$k^* = k^\times = k \setminus \{0\}$

Folgerung aus dem Satz von Lagrange

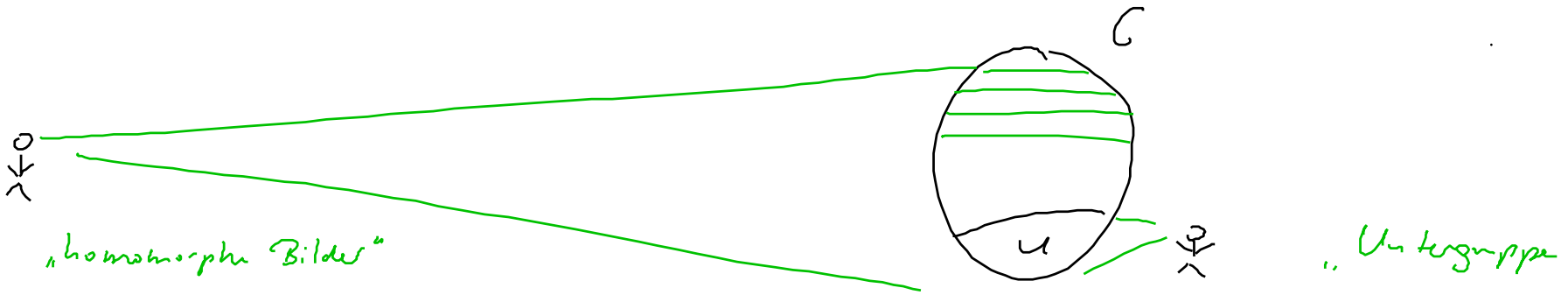
G Gruppe, $|G| = p$ Primzahl, dann ist G zyklisch, $\cong \mathbb{Z}_p$

Bew: Sei $g \in G \setminus \{e\}$, $\underbrace{\mathrm{ord}(g) > 1}$, $\mathrm{ord}(g)$ teilt p

$\Rightarrow \mathrm{ord}(g) = p$, d.h. $\langle g \rangle = G$ ☐

Bem: Jedes Element von G, $\neq e$, erzeugt die Gruppe.
Es gibt keine anderen Untergruppen außer $\{e\}$ und G.

Bsp: Falls $|G| = 6$, dann ist $G \cong \mathbb{Z}_6$ oder $G \cong S_3$
kommutativ nicht kommutativ



Gesucht sind besondere Äquivalenzrelationen $\sim$ („Kongruenzrelationen" für Gruppen),
so dass auf den Äquivalenzklassen eine Gruppenstruktur existiert, die von G kommt.
Schreibe $[g]$ für die Äquivalenzklasse von G:
Man möchte, dass $[g] \cdot [h] := [g \cdot h]$ eine sinnvolle Definition ist und eine Gruppe ergibt $G/\sim$

($\pi : G \longrightarrow G/\sim$, $g \mapsto [g]$ ist dann Homomorphismus)

Menge der Äquivalenzklassen bzgl. $\sim$

Angenommen $\sim$ ist eine Kongruenzrelation

Dann ist $[e]$ eine Untergruppe: $e \in [e]$:

$$[e]\cdot[g] = [e\cdot g] = [g]$$
$$[g]\cdot[e] = [g\cdot e] = [g]$$

$g \in [e]$, $x \in G$:

$$[g^{-1}]\cdot[x] = [g^{-1}\cdot x] = [(x^{-1}\cdot g)^{-1}] = [x^{-1}\cdot g]^{-1}$$

$$[x] = [x^{-1}]^{-1} = \left([x^{-1}]\cdot[g]\right)^{-1}$$

analog $[x]\cdot[g^{-1}] = [x]$

$g\cdot h \in [e]$, $x \in G$:

$$[g\cdot h]\cdot[x] = [g\cdot h\cdot x] = [g]\cdot[hx] = [h\cdot x] = [h]\cdot[x] = [x]$$

analog $[x]\cdot[g\cdot h] = [x]$

Wie sieht $[x]$ aus?

Falls $g \in [e]$, so $[xg] = [x]\cdot[g] = [x]$, also $xg \sim x$ bzw. $x\cdot[e] \subseteq [x]$

Analog: $[gx] = [g]\cdot[x] = [x]$, also $gx \sim x$ bzw $[e]\cdot x \subseteq [x]$

Umgekehrt: Falls $y \in [x]$, schreibe $y = x\cdot z$ $\quad z = x^{-1}y$

Dann $x \sim x\cdot z$, also$^{(*)}$ $e = x^{-1}\cdot x \sim x^{-1}\cdot x\cdot z = z$

Somit $[x] \subseteq x\cdot[e]$

Analog: $[x] \subseteq [e]\cdot x$

Also: $[x] = x\cdot[e] = [e]\cdot x$ ist Rechts- und Linksnebenklasse von der Untergruppe $[e]$.

(*) Falls $\sim$ Kongruenzrelation, so $g_1 \sim g_2 \Rightarrow g_1 h \sim g_2 h$

$$\Updownarrow \qquad [g_1 h] \qquad [g_2 h]$$
$$[g_1] = [g_2] \Rightarrow [g_1]\cdot[h] = [g_2]\cdot[h]$$

Def: Untergruppe U heißt <u>normale Untergruppe von</u> G, falls die Rechtsnebenklassenzerlegung mit der Linksnebenklassenzerlegung übereinstimmt, d.h. falls $\sim_R = \sim_L$

d.h. falls $g \cdot U = U \cdot g$ für alle $g \in G$.

Schreibweise: $U \trianglelefteq G$ für „U ist normale Untergruppe von G"

Satz: Falls $U \trianglelefteq G$, dann ist die zugehörige Äquivalenzrelation $\sim = \sim_R = \sim_L$ eine Kongruenzrelation, d.h. G/U wird zu einer Gruppe durch $gU \cdot hU = (gh) \cdot U$ und $\pi : G \to G/U$, $g \mapsto gU$ ist Homomorphismus.

G/U heißt Faktorgruppe oder Quotientengruppe

Bew: Wohldefiniertheit: $gU = g'U$, $hU = h'U$ $\overset{?}{\Rightarrow}$ $ghU = g'h'U$

$g = g' \cdot u_1$, $h = h' \cdot u_2$

Bew: $Uh' = h'U$ nach Voraussetzung, d.h. $u_3 \cdot h = h \cdot u_3$ für ein geeign. $u_3 \in U$

$g \cdot h = g' \cdot u_1 \cdot h' \cdot u_2 = g' \cdot h' \cdot \underbrace{u_3 \cdot u_2}_{\in U} \Rightarrow ghU = g'h'U$

?

G/U ist Gruppe: $gU \cdot eU = g \cdot e \cdot U = gU$, $eU \cdot gU = eg \cdot U = gU$

($eU = U$)

$gU \cdot g^{-1}U = g \cdot g^{-1} U = e \cdot U = U$

$g^{-1}U \cdot gU = g^{-1} g U = eU$

Assoziativität löst sich auf die Assoziativität von G zurückführen:

$(gU \cdot hU) \cdot iU = ghU \cdot iU = (gh) \cdot i \cdot U$

$gU \cdot (hU \cdot iU) = gU \cdot hiU = g(hi)U$ □

Bemerkung: Alle Kongruenzrelationen auf G sind von dieser Form!

Wenn $\varphi: G \to H$ ein Gruppenhomomorphismus ist, dann gehört zu φ eine Äquivalenzrelation $\sim_\varphi$, nämlich $g_1 \sim_\varphi g_2 \iff \varphi(g_1) = \varphi(g_2)$.

Dies ist eine Kongruenzrelation mit $[e] = \ker(\varphi)$.

D.L. Kerne von Homomorphismen sind normale Untergruppen

(und jede normale Untergruppe U ist Kern eines Homomorphismus, nämlich $\pi: G \to G/U$)

(Dies kann man auch direkt nachrechnen:
Falls $U = \ker(\varphi)$, dann ist $gU = Ug$ (Übung))

Beispiele: (Normale Untergruppen)

- $\{e\}$, G sind normale Untergruppen von G
  $g\cdot\{e\} = \{e\}\cdot g = \{g\}$ $\quad$ $g\cdot G = G\cdot g = G$
- Wenn G kommutativ ist, dann ist jede Untergruppe normal
  (denn $gU = \{gu \mid u \in U\} = \{ug \mid u \in U\} = Ug$)
- Insbesondere: $(\mathbb{Z}, +)$, $m\mathbb{Z} \trianglelefteq \mathbb{Z}$

  zugehörige Äquivalenzrelation $x \sim_m y \iff x - y \in m\mathbb{Z}$
  $\iff m \mid x-y$
  $\iff$ x und y lassen gleichen Rest bei der Division durch m

$\rightsquigarrow$ Faktorgruppe $\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}_m$

„additive Schreibweise der Nebenklassen $g + U$"

$\{0 + m\mathbb{Z}, 1 + m\mathbb{Z}, \dots, (m-1) + m\mathbb{Z}\}$

$\overline{0}$ $\overline{1}$ ... $\overline{m-1}$ falls m im Kontext festgelegt ist

Isom. auf $\mathbb{Z}_m$: 0 1 ... $m-1$

- Falls $U \leq G$, $\underset{\text{Index}}{G:U} = 2$, dann ist $U \trianglelefteq G$

  Denn $g \cdot U = U \cdot g = U$ für $g \in U$ ist $g \cdot U = U \cdot g = G \setminus U$ für $g \notin U$

  (f. $g \in U$ ist)

Bsp: $A_n \trianglelefteq S_n$ bzw. $Alt(M) \trianglelefteq Sym(M)$

Signum $sgn : S_n \longrightarrow (\{+1, -1\}, \cdot)$

$Ker(sgn) = A_n$ „alternierende Gruppe"

„geraden Permutationen"

- $det : GL(n,K) \longrightarrow K^\times$

  Determinante $Ker(det) = SL(n,K) \trianglelefteq GL(n,K)$

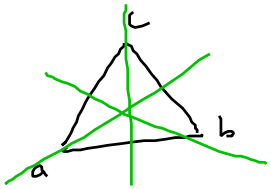
  $= (n \times n)$-Matrizen mit Determinante 1

GL = „general linear group"

allgemeine lineare Gruppe

SL = special linear group

Bsp: S_3 Symmetriegruppe vom (gleichseitigen) Dreieck



3 Spiegelungen $\hat{=}$ 3 Transpositionen (bc) (ac) (ab)

(bc): $a \mapsto a$, $b \mapsto c$, $c \mapsto b$

2 echte Drehungen $\hat{=}$ 2 3-Zyklen (abc) (acb)

(abc): $a \mapsto b$, $b \mapsto c$, $c \mapsto a$

$(acb) = (abc)^2 = (abc)^{-1}$

Untergruppen

$\{id\} \trianglelefteq S_3$

$\langle (ab) \rangle = \{id, (ab)\}$, $\langle (ac) \rangle$, $\langle (bc) \rangle$ $\not\trianglelefteq S_3$

Identität

Drehgruppe $A_3 = \{id, (abc), (acb)\} \trianglelefteq S_3$

$S_3 \trianglelefteq S_3$