1.5 Homomorphismen

1.5.1 Definition: Ein *(Gruppen)-Homomorphismus* $\varphi\colon G \to H$ ist eine Abbildung mit

$$\forall g, g' \in G\colon \varphi(gg') = \varphi(g)\varphi(g').$$

Dann heissen weiter

$$\begin{array}{rcll} \mathrm{Kern}(\varphi) & := & \{g \in G \mid \varphi(g) = 1_H\} & \text{der } \textit{Kern von } \varphi, \\ \mathrm{Bild}(\varphi) & := & \{\varphi(g) \mid g \in G\} & \text{das } \textit{Bild von } \varphi. \end{array}$$

1.5.2 Proposition: Für jeden Homomorphismus $\varphi\colon G \to H$ gilt

(a) $\varphi(1_G) = 1_H$.

(b) $\forall g \in G\colon\ \varphi(g^{-1}) = \varphi(g)^{-1}$.

(c) $\forall g \in G\colon\ \forall n \in \mathbb{Z}\colon\ \varphi(g^n) = \varphi(g)^n$.

(d) $\mathrm{Kern}(\varphi)$ ist eine Untergruppe von G.

(e) $\mathrm{Bild}(\varphi)$ ist eine Untergruppe von H.

(f) φ ist injektiv genau dann, wenn $\mathrm{Kern}(\varphi) = 1$ ist.

(g) φ ist surjektiv genau dann, wenn $\mathrm{Bild}(\varphi) = H$ ist.

Bew.: $\varphi(1_G) = \varphi(1_G \cdot 1_G) = \varphi(1_G)\cdot\varphi(1_G)$

$\varphi(1_G)\cdot 1_H \Rightarrow 1_H = \varphi(1_G)$. qed.

Bew.: $1_H = \varphi(1_G) = \varphi(g\bar{g}^{-1}) = \varphi(g)\cdot\varphi(\bar{g}^{-1})$

$\Rightarrow \varphi(g^{-1}) = \varphi(g)^{-1}$. qed.

Bew.: $1_H = \varphi(1_G) \in \mathrm{Bild}(\varphi)$.

$\forall \varphi(g), \varphi(g') \in \mathrm{Bild}(\varphi)\colon \varphi(g)\varphi(g') = \varphi(gg') \in \mathrm{Bild}(\varphi)$

$\forall \varphi(g) \in \mathrm{Bild}(\varphi)\colon \varphi(g)^{-1} = \varphi(\bar{g}^{-1}) \in \mathrm{Bild}(\varphi)$.

qed

Bew.: φ inj $\Rightarrow 1_G \in \mathrm{Kern}(\varphi) = \{1_G\}$ ✓

$\mathrm{Kern}(\varphi) = \{1_G\} \Rightarrow \forall g, g' \in G\colon \varphi(g) = \varphi(g') \Rightarrow$

$\Rightarrow 1_H = \varphi(g)^{-1}\varphi(g') = \varphi(\bar{g}^{-1})\varphi(g') = \varphi(\bar{g}^{-1}g') \Rightarrow 1_G = \bar{g}^{-1}g' \Rightarrow g = g' \Rightarrow \varphi$ inj. qed

1.5.3 Beispiel: Die konstante Abbildung $G \to H$, $g \mapsto 1_H$ ist ein Homomorphismus.

denn $\varphi(gg') = 1_H = 1_H \cdot 1_H = \varphi(g) \cdot \varphi(g')$.

1.5.4 Beispiel: Die *identische Abbildung* $\mathrm{id}_G \colon G \to G$, $g \mapsto g$ ist ein Homomorphismus.

$\mathrm{id}(gg') = \mathrm{id}(g) \cdot \mathrm{id}(g')$

1.5.5 Beispiel: Für jedes $g \in G$ ist die Abbildung $\mathbb{Z} \to G$, $n \mapsto g^n$ ein Homomorphismus.

denn $g^{n+m} = g^n \cdot g^m$ für alle $n, m \in \mathbb{Z}$.

1.5.6 Beispiel: Ist G abelsch, so ist für jedes $n \in \mathbb{Z}$ die Abbildung $G \to G$, $g \mapsto g^n$ ein Homomorphismus. Ist umgekehrt $g \mapsto g^{-1}$ ein Homomorphismus, so ist G abelsch.

$\forall g, g' \in G: \ (gg')^n = g^n \cdot g'^n$.

$\forall g, h \in G: \ (gh)^{-1} = g^{-1}h^{-1} \quad | \cdot h \cdot g$

$\iff (gh)^{-1} hg = 1_G \quad | gh \cdot$

$\iff hg = gh$.

Gut.

1.5.7 Beispiel: Die Inklusion einer Untergruppe $H \hookrightarrow G$ ist ein Homomorphismus.

1.5.8 Proposition: Die Komposition zweier Homomorphismen ist ein Homomorphismus.

$G \xrightarrow{\varphi} H \xrightarrow{\psi} K$

$\forall g, g' \in G: \ \psi\varphi(gg') = \psi(\varphi(g)\varphi(g')) = \psi\varphi(g) \cdot \psi\varphi(g')$

1.6 Isomorphismen

$\varphi \circ \varphi^{-1} = id_H$
$\varphi^{-1} \circ \varphi = id_G$

1.6.1 Definition: Ein Homomorphismus $\varphi\colon G \to H$, für den ein beidseitiger *inverser Homomorphismus* $\varphi^{-1} : H \to G$ existiert, heisst ein *Isomorphismus*, und wir schreiben dann $\varphi\colon G \xrightarrow{\sim} H$. Existiert ein Isomorphismus $G \xrightarrow{\sim} H$, so heissen G und H *isomorph* und wir schreiben $G \cong H$.

1.6.2 Proposition: Ein Homomorphismus ist ein Isomorphismus genau dann, wenn er bijektiv ist.

Bew.: $\varphi^{-1} \circ \varphi = id_G \Rightarrow \varphi$ injektiv. $\left.\begin{array}{l}\\\\\end{array}\right\} \Rightarrow \varphi$ bijektiv.
$\varphi \circ \varphi^{-1} = id_H \Rightarrow \varphi$ surjektiv.

φ bijektiv $\Rightarrow$ Zu jedem $h \in H$ gibt es genau ein $g \in G$ mit $\varphi(g) = h$. Definiere $\varphi^{-1}\colon H \to G$ durch $\varphi^{-1}(h) = g$.
φ^{-1} ist Homo.
$\forall h, h' \in H : \varphi^{-1}(hh') = \varphi^{-1}(\varphi(\varphi^{-1}(h)) \cdot \varphi(\varphi^{-1}(h')))$
$= \varphi^{-1}(\varphi(\varphi^{-1}(h) \cdot \varphi^{-1}(h')))$
$= \varphi^{-1}(h) \cdot \varphi^{-1}(h')$. qed

1.6.3 Proposition: Die Komposition zweier Isomorphismen ist ein Isomorphismus. Das Inverse eines Isomorphismus ist eindeutig bestimmt und selbst ein Isomorphismus. Isomorphie von Gruppen ist eine Äquivalenzrelation.

$G \cong H \wedge H \cong K \Rightarrow G \cong K$
$G \cong H \Rightarrow H \cong G$
$G \cong G$.

1.6.4 Bemerkung: Alle inneren Eigenschaften und Invarianten einer Gruppe sind invariant unter Isomorphismen, zum Beispiel die Kommutativität, die Ordnung, der Exponent.

Zahlentheorie: $\mathbb{Z}_p \neq \mathbb{Z}/p\mathbb{Z}$

1.6.5 Proposition: Jede zyklische Gruppe ist isomorph zur additiven Gruppe von $\mathbb{Z}$ oder $\mathbb{Z}/n\mathbb{Z}$ für eine eindeutige natürliche Zahl $n > 0$.

Sei $G = \langle g \rangle$. $\operatorname{ord}(g) = \infty \Rightarrow \mathbb{Z} \to G$ injektiv & surjektiv $\Rightarrow$ Isomorphismus.

" $\{g^i \mid i \in \mathbb{Z}\}$ $\operatorname{ord}(g) = n \Rightarrow \mathbb{Z}/n\mathbb{Z} \to G$, $[i] \mapsto g^i$. ... Genauer: siehe §1.9.

1.6.6 Konvention: Eine nicht näher bestimmte zyklische Gruppe der Ordnung $n > 0$ wird bezeichnet mit Z_n oder C_n.

1.6.7 Beispiel: Die Homomorphismen bzw. Isomorphismen zwischen additiv geschriebenen abelschen Gruppen sind genau die $\mathbb{Z}$-Modul-Homomorphismen bzw. -Isomorphismen.

1.6.8 Beispiel: Die Abbildung $x \mapsto \exp(x)$ ist ein Isomorphismus $(\mathbb{R}, +) \to (\mathbb{R}^{>0}, \cdot)$.

$$\exp(x+y) = \exp(x) \cdot \exp(y)$$

1.7 Automorphismen

1.7.1 Definition: Ein Isomorphismus $G \xrightarrow{\sim} G$ heisst ein *Automorphismus von G*. Die Menge aller Automorphismen von G heisst die *Automorphismengruppe von G* und wird bezeichnet mit $\mathrm{Aut}(G)$.

1.7.2 Proposition: Die Menge $\mathrm{Aut}(G)$ ist eine Gruppe bezüglich der Komposition von Abbildungen $\circ$ und dem neutralen Element id_G.

Bew.: $\mathrm{Aut}(G) \times \mathrm{Aut}(G) \to \mathrm{Aut}(G)$, $(\varphi, \psi) \mapsto \varphi \circ \psi$ wohldef.

$\varphi \circ (\psi \circ \omega) = (\varphi \circ \psi) \circ \omega$.
$\mathrm{id}_G \circ \varphi = \varphi$.
$\varphi^{-1} \circ \varphi = \mathrm{id}_G$. qed.

1.7.3 Beispiel: Sei G eine zyklische Gruppe der Primzahlordnung p. Dann ist

$$L : \mathbb{F}_p^\times \xrightarrow{\sim} \mathrm{Aut}(G), \quad [i] \mapsto (g \mapsto g^i).$$

Bew.: $\forall a, b \in \mathbb{Z}$: $g^{a+pb} = g^a \cdot g^{pb} = g^a \cdot (g^p)^b = g^a \cdot 1^b = g^a \cdot 1 = g^a$.
($g^p = 1$)
$\Rightarrow$ g^a hängt nur von $[a] \in \mathbb{F}_p$ ab.

- $g \mapsto g^a$ ist Homo.
- $p \nmid a \Rightarrow \exists b$: $ab \equiv 1 \bmod (p) \Rightarrow \forall g \in G$; $(g^a)^b = g^{ab} = g = (g^b)^a$
  $\Rightarrow$ $G \to G$, $g \mapsto g^b$ ist (beidseitig) Umkehrung von $g \mapsto g^a$. $\Rightarrow$ $g \mapsto g^a$ ist Hom. $\Rightarrow$ in $\mathrm{Aut}(G)$.
- $\forall [a], [b] \in \mathbb{F}_p^\times$: $\forall g \in G$; $g^{ab} = (g^a)^b \Rightarrow L$ ist Homo.

- $\ker(L) \ni [a] \Leftrightarrow \forall g \in G: g^a = g \Leftrightarrow g^{a-1} = 1_G \Leftrightarrow p \mid a-1 \Leftrightarrow [a] = 1$ in $\mathbb{F}_p^k$.
  $\rightsquigarrow L$ injektiv.

- $\varphi \in \mathrm{Aut}(G)$ beliebig. Wähle $g_0 \in G$ mit $G = \langle g_0 \rangle$. $\Rightarrow \varphi(g_0) = g_0^a$ für ein $a \in \mathbb{Z}$.

  $|G| = p \Rightarrow g_0 \neq 1 \Rightarrow \varphi(g_0) \neq 1 \Rightarrow a \not\equiv 0 \ (p)$.

  $\Rightarrow \varphi(g_0) = L([a])(g_0)$

  $\Rightarrow \forall i \in \mathbb{Z}: \varphi(g_0^i) = L([a])(g_0^i)$

  $\Rightarrow \varphi = L([a]) \Rightarrow L$ surjektiv. q.ed.

1.7.4 Definition: Für alle $g, x \in G$ kürzen wir ab

$$ {}^g x := gxg^{-1} $$

und nennen x und ${}^g x$ *zueinander konjugiert.*

1.7.5 Proposition: Für alle $g, h, x, y \in G$ gilt

$$
\begin{aligned}
{}^g({}^h x) &= {}^{gh} x \\
{}^g(xy) &= {}^g x \, {}^g y \\
{}^g(x^{-1}) &= ({}^g x)^{-1} \\
{}^g 1 &= 1 \\
{}^1 x &= x
\end{aligned}
$$

1.7.6 Proposition: Für jedes $g \in G$ ist die Abbildung

$$ \mathrm{int}_g \colon G \to G, \; x \mapsto {}^g x $$

ein Automorphismus von G. Weiter ist die Abbildung

$$ G \to \mathrm{Aut}(G), \; g \mapsto \mathrm{int}_g $$

ein Homomorphismus mit Kern $Z(G)$.

1.7.7 Definition: Die Abbildung $\mathrm{int}_g \colon G \to G$ heisst *Konjugation mit g.* Ein Automorphismus der Form int_g heisst ein *innerer Automorphismus von G.*

1.7.8 Definition: Für jedes $g \in G$ und jede Teilmenge $X \subset G$ schreiben wir analog

$$^gX := gXg^{-1},$$

mit den entsprechenden Grundeigenschaften. Für jede Untergruppe $H < G$ ist auch ^gH eine solche.

$g({}^hX) = {}^{gh}X$ etc. ...

Allgemein: $\forall \varphi : G \to H$ Hom.

(a) $\forall G' < G : \varphi(G') < H$.

(b) $\forall H' < H : \varphi^{-1}(H') < G$.

$1_G \in \{g \in G \mid \varphi(g) \in H'\}$.

$$\begin{array}{ccc} G & \xrightarrow{\varphi} & H \\ \vee & & \vee \\ G' & \cdots\cdots & \varphi(G') \end{array}$$

$$\begin{array}{ccc} G & \xrightarrow{\varphi} & H \\ \vee & & \vee \\ \varphi^{-1}(H') & & H' \end{array}$$