Satz (2. Isomorphiesatz): Sei G eine Gruppe. $M \trianglelefteq N \trianglelefteq G$.

Dann sind folgende Mengen isomorph:

$$(G/M)/(N/M) \cong G/N.$$

Das ganze kann man auch als Kürzungsregel bezeichnen.

<u>Beweis</u>: Vorab: $M \trianglelefteq G$ offensichtlich ist $M < G$, da $M < N < G$.

Da M als Untergruppe von N mit der gegebenen Verknüpfung eine Gruppe ist, ist $M \leq G$. $(U \leq V \leq G \Rightarrow U \leq G)$.

Formal: $\forall g \in G \ \forall m \in M: gmg^{-1} \in M$

letztres liegt schonmal in N, da $N \trianglelefteq G$ und $M < N$

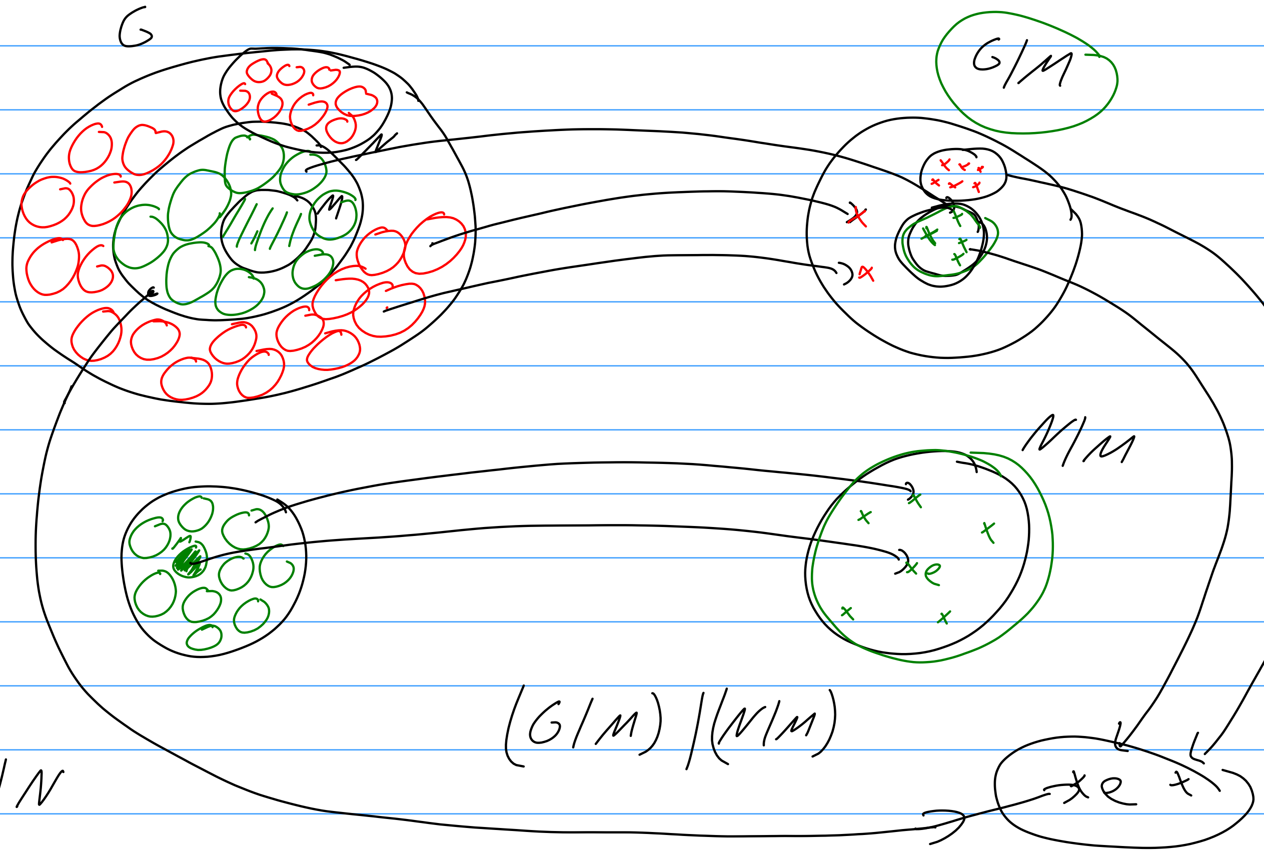
Da M außerdem Normalteiler von N gilt

$$\forall n \in N \ \forall m \in M: \boxed{\tilde{n}\, m\, n^{-1} \in M}$$

$\Rightarrow$ $gmg^{-1} \in N$ (bereits gesehen)

$$g\underbrace{m g^{-1}\, \tilde{m}\, g m^{-1}}_{\in M} g^{-1} \in M$$

Durch geeignete Wahl von m und $\tilde{m}$ bekommt man beliebige Elemente aus M, durch $m g^{-1} \tilde{m} g m^{-1}$



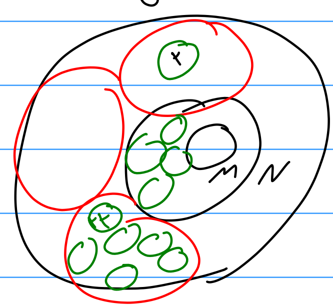
Wir benutzen für den Beweis den Homomorphiesatz.

⇒ Wir definieren dazu eine surjektive Abbildung

$\alpha : G/M \longrightarrow \underbrace{G/N}_{\operatorname{Im}\alpha}$ mit $\ker \alpha = N/M$.

$\Rightarrow \quad \bar{\alpha} : (G/M)/_{\underset{(N/M)}{\ker\alpha}} \longrightarrow \operatorname{Im}\alpha = G/N$

α :



α bildet meine „M-Nebenklassen" ab auf die „N-Nebenklasse" in der sie liegt.

$$\alpha : gM \longrightarrow gN$$

Dieses α ist wohldefiniert: Es gilt falls $g, h \in gM$

$\Rightarrow \alpha(g) = \alpha(h)$, da $g \underset{M}{\sim} h$ also $gh^{-1} \in M \subset N$

$g \underset{N}{\sim} h$

α ist Homomorphismus: $\alpha(\bar{g}\bar{h}) = \alpha(\overline{gh}) = \alpha(gh \cdot M)$

$= ghN = gN \; hN = \alpha(\bar{g})\,\alpha(\bar{h})$

$= \alpha(gM)\,\alpha(hM)$ ✓

„Surjektivität, d.h. $\operatorname{Im}\alpha = G/N$".

Sei $\tilde{g} \in G/N$ beliebig $(\tilde{g} = g \cdot N, \quad \bar{g} = gM)$

d.h. $\tilde{g} = gN$ $\quad \boxed{g \in G}$

betrachte $\bar{g} := gM$

(Wähle beliebiges Element aus G/N, in dieser Nebenklasse einen beliebigen Repräsentanten g)

$\bar{g} = gM \xrightarrow{\alpha} gN$. ✓

„$\ker\alpha = N/M$": $\alpha(gM) = \tilde{e}$

$gN = \tilde{e} \iff g \in N \quad (g \sim e, \; g e^{-1} \in N$

$g \in N \Rightarrow gM \in N/M$ ✓ $\square$

Zyklische Gruppen

Erinnerung: Eine Gruppe G heißt zyklisch $:\Leftrightarrow G = \langle g \rangle$

Satz: Sei $G = \langle g \rangle$ eine beliebige zyklische Gruppe.

a) $G \cong \mathbb{Z}$ falls $|G| = \infty$

b) $G \cong \mathbb{Z}_n := \mathbb{Z}/n\mathbb{Z}$ falls $|G| = n < \infty$

Beweis: In beiden Fällen betrachten wir die Abbildung

$\alpha : \mathbb{Z} \longrightarrow G$

$\alpha(z) = g^z$ (hierbei ist $\langle g \rangle = G$)

a) Die Abbildung α ist ein Gruppenhomomorphismus.

(siehe Potenzgesetze: $g^x \circ g^y = g^{x+y}$)

„Injektivität": $\alpha(x) = \alpha(y) \Rightarrow \alpha(x-y) = e$

Falls ein $z = x-y$ existiert mit $z \neq 0$ und

$\alpha(z) = g^z = e$ so hat $\langle g \rangle$ höchstens

z Elemente $\lightning$ $|G| = \infty$

$\Rightarrow x = y$ $\square$

„Surjektivität" folgt aus der Definition von $G = \langle g \rangle$

$\underline{G}$ ist also die $\underline{\text{kleinste}}$ Gruppe, die g enthält.

Da $\operatorname{Im} \alpha$ g enthält folgt $G \subset \operatorname{Im}\alpha \subset G$

$\alpha : ? \to G$

$\Rightarrow G = \operatorname{Im} \alpha$.

$\Rightarrow$ a)

b): $\alpha : \mathbb{Z} \to G$ $\alpha(z) = g^z$

Wir werden den Homomorphiesatz benutzen, dazu

benötigen wir $\operatorname{Ker} \alpha$ und $\operatorname{Im} \alpha$.

Wie oben ist α ein Homomorphismus.

$\alpha(z) = g^z$ $\qquad \langle g \rangle = G$

Sei k die kleinste natürliche Zahl, so dass $g^k = e$

$\longrightarrow$ $G = \{e, g, g^2, \dots g^{k-1}\}$ sind alle unterschiedlich.

$(g^x = g^y \Rightarrow g^{x-y} = e)$

$G = \langle g \rangle$ hat mindestens k Elemente.

$\{e, g, g^2 \dots g^{k-1}\}$ ist aber bereits eine Gruppe die G enthält.

$\Rightarrow$ G hat höchstens k Elemente $\Rightarrow |G| = n = k$.

$\ker(\alpha) = n\mathbb{Z}$ offensichtlich ist $g^z = e \ \forall z \in n\mathbb{Z}$

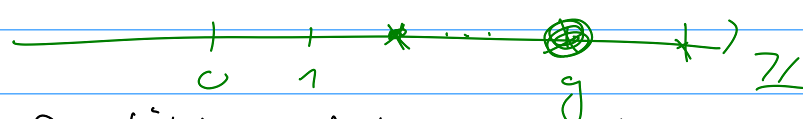
$g^z \neq e \ \forall z \notin n\mathbb{Z}$

Das Bild unserer Abbildung ist G.

$\Rightarrow$ (Homomorphiesatz): $\mathbb{Z}/n\mathbb{Z} \cong G$ $\square$

<u>Bemerkung</u>: Die Konsequenz dieses Satzes ist, dass wir Eigenschaften beliebiger zyklischer Gruppen auf $\mathbb{Z}$ bzw $\mathbb{Z}_n$ zurückführen können.

Beispiele dazu: a) Wir hatten bereits gesehen, dass Untergruppen von $\mathbb{Z}$ (und $\mathbb{Z}_n$) immer zyklisch sind (Vorlesung 9.11. ganz am Ende).



Dies führt zu folgendem Satz:

<u>Satz</u>: Alle Untergruppen von zyklischen Gruppen sind selbst zyklisch.

b) Sei $G = \langle g \rangle$. Betrachte g^m für beliebiges m.
(ein beliebiges Element von G)

Es gilt, falls $|G| < \infty$, dass $(g^m)^k$ wieder das neutrale wird, insbesondere ist $\langle g^m \rangle$ zyklisch.

$\langle g^m \rangle$ ist nicht notwendigerweise gleich G !

<u>Satz</u>: $|\langle g^m \rangle| = \frac{kgV(n,m)}{|m|}$

Diesen Satz kann man sich an Hand von $\mathbb{Z}_n$ klar machen. $\{0, 1, \dots, n-1\}$

Falls $m \notin \{0, 1 \dots n-1\}$ wähle $m = \bar{m} = m - k \cdot n$

$$g^{\bar{m}} = g^m$$

Für welches $k \in \mathbb{N}$ gilt nun, dass $(g^{\bar{m}})^k$ zum ersten Mal e wird? Das ist das kleinste k, so dass $\bar{m}k$ ein Vielfaches von n ist.

$\bar{m}k$ ist also das kleinste gemeinsame Vielfache von $\bar{m}$ und n. $\Rightarrow k = \frac{kgV(n, \bar{m})}{\bar{m}}$