißen Rechtsnebenklassen und sind von der Form

$$Ug = \{ug \mid u \in G\}$$

- Die Nebenklasse von e ist wieder U.
- $U \cdot g = U \cdot h \Leftrightarrow g \sim_r h \Leftrightarrow hg^{-1} \in U$

$U \cdot g = U \cdot h$
$\Leftrightarrow U \cdot gh^{-1} = U$
$\Leftrightarrow gh^{-1} \in U \Leftrightarrow hg^{-1} \in U$
$\Leftrightarrow U = Uh \cdot g^{-1}$

Notation: Die Menge der Rechtsnebenklassen wird mit $U \backslash G$ bezeichnet.

Satz: Sei $U \leq G$.

- Je zwei Nebenklassen sind „gleich groß", d.h. es gibt eine Bijektion dazwischen
- Es gibt ebenso viele Rechts- wie Linksnebenklassen, d.h. eine Bijektion $G/U \to U\backslash G$

Bew: a) $U \to Ug$, $u \mapsto u \cdot g$ ist Bijektion, denn $Ug \to U$, $x \mapsto x \cdot g^{-1}$ ist Umkehrabbildung
($x \in Ug$, $x \cdot g^{-1} \in U$)

$U \to gU$, $u \mapsto gu$ ist Bijektion, denn $x \mapsto g^{-1} \cdot x$ ist Umkehrabbildung.

Zwischen zwei beliebigen Nebenklassen: setze diese Bijektionen zusammen!

b) $G/U \to U\backslash G$, $gU \mapsto Ug^{-1}$ ist Bijektion:

„$\Rightarrow$" Wohldefiniertheit & Injektivität „$\Leftarrow$"

$gU = hU \Leftrightarrow g^{-1}h \in U \Leftrightarrow Ug^{-1} = Uh^{-1}$

$U = g^{-1}h \cdot U \Leftrightarrow Ug^{-1}h = U$

Surjektivität: Uh ist Bild von $h^{-1} \in U$ ∎

c) Folgt

Satz von Lagrange: Wenn G endlich ist und $U \leq G$,

dann ist $|U|$ ein Teiler von $|G|$, genauer $|G| = |U| \cdot |G:U|$

Index von U in G $= |G/U| = |U\backslash G|$

Insbesondere: Die Ordnung eines Gruppenelementes teilt die Gruppenordnung.