

Sätzchen: Die zykl. Gruppe $Z_n \cong C_n$ ist isomorph zu einer Untergruppe von S_n .

Bew.: Betrachte $\pi = \begin{pmatrix} 1 & 2 & 3 & \dots & n-1 & n \\ 2 & 3 & 4 & \dots & n & 1 \end{pmatrix}$.

Dann ist:

$$\pi^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \dots & n-2 & n-1 & n \\ 3 & 4 & 5 & 6 & 7 & \dots & n & 1 & 2 \end{pmatrix}$$

etc., und $\pi^n = e$, wobei n der kleinste Exponent mit dieser Eigenschaft ist. $\square$

Geht das allgemeiner? Ja!

• Satz: (Cayley)

Jede (endliche) Gruppe G ist isomorph zu einer Gruppe von Permutationen.

Bew.:

(1) G als Menge $\Rightarrow S_G$ ist eine Gruppe (s.o.)

Bem.: Falls $|G| = n$, so ist $|S_G| = n!$, also ist S_G selbst natürlich viel zu groß!

Für $a \in G$ setzen wir: $\lambda_a(x) = ax$ (linkes-Mult.)

Dann ist λ_a eine Permutation von G , denn:

$$\lambda_a(x) = \lambda_a(y) \Rightarrow ax = ay \Rightarrow x = y \Rightarrow \text{injektiv}$$

$$y \in G \Rightarrow a^{-1}y \in G \Rightarrow \lambda_a(a^{-1}y) = y \Rightarrow \text{surjektiv}$$

Also ist $\lambda_a \in S_G$. Wir setzen:

$$G' = \{ \lambda_a \mid a \in G \}$$

(Kandidat!)

(2) G' ist eine Untergruppe von S_G . Denn:

$$(\lambda_a \circ \lambda_b) x = \lambda_a (\lambda_b x) = \lambda_a (bx) = abx = \lambda_{ab} x$$

$$\Rightarrow \lambda_a \lambda_b = \lambda_{ab}, \quad \text{mit } \lambda_e = \text{id (klar)}.$$

Hiermit bekommen wir: $\lambda_{a^{-1}} = (\lambda_a)^{-1}$

und:

$$\lambda_a (\lambda_b)^{-1} = \lambda_a \lambda_{b^{-1}} = \lambda_{ab^{-1}} \in G'$$

$\Rightarrow G'$ ist Untergruppe.

(3) Nun zeigen wir die Isomorphie $G \cong G'$.

Sei $\phi: G \rightarrow G'$

$$a \mapsto \phi(a) = \lambda_a$$

ϕ ist surjektiv per Def., aber auch injektiv:

$$\phi(a) = \phi(b) \Rightarrow \lambda_a x = \lambda_b x, \quad \forall x$$

$$\Rightarrow \underbrace{\lambda_a e}_{=a} = \underbrace{\lambda_b e}_{=b} \Leftrightarrow a = b.$$

Außerdem ist ϕ ein Homomorphismus:

$$\phi(ab) = \lambda_{ab} = \lambda_a \lambda_b = \phi(a) \phi(b).$$

□

「Dabei heißt λ_a auch links-reguläre Darstellung von G , und ρ_a (mit $\rho_a x = xa$) rechts-reguläre Darstellung.»

-17-

Auf die Bedeutung der Permutationen werden wir noch zurückkommen.

Sei nun $H \subset G$ Untergruppe.

Nebenklassen (links): $x \cdot H, x \in G$

$$\rightarrow \boxed{x \cdot H = y \cdot H \Leftrightarrow x^{-1}y \in H}$$

$$\begin{aligned} \text{denn: } xH = yH &\Rightarrow x = y \cdot z \text{ mit } z \in H \\ &\Rightarrow e = x^{-1}y z \Rightarrow x^{-1}y = z^{-1} \in H \end{aligned}$$

$$\text{und: } x^{-1}y \in H \Rightarrow x^{-1}y \cdot H = H \Rightarrow yH = xH$$

Äquiv.-Rel.: $x \sim y \Leftrightarrow x^{-1}y \in H$

$$\rightarrow \boxed{\text{Nebenklassen} \hat{=} \text{Äquivalenzklassen}}$$

Spezialfall: Normalteiler!

$$gNg^{-1} = N \Leftrightarrow \boxed{gN = Ng}$$

$N \subset G \rightarrow$ Nebenklassen $gN, g \in G$

$\rightarrow$ "Multiplikation":

$$gN \cdot hN = g(Nh)N$$

$$= g(hN)N = ghNN = ghN$$

$\rightarrow$ Def. einer Faktorgruppe G/N
konsistent ($\rightarrow$ Übung!)

Satz: Sei G endl. Gruppe, mit Untergruppe H .
Dann sind die Nebenklassen disjunkte Teilmengen von G , deren Vereinigung G liefert. Die Nebenklassen enthalten stets gleichviele Elemente, nämlich $|H|$, und es gilt:

$$|G| = |H| \cdot \overbrace{|(G/H)|}^{\text{Repräsentantensystem}}.$$

Insbesondere ist $|H|$ ein Teiler von $|G|$, wobei $|G|/|H|$ $\textcircled{*}$
Index heißt. Man schreibt:

$$[G : H] = |G|/|H| = |(G/H)| \in \mathbb{N}.$$

(Lagrange)

Bew.: Falls $xH \cap yH \neq \emptyset$, so ist $xg = yh$, und $x^{-1}y = gh^{-1}$, also $x^{-1}y \in H$ und $xH = yH$. Die Vereinigung der xH ist aber G , mit $G = \bigcup_{x \in G} xH = \bigcup_{x \in (G/H)} xH$.

Nun ist $\tau_x^{(1)}(g) = xg$ eine Bijektion auf G , und $\tau_x^{(1)}(H) = xH$, so daß $|H| = |xH|$. Dann folgt $\textcircled{*}$ etc. $\square$

Kor. 1: $\mathbb{Z}_p^{\times}$, p prim, enthält keine nicht-triv. Untergruppen. (klar!)

Kor. 2: Sei $a \in G$, G endlich. Dann ist $a^{|G|} = e$. (kleiner Fermat'scher Satz).

Bew.: $\langle a \rangle$ ist Untergruppe von G , also $a^n = e$, und $n \mid |G|$. $\Rightarrow a^{|G|} = e$. $\square$

Neue Gruppen aus alten Gruppen

① Direktes Produkt

G, H : Gruppen

$$G \times H = \{ (g, h) \mid g \in G, h \in H \}$$

$$\text{mit: } (g, h) (g', h') = (gg', hh')$$

$$e_{G \times H} = (e_G, e_H)$$

$$(g, h)^{-1} = (g^{-1}, h^{-1})$$

$$\tilde{G} := \{ (g, e_H) \mid g \in G \} \cong G$$

$$\tilde{H} := \{ (e_G, h) \mid h \in H \} \cong H$$

Prop.: Für $G \times H$ gilt:

(1) $\tilde{G}$ und $\tilde{H}$ sind Normalteiler

$$(2) \tilde{G} \cap \tilde{H} = \{ e_{G \times H} \}$$

(3) Jedes $x \in G \times H$ besitzt eindeutige Darstellung
als $x = \tilde{g} \cdot \tilde{h}$ mit $\tilde{g} \in \tilde{G}$ und $\tilde{h} \in \tilde{H}$.

Ist X umgekehrt eine Gruppe, die (1) - (3) erfüllt,
so ist $X \cong G \times H$.

(Bew.: Übung)

ⓔ $C_2 \times C_2$ (Klein'sche Vierergruppe)

$$C_{p \cdot q} \cong C_p \times C_q \quad (p, q \text{ teilerfremd})$$

$$O(3) \cong C_2 \times SO(3) \quad (!)$$

② Semidirektes Produkt

Situation: $N, H < X$, $N \cap H = \{e\}$, $X = \langle N, H \rangle$,
aber nur N sei Normalteiler

$$\rightarrow (n \cdot h) \cdot (n' \cdot h') = \underbrace{n \cdot (h n' h^{-1})}_{\beta_h(n')} \cdot \underbrace{h h'}_{= h h'} = n \beta_h(n') h h'$$

Allg.: $\beta: H \rightarrow \text{Aut}(N)$ (Homomorphismus)
 $h \mapsto \beta_h$

Def. eines Produktes: $(n, h) \cdot (n', h') := (n \cdot \beta_h(n'), h h')$

Satz & Def.: N, H seien Gruppen, und $\beta: H \rightarrow \text{Aut}(N)$ sei Homomorphismus. Dann wird $\{(n, h) \mid n \in N, h \in H\}$ mit obigem Produkt eine Gruppe, $N \rtimes H$, das semidirekte Produkt von N und H .

Bew.: Nachrechnen, mit

$$e_{N \rtimes H} = (e_N, e_H)$$

$$(n, h)^{-1} = (\beta_{h^{-1}}(n^{-1}), h^{-1})$$

(Beachte: $\beta_{e_H} = \text{Id}$
und $\beta_h(e_N) = e_N$) $\square$

ⓔ Directes Produkt: $\beta_h \equiv \text{Id}$

$$\mathbb{D}_3 \simeq C_3 \rtimes C_2$$

$$O(2) \simeq SO(2) \rtimes C_2$$

} geometrisch klarmachen!

Prop.: Sei $G = N \rtimes H$, $\tilde{N} = \{(n, e_H) \mid n \in N\}$,
 $\tilde{H} = \{(e_N, h) \mid h \in H\}$. Dann gilt:

- (1) $\tilde{H}$ ist Untergruppe, $\tilde{N}$ ist Normalteiler
- (2) $\tilde{N} \cap \tilde{H} = \{e_G\}$
- (3) Jedes $g \in G$ besitzt eindeutige Darstellung
als $g = \tilde{n} \cdot \tilde{h}$ mit $\tilde{n} \in \tilde{N}$ und $\tilde{h} \in \tilde{H}$
- (4) Es gilt $(e_N, h) (n, e_H) (e_N, h)^{-1} = (\beta_h(n), e_H)$

Bew.: $\tilde{H}, \tilde{N}$ sind Untergruppen, (4) rechnet man
 nach; damit ist $\tilde{N}$ Normalteiler. (2) ist klar.
 Sei $g = \tilde{n} \cdot \tilde{h}$ (geht immer). Wenn auch $g = \tilde{n}' \cdot \tilde{h}'$,
 so folgt

$$(n, e_H) (e_N, h) = (n', e_H) (e_N, h')$$

$$\begin{aligned} \Rightarrow (e_N, e_H) &= \underbrace{(n, e_H)^{-1}}_{= (n^{-1}, e_H)} (n', e_H) (e_N, h') \underbrace{(e_N, h)^{-1}}_{= (e_N, h^{-1})} \\ &= (n^{-1} n', e_H) (e_N, h' h^{-1}) = (\tilde{n}^{-1} n', h' h^{-1}) \end{aligned}$$

$\Rightarrow n' = n$ und $h' = h$, also eindeutig! $\square$

Satz: G ist genau dann das semidirekte Produkt
 der Untergruppen N und H , $G \cong N \rtimes H$, wenn
 N Normalteiler ist und jedes Element $g \in G$
 auf genau eine Weise als $g = n \cdot h$ mit
 $n \in N$ und $h \in H$ geschrieben werden kann.

Bew.: " $\Rightarrow$ " klar aus Prop.

" $\Leftarrow$ " $g \cdot g' = n \cdot h \cdot n' \cdot h' = n \cdot \underbrace{h \cdot n' \cdot h^{-1}}_{\beta_h(n') \in N} \cdot h \cdot h' = (n \cdot \beta_h(n')) \cdot (h \cdot h')$
eindeutig.

Dabei ist $\beta: H \rightarrow \text{Aut}(N)$
 $h \mapsto \beta_h = h \cdot h^{-1}$

Homomorphismus, denn $\beta_{e_H} = \text{Id}$ und
 $\beta_{h'} \circ \beta_h = h' (h \cdot h^{-1}) h'^{-1} = h' h \cdot (h' h)^{-1} = \beta_{h' h}$.

$g \in N \cap H \Rightarrow g = n \cdot h = e \cdot g = g \cdot e$ eind. $\Rightarrow g = e$. $\square$

(Ex) Kranzprodukt: $C_2 \times S_n \cong (C_2)^n \rtimes S_n = W_n$

"Würfelgruppe"

1	-1
2	-2
$\vdots$	$\vdots$
n	-n

C_2^n : Vertauschungen in
einzelnen Zeilen

S_n : Permutation der Zeilen

Würfelseiten



Übung: Man übersetze die
geometr. Operationen in die
symbol. Kodierung und
umgekehrt!

Folgerung:

$$|W_n| = 2^n \cdot n!$$