Die primen Restklassengruppen

Nach § 1 bildet die Teilmenge $(\mathbb{Z}/n\mathbb{Z})^\times$ der invertierbaren Elemente im Monoid $(\mathbb{Z}/n\mathbb{Z}, \cdot)$ eine Gruppe. Man bezeichnet sie als prime Restklassengruppe.

Proposition (4.14)

Sei $n \in \mathbb{N}$ und $a \in \mathbb{Z}$. Das Element $a + n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z}$ ist genau dann in $(\mathbb{Z}/n\mathbb{Z})^\times$ enthalten, wenn $\mathrm{ggT}(a, n) = 1$ ist.

Daraus folgt, dass die Gruppe $(\mathbb{Z}/n\mathbb{Z})^\times$ aus $\varphi(n)$ Elementen besteht.

Struktur der Automorphismengruppen zyklischer Gruppen

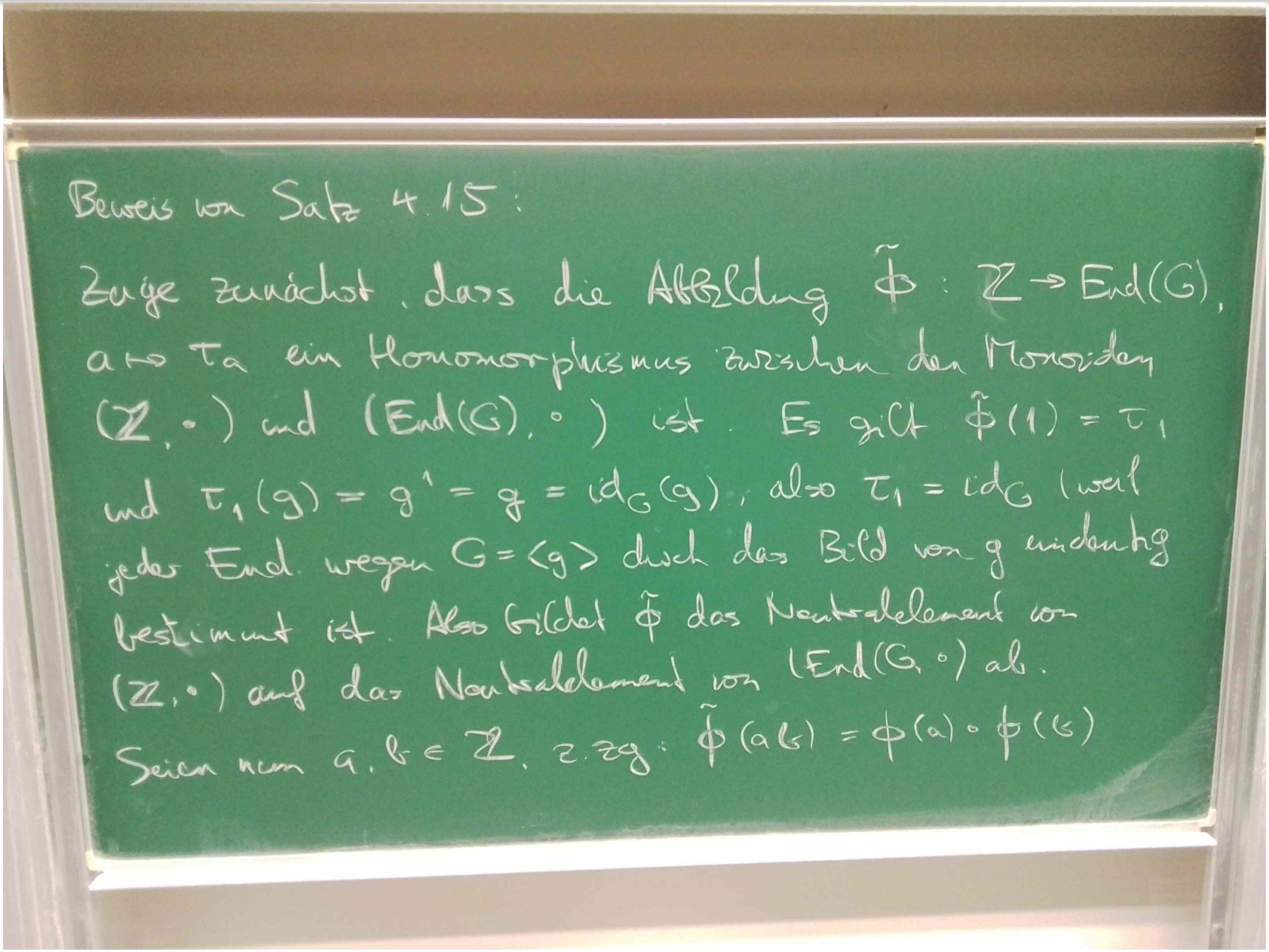
Sei nun G eine zyklische Gruppe der endlichen Ordnung n und $g \in G$ mit $G = \langle g \rangle$. Für jedes $a \in \mathbb{Z}$ ist $\operatorname{ord}(g^a) = |\langle g^a \rangle|$ nach dem Satz von Lagrange ein Teiler von n. Nach Satz 4.12 existiert somit ein eindeutig bestimmter Endomorphismus

$$\tau_a : G \to G \qquad \text{mit} \qquad \tau_a(g) = g^a.$$

Satz (4.15)

Die Abbildung $\phi : (\mathbb{Z}/n\mathbb{Z})^\times \to \operatorname{Aut}(G)$, $a + n\mathbb{Z} \mapsto \tau_a$ ist ein Isomorphismus von Gruppen.

Im Fall, dass $G = \langle g \rangle$ unendlich ist, gilt $\operatorname{Aut}(G) \cong (\mathbb{Z}/2\mathbb{Z}, +)$.



Hinweis: Am Ende der letzten Zeile muss es $\tilde{\phi}(a) \circ \tilde{\phi}(b)$ heißen.
Die Tilde $\sim$ fehlt auch in den ersten drei Zeilen der folgenden Seite.

Es gilt $(\phi(a)\circ\phi(b))(g) = (\tau_a\circ\tau_b)(g) = \tau_a(g^b) =$
$\tau_a(g)^b = (g^a)^b = g^{ab} = \tau_{ab}(g) = \phi(ab)(g) \Rightarrow$
$\phi(a)\circ\phi(b) = \phi(ab)$ $(\Rightarrow \tilde{\phi}$ ist Monoidhom.$)$

Definiere nun $\phi : (\mathbb{Z}/n\mathbb{Z})^\times \to \mathrm{End}(G)$ durch $\phi(a+n\mathbb{Z}) =$
$\tau_a = \tilde{\phi}(a)$ für alle $a \in \{0, 1, \ldots, n-1\}$ mit $\mathrm{ggT}(a,n) = 1$

Beh. $\phi(a+n\mathbb{Z}) = \tilde{\phi}(a)$ für alle $a \in \mathbb{Z}$ mit $\mathrm{ggT}(a,n) = 1$

Sei $a \in \mathbb{Z}$ mit $\mathrm{ggT}(a,n) = 1$. Division mit Rest $\Rightarrow$
$\exists q, r \in \mathbb{Z}$ mit $0 \leq r < n$ und $a = qn + r$. Es gilt dann
$a \equiv r \bmod n$, also $a + n\mathbb{Z} = r + n\mathbb{Z}$, und wegen $\mathrm{ggT}(a,n) = 1$
gilt auch $\mathrm{ggT}(r,n) = 1$ (denn: $d \in \mathbb{N}$, $d \mid r$, $d \mid n \Rightarrow$
$d \mid (qn+r) \Rightarrow d \mid a$, $d \mid n \overset{\mathrm{ggT}(a,n)=1}{\Rightarrow} d = 1$)

Weiter gilt $\tau_a(g) = g^a = g^{qn+r} = (g^q)^n \cdot g^r$

$= e_G \, g^r = g^r = \tau_r(g) \Rightarrow \tau_a = \tau_r$

insgesamt: $\phi(a+n\mathbb{Z}) = \phi(r+n\mathbb{Z})$

$= \tau_r = \tau_a = \Phi(a)$ ($\Rightarrow$ Beh.)

Σ nach Def. von ϕ

Beh.: $\phi(a+n\mathbb{Z}) \in \mathrm{Aut}(G)$ $\forall a \in \mathbb{Z}$ mit

$\mathrm{ggT}(a,n) = 1$ ($\Rightarrow \phi$ ist Abb. $(\mathbb{Z}/n\mathbb{Z})^* \to \mathrm{Aut}(G)$)

Sei $a \in \mathbb{Z}$ mit $\mathrm{ggT}(a,n) = 1 \Rightarrow a+n\mathbb{Z}$ ist

invertierbar in $\mathbb{Z}/n\mathbb{Z}$, d.h. $\exists b \in \mathbb{Z}$ mit

$\mathrm{ggT}(b,n) = 1$ und $(a+n\mathbb{Z})(b+n\mathbb{Z}) = 1+n\mathbb{Z}$

$\Rightarrow \phi(a+n\mathbb{Z}) \cdot \phi(b+n\mathbb{Z}) = \tilde{\phi}(a) \circ \tilde{\phi}(b) =$

$\tilde{\phi}(ab) = \phi(ab+n\mathbb{Z}) = \phi((a+n\mathbb{Z})(b+n\mathbb{Z}))$

$= \phi(1+n\mathbb{Z}) = \tilde{\phi}(1) = id_G \rightarrow \phi(a+n\mathbb{Z})$ ist (*)

in $End(G)$ ein invertierbares Element, also ein Element von $Aut(G)$

Die Rechnung (*) zeigt, dass die Abbildung $\phi : (\mathbb{Z}/n\mathbb{Z})^\times \rightarrow Aut(G)$ verträglich mit den Verknüpfungen ist. $\Rightarrow \phi$ ist Gruppenhom.

noch z.zg: (1) ϕ ist injektiv (2) ϕ ist surj.

zu (1) genügt z.zg: $ker(\phi) \subseteq \{1+n\mathbb{Z}\}$

Sei $a+n\mathbb{Z} \in ker(\phi)$ mit $a \in \mathbb{Z}$, $ggT(a,n) = 1$

$\Rightarrow \phi(a+n\mathbb{Z}) = id_G \Rightarrow \tau_a = id \Rightarrow$

$\tau_a(g) = id_G(g) = g \Rightarrow g^a = g \Rightarrow g^{a-1} = e$

$ord(g) = n$

$\Rightarrow n \mid (a-1) \Rightarrow a \equiv 1 \ (n) \Rightarrow a+n\mathbb{Z} = 1+n\mathbb{Z}$

Satz 3.3

zu (2) Sei $\tau \in Aut(G)$ z.zg.: $\exists a \in \mathbb{Z}$ mit

$ggT(a,n) = 1$ und $\phi(a+n\mathbb{Z}) = \tau$

$\tau(g) \in \langle g \rangle$ (wegen $G = \langle g \rangle$) $\Rightarrow \exists a \in \mathbb{Z}$ mit

$\tau(g) = g^a$, d.h. $\tau = \tau_a$ Ang. $d = ggT(a,n)$

ist größer als 1. $\Rightarrow ord(g^a) = \frac{n}{d} < n$.

$\tau(g^{n/d}) = \tau(g)^{n/d} = (\tau^a)^{n/d} = e$, d.h. $g^{n/d}$ wäre

nichttriv. Elt. im Kern von τ $\lightning$ da $\tau \in Aut(G)$

also: $ggT(a,n) = 1 \Rightarrow a+n\mathbb{Z} \in (\mathbb{Z}/n\mathbb{Z})^*$, $\phi(a+n\mathbb{Z}) = \tau$ $\square$

Definition der Normalteiler

Definition (4.16)

Sei G eine Gruppe. Eine Untergruppe U von G wird Normalteiler von G genannt, wenn $gU = Ug$ für alle $g \in G$ gilt.

Notation: Sei G eine Gruppe.

- $U \leq G$ bedeutet: U ist Untergruppe von G
- $N \trianglelefteq G$ bedeutet: N ist Normalteiler von G

Kriterien für Normalteiler

Proposition (4.17)

Sei G eine Gruppe und U eine Untergruppe. Dann sind die folgenden Bedingungen äquivalent:

(i) U ist Normalteiler von G.

(ii) Es gilt $gUg^{-1} \subseteq U$ für alle $g \in G$, wobei $gUg^{-1} = \{gug^{-1} \mid u \in U\}$ ist.

(iii) Es gilt $gUg^{-1} = U$ für alle $g \in G$.

Beweis von Prop. 4.17:

„(i) $\Rightarrow$ (ii)" Sei $g \in G$. Vor. $\Rightarrow gU = Ug$

Sei nun $u \in U$ beliebig. z.zg: $gug^{-1} \in U$

$gu \in gU \overset{\text{s.o.}}{\Longrightarrow} gu \in Ug \Rightarrow \exists v \in U$ mit $gu = vg$

$\rightarrow gug^{-1} = v \overset{v \in U}{\Longrightarrow} gug^{-1} \in U$

„(ii) $\Rightarrow$ (iii)" Vor.: $\forall g \in G: gUg^{-1} \subseteq U$

Sei $g \in G$. z.zg: $gUg^{-1} = U$

„$\subseteq$" gilt auf Grund der Vor. „$\supseteq$" Sei $u \in U$.

Vor. $\Rightarrow g^{-1}U(g^{-1})^{-1} \subseteq U \Rightarrow g^{-1}Ug \subseteq U$

„$\subseteq$" gilt auf Grund der Vor. „$\supseteq$" Sei $u \in U$.

$\Rightarrow g^{-1}ug \in U \Rightarrow g(g^{-1}ug)g^{-1} \in gUg^{-1}$

$\Rightarrow eug^{-1} \in gUg^{-1} \Rightarrow u \in gUg^{-1}$

„(iii) $\Rightarrow$ (i)" Vor. $\Rightarrow \forall g \in G: gUg^{-1} = U$

Sei $g \in U$, z.Zg: $gU = Ug$ „$\subseteq$" Sei $a \in gU$.

$\Rightarrow \exists u \in U: a = gu$ Vor. $\Rightarrow gug^{-1} \in U \rightarrow$

$a = gu = (gug^{-1})g \in Ug$

„$\supseteq$" Sei $a \in Ug$. $\Rightarrow \exists u \in U$ mit $a = ug$

Vor. $\Rightarrow U = g^{-1}U(g^{-1})^{-1} = g^{-1}Ug$ also: $g^{-1}ug \in g^{-1}Ug$

$\Rightarrow g^{-1}ug \in U \Rightarrow a = ug = g(g^{-1}ug) \in gU$. □

Eigenschaften von Normalteilern

Satz (4.18)

(i) Ist G eine Gruppe und U eine Untergruppe mit $(G : U) = 2$, dann gilt $U \trianglelefteq G$.

(ii) Ist G eine Gruppe und $(N_i)_{i \in I}$ eine Familie von Normalteilern, dann ist auch $N = \bigcap_{i \in I} N_i$ ein Normalteiler von G.

(iii) Sei nun $\phi : G \to H$ ein Gruppenhomomorphismus. Ist N ein Normalteiler von H, dann ist $\phi^{-1}(N)$ ein Normalteiler von G.

(iv) Ist ϕ surjektiv und N Normalteiler von G, dann ist $\phi(N)$ Normalteiler von H.

Beweis von Satz 4.18

zu (i) $(G:U) > 1 \rightarrow U \subsetneq G \Rightarrow \exists g \in G \setminus U$

Wegen $(G:U) = 2$ sind U und gU die einzigen beiden Linksnebenklassen (wobei $gU \neq U$ wg. $g \notin U$) $\rightarrow$

$G = U \cup gU$, und die Zerlegung ist disjunkt

$\Rightarrow gU = G \setminus U$ Mit derselben Argumentation zeigt man auch $Ug = G \setminus U$ also: $gU = G \setminus U = Ug$

für alle $g \in G \setminus U$. Für alle $g \in U$ gilt $gU = U = Ug$

damit gezeigt: $gU = Ug \; \forall g \in G \Rightarrow U \trianglelefteq G$

damit gezeigt: $gU = Ug \ \forall g \in G \Rightarrow U \trianglelefteq G$

zu iii) geg.: Familie $(N_i)_{i \in I}$ von Normalteilern von G

Sei $N = \bigcap_{i \in I} N_i$, z.Zg.: $N \trianglelefteq G$

$\forall i \in I: N_i \trianglelefteq G \overset{\text{Prop. 4.17}}{\Rightarrow} gN_ig^{-1} \subseteq N_i \ \forall g \in G$ (*)

Sei nun $g \in G$ und $n \in N$. Nach Prop. 4.17 genügt es zu zeigen, dass $gng^{-1} \in N$ (denn daraus folgt dann $gNg^{-1} \subseteq N \ \forall g \in G$)

Für jedes $i \in I$ gilt: $g \in G, n \in N_i \overset{(*)}{\Rightarrow} gng^{-1} \in N_i$

also: $\forall i \in I: gng^{-1} \in N_i \Rightarrow gng^{-1} \in \bigcap_{i \in I} N_i \Rightarrow gng^{-1} \in N$

zu iii) geg.: Gruppenhom. $\phi: G \to H$, $N \trianglelefteq H$, z.Zg.: $\phi^{-1}(H) \trianglelefteq G$

bereits gezeigt: $\phi^{-1}(N) \leq G$ Sei nun $g \in G$ und $n \in \phi^{-1}(N)$

genügt z.Zg (nach Prop. 4.17): $gng^{-1} \in \phi^{-1}(N)$ gleichbedeutend:

$\phi(gng^{-1}) \in N$ $N \trianglelefteq H, \phi(g) \in H, \phi(n) \in N$ wg. $n \in \phi^{-1}(N)$

$\Rightarrow \phi(g)\,\phi(n)\,\phi(g^{-1}) \in N$

also: $\phi(gng^{-1}) = \phi(g)\phi(n)\phi(g^{-1}) =$

$\phi(g)\,\phi(n)\,\phi(g)^{-1} \in N$

zu (iv) geg: surjektiver Gruppenhom $\phi: G \to H$

und $N \trianglelefteq G$ zzg: $\phi(N) \trianglelefteq H$

bereits bekannt: $\phi(N) \leq H$

Sei nun $h \in H$ und $n \in \phi(N)$. zzg: $hnh^{-1} \in \phi(N)$

ϕ surjektiv $\Rightarrow \exists g \in G$ mit $\phi(g) = h$

$n \in \phi(N) \Rightarrow \exists n_1 \in N$ mit $\phi(n_1) = n$

$N \trianglelefteq G$, $g \in G$, $n_1 \in N \Rightarrow gn_1g^{-1} \in N$

$\Rightarrow hnh^{-1} = \phi(g)\phi(n_1)\phi(g)^{-1} = \phi(g)\phi(n_1)\phi(g^{-1})$

$= \phi(g n_1 g^{-1})$ also $g n_1 g^{-1} \in N \Rightarrow$

$h n h^{-1} = \phi(g n_1 g^{-1}) \in \phi(N)$ □

Bem: Ist $\phi: G \to H$ ein nicht surjektiver Hom., dann kann es Normalteiler in G geben, deren Bilder keine Normalteiler von H sind.

Bsp: $G = \langle (12) \rangle \leq S_3$, $H = S_3$

$\phi: G \to H, \sigma \mapsto \sigma$

Betrachte nun $N = G$. Dann gilt $N \trianglelefteq G$, denn jede Gruppe ist (offensichtlich) Normalteiler von sich selbst ($gG = G = Gg \ \forall g \in G$)

Aber $\phi(N) = \langle (12) \rangle$ ist kein Normalteiler von $H = S_3$ (hatten in §2 die Links- und Rechtsneben-

klassen ausgerechnet und gesehen. dass nicht
jede Linksnebenklasse eine Rechtsnebenklasse ist).

Definition der Komplexprodukte

Definition (4.19)

Sei G eine Gruppe, und seien $A, B \subseteq G$ beliebige Teilmengen. Dann nennt man die Teilmenge $AB = \{ab \mid a \in A, b \in B\}$ das Komplexprodukt von A und B.

Bei Gruppen in additiver Schreibweise verwendet man für das Komplexprodukt die Schreibweise $A + B$ statt AB.

Komplexprodukte und Normalteiler

Lemma (4.20)

Sei G eine Gruppe, und seien U und N Untergruppen von G.

(i) Gilt $U \cap N = \{e\}$, dann hat jedes Element $g \in UN$ eine eindeutige Darstellung der Form $g = un$, mit $u \in U$ und $n \in N$.

(ii) Gilt $U \subseteq N$, dann folgt $UN = N$.

(iii) Gilt $UN = NU$, dann ist UN eine Untergruppe von G. Ersteres ist insbesondere dann gegeben, wenn N ein Normalteiler von G ist.

(iv) Sind N und U Normalteiler von G, dann folgt $UN \trianglelefteq G$.

Beweis von Lemma 4.20:

zu (i) Vor.: $U \cap N = \{e\}$ Zzg.: Jedes $g \in NU$ hat eine eindeutige Darstellung $g = nu$ mit $n \in N$, $u \in U$

Die Existenz folgt aus der Def. von NU. Zur Eindeutigkeit:

Sei $g \in G$, ang $g = nu = n_1 u_1$ für $n, n_1 \in N$, $u, u_1 \in U$

$nu = n_1 u_1 \Rightarrow n = n_1 u_1 u^{-1} \Rightarrow n_1^{-1} n = u_1 u^{-1} \in N \cap U$

Vor. $\Rightarrow n_1^{-1} n = e$, $u_1 u^{-1} = e \Rightarrow n = n_1$, $u_1 = u$

$nu = n_1 u_1 \Rightarrow n = n_1 u_1 u^{-1} \Rightarrow n_1^{-1} n = u_1 u^{-1} \in N \cap U$

Vor.

$\Rightarrow n_1^{-1} n = e \quad u_1 u^{-1} = e \Rightarrow n = n_1 \quad u_1 = u$

Bem. Sind $U, V \leq G$, dann ist UV im Allgemeinen keine Untergruppe von G.

Betrachte $G = S_3$, $U = \langle (12) \rangle = \{id, (12)\}$, $V = \langle (13) \rangle = \{id, (13)\}$

Es gilt $UV = \{id \circ id, id \circ (13), (12) \circ id, (12) \circ (13)\}$

$= \{id, (12), (13), (132)\}$. $|UV| = 4$, kein Teiler von $|S_3| = 6$

$\xrightarrow{\text{Lagrange}}$ UV kann keine Untergr. von S_3 sein!