

1.1.7 Def (i) Seien G, G' Gruppen. Eine Abbildg $\varphi: G \rightarrow G'$ heißt Gruppen-Homomorphismus, wenn $\varphi(ab) = \varphi(a)\varphi(b)$ für alle $a, b \in G$.

φ Isomorphismus $\Leftrightarrow \varphi$ bijektiver Homomorph.

G, G' sind isomorph $\Leftrightarrow \exists \varphi: G \rightarrow G'$ Isomorphismus

Schreibweise: $G \cong G'$

Notation: $\text{Hom}(G, G') = \{\varphi: G \rightarrow G' : \varphi \text{ Homomorph.}\}$

(ii) $\varphi \in \text{Hom}(G, G)$ heißt Endomorphismus.

Notation: $\text{End}(G) := \text{Hom}(G, G)$

Ein Isomorphismus $\varphi: G \rightarrow G$ heißt Automorphismus

Notation: $\text{Aut}(G) = \{\varphi \in \text{End}(G) : \varphi \text{ Isomorphismus}\}$.

1.1.8 Proposition Sei $\varphi \in \text{Hom}(G, G')$. Dann

(i) $\varphi(e) = e'$, $\varphi(a^{-1}) = \varphi(a)^{-1} \quad \forall a \in G$

(ii) $H < G \rightsquigarrow \varphi(H) < G'$; insb. $\text{Im } \varphi := \varphi(G) < G'$

(iii) $H' < G' \rightsquigarrow \varphi^{-1}(H') < G$; insb. $\text{Ker } \varphi := \varphi^{-1}(e') < G$

(iv) φ Isom. $\Rightarrow \varphi^{-1}$ Isom.

Beweis (i) $\varphi(e) = \varphi(e \cdot e) = \varphi(e)\varphi(e) \xrightarrow{\cdot \varphi(e)^{-1}} e' = \varphi(e)$

$\varphi(a)\varphi(a^{-1}) = \varphi(aa^{-1}) = \varphi(e) = e' \Rightarrow \varphi(a^{-1}) = \varphi(a)^{-1}$

(ii), (iii), (iv) leicht □

1.1.9 Bsp. (i) $a \in G \rightsquigarrow \varphi: \mathbb{Z} \rightarrow G, \varphi(m) = a^m$
ist Homom. (denn: $a^{m+n} = a^m \cdot a^n, m, n \in \mathbb{Z}$)

(ii) Sei D_3 die Dieder-Gruppe (Bsp. 1.1.7(vi)). Sei $\varphi: D_3 \rightarrow S_3, a \mapsto$ zugehörige Perm. der Ecken
 $\Rightarrow \varphi$ Isomorphismus.

(10)

(iii) Sei G eine Gruppe, $a \in G$. Sei $z_a: G \rightarrow G$, $z_a(b) = ab$ die zugeh. Linkstranslation (bijektiv, kein Homom.)

Dann ist $\varphi: G \rightarrow S(G)$, $\varphi(a) = z_a$ injektiver Homom.

Denn: $z_{ab}(c) = (ab)c = a(bc) = (z_a \circ z_b)(c)$,

$$z_a = z_b \Rightarrow a = z_a(e) = z_b(e) = b.$$

Also ist G isomorph zu einer UG von $S(G)$.

Sei $\text{ord}(G) := |G| := \text{Anzahl der Elem. von } G$,
 $\text{ord}(G) \in \mathbb{N} \cup \{\infty\}$.

Falls G endlich, $n = \text{ord}(G)$, so $S(G) \cong S_n$

1.1.10 Satz (Cayley) Jede n -elem. Gruppe G ist isomorph zu einer Untergruppe von S_n .

(iv) G Gruppe, $a \in G \mapsto \text{int}_a: G \rightarrow G$, $\text{int}_a(b) = aba^{-1}$ ist ein Automorphismus, genannt innerer Autom. von G . Es gilt $\text{int}_{a^{-1}} = (\text{int}_a)^{-1}$.

1.1.11 Bemerkung $\varphi \in \text{Hom}(G, G')$, $\psi \in \text{Hom}(G', G'') \Rightarrow \psi \circ \varphi \in \text{Hom}(G, G'')$. Es folgt, dass $(\text{Aut}(G), \circ)$ ist eine UG von $(S(G), \circ)$.

Die Abbildg $\text{int}: G \rightarrow \text{Aut}(G)$, $a \mapsto \text{int}_a$ ist ein Homom.

1.1.12 Lemma $\varphi \in \text{Hom}(G, G')$ injektiv $\Leftrightarrow \text{Ker } \varphi = \{e\}$.

Beweis " $\Rightarrow$ " klar; " $\Leftarrow$ " $\varphi(a) = \varphi(b) \Rightarrow e' = \varphi(a)^{-1} \varphi(b) = \varphi(a^{-1}b)$ also $a^{-1}b \in \text{Ker } \varphi \Rightarrow a^{-1}b = e \Rightarrow a = b$. $\square$

1.1.13 Def. $H < G$ heißt Normalteiler, wenn $\forall a \in G$ $\text{int}_a(H) = H$, d.h. $aHa^{-1} = \{aha^{-1} : h \in H\} = H$.

Schreibweise: $H \triangleleft G$.

1.1.14 Lemma $\varphi \in \text{Hom}(G, G') \leadsto \text{Ker } \varphi \triangleleft G$

Beweis: $b \in \text{Ker } \varphi, a \in G \Rightarrow$

$$\varphi(ab\bar{a}^{-1}) = \varphi(a)\varphi(b)\varphi(\bar{a}^{-1}) = \varphi(a)e'\varphi(\bar{a}^{-1}) = \varphi(a\bar{a}^{-1}) = e' \\ \Rightarrow ab\bar{a}^{-1} \in \text{Ker } \varphi. \quad \square$$

§2 Nebenklassen und Quotientengruppen

1.2.1 Lemma Sei $H < G$. Die Relation $a \sim b : \Leftrightarrow$

$$\bar{a}^{-1}b \in H \text{ und die Relation } a \approx b : \Leftrightarrow ab^{-1} \in H$$

sind Äquivalenzrelationen. Die Äquivalenzklasse von $a \in G$ bzgl. $\sim$ ist $aH = \{ah : h \in H\}$ und heißt Linksnebenklasse. Die Äquivalenzklasse von $a \in G$ bzgl. $\approx$ ist $Ha = \{ha : h \in H\}$ und heißt Rechtsnebenklasse.

Beweis: $a \sim a$ denn $\bar{a}^{-1}a = e \in H$

$$a \sim b \Leftrightarrow \bar{a}^{-1}b \in H \Leftrightarrow \underbrace{(\bar{a}^{-1}b)^{-1}}_{= \bar{b}^{-1}a} \in H$$

$$a \sim b \& b \sim c \Rightarrow \bar{a}^{-1}b, \bar{b}^{-1}c \in H \Rightarrow \underbrace{\bar{a}^{-1}b \cdot \bar{b}^{-1}c}_{= \bar{a}^{-1}c} \in H \\ \Rightarrow a \sim c.$$

Außerdem $a \sim b \Leftrightarrow \bar{a}^{-1}b \in H \Leftrightarrow b \in aH. \quad \square$

Es folgt insb. dass je zwei verschiedene Linksnebenkl. disjunkt sind und G disjunkte Vereinigung von Linksnebenkl. ist.

1.2.2 Satz (i) Alle Linksnebenklassen sind gleichmächtig.

(ii) Die Abbildung $G/\sim \xrightarrow{\varphi} G/\approx, aH \rightarrow Ha^{-1}$
ist bijektiv. $[a]_{\sim} \mapsto [a^{-1}]_{\approx}$

(12)

Beweis (i) Definiere $\psi: H \rightarrow aH$, $\psi(h) = ah$
 ψ ist bijektiv: $ah = ah' \Rightarrow a^{-1}(ah) = a^{-1}(ah') \Rightarrow h = h'$
 $\Rightarrow \psi$ injektiv; ψ ist offensichtlich surjektiv.

(ii) ψ wohldefiniert: $a \sim b \Leftrightarrow a^{-1}b \in H \Leftrightarrow a^{-1}(b^{-1})^{-1} \in H$
 $\Leftrightarrow a^{-1} \approx b^{-1}$

ψ injektiv: $\psi(aH) = \psi(bH) \Leftrightarrow a^{-1} \approx b^{-1} \Leftrightarrow a \sim b$
 $\Leftrightarrow aH = bH$

ψ surjektiv: klar $\psi(a^{-1}H) = H(a^{-1})^{-1} = Ha$. $\square$

1.2.3 Def. Sei $H < G$. Wir bezeichnen $G/H := G/\sim$
 und $G//H := G/\approx$. Nach 1.2.2(ii) sind G/H , $G//H$
 gleichmächtig. Setze

$(G:H) := \text{Anzahl der Linksnebenklassen (d.h. } |G/H|)$
 $= \text{Rechtsnebenklassen (d.h. } |G//H|)$
 $\in \mathbb{N} \cup \{\infty\}$

der Index von H in G .

1.2.4. Satz (Lagrange) Sei G endliche Gruppe, $H < G$
 Dann gilt $\text{ord } G = (G:H) \cdot \text{ord } H$, insb. $\text{ord } H \mid \text{ord } G$.

Beweis Folgt aus 1.2.2(i). $\square$

Ist also $\text{ord } G$ eine Primzahl, so sind $\{e\}$ und G ihre
 einzigen Untergruppen.

1.2.5 Bem. $N \triangleleft G \Leftrightarrow \forall a: aN = Na \Leftrightarrow \sim = \approx$

1.2.6 Lemma Ist $N \triangleleft G$ so ist die Verknüpfung auf
 G/H , $aH \cdot bH := abH$ wohldefiniert und
 damit wird G/H eine Gruppe, genannt Quotienten-
gruppe von G modulo N .