§ 4 Homomorphismen von Halbgruppen und Gruppen

M ↓

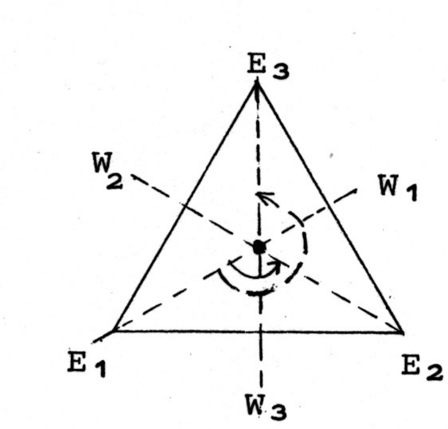
Bei der Betrachtung der Gruppe $\mathfrak{S}_3$ hatten wir auf die Ähnlichkeit im Verhalten der Permutationen von $\{1, 2, 3\}$ mit dem der Symmetrien (Deckbewegungen) eines gleichseitigen Dreiecks hingewiesen. Diesen Zusammenhang zwischen der Gruppe

$$\mathfrak{S}_3 = (\{\delta_0, \delta_1, \delta_2, \sigma_1, \sigma_2, \sigma_3\}, \circ) \qquad \text{(s. Figur 3.3 !)}$$

und der Gruppe

$$\mathfrak{D}_3 = (\{D_0, D_{120}, D_{240}, S_{W_1}, S_{W_2}, S_{W_3}\}, \circ)$$

(mit D_i als der Drehung um den Schwerpunkt des Dreiecks um $i°$ und S_{W_j} als der Spiegelung an der Halbierenden des Winkels im Punkt E_j, vgl. Figur 4.1)



Figur 4.1: Zur Symmetriegruppe eines gleichseitigen Dreiecks

wollen wir nun präzisieren:
Es existiert eine Bijektion $f : \{D_0, \dots, S_{w_3}\} \to \{\delta_0, \dots, \sigma_3\}$, definiert durch $D_{i \cdot 120} \mapsto \delta_i$ $(i = 0, 1, 2)$ und $S_{W_j} \mapsto \sigma_j$. Diese Zuordnung allein reicht nicht zur Beschreibung aus; es wären nur Eigenschaften der zugrunde liegenden Mengen in Beziehung gebracht („gleiche Kardinalzahl"), nicht die der Verknüpfungen, wie z.B.

$$\begin{array}{ccccc} D_{120} & \circ & S_{W_1} & = & S_{W_3} \\ \updownarrow & & \updownarrow & & \updownarrow \\ \delta_1 & \circ & \sigma_1 & = & \sigma_3 \end{array}$$

oder allgemeiner $f(B_1 \circ B_2) = f(B_1) \circ f(B_2)$ für $B_1, B_2 \in \{D_0, \dots, S_{W_3}\}$.
Mit Abbildungen, die in diesem Sinne „mit der Gruppenstruktur verträglich" sind, wollen wir uns beschäftigen. Derartige Bijektionen bestehen zwischen solchen Gruppen, die mit den Mitteln der Gruppentheorie nicht unterschieden werden können. Aber auch nicht-bijektive strukturbeachtende Abbildungen von (Halb-)Gruppen sind von Bedeutung, übertragen sich doch auch so viele Eigenschaften auf die Bildstruktur; z.B. werden Untergruppen auf Untergruppen abgebildet.
Als **Beispiel** für eine **strukturverträgliche Abbildung**, die keine Bijektion ist, betrachten wir die „kanonische" Abbildung von $\mathbb{Z}$ auf die Menge der Äquivalenzklassen $\mod m$ (für $m \in \mathbb{N}$ fest gewählt): Bezeichnen wir mit $\overline{x}$ die „Restklasse[32] " $\{y \in \mathbb{Z} : y \equiv x \pmod m\}$ von $x \in \mathbb{Z}$, mit $\mathbb{Z}_m$ die Menge all

[32]Zur Erklärung des Namens: $y \equiv x \pmod m$ bedeutet, dass m Teiler von $y - x$ ist und damit x und y den gleichen Rest bei der Division durch m haben.
Beispiel: $5 \equiv 8 \pmod 3$ heißt u.a., dass 5 und 8 den gleichen Rest, nämlich 2, bei der Division durch 3 besitzen.

dieser Restklassen (also $\mathbb{Z}_m := \mathbb{Z}/_{\equiv \pmod m}$), und definieren wir durch

$$\overline{x} + \overline{y} := \overline{x+y} \quad \text{für alle } x, y \in \mathbb{Z}$$

eine Addition auf $\mathbb{Z}_m$, so gilt (Übungsaufgabe): Diese Addition ist wohldefiniert, d.h. $\overline{x} + \overline{y}$ ist – wegen $\overline{x} = \overline{x_1} \wedge \overline{y} = \overline{y_1} \Rightarrow \overline{x} + \overline{y} = \overline{x_1} + \overline{y_1}$ – von den Repräsentanten x und y unabhängig, und

$$(\mathbb{Z}_m, +) \text{ ist eine kommutative Gruppe.}$$

Für die kanonische Abbildung

$$\kappa : \begin{cases} \mathbb{Z} \to \mathbb{Z}_m \\ x \ \mapsto \overline{x} \end{cases}$$

ist nach Definition der Addition die Gleichung $\kappa(x+y) = \kappa(x) + \kappa(y)$ für alle $x, y \in \mathbb{Z}$ erfüllt.

Beispiel. $\mathbb{Z} \to \mathbb{Z}_2$ mit $z \mapsto \overline{z} = \begin{cases} \overline{0} & \text{für } z \text{ gerade} \\ \overline{1} & \text{für } z \text{ ungerade} \end{cases}$ ist eine strukturverträgliche Abbildung (Homomorphismus) von $(\mathbb{Z}, +)$ auf $(\mathbb{Z}_2, +)$.

Ähnlich gilt für die durch $\overline{x} \cdot \overline{y} := \overline{x \cdot y}$ (wohl-)definierte Multiplikation:

$$(\mathbb{Z}_m, \cdot) \text{ ist eine kommutative Halbgruppe,}$$

und κ ist eine auch mit dieser Struktur verträgliche Abbildung von $\mathbb{Z}$ auf $\mathbb{Z}_m$.

Beispiel (Anwendung). $\boxed{\text{„Neunerprobe“}}$ Gegeben sei $n \in \mathbb{N}$! Wir fragen: Ist 9 ein Teiler von n ?

Seien $a_0, \ldots, a_k$ die Ziffern der Dezimaldarstellung von n, also $n = \sum_{i=0}^{k} a_i 10^i$ (nach Identifikation der Ziffern $0, \ldots, 9$ mit den entsprechenden Zahlen). Gehen wir zur Kongruenz mod 9 über, so lautet die Frage: $\overline{n} = \overline{0}$? Nun ist $\overline{10^i} = \overline{10}^i = (\overline{1})^i = \overline{1^i} = \overline{1}$ und

$$\overline{n} = \overline{\sum_{i=0}^{k} a_i \cdot 10^i} = \sum_{i=0}^{k} \overline{a_i \cdot 10^i} = \sum_{i=0}^{k} \overline{a_i} \cdot \overline{10^i} = \sum_{i=0}^{k} \overline{a_i} \cdot \overline{1} = \overline{\sum_{i=0}^{k} a_i}.$$

Daher gilt: ***n* ist genau dann durch 9 teilbar, wenn die Quersumme von *n* (in der Dezimaldarstellung) durch 9 teilbar ist.**

Zahlenbeispiel. 9 teilt 49068, da $9 | (4+9+0+6+8)$.

Untersuchen Sie analog die „ **Dreierprobe** “ und die „ **Elferprobe** “ !

↑
M

4.1 Definition. (Halb-) Gruppen-Homomorphismen, -Isomorphismen

Seien $(H_1, *_1)$ und $(H_2, *_2)$ Halbgruppen!

(a) Eine Abbildung $f : H_1 \to H_2$ heißt **Homomorphismus** (Hom) von H_1 in H_2, falls gilt:
$$\forall a, b \in H_1 : f(a *_1 b) = f(a) *_2 f(b).$$

(b) Ist f zusätzlich bijektiv, so heißt f **Isomorphismus** (Iso). Ein Isomorphismus einer Halbgruppe auf sich selbst (also für $H_1 = H_2$) heißt **Automorphismus** (Aut).

(c) $(H_1, *_1)$ und $(H_2, *_2)$ heißen **isomorph**, falls es einen Isomorphismus von $(H_1, *_1)$ auf $(H_2, *_2)$ gibt.
In Zeichen : $H_1 \cong H_2$.

M
↓

Beispiele.

(1) Die am Anfang dieses Paragraphen angegebene Abbildung zwischen der Gruppe $\mathfrak{D}_3$ der Deckabbildungen eines gleichseitigen Dreiecks und der symmetrischen Gruppe $\mathfrak{S}_3$ ist ein (Gruppen-) Isomorphismus. Also gilt $\mathfrak{D}_3 \cong \mathfrak{S}_3$.

(2) Für die Würfelgruppe $\mathfrak{W}$ (vgl. Anhang zu §3) gilt $\mathfrak{W} \cong \mathfrak{S}_4$.

(3) Die Abbildung „$^-$ “ : $\begin{cases} \mathbb{Z} \to \mathbb{Z}_m \\ x \mapsto \overline{x} \end{cases}$ liefert einen (surjektiven) Homomorphismus der Gruppe $(\mathbb{Z}, +)$ auf die Gruppe $(\mathbb{Z}_m, +)$, sowie einen (surjektiven) Homomorphismus der Halbgruppe $(\mathbb{Z}, \cdot)$ auf die Halbgruppe $(\mathbb{Z}_m, \cdot)$.

(4) Die Abbildung $\begin{cases} \overline{0} \mapsto g \\ \overline{1} \mapsto u \end{cases}$ liefert einen Isomorphismus von $(\mathbb{Z}_2, +)$ auf $(\{g, u\}, \oplus)$ (s. §1 !).

(5) $g : \begin{cases} \mathbb{Z} \to \mathbb{R}^* \\ z \mapsto r^z \end{cases}$ (für $r \in \mathbb{R}^*$ fest) ist ein Homomorphismus von $(\mathbb{Z}, +)$ in $(\mathbb{R}^*, \cdot)$.

Beweis. g ist wohldefiniert, $g(z_1 + z_2) = r^{z_1+z_2} = r^{z_1} \cdot r^{z_2} = g(z_1) \cdot g(z_2)$. □

(6) $h : \begin{cases} \mathbb{C} \to \mathbb{C} \\ z = a + bi \mapsto \overline{z} = a - bi \end{cases}$ ist ein Isomorphismus von $(\mathbb{C}, +)$ auf sich (Automorphismus).
$h|_{\mathbb{C}^* \to \mathbb{C}^*}$ ist ein Isomorphismus von $(\mathbb{C}^*, \cdot)$ auf sich.

(7) Seien $(\mathbb{R}^2, +) := (\{(x, y) : x, y \in \mathbb{R}\},$ komponentenweise Addition) und
$(\mathcal{V}, +) := \left(\left\{ \begin{pmatrix} x \\ y \end{pmatrix}_{\vec{e}_1, \vec{e}_2} : x, y \in \mathbb{R} \right\}, \text{ komponentenweise Addition} \right)$; dann ist
$$f : \begin{cases} \mathbb{R}^2 \to \mathcal{V} \\ (x, y) \mapsto \begin{pmatrix} x \\ y \end{pmatrix}_{\vec{e}_1, \vec{e}_2} \end{cases}$$ ein Isomorphismus von $(\mathbb{R}^2, +)$ auf $(\mathcal{V}, +)$.

(8) $\mathrm{pr}_1 : \begin{cases} \mathcal{V} \to \mathbb{R} \\ \begin{pmatrix} x \\ y \end{pmatrix}_{\vec{e}_1,\vec{e}_2} \mapsto x \end{cases}$ ist Homomorphismus von $(\mathcal{V}, +)$ auf $(\mathbb{R}, +)$.

Beweis.
$$\mathrm{pr}_1 \left[\begin{pmatrix} x_1 \\ y_1 \end{pmatrix}_{\vec{e}_1,\vec{e}_2} + \begin{pmatrix} x_2 \\ y_2 \end{pmatrix}_{\vec{e}_1,\vec{e}_2} \right] = \mathrm{pr}_1 \begin{pmatrix} x_1 + x_2 \\ y_1 + y_2 \end{pmatrix}_{\vec{e}_1,\vec{e}_2} = x_1 + x_2 = \mathrm{pr}_1 \begin{pmatrix} x_1 \\ y_1 \end{pmatrix}_{\vec{e}_1,\vec{e}_2} + \mathrm{pr}_1 \begin{pmatrix} x_2 \\ y_2 \end{pmatrix}_{\vec{e}_1,\vec{e}_2}. \quad \square$$

↑
M

4.2 Hilfssatz. Bilder von neutralem Element und von Inversen

Seien $(G, *)$ Gruppe mit neutralem Element e, $(G', *')$ Gruppe mit neutralem Element e' und $f : G \to G'$ ein Homomorphismus. Dann gilt:

(a) $f(e) = e'$;

(b) $\forall a \in G : f(a^{-1}) = [f(a)]^{-1}$.

D.h.: Bei einem Gruppenhomomorphismus wird das neutrale Element auf das neutrale Element und das Inverse eines Elements auf das Inverse des Bildelements abgebildet.

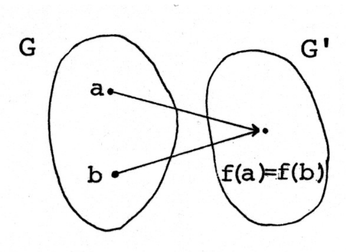
Beweis. (a) $f(e) *' e' = f(e) = f(e * e) = f(e) *' f(e) \underset{\text{Mult. mit } [f(e)]^{-1}}{\Rightarrow} e' = f(e)$;

(b) $f(a^{-1}) *' f(a) \underset{(4.1(\mathrm{a}))}{=} f(a^{-1} * a) = f(e) \underset{(\mathrm{a})}{=} e' \Rightarrow f(a^{-1}) = [f(a)]^{-1}$.

$\square$

M
↓

Bei einem Homomorphismus werden u.U. mehrere Elemente der Urbildgruppe auf dasselbe Element der Bildgruppe abgebildet. (Beispiele?) Wir untersuchen „Urbildmengen" der Elemente von G'.



Figur 4.2: Bildelement mit zwei Urbildern

Sei also $f(a) = f(b)$ (vgl. Figur 4.2 !); dann gilt
$e' = f(a)^{-1} *' f(b) \underset{4.2(\mathrm{b})}{=} f(a^{-1}) *' f(b) = f(a^{-1} * b)$, d.h.
$f(a) = f(b) \Rightarrow a^{-1} * b \in f^{-}(\{e'\})$ (und umgekehrt).

Es ist also sinnvoll, sich näher mit $f^{-}(\{e'\})$ zu beschäftigen; Ziel dieses Paragraphen ist der Nachweis, dass (erstaunlicher Weise) durch diese Menge f schon weitgehend festgelegt ist.

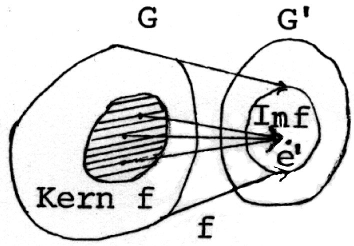
↑
M

4.3 Definition. Kern, Bild eines Homomorphismus

Seien $(G,*)$, $(G',*')$ Gruppen mit neutralem Element e bzw. e' und $f: G \to G'$ Homomorphismus. Dann heißt

$\operatorname{Kern} f := \{x \in G : f(x) = e'\} = f^-(\{e'\})$ der **Kern** von f (vgl. Figur 4.3 !) und

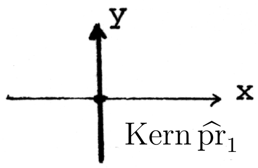
$\operatorname{Bild} f := \operatorname{Im} f := \{f(x) : x \in G\} = f(G)$ das **Bild** von f.



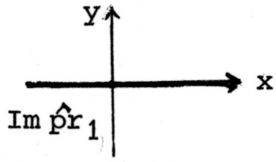
Figur 4.3: Kern f und Bild f

Beispiele.

1. $\widehat{\mathrm{pr}}_1 : \begin{cases} \mathbb{R}^2 \to \mathbb{R}^2 \\ (x,y) \mapsto (x,0) \end{cases}$ ist Homomorphismus von $(\mathbb{R}^2,+)$ in $(\mathbb{R}^2,+)$.



Figur 4.4: $\operatorname{Kern} \widehat{\mathrm{pr}}_1 = \{(0,y) : y \in \mathbb{R}\}$



Figur 4.5: $\operatorname{Bild} \widehat{\mathrm{pr}}_1 = \{(x,0) : x \in \mathbb{R}\}$

2. Für $m \in \mathbb{N}$ ist $\kappa : \begin{cases} \mathbb{Z} \to \mathbb{Z}_m \\ x \mapsto \overline{x} \end{cases}$ Homomorphismus von $(\mathbb{Z},+)$ auf $(\mathbb{Z}_m,+)$ (s.o.!).

   Es gilt $\operatorname{Bild} \kappa = \mathbb{Z}_m$ (da κ surjektiv ist) und

   $\operatorname{Kern} \kappa = \kappa^-(\overline{0}) = \{x \in \mathbb{Z} : x \equiv 0 \mod m\} = \{x \in \mathbb{Z} : m|x\} = \{my : y \in \mathbb{Z}\} =: m\mathbb{Z}$.

4.4 Hilfssatz: Kern und Bild als Untergruppen

> Seien $(G,*)$, $(G',*')$ Gruppen und $f : G \to G'$ Homomorphismus. Dann gilt:
>
> (1) $\operatorname{Kern} f$ ist UG von $(G,*)$.
>
> (2) $\operatorname{Bild} f$ ist UG von $(G',*')$.

Beweis. (1) $f(e) = e' \Rightarrow e \in \operatorname{Kern} f \Rightarrow \operatorname{Kern} f \neq \emptyset$.

Seien $u, v \in \operatorname{Kern} f$, also $f(u) = e' = f(v)$. Dann gilt

$$f(u * v^{-1}) \underset{(4.1)\text{a}}{=} f(u) *' f(v^{-1}) \underset{(4.2)\text{b}}{=} f(u) *' f(v)^{-1} = e' *' e'^{-1} = e'$$

Also $u * v^{-1} \in \operatorname{Kern} f$. Aus dem Untergruppen-Kriterium (3.16) folgt die Behauptung.

(2) $e' = f(e) \in f(G) = \operatorname{Bild} f \Rightarrow \operatorname{Bild} f \neq \emptyset$.

Seien $u', v' \in \operatorname{Bild} f$; dann $\exists u, v \in G : f(u) = u'$ und $f(v) = v'$; damit gilt
$$u' *' (v')^{-1} = f(u) *' (f(v))^{-1} = f(u) *' f(v^{-1}) = f(u * v^{-1}) \in \operatorname{Bild} f.$$
Wieder nach (3.16) folgt die Behauptung.

□

4.5 Hilfssatz: Kern bei injektiven Homomorphismen

Ist f Gruppenhomomorphismus, dann gilt
$$f \text{ injektiv} \iff \operatorname{Kern} f = \{e\} \quad .$$

Beweis. „$\Rightarrow$" Ist f injektiv, so hat e' höchstens ein Urbild (und wegen $f(e) = e'$ genau eins).

„$\Leftarrow$" Seien $a, b \in G$ mit $f(a) = f(b)$, dann folgt
$f(a^{-1} * b) = f(a)^{-1} *' f(b) = f(b)^{-1} *' f(b) = e'$,
also $a^{-1} * b \in \operatorname{Kern} f \underset{\text{(nach Voraussetzung)}}{=} \{e\}$ und damit $a = b$.

□

Weiter oben (nach (4.2)) und eben hatten wir gesehen, dass für einen Homomorphismus f gilt:
$$f(a) = f(b) \Rightarrow a^{-1} * b \in f^{-}(\{e'\}) = \operatorname{Kern} f \quad (\text{d.h. } b \in a * \operatorname{Kern} f).$$
Ist umgekehrt $b \in a * \operatorname{Kern} f$, so folgt
$$f(b) \in f(a * \operatorname{Kern} f) = f(a) *' f(\operatorname{Kern} f) = f(a) *' \{e'\} = \{f(a)\}, \text{ also } f(b) = f(a).$$
Somit gilt (vgl. Figur 4.6 !) in multiplikativer Schreibweise der erste Teil von:

4.6 Hilfssatz: Volle Urbilder

Seien $(G, \cdot)$ und $(G', \cdot')$ Gruppen und $f : G \to G'$ Homomorphismus. Dann gilt für jedes $a \in G$:

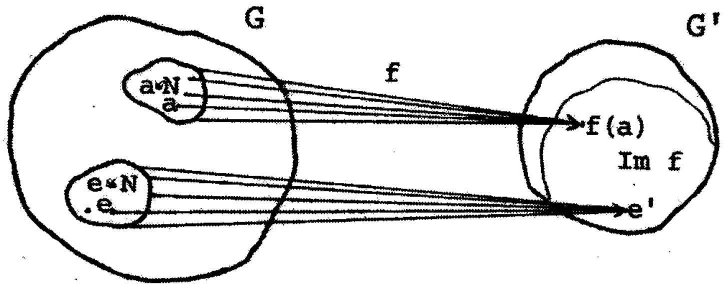
Das volle Urbild von $f(a)$ ist gleich $a \cdot \operatorname{Kern} f$ und (s.u.) gleich $\operatorname{Kern} f \cdot a$.

4.7 Definition: Nebenklasse nach einer Untergruppe

Sei $(G, \cdot)$ Gruppe und U Untergruppe von G. Für jedes $a \in G$ heißt

$a \cdot U$ **linke Nebenklasse** von U in G
$U \cdot a$ **rechte Nebenklasse** von U in G

Achtung: Manche Autoren benutzen umgekehrte Bezeichnungen: $a \cdot U$ rechte Nebenklassen etc.



Figur 4.6: Volle Urbilder (mit $N := \text{Kern}\, f$)

Anmerkung. Was für die Nebenklassen von $\text{Kern}\, f$ als volle Urbildmengen offensichtlich ist, gilt auch für die Nebenklassen einer beliebigen Untergruppe U:
Die rechten (bzw. linken) Nebenklassen von U in G bilden eine Partition der Menge G. (Beweis ...)

Jedes Element einer Nebenklasse heißt **Repräsentant** dieser Nebenklasse.

Beispiel. Für $m \in \mathbb{Z}$ ist $(m\mathbb{Z}, +)$ UG von $(\mathbb{Z}, +)$; die linken und rechten Nebenklassen von $m\mathbb{Z}$ in $(\mathbb{Z}, +)$ haben die Form $r + m\mathbb{Z}$ $(= \overline{r})$. (Ist $r \in \{0, \ldots, m-1\}$, so hat, wie schon erwähnt, jedes Element aus $r + m\mathbb{Z}$ bei der Division durch m den Rest r, weswegen man auch von **Restklassen** spricht). Ferner gilt:

$$\mathbb{Z} = \dot{\bigcup_{r=0}^{m-1}} (r + m\mathbb{Z}) = \dot{\bigcup_{r=0}^{m-1}} \overline{r} \quad (\text{Überdeckung von } \mathbb{Z} \text{ durch Restklassen} \mod m).$$

M ↓

Unser nächstes Ziel ist die Konstruktion von neuen Gruppen (aus einer gegebenen Gruppe G), die in engem Zusammenhang mit Homomorphismen von G stehen.
Auf den Restklassen $\mod m$ lässt sich, wie wir sahen, eine Addition definieren, die mit der Addition auf $\mathbb{Z}$ zusammenhängt. Für Nebenklassen einer nicht-kommutativen Gruppe nach einer beliebigen UG ist es im allgemeinen nicht möglich, auf ähnliche Weise wie im oben erwähnten Fall eine Verknüpfung zu definieren. Dafür benötigt man eine zusätzliche Eigenschaft der UG, die aber von $\text{Kern}\, f$ erfüllt wird.

↑ M

Aus $f(a) = f(b)$ erhält man nämlich auch $f(b \cdot a^{-1}) = f(b) \cdot' f(a^{-1}) = f(b) \cdot' f(a)^{-1} = e'$, also $b \in \text{Kern}\, f \cdot a$; da $f(\text{Kern}\, f \cdot a) = f(a)$ ist, folgt daraus: Auch $(\text{Kern}\, f) \cdot a$ ist das volle Urbild von $f(a)$. Es gilt also:

$$(\text{Kern}\, f) \cdot a = a \cdot (\text{Kern}\, f).$$

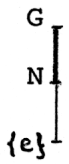
4.8 Definition: Normalteiler

Eine Untergruppe N der Gruppe $(G, \cdot)$ heißt **Normalteiler** von G, wenn gilt:

$$\forall a \in G: \; a \cdot N = N \cdot a.$$

Schreibweise: $N \trianglelefteq G$. Symbolische Darstellung s. Figur 4.7 !

Figur 4.7: Symbolische Darstellung von $N \trianglelefteq G$



Beispiel. Bei einer kommutativen Gruppe ist jede Untergruppe Normalteiler.

4.9 Satz: Kern als Normalteiler

Sind G, G' Gruppen und ist $f : G \to G'$ Homomorphismus, dann gilt:

$$\text{Kern}\, f \ \text{ ist Normalteiler von } G.$$

Bei Nebenklassen nach einem Normalteiler N ist es möglich, mit Hilfe der Verknüpfung von G eine Verknüpfung auf G/N sinnvoll zu definieren:

4.10 Definition: G/N

Sei $(G,*)$ Gruppe und N Normalteiler von $(G,*)$. Dann definiert man:

1. $G/N := \{a * N : a \in G\}$.
2. Für $a, b \in G$ sei
   $(a*N)\tilde{*}(b*N) := (a*N)*(b*N)$ (in Komplexschreibweise, vgl. (3.15) !)

Man beachte, dass die Bildung von $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$ und die Definition der Addition auf $\mathbb{Z}_m$ einen Spezialfall der eben erfolgten darstellt.

4.11 Satz: Faktorgruppe

Seien $(G,*)$ Gruppe, N Normalteiler von $(G,*)$ und G/N und $\tilde{*}$ wie eben definiert. Dann gilt:

$$(G/N, \tilde{*}) \text{ ist eine Gruppe,}$$

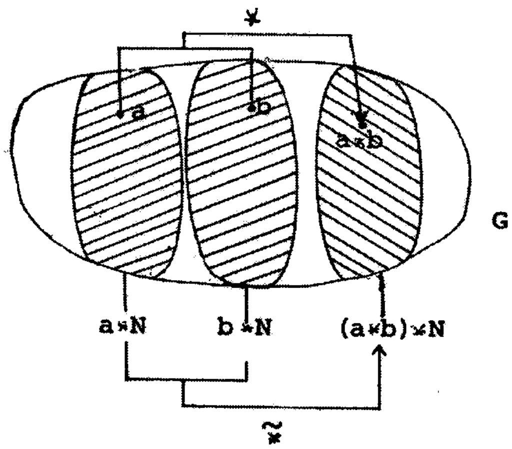
die so genannte **Faktorgruppe** von G nach N.

Anmerkung. Es gilt $\boxed{(a*N)\tilde{*}(b*N) = (a*b)*N}$ (s.u.). Auch diese Beziehung wird oft zur Definition von $\tilde{*}$ herangezogen; dann ist jedoch nachzuweisen, dass $\tilde{*}$ wohldefiniert ist.

Beweis. (G1) Seien $a*N, b*N \in G/N$ gegeben. Dann gilt (gleichzeitig ein Beweis der Anmerkung):

$$\begin{aligned}(a*N)\tilde{*}(b*N) &\underset{\text{Def.}}{=} (a*N)*(b*N) \underset{\text{Assoz.}}{=} a*(N*b)*N \\ &\underset{\text{N Nt.}}{=} a*b*N*N \underset{(N,*)\text{ abgeschl.}}{=} (a*b)*N\ .\end{aligned}$$

Insbesondere ist
$(a * N)\tilde{*}(b * N) \in G/N$.
Also:
$\tilde{*}$ ist innere Verknüpfung auf G/N
und
$\tilde{*}$ entspricht der Verknüpfung $*$ der Repräsentanten.



Figur 4.8: Zur Verknüpfung der Faktorgruppe

(G2) Unter Verwendung von (G1) unmittelbare Folgerung aus der Assoziativität von $(G, *)$.

(G3) $N = e * N$ ist neutrales Element: $N \in G/N$

$$N\tilde{*}(a * N) = (e * N)\tilde{*}(a * N) \underset{\text{s.o.}}{=} (e * a) * N = a * N$$

$$(a * N)\tilde{*}N \underset{\text{analog}}{=} a * N.$$

(G4) Sei $M \in G/N$; dann existiert $a \in G : M = a * N$, und es existiert $a^{-1} \in G$.

Behauptung: $a^{-1} * N$ ist Inverse von M.

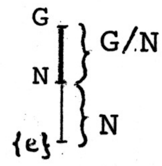
Beweis. $a^{-1} * N \in G/N$;

$$M\tilde{*}(a^{-1} * N) = (a * N)\tilde{*}(a^{-1} * N) = (a * a^{-1}) * N = N$$

$$(a^{-1} * N)\tilde{*}M = (a^{-1} * N)\tilde{*}(a * N) = (a^{-1} * a) * N = N.$$

Damit ist die Behauptung gezeigt.

Also erfüllt $(G/N, \tilde{*})$ die Gruppenaxiome. $\square$



Figur 4.9: Symbolische Darstellung der Faktorgruppe (vgl. auch Figur 4.7 !)

Wir betrachten nun die Abbildung, die jedem Element x von G diejenige Nebenklasse nach N zuordnet, in der x liegt. (Vgl. $r \mapsto \overline{r}$ im Falle $\mathbb{Z} \longrightarrow \mathbb{Z}_m$).

4.12 Hilfssatz: kanonischer Homomorphismus

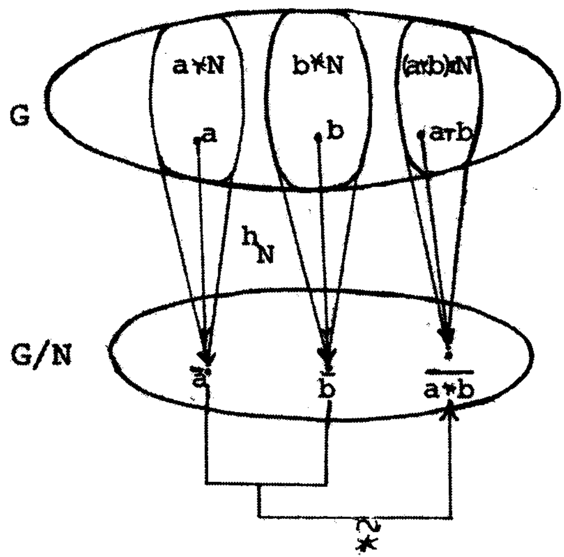
Sei N Normalteiler der Gruppe $(G, *)$. Dann ist

$$h_N : \begin{cases} G \to G/N \\ x \ \mapsto x * N \end{cases}$$

ein Homomorphismus von $(G, *)$ nach $(G/N, \tilde{*})$, der so genannte **natürliche (kanonische) Homomorphismus** von G auf G/N, und es gilt:

$$\operatorname{Kern} h_N = N.$$

Anmerkung (1). Mit $\overline{a} := a * N = h_N(a)$ gilt $\overline{a} \,\tilde{*}\, \overline{b} = \overline{a * b}$; (vgl. Figur 4.10 !).



Figur 4.10: Zur Wirkung des natürlichen Homomorphismus

Anmerkung (2). Aus (4.9) und (4.12) folgt: Jeder Kern eines Gruppenhomomorphismus ist Normalteiler, und umgekehrt ist jeder Normalteiler einer Gruppe Kern eines geeigneten Homomorphismus.

Beweis von 4.12. (a) $h_N : G \to G/N$ mit $a \mapsto \overline{a} = a * N$ ist wohldefiniert, und es gilt:

$h_N(a * b) = (a * b) * N = (a * N)\tilde{*}(b * N) = h_N(a)\tilde{*}h_N(b)$.

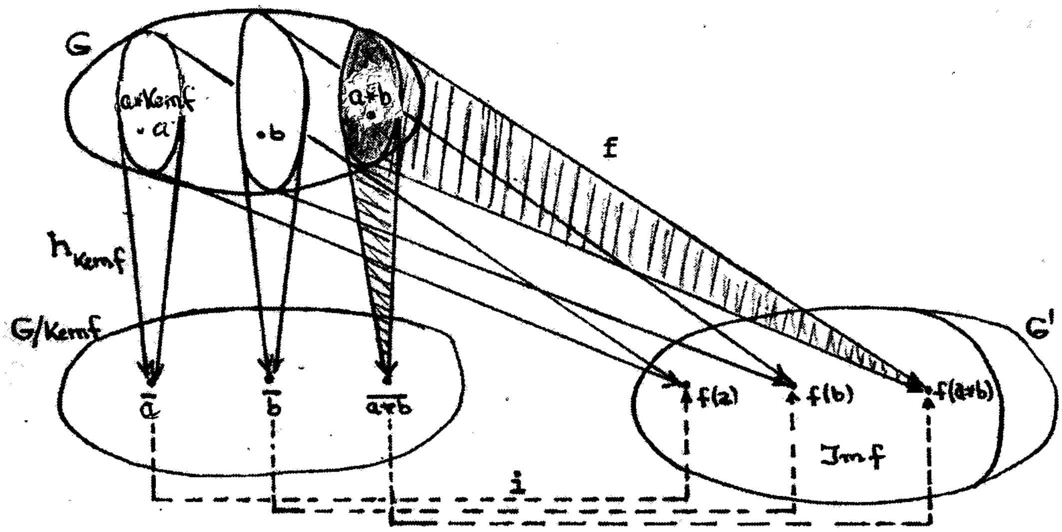
Also ist h_N Homomorphismus von G auf G/N.

(b) $x \in \operatorname{Kern} h_N \Leftrightarrow x * N = N \Leftrightarrow x \in N$.

□

Anmerkung (3). Damit ist ein Zwischenziel erreicht: Zu jeder Gruppe G können wir homomorphe Bilder konstruieren. Nun ist die Frage: Gibt es weitere homomorphe Bilder?

Sei uns daher ein beliebiger Homomorphismus $f : G \to G'$ gegeben. Wählen wir nun speziell N als $\operatorname{Kern} f$, so ergibt sich das Diagramm der Figur 4.11.



Figur 4.11 Zum Homomorphiesatz

4.13 Homomorphiesatz für Gruppen

Seien G, G' Gruppen und $f : G \to G'$ ein Homomorphismus. Dann gilt:

$$\boxed{G/\operatorname{Kern} f \cong \operatorname{Bild} f}$$

Insbesondere ist $\operatorname{Bild} f$ bis auf Isomorphie durch G und $\operatorname{Kern} f$ bestimmt.

Beweis. (a) Die Zuordnung $i : G/\operatorname{Kern} f \to \operatorname{Bild} f$ mit $a * \operatorname{Kern} f \mapsto f(a)$ ist wohldefiniert (d.h. insbesondere rechtseindeutig); denn aus zwei möglichen Darstellungen einer Nebenklasse $a * \operatorname{Kern} f = b * \operatorname{Kern} f$ folgt

$$\{f(a)\} = f(a * \operatorname{Kern} f) = f(b * \operatorname{Kern} f) = \{f(b)\}.$$

(b) i ist Homomorphismus von $(G/\operatorname{Kern} f, *)$ in $(\operatorname{Bild} f, *'|_{\operatorname{Bild} f})$; denn es gilt:

$$\begin{aligned} i[(a * \operatorname{Kern} f)\tilde{*}(b * \operatorname{Kern} f)] &\underset{\text{Eigensch. von } \tilde{*}}{=} i[(a * b) * \operatorname{Kern} f] \underset{\text{Def. v. } i}{=} f(a * b) \\ &\underset{f \text{ Hom.}}{=} f(a) *' f(b) = i[a * \operatorname{Kern} f] *' i[b * \operatorname{Kern} f]. \end{aligned}$$

(c) i ist surjektiv:

Sei $a' \in \operatorname{Bild} f$. Dann ex. $a \in G : f(a) = a'$; daraus folgt $a' = f(a) = i(a * \operatorname{Kern} f)$.

(d) i ist injektiv:

Nach Hilfssatz (4.5) reicht es zu zeigen, dass $\operatorname{Kern} i$ nur das neutrale Element, hier von $G/\operatorname{Kern} f$, enthält.

$$\begin{aligned}\operatorname{Kern} i &= \{a * \operatorname{Kern} f : a \in G \wedge i(a * \operatorname{Kern} f) = e'\} \\ &= \{a * \operatorname{Kern} f : a \in G \wedge f(a) = e'\} \\ &= \{a * \operatorname{Kern} f : a \in \operatorname{Kern} f\} = \{\operatorname{Kern} f\}.\end{aligned}$$

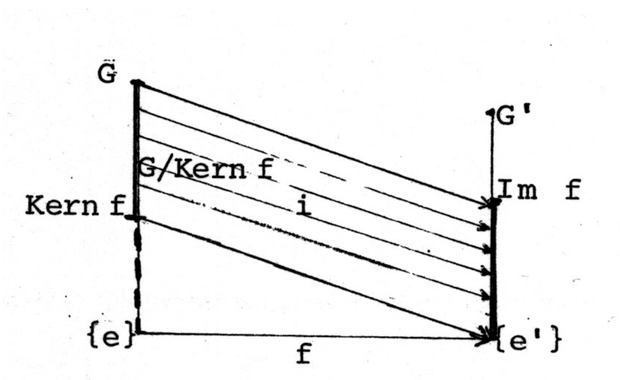
$\operatorname{Kern} f$ ist neutrales Element von $(G/\operatorname{Kern} f, \tilde{*})$ (s.o.).

Insgesamt ist also $(G/\operatorname{Kern} f, *) \cong (\operatorname{Bild} f, *'|_{\operatorname{Bild} f})$

$\square$

Damit ist geklärt, dass alle homomorphen Bilder einer Gruppe G isomorph zu Faktorgruppen von G sind. Kennt man also alle Normalteiler von G, so auch (zumindest theoretisch) die Struktur aller homomorphen Bilder von G. Homomorphismen sind insbesondere schon weitgehend durch ihren Kern festgelegt.

Eine symbolische Darstellung des Sachverhalts beim Homomorphiesatz zeigt Figur 4.12.



Figur 4.12: Symbolische Darstellung zum Homomorphiesatz

Übungsaufgaben

Aufgabe 4.1

(a) Zeigen Sie, dass eine ganze Zahl genau dann durch 3 teilbar ist, wenn ihre Quersumme durch 3 teilbar ist. („**Dreierprobe**").

(b) Wie kann (analog) eine „**Elferprobe**" aussehen?

Aufgabe 4.2

Sei G die Menge aller Elemente aus $\mathbb{Z}_9$, die eine multiplikative Inverse besitzen.
a) Zeigen Sie, dass $(G, \cdot)$ eine Gruppe ist, die von einem Element erzeugt wird.
b) Geben Sie zu jedem Element g aus G seine Ordnung[33] an!

[33] Dabei ist die Ordnung eines Gruppenelementes g definiert als die kleinste natürliche Zahl k mit $g^k = 1$.

Aufgabe 4.3 (Fortsetzung von Aufg. 3.2)
Definieren Sie eine Verknüpfung $\star$ auf $\mathbb{Z}_{10}$ derart, dass folgende Abbildung von der Gruppe der Symmetrien eines regelmäßigen 5–Ecks [34] in $(\mathbb{Z}_{10}, \star)$ ein Gruppenisomorphismus ist: $\mathfrak{D}_5 \longrightarrow \mathbb{Z}_{10}$ mit $D_{j \cdot 72°} \mapsto \overline{j}$ und $D_{j \cdot 72°} \circ S \mapsto \overline{j+5}$ (für $j = 0, \dots 4$).
Lösungshinweis: Unterscheiden Sie 4 Fälle!

Aufgabe 4.4 Sei C_n eine zyklische Gruppe (d.h. eine von einem Element erzeugte Gruppe) der endlichen Ordnung (Elementeanzahl) n und a ein erzeugendes Element von C_n ! Für jedes $k \in \{1, \dots, n\}$ ist dann folgende Abbildung ein Homomorphismus:

$$\varphi_k : C_n \to C_n \text{ mit } \varphi_k(x) = x^k \text{ für alle } x \in C_n.$$

Zeigen Sie, dass jeder Homomorphismus $\varphi : C_n \to C_n$ von dieser Form ist!
Lösungshinweis: Beachten Sie, dass φ schon durch k mit $\varphi(a) = a^k$ festgelegt ist.

Bemerkungen zur Abstraktheit

Eine Schwierigkeit beim Verstehen der gegenwärtigen Vorlesungs-Paragraphen ist die Abstraktheit der Begriffe. Statt der elementargeometrischen Vektoren, der Lösungen von Gleichungssystemen oder Differentialgleichungen bzw. von Codewörtern (s. Paragraph 1) werden *Platzhalter* für diese Objekte selbst zu Elementen der Betrachtung, die den ebenfalls abstrahierten Axiomen genügen.
Als weitere Schwierigkeit kommt hinzu, dass als Objekte nun auch Mengen zugelassen sind (z.B. Mengen von vektorgleichen Pfeilen, Restklassen von Zahlen, Nebenklassen von Unterstrukturen.) Beim Aufbau der abstrakten Algebra dient dieses ("geniale") Vorgehen aber der Anwendbarkeit auf viele Teilgebiete der Mathematik. Begriffe wie Gruppe, Ring, Körper, Vektorraum sind Grundsteine beim Aufbau vieler mathematischer Gebiete.
Die Behandlung von Gruppen und ihrer Homomorphismen (z.B. der Homomorphiesatz für Gruppen) dient als beabsichtigte Vorbereitung auf ähnliche Zusammenhänge bei Vektorräumen.
Gleichzeitig wird beim Bemühen um das Verständnis des Stoffes das Abstrahieren als eine *wesentliche mathematische Kompetenz* eingeübt.

[34] mit den Drehungen $D_{j \cdot 72°}$ um $j \cdot 72°$ um den Mittelpunkt und einer „Klappung“ S des 5–Ecks auf sich.