4. Gruppenhomomorphismen

Definition: Es seien G und H Gruppen. Eine Abbildung $\varphi : G \to H$ mit der Eigenschaft $\varphi(ab) = \varphi(a)\varphi(b)\ \forall a, b \in G$ wird (Gruppen)Homomorphismus genannt.
Ein Gruppenhomomorphismus wird Monomorphismus (bzw. Epimorphismus bzw. Isomorphismus) genannt, wenn φ injektiv (bzw. surjektiv bzw. bijektiv) ist.
Ist $G = H$ (d.h. $\varphi : G \to G$), so wird φ auch Endomorphismus genannt. Ein bijektiver Endomorphismus wird Automorphismus genannt.

Beispiele: 1) Die Gruppen G und H seien $(\mathbb{R}, +)$ und $(\mathbb{R} \setminus \{0\}, \cdot)$ und $\varphi(x) = e^x$. Dann ist φ ein Monomorphismus, da $\varphi(x + y) = e^{x+y} = e^x e^y = \varphi(x)\varphi(y)\ \forall x, y \in \mathbb{R}$ und die Exponentialfunktion injektiv ist (siehe Analysis).
2) Es seien G und H zwei beliebige Gruppen und $\varphi(x) = e\ \forall x \in G$ (wobei e das neutrale Element von H bezeichnet). Dann ist $\varphi : G \to H$ ein Homomorphismus.
3) Ist $m \in \mathbb{N} \setminus \{0, 1\}$, die Gruppen G und H seien $(\mathbb{Z}, +)$ und $(\mathbb{Z}_m, +)$ und $\varphi(x) = \overline{x}$ (mit $\overline{x}$ die Restklasse von x modulo m). Dann ist φ ein Epimorphismus (siehe Zahlentheorie).
4) Allgemeiner gilt: Ist G eine Gruppe und $N \trianglelefteq G$, so ist $\pi : G \to G/N$, $\pi(x) = xN$ ein Epimorphismus (da $\pi(xy) = xyN = (xN)(yN) = \pi(x)\pi(y)\ \forall x, y \in G$).
5) Ist K ein Körper und seien G und H die Gruppen $\big(\mathrm{GL}_n(K), \cdot\big)$ und $(K \setminus \{0\}, \cdot)$, so ist $\varphi : \mathrm{GL}_n(K) \to K \setminus \{0\}$, $\varphi(A) = \det A$ ein Epimorphismus, da $\det(AB) = \det(A)\det(B)$ für alle $A, B \in \mathrm{GL}_n(K)$ und $\det\big(\mathrm{diag}(x, 1, \ldots, 1)\big) = x\ \forall x \in K \setminus \{0\}$.
6) Es sei G die Gruppe $\big(C^\infty([0, 1]), +\big)$ aller beliebig oft differenzierbaren Funktionen auf dem Intervall $[0, 1]$. Dann ist $\varphi(f) = f^{(n)}$ (d.h. die n-te Ableitung von f mit $n \in \mathbb{N}$) ein Endomorphismus. (Dabei ist φ ein Homomorphismus nach der Ableitungsregel für Summen und surjektiv nach dem Hauptsatz der Differential- und Integralrechnung.)
7) Allgemeiner gilt: Sind V und W zwei K-Vektorräume und $\varphi : V \to W$ eine K-lineare Abbildung, so ist φ ein Homomorphismus der Gruppen $(V, +)$ und $(W, +)$.
8) Ist G eine Gruppe und $a \in G$, so ist $\varphi_a : G \to G$, $\varphi_a(x) = axa^{-1}$ ein Automorphismus. Da $\varphi_a(xy) = a(xy)a^{-1} = (axa^{-1})(aya^{-1}) = \varphi_a(x)\varphi_a(y)\ \forall x, y \in G$ ist φ_a ein Endomorphismus. Wegen $\varphi_a(x) = \varphi_a(y) \Rightarrow axa^{-1} = aya^{-1} \Rightarrow x = y$ ist φ_a injektiv und wegen $\varphi_a(a^{-1}xa) = x\ \forall x \in G$ ist φ_a surjektiv.

Definition: Ist G eine Gruppe und $a \in G$, so wird eine Abbildung der Gestalt

$$\varphi_a : G \to G,\ \varphi_a(x) = axa^{-1}$$

als innerer Automorphismus von G bezeichnet.

Lemma 22: Sind G und H Gruppen und $\varphi : G \to H$ ein Homomorphismus, so gelten:

(i) $\varphi(e) = e$ (d.h. $\varphi(e_G) = e_H$),
(ii) $\varphi(a^{-1}) = \varphi(a)^{-1}\ \forall a \in G$,
(iii) $\varphi(a^n) = \varphi(a)^n\ \forall n \in \mathbb{Z}\ \forall a \in G$.

Beweis: (i) $\varphi(e) = \varphi(e \cdot e) = \varphi(e)\varphi(e)$ und die Behauptung folgt durch Verknüpfung beider Seiten mit $\varphi(e)^{-1}$.
(ii) $\varphi(a)\varphi(a^{-1}) = \varphi(aa^{-1}) = \varphi(e) = e$ und analog $\varphi(a^{-1})\varphi(a) = \varphi(a^{-1}a) = \varphi(e) = e$, woraus $\varphi(a^{-1}) = \varphi(a)^{-1}$ folgt.
(iii) Für $n > 0$ verwende Induktion nach n. Im Fall $n = 1$ ist nichts zu beweisen und der Fall $n = 2$ folgt sofort daraus, dass φ ein Homomorphismus ist. Schließlich ist

$$\varphi(a^{n+1}) = \varphi(a^n \cdot a) = \varphi(a^n)\varphi(a) \overset{\text{IV}}{=} \varphi(a)^n\varphi(a) = \varphi(a)^{n+1}.$$

Der Fall $n = 0$ folgt sofort aus (i). Für $n < 0$ ist

$$\varphi(a^n) = \varphi\big((a^{-1})^{|n|}\big) = \varphi(a^{-1})^{|n|} \overset{\text{(ii)}}{=} \big(\varphi(a)^{-1}\big)^{|n|} = \varphi(a)^n.$$

Lemma 23: Es seien G, H und K drei Gruppen und $\varphi : G \to H$ und $\psi : H \to K$ zwei Abbildungen. Dann gelten:

(i) Sind φ und ψ Homomorphismen, so ist auch $\psi \circ \varphi : G \to K$ ein Homomorphismus.
(ii) Sind φ und ψ Monomorphismen, so ist auch $\psi \circ \varphi : G \to K$ ein Monomorphismus.
(iii) Sind φ und ψ Epimorphismen, so ist auch $\psi \circ \varphi : G \to K$ ein Epimorphismus.
(iv) Sind φ und ψ Isomorphismen, so ist auch $\psi \circ \varphi : G \to K$ ein Isomorphismus.

Beweis: (i) Für alle $a, b \in G$ gilt

$$(\psi \circ \varphi)(ab) = \psi\big(\varphi(ab)\big) = \psi\big(\varphi(a)\varphi(b)\big) = \psi\big(\varphi(a)\big)\psi\big(\varphi(b)\big) = (\psi \circ \varphi)(a)(\psi \circ \varphi)(b).$$

(ii) Folgt aus (i) und der Tatsache, dass die Verknüpfung zweier injektiver Funktionen injektiv ist.
(iii) Folgt aus (i) und der Tatsache, dass die Verknüpfung zweier surjektiver Funktionen surjektiv ist.
(iv) Folgt aus (i), (ii) und (iii).

Lemma 24: Es seien G und H Gruppen und $\varphi : G \to H$ ein Homomorphismus.
(i) Ist φ ein Isomorphismus, so ist auch die Umkehrabbildung $\varphi^{-1} : H \to G$ ein Isomorphismus.
(ii) φ ist genau dann ein Isomorphismus, wenn es einen Homomorphismus $\psi : H \to G$ mit den Eigenschaften $\psi \circ \varphi = \mathrm{id}_G$ und $\varphi \circ \psi = \mathrm{id}_H$ gibt.

Beweis: (i) Die Umkehrabbildung $\varphi^{-1} : H \to G$ ist ebenfalls bijektiv. Sind $b_1, b_2 \in H$, so $\exists! a_1, a_2 \in G : \varphi(a_1) = b_1$ und $\varphi(a_2) = b_2$. Daher ist

$$\varphi^{-1}(b_1 b_2) = \varphi^{-1}\big(\varphi(a_1)\varphi(a_2)\big) = \varphi^{-1}\big(\varphi(a_1 a_2)\big) = a_1 a_2 = \varphi^{-1}(b_1)\varphi^{-1}(b_2),$$

d.h. $\varphi^{-1} : H \to G$ ist ebenfalls ein Homomorphismus.
(ii) ($\Rightarrow$) Ist $\varphi : G \to H$ ein Isomorphismus, so ist nach (i) auch $\varphi^{-1} : H \to G$ ein Isomorphismus. Für $\psi := \varphi^{-1}$ gilt dann $\psi \circ \varphi = \varphi^{-1} \circ \varphi = \mathrm{id}_G$ und $\varphi \circ \psi = \varphi \circ \varphi^{-1} = \mathrm{id}_H$.
($\Leftarrow$) Aus $\varphi(x) = \varphi(y)$ folgt

$$x = \mathrm{id}_G(x) = (\psi \circ \varphi)(x) = \psi\big(\varphi(x)\big) = \psi\big(\varphi(y)\big) = (\psi \circ \varphi)(y) = \mathrm{id}_G(y) = y,$$

d.h. φ ist injektiv. Für $h \in H$ ist $\varphi\big(\psi(h)\big) = (\varphi \circ \psi)(h) = \mathrm{id}_H(h) = h$, d.h. φ ist surjektiv.

Lemma 25: Es seien G und H zwei Gruppen und $\varphi : G \to H$ ein Homomorphismus.

(i) Wenn $A \leq G$, dann $\varphi(A) \leq H$.
(ii) Wenn $B \leq H$, dann $\varphi^{-1}(B) \leq G$.
(iii) Ist $A \trianglelefteq G$ und φ surjektiv, so ist $\varphi(A) \trianglelefteq H$.
(iv) Ist $B \trianglelefteq H$, so ist $\varphi^{-1}(B) \trianglelefteq G$.

Beweis: (i) Sind $b_1, b_2 \in \varphi(A)$ so $\exists a_1, a_2 \in A : \varphi(a_1) = b_1, \varphi(a_2) = b_2$ und daher $b_1 b_2^{-1} = \varphi(a_1)\varphi(a_2)^{-1} = \varphi(a_1 a_2^{-1}) \in \varphi(A)$ und somit $\varphi(A) \leq H$.
(ii) Sind $a_1, a_2 \in \varphi^{-1}(B)$, so $\varphi(a_1), \varphi(a_2) \in B$. Daraus folgt $\varphi(a_1 a_2^{-1}) = \varphi(a_1)\varphi(a_2)^{-1} \in B$ und daher $a_1 a_2^{-1} \in \varphi^{-1}(B)$, also ist $\varphi^{-1}(B) \leq G$.
(iii) $\varphi(A) \leq H$ wurde in (i) gezeigt. Ist $h \in H$ und $b \in \varphi(A)$, so $\exists g \in G : \varphi(g) = h$ und $\exists a \in A : \varphi(a) = b$. Da $A \trianglelefteq G$ ist $gag^{-1} \in A$ und daher

$$hbh^{-1} = \varphi(g)\varphi(a)\varphi(g)^{-1} = \varphi(gag^{-1}) \in \varphi(A),$$

womit $\varphi(A) \trianglelefteq H$ bewiesen ist.
(iv) $\varphi^{-1}(B) \leq G$ wurde in (ii) gezeigt. Ist $g \in G$ und $a \in \varphi^{-1}(B)$, so ist $\varphi(a) \in B$ und daher $\varphi(gag^{-1}) = \varphi(g)\varphi(a)\varphi(g)^{-1} \in B$, d.h. $gag^{-1} \in \varphi^{-1}(B)$ und somit $\varphi^{-1}(B) \trianglelefteq G$.

Definition: Es seien G und H zwei Gruppen und $\varphi : G \to H$ ein Homomorphismus. Dann werden $\ker \varphi := \{x \in G \mid \varphi(x) = e\} = \varphi^{-1}\big(\{e\}\big)$ der Kern von φ und $\mathrm{Im}\, \varphi = \varphi(G)$ das Bild von φ genannt.

Lemma 26: Es seien G und H zwei Gruppen und $\varphi : G \to H$ ein Homomorphismus. Dann gelten

(i) $\ker \varphi \trianglelefteq G$ und $\mathrm{Im}\, \varphi \leq H$,
(ii) φ ist ein Monomorphismus $\Leftrightarrow \ker \varphi = \{e\}$.

Beweis: (i) Setzt man $B = \{e\}$ in Lemma 25 (iv), so erhält man $\ker \varphi = \varphi^{-1}\big(\{e\}\big) \trianglelefteq G$. Setzt man $A = G$ in Lemma 25 (i), so erhält man $\mathrm{Im}(G) = \varphi(G) \leq H$.

(ii) ($\Rightarrow$) Folgt aus Lemma 22 (i) und der Injektivität von φ.
($\Leftarrow$) Aus $\varphi(x) = \varphi(y)$ folgt $\varphi(xy^{-1}) = \varphi(x)\varphi(y)^{-1} = e$. Also ist $xy^{-1} \in \ker\varphi$, woraus man $xy^{-1} = e$ und daher $x = y$ erhält.

Beispiele: 1) Es sei K ein Körper. Dann ist $\mathrm{SL}_n(K) \trianglelefteq \mathrm{GL}_n(K)$, da $\mathrm{SL}_n(K)$ der Kern der Determinantenabbildung $\det : \mathrm{GL}_n(K) \to K \setminus \{0\}$ ist.
2) Es sei G eine Gruppe und $N \trianglelefteq G$. Bezeichnet $\pi : G \to G/N$, $\pi(x) = xN$, so ist $\ker\pi = N$ (denn $x \in \ker\pi \Leftrightarrow \pi(x) = N \Leftrightarrow xN = N \Leftrightarrow x \in N$).

Definition: Zwei Gruppen G und H heißen isomorph, wenn es einen Isomorphismus $\varphi : G \to H$ gibt. Man schreibt dafür $G \cong H$.

Bemerkung: Isomorphie von Gruppen besitzt alle Eigenschaften einer Äquivalenzrelation ($G \cong G$, da $\mathrm{id}_G : G \to G$ ein Isomorphismus ist, aus $G \cong H$ folgt $H \cong G$ wegen Lemma 24 (i) und aus $G \cong H$ und $H \cong K$ folgt $G \cong K$ wegen Lemma 23 (iv)).

Beispiele: 1) Die Gruppen $(\mathbb{Z}_2, +)$ und $\big(\{+1, -1\}, \cdot\big)$ sind isomorph, da $\varphi\big(\overline{0}\big) = +1$ und $\varphi\big(\overline{1}\big) = -1$ ein Isomorphismus ist.
2) Ist allgemeiner $m \in \mathbb{N} \setminus \{0, 1\}$, so ist $(\mathbb{Z}_m, +)$ zur Gruppe der m-ten Einheitswurzeln isomorph, da die Abbildung $\varphi\big(\overline{k}\big) = e^{2\pi i k/m}$ (für $k \in \{0, 1, \ldots, k-1\}$) ein Isomorphismus ist.
3) Es sei $m \in \mathbb{Z}\setminus\{0\}$. Dann sind die Gruppen $(\mathbb{Z}, +)$ und $(m\mathbb{Z}, +)$ isomorph, da $\varphi(k) = mk$ ein Isomorphismus ist.
4) Die Gruppen $(\mathbb{R}, +)$ und $(\mathbb{R}^+, \cdot)$ (mit $\mathbb{R}^+ = (0, +\infty)$) sind isomorph, da die Abbildung $\varphi(x) = e^x$ ein Isomorphismus ist.
5) Sind V und W isomorph als K-Vektorräume, so sind auch die Gruppen $(V, +)$ und $(W, +)$ isomorph.

Satz 27: Es seien G und H zwei Gruppen, $\varphi : G \to H$ ein Homomorphismus, $N \trianglelefteq G$ und $N \leq \ker\varphi$. Dann gibt es genau einen Homomorphismus $\overline{\varphi} : G/N \to H$, sodass $\overline{\varphi}(aN) = \varphi(a)\ \forall a \in G$. Dabei gelten $\mathrm{Im}\,\overline{\varphi} = \mathrm{Im}\,\varphi$ und $\ker\overline{\varphi} = (\ker\varphi)/N$. Weiters ist $\overline{\varphi}$ ein Isomorphismus genau dann wenn φ ein Epimorphismus ist und $N = \ker\varphi$.

Bemerkung: Man kann die Aussage von Satz 27 auch folgendermaßen formulieren: Bezeichnet π den Epimorphismus $\pi : G \to G/N$, $\pi(a) = aN$, so gibt es einen eindeutig bestimmten Homomorphismus $\overline{\varphi} : G/N \to H$ mit der Eigenschaft $\varphi = \overline{\varphi} \circ \pi$.

Beweis: Ist $bN = aN$, so ist $b \in aN$ und $\exists n \in N : b = an$. Daher

$$\varphi(b) = \varphi(an) = \varphi(a)\varphi(n) = \varphi(a)e = \varphi(a)$$

(da $N \leq \ker\varphi$). Daher ist die Abbildung $\overline{\varphi} : G/N \to H$, $\overline{\varphi}(aN) = \varphi(a)$ wohldefiniert. Wegen

$$\overline{\varphi}(aN \cdot bN) = \overline{\varphi}(abN) = \varphi(ab) = \varphi(a)\varphi(b) = \overline{\varphi}(aN)\overline{\varphi}(bN)\ \forall a, b \in G$$

ist $\overline{\varphi}$ ein Homomorphismus. Offensichtlich ist $\operatorname{Im}\overline{\varphi} = \operatorname{Im}\varphi$ und

$$aN \in \ker\overline{\varphi} \Leftrightarrow \overline{\varphi}(aN) = e \Leftrightarrow \varphi(a) = e \Leftrightarrow a \in \ker\varphi,$$

woraus $\ker\overline{\varphi} = \{aN \mid a \in \ker\varphi\} = (\ker\varphi)/N$ folgt. Es ist klar, dass die Abbildung $\overline{\varphi}$ durch die Beziehung $\overline{\varphi}(aN) = \varphi(a)\ \forall a \in G$ eindeutig bestimmt ist. Wegen $\operatorname{Im}\overline{\varphi} = \operatorname{Im}\varphi$ ist $\overline{\varphi}$ genau dann ein Epimorphismus, wenn φ ein Epimorphismus ist. Schließlich ist $\overline{\varphi}$ ein Monomorphismus genau dann, wenn

$$\ker\overline{\varphi} = \{N\} \Leftrightarrow (\ker\varphi)/N = \{N\} \Leftrightarrow \ker\varphi = N.$$

Korollar 28 (Homomorphiesatz): Es seien G und H zwei Gruppen und $\varphi : G \to H$ ein Homomorphismus. Dann gilt $G/\ker\varphi \cong \operatorname{Im}\varphi$. Ist φ ein Epimorphismus, so gilt $G/\ker\varphi \cong H$.

Beweis: Die Abbildung $\varphi : G \to \operatorname{Im}\varphi$, $x \mapsto \varphi(x)$ ist ein Epimorphismus. Wende Satz 27 mit $N = \ker\varphi$ an.

Beispiele: 1) Ist G eine Gruppe, so gilt $G/G \cong \{e\}$, da $\varphi : G \to \{e\}$, $\varphi(x) = e\ \forall x \in G$ ein Epimorphismus mit $\ker\varphi = G$ ist.
2) Ist G eine Gruppe, so ist $G/\{e\} \cong G$, da $\varphi : G \to G$, $\varphi(x) = x$ ein Epimorphismus mit $\ker\varphi = \{e\}$ ist.
3) Es sei $m \in \mathbb{N} \setminus \{0, 1\}$. Dann ist $\varphi : \mathbb{Z} \to \mathbb{Z}_m$, $\varphi(a) = \overline{a}$ (wobei $\overline{a}$ die Restklasse von a bezeichnet) ein Epimorphismus mit $\ker\varphi = m\mathbb{Z}$ und daher $\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}_m$.
4) Ist K ein Körper, so ist $\mathrm{GL}_n(K)/\mathrm{SL}_n(K) \cong K \setminus \{0\}$, da $\det : \mathrm{GL}_n(K) \to K \setminus \{0\}$ ein Epimorphismus und $\ker\det = \mathrm{SL}_n(K)$ ist.

Satz 29: Es G eine Gruppe, $H \leq G$ und $N \trianglelefteq G$. Dann gelten:

(i) $N \cap H \trianglelefteq H$,
(ii) $N \trianglelefteq \langle N \cup H \rangle$,
(iii) $\langle N \cup H \rangle = NH = HN$ (wobei NH und HN jeweils das Komplexprodukt bezeichnen, es ist also z.B. $NH = \{nh \mid n \in N, h \in H\}$).

Beweis: (i) $N \cap H \leq H$ nach Lemma 11 (i). Es sei $n \in N \cap H$ und $a \in H$. Dann ist $ana^{-1} \in N$, da $n \in N$ und $N \trianglelefteq G$ und $ana^{-1} \in H$, da $a, n \in H$ und $H \leq G$. Daher gilt $a(N \cap H)a^{-1} \subseteq N \cap H\ \forall a \in H$ und daher $N \cap H \trianglelefteq H$.

(ii) Da $N \trianglelefteq G$ gilt auch $N \trianglelefteq \langle N \cup H \rangle$.
(iii) Aus Satz 12 folgt

$$\langle N \cup H \rangle = \{n_1 h_1 \dots n_r h_r \mid n_1, \dots, n_r \in N, h_1, \dots, h_r \in H\}$$

(Im Bedarfsfall kann man immer $n_1 = e$ oder $h_r = e$ ergänzen.)
Wir zeigen nun: Ist $x \in \langle N \cup H \rangle$ und $x = n_1 h_1 \dots n_r h_r$, so $\exists n \in N : x = n h_1 \dots h_r$.
Wir verwenden Induktion nach r. Im Fall $r = 1$ ist nichts zu zeigen. Betrachte nun $n_1 h_1 \dots n_r h_r n_{r+1} h_{r+1}$. Nach Induktionsvoraussetzung $\exists n \in N : n_1 h_1 \dots n_r h_r = n h_1 \dots h_r$ und daher

$$n_1 h_1 \dots n_r h_r n_{r+1} h_{r+1} = n h_1 \dots h_r n_{r+1} h_{r+1}.$$

Da $N \trianglelefteq G$ ist

$$h_1 \dots h_r n_{r+1} h_r^{-1} \dots h_1^{-1} = (h_1 \dots h_r) n_{r+1} (h_1 \dots h_r)^{-1} \in N$$

und daher $\exists \overline{n} \in N : h_1 \dots h_r n_{r+1} h_r^{-1} \dots h_1^{-1} = \overline{n}$ und $h_1 \dots h_r n_{r+1} = \overline{n} h_1 \dots h_r$. Setzt man das ein, erhält man

$$n_1 h_1 \dots n_r h_r n_{r+1} h_{r+1} = n (h_1 \dots h_r n_{r+1}) h_{r+1} = n \overline{n} h_1 \dots h_r h_{r+1},$$

womit der Induktionsschritt abgeschlossen ist.
Daher ist $x \in NH$ und somit $\langle N \cup H \rangle \subseteq NH$. Da $NH \subseteq \langle N \cup H \rangle$ trivialerweise gilt, ist $\langle N \cup H \rangle = NH$ gezeigt. Die Identität $\langle N \cup H \rangle = HN$ zeigt man analog.

Korollar 30 (1. Isomorphiesatz): Es sei G eine Gruppe, $H \leq G$ und $N \trianglelefteq G$. Dann gilt

$$H/(N \cap H) \cong NH/N.$$

Beweis: Betrachte die Abbildung $\varphi : H \to NH/N$, $\varphi(x) = xN$. Sie ist ein Homomorphismus, da sie Verknüpfung der Einbettung $H \to NH$, $x \mapsto x$ und der Projektion $NH \to NH/N$, $x \mapsto xN$ ist, die beide Homomorphismen sind. Offenbar ist $\ker \varphi = N \cap H$. Ist $xN \in NH/N$, so $\exists n \in N \, \exists h \in H : xN = nhN$. Da $N \trianglelefteq G$, gibt es ein $\overline{n} \in N$ mit der Eigenschaft $nh = h\overline{n}$ und daher $xN = nhN = h\overline{n}N = hN = \varphi(h)$, d.h. φ ist ein Epimorphismus und nach Korollar 28 gilt

$$H/(N \cap H) = H/\ker \varphi \cong \operatorname{Im} \varphi = NH/N.$$

Satz 31: Es sei G eine Gruppe und $N \trianglelefteq G$.
(i) Wenn $N \leq H \leq G$, dann $H/N \leq G/N$. Gilt sogar $H \trianglelefteq G$, so $H/N \trianglelefteq G/N$.
(ii) Wenn $\overline{H} \leq G/N$, dann $\exists H \leq G$ mit $N \leq H$ (also $N \leq H \leq G$), sodass $H/N = \overline{H}$. Gilt sogar $\overline{H} \trianglelefteq G/N$, so $H \trianglelefteq G$.

Beweis: Die Projektion $\pi : G \to G/N$, $\pi(x) = xN$ ist ein Epimorphismus.
(i) Aus $N \leq H \leq G$ folgt $H/N = \pi(H) \leq G/N$ wegen Lemma 25 (i). Wenn $H \trianglelefteq G$ folgt

$H/N \trianglelefteq G/N$ wegen Lemma 25 (iii).
(ii) Es sei $H = \pi^{-1}(\overline{H})$. Dann ist $N \leq H \leq G$ wegen Lemma 25 (ii) und

$$H/N = \pi(H) = \pi\bigl(\pi^{-1}(\overline{H})\bigr) = \overline{H},$$

da π surjektiv ist. Ist $\overline{H} \trianglelefteq G/N$, so ist $H \trianglelefteq G$ wegen Lemma 25 (iv).

Korollar 32 (2. Isomorphiesatz): Es sei G eine Gruppe, $H \trianglelefteq G$, $K \trianglelefteq G$ und $K \leq H$. Dann gilt

$$(G/K)\big/(H/K) \cong G/H.$$

Beweis: Betrachte den Epimorphismus $\pi : G \to G/H$, $\pi(x) = xH$. Da $K \leq H = \ker \pi$, gibt es nach Satz 27 einen Homomorphismus $\varphi : G/K \to G/H$, $\varphi(aK) = \pi(a) = aH$. Da $\operatorname{Im} \varphi = \operatorname{Im} \pi = G/H$, ist φ ein Epimorphismus und $\ker \varphi = (\ker \pi)/K = H/K$. Die Behauptung folgt aus Korollar 28.

Beispiel: Es seien $m, n \in \mathbb{N} \setminus \{0, 1\}$. Verwendet man die Identitäten

$$(m\mathbb{Z}) \cap (n\mathbb{Z}) = \operatorname{kgV}(m, n)\mathbb{Z} \quad \text{und} \quad (m\mathbb{Z}) + (n\mathbb{Z}) = \operatorname{ggT}(m, n)\mathbb{Z}$$

aus der Zahlentheorie, so folgt aus Korollar 30

$$\begin{aligned}(m\mathbb{Z})\big/\bigl(\operatorname{kgV}(m, n)\mathbb{Z}\bigr) &= (m\mathbb{Z})\big/\bigl((m\mathbb{Z}) \cap (n\mathbb{Z})\bigr) \\ &\cong \bigl((m\mathbb{Z}) + (n\mathbb{Z})\bigr)\big/(n\mathbb{Z}) = \bigl(\operatorname{ggT}(m, n)\mathbb{Z}\bigr)\big/(n\mathbb{Z}).\end{aligned}$$

Gilt zusätzlich $m \mid n$ (und daher $n\mathbb{Z} \leq m\mathbb{Z}$), so folgt aus Korollar 32

$$(\mathbb{Z}/n\mathbb{Z})\big/(m\mathbb{Z}/n\mathbb{Z}) \cong \mathbb{Z}/m\mathbb{Z}.$$

Definition: Es G eine Gruppe. Man nennt

$$Z(G) := \{a \in G \mid xa = ax \ \forall x \in G\}$$

das Zentrum von G,

$$\operatorname{Aut}(G) := \{\varphi : G \to G \mid \varphi \text{ ist ein Automorphismus von } G\}$$

die Automorphismengruppe von G und

$$\begin{aligned}\operatorname{Inn}(G) &:= \{\varphi : G \to G \mid \varphi \text{ ist ein innerer Automorphismus von } G\} \\ &= \{\varphi : G \to G \mid \exists a \in G \ \forall x \in G : \varphi(x) = axa^{-1}\}\end{aligned}$$

die Gruppe der inneren Automorphismen von G.

Satz 33: Es sei G eine Gruppe. Dann gelten:

(i) $Z(G) \trianglelefteq G$,
(ii) $\bigl(\operatorname{Aut}(G), \circ\bigr)$ ist eine Gruppe,
(iii) $\operatorname{Inn}(G) \trianglelefteq \operatorname{Aut}(G)$,
(iv) $G/Z(G) \cong \operatorname{Inn}(G)$.

Beweis: (i) Da $a \in Z(G) \Rightarrow ax = xa \ \forall x \in G \Rightarrow xa^{-1} = a^{-1}x \ \forall x \in G \Rightarrow a^{-1} \in Z(G)$ und $a, b \in Z(G) \Rightarrow (ab)x = a(bx) = a(xb) = (ax)b = (xa)b = x(ab) \ \forall x \in G \Rightarrow ab \in Z(G)$ ist $Z(G) \leq G$. Da $xax^{-1} = axx^{-1} = a \ \forall x \in G \ \forall a \in Z(G)$ ist $Z(G) \trianglelefteq G$.
(ii) Sind $\varphi, \psi \in \mathrm{Aut}(G)$, so ist auch $\psi \circ \varphi \in \mathrm{Aut}(G)$ nach Lemma 23 (iv). Ist $\varphi \in \mathrm{Aut}(G)$, so ist auch $\varphi^{-1} \in \mathrm{Aut}(G)$ nach Lemma 24 (i). Daher ist $\mathrm{Aut}(G)$ eine Untergruppe der Gruppe $S_G = \{f : G \to G \mid f \text{ ist bijektiv}\}$ und somit eine Gruppe.
(iii) Bezeichnet $\varphi_a \in \mathrm{Aut}(G)$ die Abbildung $\varphi_a(x) = axa^{-1}$, so gilt $\varphi_b \circ \varphi_a = \varphi_{ba} \ \forall a, b \in G$, denn

$$(\varphi_b \circ \varphi_a)(x) = \varphi_b\big(\varphi_a(x)\big) = b(axa^{-1})b^{-1} = (ba)x(ba)^{-1} = \varphi_{ba}(x) \ \forall x \in G$$

Es folgt $\varphi_a^{-1} = \varphi_{a^{-1}} \ \forall a \in G$, da

$$\varphi_a \circ \varphi_{a^{-1}} = \varphi_{aa^{-1}} = \varphi_e = \mathrm{id}_G \text{ und } \varphi_{a^{-1}} \circ \varphi_a = \varphi_{a^{-1}a} = \varphi_e = \mathrm{id}_G.$$

Damit ist $\mathrm{Inn}(G) \leq \mathrm{Aut}(G)$ gezeigt. Ist $\psi \in \mathrm{Aut}(G)$, so ist $\psi \circ \varphi_a \circ \psi^{-1} = \varphi_{\psi(a)} \ \forall a \in G$, denn

$$(\psi \circ \varphi_a \circ \psi^{-1})(x) = \psi\big(\varphi_a\big(\psi^{-1}(x)\big)\big) = \psi\big(a\psi^{-1}(x)a^{-1}\big) = \psi(a)x\psi(a)^{-1} = \varphi_{\psi(a)}(x) \ \forall x \in G,$$

womit auch $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$ gezeigt ist.
(iv) Es sei $\Phi : G \to \mathrm{Inn}(G)$, $\Phi(a) = \varphi_a$. Dann ist Φ ein Epimorphismus, denn

$$\Phi(ab) = \varphi_{ab} = \varphi_a \circ \varphi_b = \Phi(a) \circ \Phi(b) \ \forall a, b \in G$$

und Φ ist trialerweise surjektiv. Weiters ist $\ker \Phi = Z(G)$, denn

$$\begin{aligned} a \in \ker \Phi \Leftrightarrow \Phi(a) = \mathrm{id}_G \Leftrightarrow \varphi_a = \mathrm{id}_G \Leftrightarrow \varphi_a(x) = x \ \forall x \in G \\ \Leftrightarrow axa^{-1} = x \ \forall x \in G \Leftrightarrow ax = xa \ \forall x \in G \Leftrightarrow a \in Z(G) \end{aligned}$$

Die Behauptung folgt nun aus Korollar 28.