Gruppen

Werkzeuge

Einführung in die Algebra

03.11.2005

Symmetrische Gruppe Sn

Definition **(S_n):**

S_n bezeichne die Menge aller Permutationen der Menge N_n = {1, 2, … , n}, d.h. die Menge der bijektiven Abbildungen von N_n.

S_n heißt symmetrische Gruppe.

$\pi \in S_n$ *heißt Permutation vom Grade n*

$$\pi = \begin{pmatrix} 1 & 2 & 3 & \dots & n-1 & n \\ \pi[1] & \pi[2] & \pi[3] & \dots & \pi[n-1] & \pi[n] \end{pmatrix}$$

Symmetrische Gruppe Sn

Seien

$$\pi = \begin{pmatrix} 1 & 2 & \cdots & n \\ \pi(1) & \pi(2) & \cdots & \pi(n) \end{pmatrix} \text{ u. }$$

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix} \in S_n$$

① $$\pi \circ \sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \pi(\sigma(1)) & \pi(\sigma(2)) & \cdots & \pi(\sigma(n)) \end{pmatrix}$$

② Inverse $$\pi^{-1} = \begin{pmatrix} \pi(1) & \pi(2) & \cdots & \pi(n) \\ 1 & 2 & \cdots & n \end{pmatrix}$$

Symmetrische Gruppe Sn

Beispiel

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 4 & 2 & 1 & 6 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 3 & 4 & 2 & 1 & 5 \end{pmatrix} =$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 2 & 5 & 3 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 3 & 4 & 2 & 1 & 5 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 2 & 3 & 6 & 1 \end{pmatrix}$$

Symmetrische Gruppe Sn

Satz. |Sn| = n!

Beweis: Induktion

N= 1 trivial

Annahme: Satz richtig für n

Behauptung: Satz richtig für n+1

$$\pi = \begin{pmatrix} 1 & 2 & \cdots & n & n+1 \\ \pi(1) & \pi(2) & \cdots & \pi(n) & \pi(n+1) \end{pmatrix}$$

Induktionsannahme $\Rightarrow |S_{n+1}| = |S_n|(n+1) = (n+1)!$

Gruppenhomomorphismus

Definition

Seien G und G´ zwei Gruppen, wobei die jeweiligen neutralen Elemente mit $e \in G$ bzw. mit $f \in G$ bezeichnet seien.

Ist $\varphi : G \rightarrow G´$ eine Abbildung, dann nennen wir φ einen **Gruppenhomomorphismus**, falls sie die folgende Bedingung erfüllt

$$\boxed{\forall\ x; y \in G \text{ gilt } \varphi(xy) = \varphi(x)\,\varphi(y)}$$

und in diesem Fall erfülllt φ sogar die beiden weiteren Eigenschaften

$$\varphi(e) = f \text{ und } \varphi(x^{-1}) = \varphi(x)^{-1}$$

Gruppenhomomorphismen

Definition

Seien G,G` Gruppen.

1. Ist $\varphi : G \rightarrow G'$ eine Abbildung, dann nennen wir φ einen **Gruppenhomomorphismus**, falls sie die folgende Bedingung erfüllt

$$\forall\ x; y \in G \text{ gilt } \varphi(xy) = \varphi(x)\,\varphi(y)$$

2. Ein injektiver Gruppenhomomorphismus heißt auch **Monomorphismus**.

(Cf. griechisch **μονος einzig**, z.B. der Monarch als Alleinherrscher.)

3. Ein surjektiver Gruppenhomomorphismus heißt auch **Epimorphismus**.

(Cf. griechisch **επι darauf**, z.B. das Epizentrum eines Erdbebens, das auf der Erdoberfläche ¨uber dem Zentrum im Erdinneren liegt.)

Gruppenhomomorphismen

4. *Ein bijektiver Gruppenhomomorphismus heißt auch* <u>*Isomorphismus*</u>*. (Cf. griechisch ίσος derselbe, z.B. das Iso-top als Element am selben Platz im Periodensystem.)*

5. *Zwei Gruppen heißen* <u>*isomorph*</u> *genau dann, wenn es zwischen ihnen einen Isomorphismus gibt.*

6. *Ein Gruppenhomomorphismus einer Gruppe in sich selbst heißt auch* <u>*Endomorphismus*</u>*. (Cf. griechisch ενδο in hinein, z.B. die Endo-skopie, bei der man in den Körper hinein schaut.)*

Gruppenhomomorphismus
Beispiel

Innere Automorphismen : Sei g ein beliebiges Element einer Gruppe G. Die Abbildung

$$\varphi_g : G \to G \text{ definiert durch } \varphi_g(x) = g^{-1}xg \ (\forall\ x \in G)$$

ist ein Automorphismus von G.

(Beweis:
$$\begin{aligned} \varphi_g(xy) &= g^{-1}xyg = g^{-1}x(gg^{-1})yg = (g^{-1}xg)(g^{-1}yg) \\ &= \varphi_g(x) \cdot \varphi_g(y), \end{aligned}$$

also ist φ_g ein Endomorphismus. φ_g ist bijektiv, denn φ_g^{-1} ist Umkehrabbildung zu φ_g wie man leicht nachrechnet.)

Kategorie

Eine Kategorie C ist durch folgende Daten gegeben:

Kat 1) Eine Klasse O(C) (= Objekte der Kategorie).

Kat 2) Zu jedem Paar X,Y von Objekten eine Menge Mor(X,Y),

Schreibweise: $f \in \mathrm{Mor}(X,Y) = f\colon X \to Y$.

Statt Mor(X,Y) schreibt man auch MorC(X,Y) oder auch C(X,Y).

Kat 3) Komposition von Morphismen

$\mathrm{Mor}(X,Y) \times \mathrm{Mor}(Y,Z) \to \mathrm{Mor}(X,Z)$;

$(f,g) \quad \rightarrow \quad gf$ (oder $g \circ f$) notiert.

$$\begin{tikzcd} & Y \arrow[dr, "g"] & \\ X \arrow[ur, "f"] \arrow[rr, "h"'] \arrow[r, phantom, "="] & & Z \end{tikzcd}$$

$h = g \circ f$

Kategorie

Kat 4) Dabei müssen folgende Axiome erfüllt sein:

4.1(Assoziativität) Sind Morphismen

f: $X \to Y$, g: $Y \to Z$, h: $Z \to A$ gegeben, so gilt

$$(hg)f = h(gf).$$

4.2 (Identitäten) Zu jedem Objekt X gibt es einen Morphismus id_X in Mor(X,X) mit fo id_X = f und id_X og für und alle Morphismen f: $X \to Y$ und g: $W \to X$.

Beispiele von Kategorien

Die Kategorie Men der Mengen

OBJEKTE: Mengen

MORPHISMEN: Abbildungen

Die Kategorie Grp der Gruppen

OBJEKTE: Gruppen MORPHISMEN: Gruppen-Homorphismen

Die Kategorie Ab der abelschen Gruppen

OBJEKTE: Abelsche Gruppen

MORPHISMEN: Gruppen-Homorphismen

Die Kategorie k-Vekt der Vektorräume **(über einem festen Körper k) OBJEKTE: k-Vektorräume**

MORPHISMEN: k-lineare Abbildungen

Typen von Morphismen
- Monomorhpismus -

$$\begin{tikzcd} D \arrow[r, shift left, "f"] \arrow[r, shift right, "g"'] & A \arrow[r, "m"] & B \end{tikzcd}$$

Def. **m ist ein Monomorphismus wenn gilt**

m o f = m o g impliziert f=g,.

Typen of Morphismen
- Epimorphismus -

$$\begin{tikzcd} X & B \arrow[l, shift right, "f"'] \arrow[l, shift left, "g"] & A \arrow[l, "e"'] \end{tikzcd}$$

Def. **e ist ein Epimorphismus wenn gilt**

f o e = g o e impliziert f=g,.

Typen of Morphismen
- Isomorphismus -

$$A \xrightarrow{f} B$$

Definition: Ein Morphismus f heißt **Isomorphismus** genau wenn es einen Morphismus g gibt mit

$$A \xleftarrow{g} B$$

$$\mathbf{f*g = id_B} \qquad \mathbf{g*f = id_A}$$

Produkte in Kategorien

Sei $(A_i,\ i \in I)$ **eine Familie von Objekten in einer Kategorie C.**

Ein Objekt X zusammen mit einer Familie von Morphismen

p_i: X → A_i heißt **Produkt** der $(A_i,\ i \in$ **I), wenn folgendes gilt:**

Zu jedem Objekt Y und jeder Familie von Morphismen

$f_i : Y \to A_i$ existiert genau ein Morphismus $f^*: Y \to X$ mit

$$\mathbf{p_i}^{*}\ f^{*} = f_i$$

$$\begin{tikzcd}
A_i & & X \arrow[ll, "p_i"'] \\
 & & Y \arrow[ull, "\forall f_i"] \arrow[u, "\exists!\, f^*"'] \arrow[ul, phantom, "="]
\end{tikzcd}$$

Produkte in Kategorien

Satz: Ein Produkt ist bis auf Isomorphie eindeutig.

Beweis: Seien $(X1,p_i)$ und $(X2,p'_i)$ Produkte der Objekte $(Ai,\ i \in \mathbf{I})$

$$f^* \circ g^* = id$$

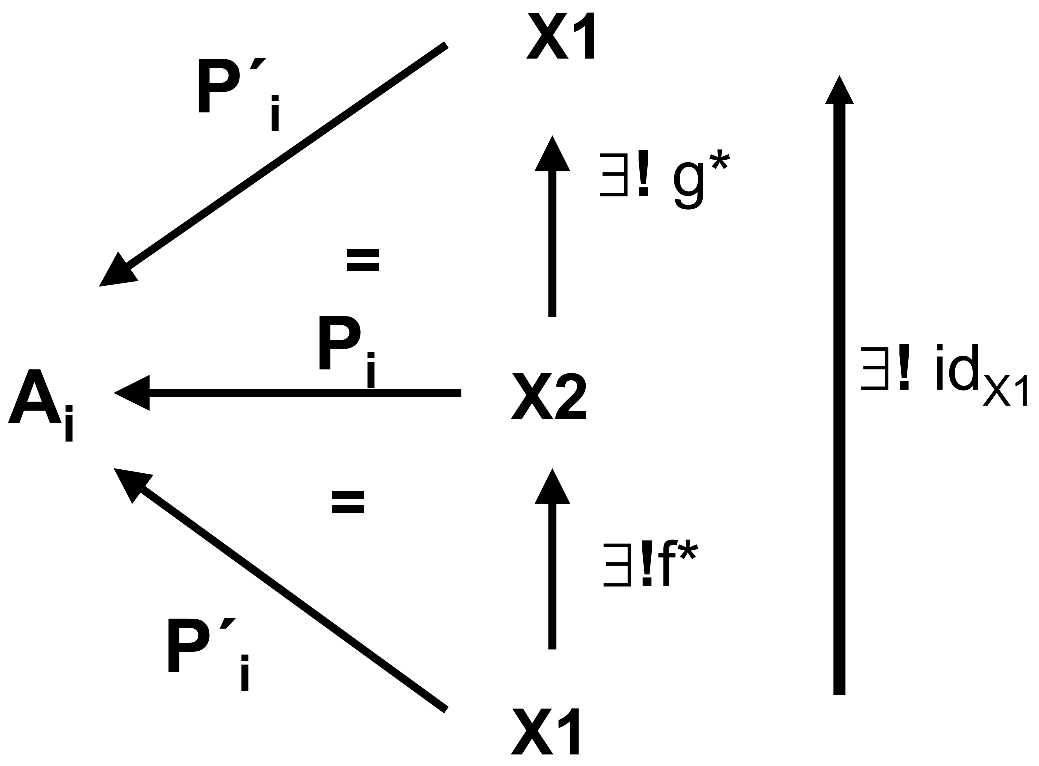
$$\begin{tikzcd}
 & X2 \arrow[dl, "p_i"'] \arrow[d, phantom, "="] & \\
A_i & X1 \arrow[l, "P'_i"'] \arrow[u, "\exists!\, f^*"'] \arrow[d, phantom, "="] & \\
 & X2 \arrow[ul, "p_i"] \arrow[u, "\exists!\, g^*"'] \arrow[uu, bend right=60, "\exists!\, id_{X2}"'] &
\end{tikzcd}$$

Produkte in Kategorien

Satz: Ein Produkt ist bis auf Isomorphie eindeutig.

Beweis: Seien $(X1,p_i)$ und $(X2,p'_i)$ Produkte der Objekte $(Ai,\ i \in \mathbf{I})$

$g^* \circ f^* = id$



Beispiel
Produkt von Gruppen

Sei (G_i, $i \in$ **I) eine Familie von Gruppen.**

Eine Gruppe X zusammen mit einer Familie von Gruppenhomomorphismen p_i: X → G_i heißt **Produkt** der (G_i, $i \in$ **I),** **wenn folgendes gilt:**

Zu jeder Gruppe Y und jeder Familie von Gruppenhomomorphismen $f_i : Y \to G_i$ existiert genau ein **Gruppenhomomorphismus** $f^*: Y \to X$ mit

$$\mathbf{p_i} * f^* = f_i$$

$$\begin{tikzcd}
G_i & & X \arrow[ll, "p_i"'] \\
& {} \arrow[u, phantom, "="] & \\
& & Y \arrow[uull, "\forall f_i"] \arrow[uu, "\exists!\, f^*"']
\end{tikzcd}$$

Produkte in Gruppen

Seien $(G_i, i \in \mathbf{I})$ **eine Familie von Gruppen.**

Dann ist $\prod G_i$ **:= {** $(g_i ; i \in \mathbf{I})$ **|** $g_i \in G_i$ für alle $i \in \mathbf{I}$**} =: mit der komponentenweisen Verknüpfung**

$\mathbf{g} := (g_i ; i \in \mathbf{I})$ **und** $\mathbf{h} := (h_i ; i \in \mathbf{I}) \in \prod G_i$

$\mathbf{g*h} := (g_i * h_i ; i \in \mathbf{I})$ **eine Gruppe.**

Es gelten:

1) **Inverse:**
   $\mathbf{g} := (g_i ; i \in \mathbf{I}) \in \prod G_i \rightarrow \mathbf{g^{-1}} := (g_i^{-1} ; i \in \mathbf{I}) \in \prod G_i$
2) **Einselement:**
   $\mathbf{e} := (e_i ; i \in \mathbf{I})$ **;** $e_i \in G_i$ Einselement **in** G_i
3) p_j: $\prod G_i \rightarrow G_j$ $(g_i ; i \in \mathbf{I}) \rightarrow g_j$ heißt j-te Projektion

Universelle Eigenschaft von Produkten

Zu jeder Gruppe Y und jeder Familie von Gruppenhomorphismen

$f_i : Y \rightarrow G_i$ existiert genau ein Morphismus $f^*: Y \rightarrow \prod G_i$ mit

$$\mathbf{p_i}{*}\, f^* = f_i$$

$$\begin{tikzcd}
\mathbf{G_i} & & \prod Gi \arrow[ll, "\mathbf{p_i}"'] \\
& & \\
& & \mathbf{Y} \arrow[uull, "\forall\, f_i"] \arrow[uu, "\exists!\, f^*"'] \arrow[uul, phantom, "\mathbf{=}"]
\end{tikzcd}$$

$$\forall\, y \in Y;\ f^*(y) := \mathbf{(}f_i(y)\ ;\ i \in \mathbf{I)}$$

Untergruppen

Definition. Sei H eine Teilmenge einer Gruppe G.
H heißt **Untergruppe**, wenn gilt:

(H1) $e \in H$ (additive Schreibweise: $0 \in H$

(H2) $g, h \in H \Rightarrow g \cdot h \in H$ $\qquad g, h \in H \Rightarrow g + h \in H$

(H3) $g \in H \quad \Rightarrow g^{-1} \in H$ $\qquad g \in H \Rightarrow -g \in H$)

Die Eigenschaften (H2) und (H3) kann man zusammenfassen zu einer einzigen dazu äquivalenten:

(H2/3) $g, h \in H \Rightarrow gh^{-1} \in H$ $\qquad g, h \in H \Rightarrow g - h \in H$

Beispiele

$(\mathbb{Z}, +)$ ist Untergruppe von $(\mathbb{Q}, +)$
$(\mathbb{Q}, +)$ ist Untergruppe von $(\mathbb{R}, +)$
$(\mathbb{R}, +)$ ist Untergruppe von $(\mathbb{C}, +)$

Definition. Sei G eine Gruppe, $H \leq_g G$ eine Untergruppe und

$x \in G$ beliebig.

(i) Die Menge $xH := \{xb: b \in H\}$ heißt eine **Linksnebenklasse** von H in G.

(ii) Die Menge $Hx := \{bx: b \in H\}$ heißt eine **Rechtsnebenklasse** von H in G.

(iii) Mit G/H bezeichnen wir die Menge der Linksnebenklassen von H in G.

(iv) Mit $H \backslash G$ bezeichnen wir die Menge der Rechtsnebenklassen von H in G.

Im Folgenden betrachten wir nur Rechtsnebenklassen. Alle Aussagen gelten jedoch analog für Linksnebenklassen.

Nebenklassen

Sei H $\leq_g$ G eine Untergruppe einer Gruppe G

Definition g, g* $\in$G.

$\mathbf{g^* \sim g \Leftrightarrow \quad g^{-1} g^* \in H}$

definiert eine Relation auf G

Sei [g] := {g* $\in$G; g* ~ g}

$g^* \in [g] \Leftrightarrow g^{-1} g^* \in H \Leftrightarrow g^* \in gH$

Daher folgt $[g] = gH$

Satz Für jede Untergruppe H einer Gruppe G definiert

$\mathbf{g^* \sim g \Leftrightarrow g^{-1} g^* \in H}$

eine Äquivalenzrelation auf G. Die Äquivalenzklassen sind die Linksnebenklassen von H in G

Nebenklassen

Lemma. Sei G eine Gruppe und $H \leq_g G$ eine Untergruppe.

Seien aH und bH **Links**nebenklassen von H in G. Dann sind folgende Aussagen äquivalent:

(i) $aH = bH$,

(ii) $aH \cap \mathbf{b}H \neq \emptyset$,

(iii) $a \in bH$,

(iv) $b^{-1} a \in H$.

Folgerung. Zwei **Links**nebenklassen sind entweder gleich oder disjunkt.

Nebenklassen

Satz. Sei H eine Untergruppe einer Gruppe G. Dann gilt:

G/H die Menge der Linksnebenklassen ist eine Partition auf G.

Die Anzahl der Linksnebenklassen heißt der

Index von H in G.

Satz. (Lagrange) Sei H eine Untergruppe einer endlichen Gruppe G. Dann gilt

$$|G| = |G/H| * |H|$$

Beweis: x: H → xH h → xh ist eine Bijektion

Nebenklassen

Folgerung Sei G eine endliche Gruppe. Dann gelten

(i) Die Ordnung einer Untergruppe muss die Gruppenordnung teilen.

(ii) Der Index, d.h. die Anzahl der verschiedenen Nebenklassen, einer Untergruppe ist ein Teiler der Gruppenordnung

(iii) Ist G eine Gruppe mit Primzahlordnung, dann besitzt G nur die trivialen Untergruppen.

Beispiel

Beispiel. (a) $G = (\mathbb{Z}, +)$, $H = n\mathbb{Z}$. Nebenkassen:

$$\overline{0} = 0 + n\mathbb{Z},\ \overline{1} = 1 + n\mathbb{Z},\ \ldots\ ,\overline{n-1} = n - 1 + n\mathbb{Z}$$

Die zugehörige Äquivlenzrelation ist die übliche Kongruenz modulo n:

$$a \in b + n\mathbb{Z} \Leftrightarrow b - a \in n\mathbb{Z} \Leftrightarrow a \equiv b(\mod n)\,.$$

Untergruppen und Normalteiler

DEFINITION

Wir nennen H eine **Untergruppe** der Gruppe $(G, \circ)$, falls erfüllt sind

- $\emptyset \neq H \subseteq G$ ist eine nicht-leere Teilmenge
- $\forall\, x, y \in H$ gilt $xy \in H$ multiplikativ abgeschlossen
- $\forall\, x \in H$ gilt $x^{-1} \in H$ invers abgeschlossen

Und eine Untergruppe H von G heisst ein **Normalteiler** von G falls weiterhin eine der folgenden drei äquivalenten Aussagen erfüllt ist

(a) $\forall\, x \in G$ gilt $xH = Hx$

(b) $\forall\, x \in G$ gilt $H^x = H$ mit $H^x := \{xhx^{-1}; h \in H\} = \{h^x; h \in H\}$

(c) $\forall\, x \in G$ gilt $H^x \subseteq H$

Gruppen

Schreibweise

U ist eine Untergruppe von G:

$$U \leq_g G$$

N ist ein Normalteiler von G:

$$N \leq_n G$$

Normalteiler

Sei H ein Normalteiler von G und x ∈ G

$$\overline{x} = xH = Hx$$

die Nebenklasse von x.

Wir stellen fest: Für beliebige

$$x' \in \overline{x},\ \ y' \in \overline{y} \text{ gilt } x'y' \in \overline{xy}$$

(denn $x' \in \overline{x},\ \ y' \in \overline{y}$ impliziert $x'y' \in x \underbrace{Hy}_{=yH} H = xyHH = xyH$).

Wir können also auf der Menge

$$G/H := \{\overline{x} \mid x \in G\}$$

aller Nebenklassen von H in G eine Multiplikation erklären durch

$$\overline{x} \cdot \overline{y} = \overline{xy}$$

Normalteiler

Satz Sei H ein Normalteiler in der Gruppe G.

Dann gelten

1. G/H ist eine Gruppe mit der Verknüpfung
   [a]*[b] : = [a*b]
2. Die kanonische Abbildung
   e: G → G/H a →[a] ist ein Epimorphismus
3. Ist G endlich, so ist |G/H| ein Teiler der Gruppenordnung |G|.

Beispiel

$$G = (\mathbb{Z}, + \ ), \ \ H = n\mathbb{Z} \ (\ n \in \mathbb{N}):$$

$$\mathbb{Z}_n := \mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \ \overline{1}, \ \overline{2}, \ldots \overline{n-1}\} \qquad \text{wobei } \overline{a} = a + n\mathbb{Z}$$

ist eine Gruppe mit der Operation $\overline{a} + \overline{b} = \overline{a+b}$, die Gruppe der Restklassen modulo n.

Spezialfall $n = 5$: $\mathbb{Z}_5 := \mathbb{Z}/5\mathbb{Z} = \{\overline{0}, \ \overline{1}, \ \overline{2}, \ \overline{3}, \ \overline{4}\}$

Gruppentafel:

$$\begin{array}{c|ccccc}
_ & \overline{0} & \overline{1} & \overline{2} & \overline{3} & \overline{4} \\
\hline
\overline{0} & \overline{0} & \overline{1} & \overline{2} & \overline{3} & \overline{4} \\
\overline{1} & \overline{1} & \overline{2} & \overline{3} & \overline{4} & \overline{0} \\
\overline{2} & \overline{2} & \overline{3} & \overline{4} & \overline{0} & \overline{1} \\
\overline{3} & \overline{3} & \overline{4} & \overline{0} & \overline{1} & \overline{2} \\
\overline{4} & \overline{4} & \overline{0} & \overline{1} & \overline{2} & \overline{3}
\end{array}$$

Gruppen

LEMMA UND DEFINITION

- Ist (H_λ) eine beliebige $(\lambda \in \Lambda)$ Familie von Untergruppen von G, so ist deren Schnitt wiederum eine Untergruppe von G

$$\bigcap_{\lambda \in \Lambda} H_\lambda \quad = \quad \{ x \in G \mid \forall\, \lambda \in \Lambda \text{ gilt } x \in H_\lambda \} \quad \leq_{\mathrm{g}} \quad G$$

- Analog ist ein beliebiger Schnitt von Normalteilern (N_λ) von G wiederum ein Normalteiler von G.

- Für eine beliebige Teilmenge $A \subseteq G$ definieren wir also die von A in G erzeugte Untergruppe durch

$$\begin{aligned} \langle A \rangle_{\mathrm{g}} \quad &:= \quad \bigcap \{ H \leq_{\mathrm{g}} G \mid A \subseteq H \} \\ &= \quad \{ a_1^{\varepsilon_1} \ldots a_r^{\varepsilon_r} \mid r \in \mathbb{N}, a_i \in A, \varepsilon_i \in \pm 1 \} \end{aligned}$$

Beispiele

Beispiel. (a) $\begin{array}{c} A \mapsto \det(A) \\ Gl(n,\mathbb{K}) \to \mathbb{K}^* \end{array}$ ist ein Gruppenhomomorphismus: denn $\det(AB) = \det(A)\det(B)$.

$Sl(n,\mathbb{K}) := \{A \in Gl(n,\mathbb{K}) \mid \det(A) = 1\}$ ist der Kern dieses Homomorphismus. Also ist $Sl(n,\mathbb{K})$ eine normale Untergruppe von $Gl(n,\mathbb{K})$, genannt die *spezielle lineare Gruppe*.

Die Signatur (=signum) $\left\{ \begin{array}{c} \sigma \mapsto \operatorname{sign}(\sigma) \\ \mathcal{S}_n \to \{-1,1\} \end{array} \right.$ ist ein Homomorphismus von $\mathcal{S}_n$ in die multiplikative Gruppe $\{-1,+1\}$, denn $\operatorname{sign}(\sigma \cdot \tau) = \operatorname{sign}(\sigma) \cdot \operatorname{sign}(\tau)$.

Der Kern dieses Homomorphismus besteht aus den Permutationen mit $\operatorname{sign}(\sigma) = +1$, d.h. den geraden Permutationen. Also ist die Menge $\mathcal{A}_n$ aller geraden Permutationen eine normale Untergruppe von $\mathcal{S}_n$. Man nennt sie die *alternierende* Gruppe

Kern und Bild eines Gruppenhomomorphismus

Lemma. Sei f: G → H ein Gruppenhomomorphismus.

1. **Der Kern** (englisch kernel, französisch noyeau) $\ker(f)= f^{-1}(e_H)$ **von f ist ein Normalteiler von G**.

2. **Das Bild** (engl. image) Im(f) = f(G) **von f ist eine Untergruppe von H.**

3. Genau dann ist f injektiv, wenn gilt $\ker(f) = \{e_G\}$.

Kern und Bild eines Gruppenhomomorphismus

Beweis.

1) $\ker(f) = f^{-1}(e_H)$ von f ist ein Normalteiler von G

$a, b \in \ker(f) \to f(a*b) = f(a)*f(b) = e_H * e_H = e_H$

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

$f(x*a*x^{-1}) = f(x)*f(a)*f(x^{-1}) = f(x)* e_H * f(x^{-1}) = e_H$

2) Klar

3) f injektiv $\leftarrow>$ $\ker(f) = \{e_G\}$.

Beweis: „→“ f injektiv → $f(x) = f(e_G) = \mathbf{e_H}$ → $x=e_{G;}$

„←“ $f(x)=f(y)$ → $f(xy^{-1}) = \mathbf{e_H}$ → $xy^{-1} \in$ **ker(f)** $= \{e_G\}$ → $x=y$

q.e.d..

Normalteiler = Kern eines Homomorphismus

Satz. Eine nichtleere Teilmenge U einer Gruppe G ist genau dann ein Normalteiler, wenn U der Kern eines Homomorphismus $f: G \to H$ ist

Beweis. U Normalteiler von G $\to$

U ist Kern von $e: G \to G/U$.

Umkehrung ist klar

$$
\begin{tikzcd}
A \arrow[r, "f"] \arrow[d, "c"', "\text{surj}\;"'] \arrow[dr, phantom, "="] & B \\
A/\sim \arrow[ur, "m"', "\;\text{inj}"'] &
\end{tikzcd}
$$

$c: A \longrightarrow A/\sim \,:\, a \longmapsto [a]$

$m: A/\sim \longrightarrow B \,:\, [a] \longmapsto f(a)$

Satz (Homomorphiesatz)

$$A/\sim \;\cong\; f(A)$$

Sei $f \in S_n$, $\operatorname{sign}(f) := \prod_{1 \le i < j \le n} \frac{f(i) - f(j)}{i - j}$

heißt Signatur von f.

Lemma. $\operatorname{sign} : S_n \longrightarrow \{1, -1\}$ ist ein Gruppenhomomorphismus

$$\operatorname{sign}(f \cdot g) = \prod_{1 \le i < j \le n} \frac{fg(i) - fg(j)}{i - j} =$$

$$\prod_{1 \le i < j \le n} \frac{fg(i) - fg(j)}{g(i) - g(j)} \, \frac{g(i) - g(j)}{i - j} = \operatorname{sign}(f) * \operatorname{sign}(g)$$

Universität Bremen

$$\ker(\varepsilon) = \{ f \in S_n \,;\, \text{sign}(f) = 1 \}$$

$= A_n$ Menge der geraden Permutationen

A_n heißt die alternierende Gruppe

$$|S_n| = |S_n/A_n|\,|A_n|$$

da $S_n/A_n \cong \{1,-1\} \Rightarrow$

$$|A_n| = \frac{n!}{2}$$

Homomorphie- / Isomorphiesätze

Satz (**Homomorphiesatz**)

Sei $\varphi : G \longrightarrow H$ *ein Gruppenhomomorphismus. So induziert* φ *einen Isomorphismus* $\tilde{\varphi} : G/\ker\varphi \xrightarrow{\sim} \mathrm{Im}\varphi$.

Satz (**Noetherscher Isomorphiesatz**)

Sei G *eine Gruppe und seien* $K \subset H \subset G$ *zwei Normalteiler von* G. *So ist* H/K *ein Normalteiler von* G/K. *Die Komposition von kanonischen Abbildungen* $G \twoheadrightarrow (G/K) \twoheadrightarrow (G/K)/(H/K)$ *induziert einen Isomorphismus*

$$G/H \xrightarrow{\sim} (G/K)/(H/K)$$

Homomorphie- / Isomorphiesätze

Sei G eine Gruppe und seien $K \subset H \subset G$ zwei Normalteiler von G. So ist H/K ein Normalteiler von G/K. Die Komposition von kanonischen Abbildungen $G \twoheadrightarrow (G/K) \twoheadrightarrow (G/K)/(H/K)$ induziert einen Isomorphismus

$$G/H \xrightarrow{\sim} (G/K)/(H/K)$$

Beweis: $\varphi : G/K \longrightarrow G/H$

$$gK \longmapsto gH$$

$gK \in \ker(\varphi) \Leftrightarrow gH = H \Leftrightarrow g \in H \Rightarrow$

$\ker(\varphi) = H/K \Rightarrow (G/K)/(H/K) \cong G/H$ $\square$

Homomorphie- / Isomorphiesätze

Satz Sei U eine untergruppe und H ein Normalteiler einer Gruppe G. Dann gilt

$U/U \cap N \cong UN/N$

Beweis. UN ist Untergruppe von G

- UN = NU da uN=Nu für alle u $\in$ U

- **$(UN)(UN)^{-1} = (UN)N^{-1}U^{-1} = U(NN^{-1})U^{-1} = UNU^{-1} = UU^{-1}N = UN$**
- **can: U $\rightarrow$ UN/N u $\rightarrow$ uN**
- **x $\in$ Ker(can) $\leftrightarrow$ xN = N $\leftrightarrow$ x** $\in$N und x $\in$U $\leftrightarrow$x $\in$U $\cap$**N**

Homomorphie- / Isomorphiesätze

- Seien $(E, \circ)$ und $(F, \circ)$ zwei Gruppen und $\varphi : E \to F$ ein Homomorphismus zwischen ihnen. Dann induziert φ einen Isomorphismus

$$E/_{\mathrm{kn}\,\varphi} \quad \cong_{\mathrm{g}} \quad \mathrm{im}\,\varphi \quad : \quad x\,(\mathrm{kn}\,\varphi) \mapsto \varphi(x)$$

- Seien H eine Untergruppe und N ein Normalteiler der Gruppe $(G, \circ)$, dann erhalten wir einen Isomorphismus durch

$$H/_{H \cap N} \quad \cong_{\mathrm{g}} \quad HN/_N \quad : \quad x\,(H \cap N) \mapsto xN$$

- Seien $M, N \trianglelefteq_{\mathrm{n}} G$ zwei Normalteiler der Gruppe $(G, \circ)$ mit $M \subseteq N$, dann erhalten wir einen Isomorphismus durch

$$G/M/_{N/M} \quad \cong_{\mathrm{g}} \quad G/_N \quad : \quad xM\,(N/M) \mapsto xN$$