

§2 Gruppen

Sei M eine Menge

(2.1) Definition

Eine **Verknüpfung** auf M ist eine Abbildung

$$\begin{aligned} \bullet : M \times M &\longrightarrow M \\ a, b &\mapsto a \cdot b \\ b, a &\mapsto b \cdot a \end{aligned}$$

(2.2) Definition

Eine **Gruppe** ist eine Menge G auf der eine Verknüpfung

$$\bullet : G \times G \longrightarrow G$$

gegeben ist derart, dass folgendes gilt:

- (a) Assoziativgesetz $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
- (b) $\exists e \in G$ mit $e \cdot a = a \cdot e = a \quad \forall a \in G$
- (c) $\forall a \in G \exists a' \in G : a \cdot a' = a' \cdot a = e$

(2.3) Beispiele

(1) $(\mathbb{Z}, +)$ ist Gruppe

$$e = 0, \quad a \in \mathbb{Z}, \quad a' = -a$$

(2) $(\mathbb{Q}, +), (\mathbb{R}, +)$

(3) $\mathbb{Q}^\times := \mathbb{Q} \setminus \{0\}, (\mathbb{Q}^\times, \bullet)$ ist Gruppe

(4) Sei M eine Menge, $M \neq \emptyset$

$$\Sigma(M) := \{f : M \longrightarrow M : f \text{ ist bijektiv}\}$$

$$g \circ f := \text{Komposition} \quad \Rightarrow \Sigma(M) \text{ ist Gruppe}$$

Zunächst ist $\circ$ eine Verknüpfung auf $\Sigma(M)$

G(2.21),(2)

(a) Assoziativgesetz **G(2.9)**

$$h \circ (g \circ f) = (h \circ g) \circ f$$

$$\begin{aligned} \text{(b) } e = id_M \quad M &\longrightarrow M \quad f \circ id_M = f \\ x &\mapsto x \quad id_M \circ f = f \end{aligned}$$

(c) Sei $M \xrightarrow{f} M$ bijektiv

$$f' := f^{-1} \Rightarrow f \circ f^{-1} = f^{-1} \circ f = id_M$$

Bezeichnung:

Eine Gruppe G heißt **abelsch** $\Leftrightarrow$ Kommutativgesetz $a \cdot b = b \cdot a \quad \forall a, b$

Hat M mindestens 3 Elemente, so ist $\Sigma(M)$ nicht abelsch

$$f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

$$g = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

$$g \circ f = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$f \circ g = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

(2.4) Satz

Sei G eine Gruppe $a, b \in G$

- (a) Es gibt genau ein neutrales Element in G (e)
- (b) Es gibt genau ein inverses Element von a in G . Dieses wird mit a^{-1} bezeichnet. ($a' = a^{-1}$)
- (c) Die Gleichung $ax = b$ hat genau die Lösung $x = a'b$
- (d) Die Gleichung $xa = b$ hat genau die Lösung $x = ba'$
- (e) $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$

Beweis:

(a) Seien $e, \tilde{e}$ neutrale Elemente, d.h.

$$\text{und } \left. \begin{array}{l} a \cdot e = a = e \cdot a \\ a \cdot \tilde{e} = a = \tilde{e} \cdot a \end{array} \right\} \begin{array}{l} \forall a \in G \\ \forall a \in G \end{array} \left/ \begin{array}{l} \tilde{e} \cdot e = \tilde{e} \\ \tilde{e} \cdot e = e \end{array} \right. \begin{array}{l} a = \tilde{e} \\ a = e \end{array} \Rightarrow e = \tilde{e}$$

(b) Seien a', a'' Inverse von a , d.h.

$$aa' = a'a = e = aa'' = a''a$$

$$\Rightarrow aa' = aa''$$

$$\Rightarrow \underbrace{a'}_e aa' = \underbrace{a'}_e aa''$$

$$\Rightarrow ea' = ea''$$

$$\Rightarrow a' = a''$$

(c) Sei $x = a^{-1}b \Rightarrow ax = a \cdot a^{-1} \cdot b = b$

$\Rightarrow x$ ist Lösung

Sei x Lösung $\Rightarrow ax = b$

$$\Rightarrow a^{-1}ax = a^{-1}b$$

$$\Rightarrow x = a^{-1}b$$

(d) genauso

(e) $ab \cdot b^{-1} \cdot a^{-1} = a \cdot e \cdot a^{-1} = aa^{-1} = e \Rightarrow$ Behauptung q.e.d.

	Additive Schreibweise ($a+b$)	Multiplikative Schreibweise ($a \cdot b$)
- inverses Element:	$-a$	a^{-1}
- neutrales Element :	$0 = e$	$1 = e$

(2.5) Definition

Sei $H \subseteq G$ Teilmenge

H heißt **Untergruppe** wenn gilt:

- (a) $e \in H$
- (b) Sind $a, b \in H \Rightarrow a \cdot b \in H$
- (c) Ist $a \in H \Rightarrow a^{-1} \in H$

Eine Untergruppe ist selber eine Gruppe.

(2.6) Beispiele

(1) $G = (\mathbb{Z}, +)$, $H = \{n \cdot a : a \in \mathbb{Z}\}$ wobei $n \in \mathbb{N}_+$

(2) $\mathbb{Z} \subseteq (\mathbb{R}, +)$, $(\mathbb{Q}^\times, \cdot) \subseteq (\mathbb{R}^\times, \cdot)$

(3) Sei $(G, \cdot)$ Gruppe, sei $a \in G$

$$a^n := a^0 = e \quad a^{n+1} = a^n \cdot a = \overbrace{a \cdot \dots \cdot a}^{n+1}$$

$$a^{-n} := (a^{-1})^n \text{ für } n \in \mathbb{N}$$

$H = \{a^n, n \in \mathbb{Z}\} \subseteq G$ ist **Untergruppe**

- $e \in H$

- $a^n a^m = a^{n+m}$

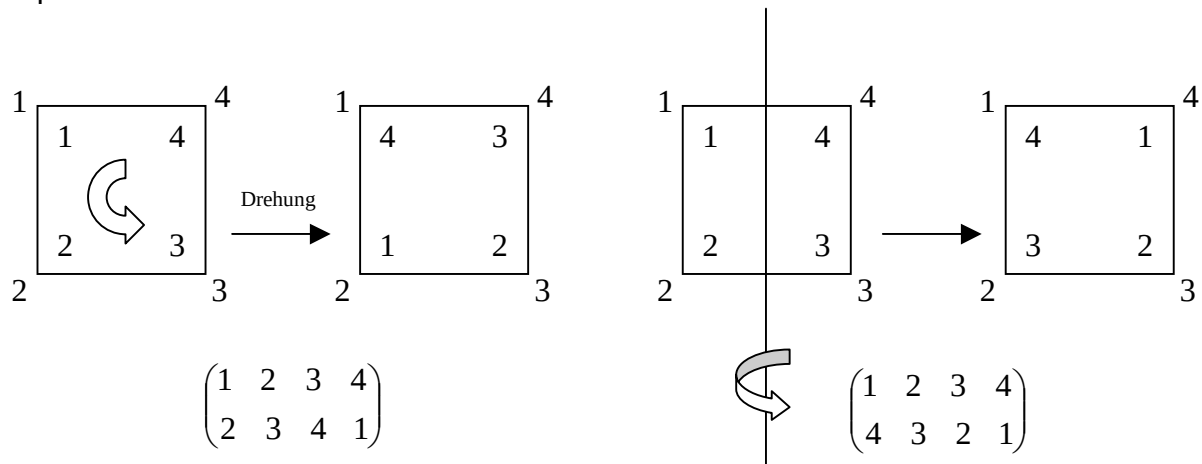
- $(a^n)^{-1} = (a^{-1})^n = a^{-n} \quad \forall n, m \in \mathbb{Z}$

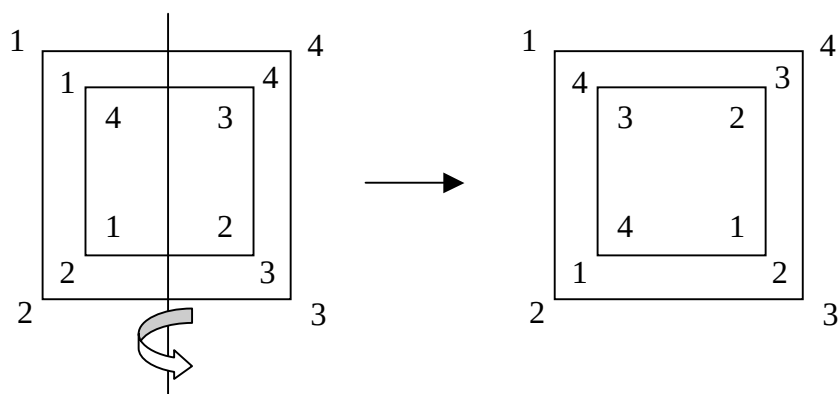
Eine Gruppe G heißt **zyklisch** $\Leftrightarrow \exists a \in G : G = \{a^n, n \in \mathbb{Z}\}$

Dann ist G abelsch.

$G = \Sigma_n := \Sigma(\{1, \dots, n\})$ G hat $n!$ Elemente

$n = 4$





Drehungen und Spiegelungen ergeben eine Untergruppe von 8 Permutationen $\subseteq$ 24 Permutationen

Ebenso:

- Tetraeder $12 P. \subseteq 24 P.$
- Würfel: $6 \cdot 4 = 24 P. \subseteq 8! P.$ (6 Seiten, 8 Ecken)
- Oktaeder: $8 \cdot 3 = 24 P. \subseteq 6! P.$ (8 Seiten, 6 Ecken)
- Dodekaeder: $12 \cdot 5 = 60 P. \subseteq 20! P.$ (12 Seiten, 20 Ecken)
- Ikosaeder: $20 \cdot 3 = 60 P. \subseteq 12! P.$ (20 Seiten, 12 Ecken)

Sei $H \subseteq G$

Definiere Relationen

$$\sim: a \sim b \Leftrightarrow b^{-1}a \in H$$

$$\approx: a \approx b \Leftrightarrow ba^{-1} \in H$$

(2.7) Lemma

$\sim$ und $\approx$ sind Äquivalenzrelationen

Beweis: (vgl. Lemma 1.16)

(r) $a \sim a$, da $a^{-1} \cdot a = e \in H$

(s) $a \sim b \Rightarrow b \sim a$, da $b^{-1}a \in H \Rightarrow (b^{-1}a)^{-1} \in H$
und $(b^{-1}a)^{-1} = a^{-1}b \in H \Rightarrow b \sim a$

(t) $a \sim b, b \sim c \Rightarrow a \sim c$, da $b^{-1}a \in H, c^{-1}b \in H \Rightarrow c^{-1}bb^{-1}a \in H$
 $= c^{-1}a \Rightarrow a \sim c$

Beweis für $\approx$ analog

q.e.d.

Bezeichnung:

- $a \cdot H := \{a \cdot h : h \in H\}$ Die Mengen heißen Linksnebenklassen
- $H \cdot a := \{h \cdot a : h \in H\}$ Die Mengen heißen Rechtsnebenklassen

Behauptung:

- $[a]_{\sim} = a \cdot H$
- $[a]_{\approx} = H \cdot a$

Beweis:

Sei $b \in [a]_{\sim} \Leftrightarrow b \sim a$

$$\Leftrightarrow \underbrace{a^{-1}b}_h \in H$$

$$\Rightarrow b = a \cdot h = aa^{-1}b \quad \Rightarrow b \in a \cdot H$$

Sei umgekehrt $b \in a \cdot H \Rightarrow \exists h \in H : b = a \cdot h$

$$\Rightarrow h = a^{-1} \cdot b$$

$$\Rightarrow a^{-1}b \in H \Rightarrow a \sim b \Rightarrow b \in [a]_{\sim} \quad \Rightarrow \text{Behauptung}$$

$[a]_{\approx}$ analog

q.e.d.

Folgerung:

Es gilt entweder $a \cdot H = b \cdot H$ oder $a \cdot H \cap b \cdot H = \emptyset$

Folgt aus **G(3.7)**

(2.8) Lemma

Sei $a \in G$ und seien

$$\begin{array}{ccc} G & \xrightarrow{\tau_a} & G \\ x \mapsto a \cdot x & , & x \mapsto x \cdot a \end{array} \quad G \xrightarrow{\sigma_a} G$$

Dann sind τ_a (Tau) und σ_a (Sigma) bijektiv und $(\tau_a)^{-1} = \tau_{a^{-1}}$

Beweis:

Injektiv: Sei $\tau_a(x_1) = \tau_a(x_2) = ax_1 = ax_2 = x_1 = x_2$

Surjektivität: Sei $b \in G$, $\tau_a(a^{-1}b) = aa^{-1}b = b \Rightarrow$ Behauptung q.e.d.

$$\tau_{a^{-1}} \circ \tau_a(x) = a^{-1} \cdot a \cdot x = x$$

Notation:

Sei G/H die Menge der „ $\sim$ “-Äquivalenzklassen $G/H = \{a \in H : a \in G\}$

Sei $H \setminus G$ die Menge der „ $\approx$ “-Äquivalenzklassen

Ist H endlich, so sei $|H|$ die Anzahl der Elemente von H

$|H| = \infty$, wenn H nicht endlich.

$$\begin{array}{ccc} \tau_a : G & \rightarrow & G \\ x \mapsto ax & & \tau_a(H) = a \cdot H \end{array}$$

$\Rightarrow H$ und $a \cdot H$ haben gleich viele Elemente (falls $|H|$ endlich)

(2.9) Satz

Sei G endliche Gruppe, sei $H \subseteq G$ Untergruppe. Dann gilt:

$$\begin{aligned} |G| &= |H| \cdot |G/H| \\ &= |H| \cdot |H \backslash G| \end{aligned}$$

Beweis:

Verschiedene Nebenklassen sind disjunkt und haben gleich viele (nämlich $|H|$) Elemente.

$\Rightarrow$ Behauptung q.e.d.

Sei G endlich, $a \in G$

Betrachte $\langle a \rangle := \{a^n, n \in \mathbb{Z}\} \subseteq G$

Sei n_0 die kleinste Zahl > 0 so dass

$$a^{n_0} \in \{a^0, a^1, \dots, a^{n_0-1}\}$$

$a^0, \dots, a^{n_0-1}$ sind alle verschieden

$\Rightarrow \exists k < n_0 : a^{n_0} = a^k$. Wäre $k > 0 \Rightarrow a^{n_0-k} = a^0 = e$ ✗

$$\Rightarrow a^{n_0} = e$$

$$\Rightarrow a^{-k} = a^{n_0-k}$$

$\Rightarrow \langle a \rangle$ hat n_0 Elemente

n_0 heißt die **Ordnung** von a , $\text{ord}(a)$

$$|G| = \text{ord}(a) \cdot |G/\langle a \rangle|$$

(2.10) Korollar

Sei $a \in G$, G endlich. Dann gilt

(1) $\text{ord}(a)$ teilt $|G|$

(2) $\forall a : a^{|G|} = 1$ (kleiner Fermatscher Satz)

Beweis:

(1) folgt aus (2.9) ($H = \langle a \rangle$)

(2) $a \in G \Rightarrow \exists m : |G| = \text{ord}(a) \cdot m$

$$\Rightarrow 1 = a^{\text{ord}(a)} = (a^{\text{ord}(a)})^m = a^{|G|}$$

(2.11) Satz

Sei $H \subseteq \mathbb{Z}$ eine Untergruppe

$\Rightarrow H = (0)$ oder $H = \mathbb{Z} \cdot n$ für ein $n \in \mathbb{N}_+$

Es gibt keine weiteren Untergruppen.

Beweis:

Sei $H \neq (0)$. Sei $n \in H \cap \mathbb{N}_+$ minimal

Sei $m \in H \Rightarrow \exists q \in \mathbb{Z}, r : 0 \leq r < n$

$$m = q \cdot n + r$$

$$\Rightarrow r = m - q \cdot n \in H$$

$$\Rightarrow r = 0 \quad \text{da } n \text{ minimal}$$

$$\Rightarrow m \in \mathbb{Z} \cdot n \Rightarrow H = \mathbb{Z} \cdot n \quad \text{q.e.d.}$$

Seien G_1, G_2 Gruppen

(2.12) Definition

Ein **Homomorphismus** von G_1 nach G_2 ist eine Abbildung $G_1 \xrightarrow{f} G_2$ derart, dass gilt

$$f(a \cdot b) = f(a) \cdot f(b) \quad \forall a, b \in G_1$$

Ein injektiver Homomorphismus heißt **Monomorphismus**.

Ein surjektiver Homomorphismus heißt **Epimorphismus**.

Ein bijektiver Homomorphismus heißt **Isomorphismus**.

Ein Homomorphismus von G_1 in sich selbst heißt **Endomorphismus**.

Ein Isomorphismus von G_1 in sich selbst heißt **Automorphismus**.

(2.13) Lemma

Sei $G_1 \xrightarrow{f} G_2$ Homomorphismus. Dann gilt

(a) $f(1_{G_1}) = 1_{G_2}$

(b) $f(a^{-1}) = f(a)^{-1}$

Beweis:

$$\begin{aligned} \text{(a) } f(1_{G_1}) &= f(1_{G_1} \cdot 1_{G_1}) \\ &= f(1_{G_1}) \cdot f(1_{G_1}) \Rightarrow 1_{G_2} = f(1_{G_1}) \end{aligned}$$

$$\begin{aligned} \text{(b) } f(a \cdot a^{-1}) &= f(1_{G_1}) \\ &= 1_{G_2} = f(a) \cdot f(a^{-1}) \\ &\Rightarrow f(a^{-1}) = f(a)^{-1} \quad \text{q.e.d.} \end{aligned}$$

(2.14) Beispiele

(1) $\mathbb{Z} \rightarrow \mathbb{Z}/\mathbb{Z} \cdot n, n \in \mathbb{N}_+$

$$a \mapsto [a]$$

ist Homomorphismus nach Definition der Addition in $\mathbb{Z} / \mathbb{Z}n$

$$a + b \mapsto [a + b] = [a] + [b]$$

(2) Sei $H \subseteq G$ Untergruppe

$$\Rightarrow \text{kanonische Injektion } \begin{matrix} H \rightarrow G \\ a \mapsto a \end{matrix} \text{ ist Homomorphismus}$$

(3) G_1, G_2 Gruppen

$$\begin{matrix} G_1 \rightarrow G_2 \\ a \mapsto 1_{G_2} \end{matrix} \text{ ist Homomorphismus (trivialer Homomorphismus)}$$

(4) Sei G abelsch, $n \in \mathbb{Z}$

$$\begin{matrix} G \rightarrow G \\ a \mapsto a^n \end{matrix}, (a \cdot b)^n = a^n \cdot b^n \text{ ist Homomorphismus}$$

(kein Homomorphismus für G nicht abelsch)

(5) Sei G eine Gruppe, $x \in G$

$$\Rightarrow G \xrightarrow{\kappa_x} G \text{ ist Automorphismus von } G$$

$$a \mapsto x \cdot a \cdot x^{-1}$$

$$\begin{aligned} \kappa_x(a \cdot b) &= x \cdot ab \cdot x^{-1} = x \cdot a \cdot x^{-1} \cdot x \cdot b \cdot x^{-1} \\ &= \kappa_x(a) \cdot \kappa_x(b) \end{aligned}$$

$$\begin{matrix} G \xrightarrow{\tau_x} G \xrightarrow{\sigma_x} G \\ a \mapsto xa \mapsto xax^{-1} \end{matrix} \Rightarrow \kappa_x \text{ (Kappa) bijektiv } \kappa_x^{-1} = \kappa_{x^{-1}}$$

κ_x heißt **Konjugation** mit x

(2.15) Definition

Sei $G_1 \xrightarrow{f} G_2$ Homomorphismus

Die Menge $\text{Ker}(f) := \{a \in G_1 : f(a) = 1_{G_2}\}$ heißt der **Kern** von f .

(2.16) Satz

- (a) $\text{Ker}(f)$ ist eine Untergruppe von G_1
 (b) Folgendes ist äquivalent
 (1) $\text{Ker}(f) = \{1_{G_1}\}$
 (2) f ist injektiv
 (c) Sei $b \in \text{Bild}(f)$, etwa $b = f(a)$
 Dann gilt $f^{-1}(b) = a \cdot \text{Ker}(f) = \text{Ker}(f) \cdot a$
 Insbesondere: Linksnebenklasse = Rechtsnebenklasse

Beweis:

- (a) $1_{G_1} \in \text{Ker}(f)$
 Sei $a, b \in \text{Ker}(f)$
 $\Rightarrow f(a \cdot b) = f(a) \cdot f(b) = 1_{G_2} \cdot 1_{G_2} = 1_{G_2} = ab \in \text{Ker}(f)$

$$f(a^{-1}) = f(a)^{-1} = 1_{G_2}^{-1} = 1_{G_2} \Rightarrow a^{-1} \in \text{Ker}(f)$$

- (b)
 (2) $\Rightarrow$ (1) klar, da $f(1_{G_1}) = 1_{G_2}$
 (1) $\Rightarrow$ (2) Seien $a, b \in G_1 : f(a) = f(b)$
 $\Rightarrow f(a) \cdot f(b)^{-1} = f(a \cdot b^{-1}) = 1$
 $\Rightarrow ab^{-1} \in \text{Ker}(f) \Rightarrow a \cdot b^{-1} = 1_{G_1} \Rightarrow a = b$

- (c)
 Sei $\tilde{a} \in f^{-1}(b)$
 $\Leftrightarrow f(\tilde{a}) = b = f(a)$
 $\Leftrightarrow f(a^{-1}\tilde{a}) = 1_{G_2}$
 $\Leftrightarrow a^{-1}\tilde{a} \in \text{Ker}(f)$
 $\Leftrightarrow \tilde{a} \in a \cdot \text{Ker}(f)$ q.e.d.

Ebenso:

$$\begin{aligned} f(\tilde{a}) &= b = f(a) \\ \Leftrightarrow f(\tilde{a}a^{-1}) &= 1_{G_2} \\ \Leftrightarrow \tilde{a}a^{-1} &\in \text{Ker}(f) \\ \Leftrightarrow \tilde{a} &\in \text{Ker}(f) \cdot a \end{aligned}$$

(2.17) Definition

Sei G Gruppe, $H \subseteq G$ Untergruppe
 H heißt **Normalteiler** in G , wenn $\forall a \in G : a \cdot H = H \cdot a$
 $\left(\begin{aligned} &\Leftrightarrow \forall h \in H \exists h' \in H : a \cdot h = h' \cdot a \\ &\Leftrightarrow \forall h \in H \forall a \in G : a \cdot h \cdot a^{-1} \in H \end{aligned} \right)$

(2.18) Satz

- (1) Ist $H \subseteq G$ Kern eines Homomorphismus $G \xrightarrow{f} \tilde{G}$, so ist H Normalteiler.
 (2) Ist umgekehrt H Normalteiler, so existiert eine Gruppe $\tilde{G}$ und ein Homomorphismus, $G \xrightarrow{f} \tilde{G}$ mit $\text{Ker}(f) = H$

Beweis:

(1) (c) von (2.17)

(2.19) LemmaSeien $a, a', b, b' \in G$, $H \subseteq G$ NormalteilerFalls $a \sim a'$ d.h. $a'^{-1} \cdot a \in H$ und $b \sim b'$ d.h. $b'^{-1} \cdot b \in H$

$$\Rightarrow a \cdot b \sim a' b' \quad \wedge \quad a^{-1} \sim a'^{-1}$$

Beweis:

$$\begin{aligned} ab \sim a'b' &\Leftrightarrow (a'b')^{-1}ab \in H \\ &\Leftrightarrow b'^{-1} \underbrace{a'^{-1}a}_{:=h} b \in H \\ &\Leftrightarrow b'^{-1}hb \in H \\ &\exists b' \in H : h'b'^{-1} = b'^{-1} \cdot h \\ &\Rightarrow b'^{-1}hb = h' \underbrace{b'^{-1}b}_{\in H} \in H \end{aligned}$$

$$\begin{aligned} a \sim a' &\Rightarrow \underbrace{a'^{-1}a}_h \in H \\ &\Rightarrow a = a'h \Rightarrow a^{-1} = h^{-1} \cdot a'^{-1} \\ &\exists \tilde{h} \in H \\ &h^{-1}a'^{-1} = a'^{-1}\tilde{h} \\ &\Rightarrow a^{-1} \sim a'^{-1} \end{aligned}$$

$[a]_{\sim} \cdot [b]_{\sim} = [a \cdot b]_{\sim}$ ist eine wohldefinierte Verknüpfung.
 Diese macht G/H zu einer Gruppe

$$[a]_{\sim}^{-1} = [a^{-1}]_{\sim}$$

zu (2.18)(2)Sei $\tilde{G} = G/H$ Sei $G \xrightarrow{f} G/H$ f ist Homomorphismus
 $a \mapsto [a]_{\sim}$

$$\text{Ker}(f) = H$$