§2 Gruppenwirkungen und Sylow-Sätze

1. <u>Def</u> (Gruppenwirkungen) Sei G eine Gruppe, sei X eine nichtleere Menge. Eine <u>Wirkung von G auf X</u> ist ein Homomorphismus

$$\alpha : G \to \mathrm{Sym}(X)$$

Für $g \in G$, $x \in X$ schreibt man kurz

$$\alpha(g)(x) = gx$$

(es muss dann klar sein, welches α gemeint ist).

Die Abbildung $G \times X \to X$; $(g,x) \longmapsto gx$ erfüllt dann folgendes.

(W1) $\quad ex = x$ für alle $x \in X$

(W2) $\quad (gh)x = g(hx)$ für alle $g,h \in G$, $x \in X$.

Ist umgekehrt eine Abbildung $G \times X \to X$ gegeben, die (W1) und (W2) erfüllt, dann liegt auch eine Wirkung vor. Denn: definiere $\alpha(g) : X \to X$, $x \longmapsto gx$

es folgt $\alpha(g^{-1})\alpha(g) = \mathrm{id}_X = \alpha(g)\alpha(g^{-1}) \Rightarrow \alpha(g) \in \mathrm{Sym}(X)$

sowie $\alpha(gh) = \alpha(g)\alpha(h)$.

Fazit: Wirkungen lassen sich auch durch (W1) und (W2) charakterisieren.

Andere Bezeichnungen für Wirkungen sind <u>G-Wirkung</u> oder <u>G-Aktion</u>. #

2. <u>Def</u> Sei $G \times X \to X$ eine Wirkung.

Der <u>Stabilisator</u> von $z \in X$ ist

$$G_z = \{ g \in G \mid gz = z \},$$

der <u>Kern</u> der Wirkung ist $\bigcap_{z \in X} G_z \leq G$

die <u>Bahn</u> (der <u>Orbit</u>) von z ist $G(z) = \{ gz \mid g \in G \} \subseteq X$.

<u>Satz</u> Stabilisatoren sind Untergruppen und der Kern ist ein Normalteiler.

<u>Beweis</u> Es gilt $e \in G_z$ und für $g, h \in G_z$ gilt $(gh)z = g(hz) = gz = z$ sowie $z = (g^{-1}g)z = g^{-1}z \Rightarrow gh, g^{-1} \in G_z \Rightarrow G_z$ Untergruppe.

Weiter ist $\bigcap_{z \in X} G_z = \{ g \in G \mid$ für alle $z \in X$ ist $gz = z \}$ $= \ker(\alpha)$, wobei $\alpha : G \to \mathrm{Sym}(X)$ der zugehörige Homomorphismus ist. $\square$

3. Bsp. (a) G Gruppe, $X = G$

Wirkung $G \times G \to G$, $(g, x) \longmapsto gx$

erfüllt (W1), (W2).

Es gilt $G(z) = \{ gz \mid g \in G \} = G$

sowie $G_z = \{ g \in G \mid gz = z \} = \{e\}$

Das ist die linksreguläre Wirkung von G auf sich.

(b) G Gruppe, $H \leq G$ Untergruppe, $X = G/H$

Wirkung $G \times G/H \to G/H$, $(g, aH) \longmapsto gaH$

erfüllt auch (W1), (W2).

Es gilt $G(aH) = \{ gaH \mid g \in G \} = G/H$

sowie $G_{aH} = \{ g \in G \mid gaH = aH \}$

$= \{ g \in G \mid a^{-1} g a \in H \} = aHa^{-1}$

Der Kern dieser Wirkung ist $\bigcap_{a \in G} aHa^{-1}$.

(c) G Gruppe, $X = G$, Wirkung

$G \times G \to G$, $(g, a) \longmapsto gag^{-1}$

erfüllt (W1), (W2). Das ist die

Konjugationswirkung von G auf sich.

$G(a) = \{ gag^{-1} \mid g \in G \}$ Konjugationsklasse von a

$G_a = \{ g \in G \mid gag^{-1} = a \}$ Zentralisator von a

$\to$ später mehr.

4. <u>Theorem</u> (<u>Satz von Cayley</u>)

Zu jeder Gruppe G gibt es eine Menge X und einen injektiven Homomorphismus $\alpha : G \to \mathrm{Sym}(X)$.

<u>Beweis</u> Setze $X = G$ wie in Bsp §2.3 (a). Der Kern der Wirkung $G \times G \to G$, $(g, a) \mapsto ga$ ist $\{e\}$, also ist $\alpha : G \to \mathrm{Sym}(X)$ injektiv. $\square$

"Jede Gruppe ist Untergruppe einer symmetrischen Gruppe".

Untergruppen von $\mathrm{Sym}(X)$ nennt man auch <u>Permutationsgruppen.</u>

5. <u>Satz</u> Sei $G \times X \to X$ eine Wirkung. Dann gilt:

(i) Für $u, v \in X$ ist entweder $G(u) = G(v)$ oder $G(u) \cap G(v) = \emptyset$ (Bahnen sind gleich oder disjunkt).

(ii) Für $u \in X$ ist die Abbildung

$$G/G_u \to G(u), \quad gG_u \longmapsto gu$$

bijektiv. Insbesondere ist $|G/G_u| = |G(u)|$.

<u>Beweis</u> (i) Angenommen, es gibt $z \in G(u) \cap G(v)$.

Also $z = au = bv$ für $a, b \in G$. Damit

$G(z) = \{ g a u \mid g \in G \} = G(u)$, genauso $G(z) = G(v)$

$\Rightarrow G(u) = G(v)$. $\square$

(ii) Betrachte die Abbildung $\xi : G \to G(z)$
$g \mapsto gz$

Es gilt $\xi(g) = \xi(h) \Leftrightarrow gz = hz \Leftrightarrow g^{-1}h \in G_z$

$\overset{\S 1.11}{\Longleftrightarrow} gG_z = hG_z$, damit ist $gG_z \mapsto gz$

wohldefiniert und bijektiv. $\square$

<u>Bemerkung</u> Ist $G \times X \to G$ eine Wirkung,

$z \in X$, $a \in G$, $u = az$, so gilt

$$G_u = a\, G_u\, a^{-1}$$

Denn: $gu = u \Leftrightarrow gaz = az \Leftrightarrow a^{-1}ga \in G_z$

$\Leftrightarrow g \in a G_u a^{-1}$. $\square$

6. <u>Def</u> Eine Wirkung $G \times X \to X$ heißt

<u>transitiv</u>, wenn es für alle $u, v \in X$

ein $g \in G$ gibt mit $gu = v$.

Äquivalent dazu: $X = G(u)$ gilt für

ein (bzw. für alle) $u \in X$.

Dann erhalten wir nach §2.5 eine

<u>Bijektion</u> $G/G_u \to X$, $gG_u \mapsto gu$.

Ein Element $w \in X$ heißt *Fixpunkt* der Wirkung, wenn $G_w = G$ gilt, d.h. wenn $gw = w$ für alle $g \in G$ gilt.

Die Wirkungen in §2.3 Bsp (a), (b) sind transitiv. In Bsp (c) ist $e \in G$ ein Fixpunkt der Konjugationswirkung, also ist diese Wirkung *nicht* transitiv, falls $G \neq \{e\}$.

7. Sei $G \times X \to X$ eine Gruppenwirkung.

Der *Bahnraum* (*Orbitraum*) ist die Menge

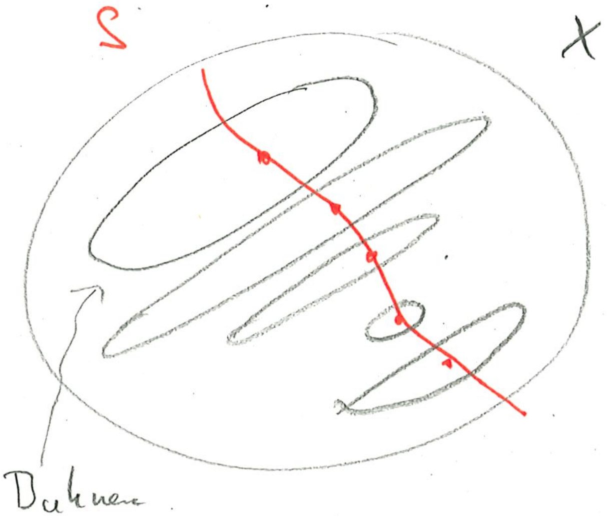
$$G\backslash X = \{ G(x) \mid x \in X \}$$ aller Bahnen.

Das passt zur Notation für Rechtsnebenklassen: ist $H \leq G$ eine Untergruppe, so wirkt H auf $G = X$ durch $(h, g) \mapsto hg$. Die Bahn von $g \in G$ ist Hg und $H\backslash G = \{ Hg \mid g \in G \}$. #

Eine Teilmenge $S \subseteq X$ heißt *Schnitt* oder *Transversale*, falls gilt:

(S) Jede Bahn $G(x) \subseteq X$ enthält genau ein Element aus S.

Schnitte existieren immer (mit dem Auswahlaxiom, falls X unendlich ist)



<u>Theorem</u> (Die Bahnengleichung)

Sei $G \times X \to X$ eine Wirkung, sei X endlich.
Sei $S \subseteq X$ ein Schnitt. Dann gilt

$$|X| = \sum_{s \in S} [G : G_s]$$

<u>Beweis</u> Sei $|S| = m$, $S = \{s_1, \dots, s_m\}$

$\Rightarrow |G(s_i)| = [G : G_{s_i}]$ nach § 2.5 (ii).

Für $i \neq j$ ist $G(s_i) \cap G(s_j) = \emptyset$, und

$X = G(s_1) \dot\cup G(s_2) \dot\cup \dots \dot\cup G(s_m)$

$$\Rightarrow |X| = \sum_{i=1}^{m} |G(s_i)| = \sum_{i=1}^{m} [G : G_{s_i}] . \qquad \square$$

8. Automorphismen und Konjugation

Sei G eine Gruppe. Ein Isomorphismus $\alpha : G \to G$ heißt <u>Automorphismus</u> von G. Die Menge $\mathrm{Aut}(G)$ aller Automorphismen von G ist eine Gruppe bzgl. Komposition, mit Neutralelement id_G, die <u>Automorphismengruppe</u> von G.

Für $a \in G$ definieren wir $\gamma_a : G \to G$ durch $\gamma_a(g) = aga^{-1}$. Dann gilt $\gamma_a(gh) = \gamma_a(g)\gamma_a(h)$ $(agha^{-1} = aga^{-1}aha^{-1})$ und $\gamma_{a^{-1}} = (\gamma_a)^{-1}$, also $\gamma_a \in \mathrm{Aut}(G)$.

<u>Satz</u> Die Abbildung
$$G \to \mathrm{Aut}(G)$$
$$a \mapsto \gamma_a$$
ist ein Homomorphismus. Der Kern ist das <u>Zentrum</u> $\mathrm{Cen}(G) = \{z \in G \mid zg = gz \text{ für alle } g \in G\}$

<u>Beweis</u> $\gamma_{ab}(g) = abg(ab)^{-1} = abgb^{-1}a^{-1}$

$= \gamma_a(\gamma_b(g))$, d.h. $\gamma_{ab} = \gamma_a \circ \gamma_b$

Damit ist die Abbildung $a \longmapsto \gamma_a$ ein Homomorphismus. Der Kern ist

$$\{ z \in G \mid \text{für alle } g \in G \text{ ist } zgz^{-1} = g \}$$
$$= \{ z \in G \mid \text{für alle } g \in G \text{ ist } zg = gz \} = \mathrm{Cen}(G). \quad \square$$

Die Automorphismen der Form γ_a heißen <u>innere Automorphismen</u> von G.

Die Bahnen der Wirkung $G \times G \longrightarrow G$
(<u>Konjugationswirkung</u>) $(a,g) \longmapsto aga^{-1}$
nennt man <u>Klassen</u> oder <u>Konjugiertenklassen</u> in G, $G(g) = \{ aga^{-1} \mid a \in G \} \subseteq G$

Klassen sind keine Untergruppen!

Beachte auch: $G(g) = \{g\} \iff g \in \mathrm{Cen}(G)$.

9. <u>Theorem</u> (<u>Die Klassengleichung</u>)

Sei G eine endliche Gruppe, sei $S \subseteq G$ eine Transversale der Konjugationswirkung.

Sei $Z \subseteq G$ das Zentrum von G und sei

$$\mathcal{K} = \{ s \in S \mid s \notin Z \}^{*}.$$

* Also ist $S = \mathcal{K} \cup Z$

Dann gilt

$$|G| = |Z| + \sum_{s\in \mathcal{K}} [G : \mathrm{Cen}_G(s)]$$

wobei $\mathrm{Cen}_G(s) = \{g\in G \mid gs = sg\}$ der Zentralisator von s ist.

<u>Beweis</u> Nach der Bahngleichung gilt

$$|G| = \sum_{s\in S} [G : \mathrm{Cen}_G(s)] .$$

Für $s \in \mathrm{Cen}(G) = Z$ gilt $\mathrm{Cen}_G(s) = G$, also $[G : \mathrm{Cen}_G(s)] = 1$. Damit

$$|G| = |Z| + \sum_{s\in \mathcal{K}} [G : \mathrm{Cen}_G(s)]$$ □

10. <u>Def</u> Sei p eine Primzahl. Eine endliche Gruppe G heißt <u>p-Gruppe</u>, falls gilt
$|G| = p^m$ für ein $m \geq 1$.

<u>Satz</u> Sei G eine p-Gruppe. Dann hat G ein nichttriviales Zentrum, $\mathrm{Cen}(G) \neq \{e\}$.

<u>Beweis</u> Sei $|G| = p^m$, sei $S \subseteq G$ eine Transversale der Konjugationswirkung. Für $s \in S - \mathrm{Cen}(G)$ gilt $\mathrm{Cen}_G(s) \neq G$. Nach dem Satz von Lagrange ist
$|\mathrm{Cen}_G(s)| = p^l$ für ein $l < m$.

damit $[G : \mathrm{Cen}_G(s)] = p^{m-l} > 1$. Also teilt p die Zahl $\sum_{s \in K} [G : \mathrm{Cen}_G(s)]$ und damit auch die Zahl $|\mathrm{Cen}(G)|$. Insbesondere ist $|\mathrm{Cen}(G)| > 1$. $\square$

11. Theorem (Satz von Cauchy) Sei G eine endliche Gruppe, sei p eine Primzahl. Wenn p ein Teiler von $|G|$ ist, dann gibt es $g \in G$ mit Ordnung $o(g) = p$.

Beweis Setze $X = \{ (g_1, \dots, g_p) \in G^p \mid g_1 g_2 \cdots g_p = e \}$

Da g_p durch $g_1, \dots, g_{p-1}$ eindeutig festgelegt ist, folgt $|X| = |G|^{p-1}$, und p teilt $|X|$.

Wir setzen $H = \mathbb{Z}/p\mathbb{Z}$ und lassen H wirken durch "schieben der Indizes": $l + p\mathbb{Z} \in H$ wirkt durch

$$(g_1, \dots, g_p) \mapsto (g_{1+l}, g_{2+l}, \dots, g_{p+l}).$$

Sei $S \subseteq X$ eine Transversale dieser H-Wirkung auf X. Es folgt

$$|G|^{p-1} = \sum_{s \in S} [H : H_s] \qquad \text{und } \underbrace{[H : H_s]}_{\text{Bahnlänge}} \in \{1, p\}$$

Da $(e, e, \dots, e) \in X$ ein Fixpunkt ist, kann es nicht sein, dass alle anderen Bahnen Länge p haben. Es gibt also noch einen Fixpunkt

$(g, \dots, g)$, $g \neq e$ und $g \cdots g = g^p = e$ $\square$

12. Def Sei G eine Gruppe, $H \leq G$ eine Untergruppe. Der Normalisator von H in G ist die Untergruppe

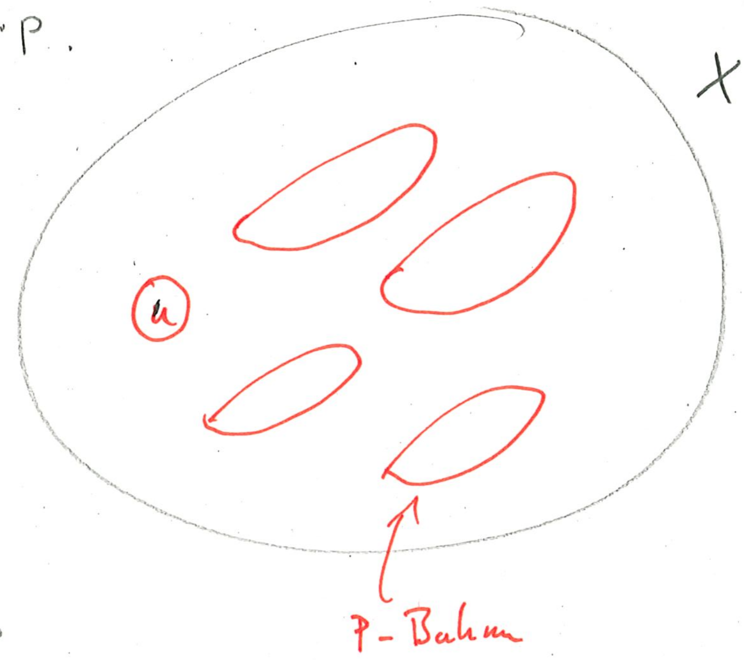
$Nor_G(H) = \{g \in G \mid gH = Hg\}$. Es folgt $H \trianglelefteq Nor_G(H)$.

Ist also $K \leq Nor_G(H)$ eine Untergruppe, so ist auch HK eine Untergruppe nach § 1.22 Lemma A. #

13. Lemma Sei $G \times X \to X$ eine Wirkung mit G und X endlich. Sei p eine Primzahl. Falls es zu jedem $u \in X$ eine p-Gruppe $P \leq G$ gibt, die genau u als Fixpunkt hat, dann wirkt G transitiv auf X und $|X| = 1 + kp$ für ein $k \geq 0$.

Beweis Sei $u \in X$, sei $P \leq G$ p-Gruppe mit u als einzigem Fixpunkt. Da $|P| = p^m$ für ein $m \geq 1$ gilt für jedes $v \neq u$, dass p ein Teiler ist von $\underbrace{|P(v)|}_{\geq 1} = \frac{|P|}{|P_v|}$.

Es folgt $|X| = 1 + k \cdot p$.



Die G-Bahn $G(u)$ ist Vereinigung von P-Bahnen, also auch

$|G(u)| = 1 + k' \cdot p$

Wäre $w \notin G(u)$, so wäre $|G(w)|$ ein Vielfaches von p (da Vereinigung von P-Bahnen $\neq \{u\}$) ↯. Also ist $G(u) = X$. □

14. Die Sylow-Sätze (P. Sylow, norweg. Mathematiker, 1832–1918) Sei G eine endliche Gruppe, sei p eine Primzahl, die $|G|$ teilt. Schreibe $|G| = p^m \cdot r$, $r \in \mathbb{N}$ teilerfremd zu p. Eine Untergruppe $P \leq G$ heißt Sylow-p-Gruppe, falls gilt $|P| = p^m$. Die Menge der Sylow-p-Gruppen in G ist $\mathrm{Syl}_p(G) = \{ P \leq G \mid P \text{ Untergruppe}, |P| = p^m \}$. (Im Moment wissen wir noch nicht, ob $\mathrm{Syl}_p(G) \neq \emptyset$).

Beobachtung: ist $Q \leq G$ eine p-Gruppe, $a \in G$, so ist $a Q a^{-1} \leq G$ ebenfalls eine p-Gruppe

<u>Theorem</u> ("Die Sylow-Sätze") Sei G eine endliche Gruppe, sei p eine Primzahl, die $|G|$ teilt. Schreibe $|G| = p^m \cdot r$, r teilerfremd zu p. Dann gilt Folgendes.

(1) $Syl_p(G) \neq \emptyset$, es gibt Sylow-p-Gruppen.

(2) G wirkt durch Konjugation transitiv auf $Syl_p(G)$, d.h. zu $P, Q \in Syl_p(G)$ gibt es stets $a \in G$ mit $Q = aPa^{-1}$!

(3) $|Syl_p(G)| = 1 + k \cdot p$ für ein $k \geq 0$ und $r = s \cdot (1 + k \cdot p)$ für ein $s \geq 1$.

(4) Ist $H \leq G$ eine p-Gruppe, dann gibt es $P \in Syl_p(G)$ mit $H \leq G$.

<u>Beweis</u> (Nach M. Aschbacher) Sei X die Menge aller p-Gruppen in G. Nach Cauchys Satz §2.11 ist $X \neq \emptyset$. Wir nennen eine p-Gruppe $P \leq G$ <u>maximal</u>, wenn sie in keiner größeren p-Gruppe enthalten ist.

Sei $\Omega \subseteq X$ die Menge der maximalen p-Gruppen.

$\Rightarrow$ $\Omega \neq \emptyset$ (weil G endlich ist).

Für $P \in X$ ist $|P| = p^l \leq p^m$, also $Syl_p(G) \subseteq \Omega$.

Die Gruppe G wirkt auf Ω durch Konjugation,

$G \times \Omega \to \Omega$, $(a, P) \longmapsto aPa^{-1}$.

<u>Beh. A</u> <u>G wirkt transitiv auf Ω und es gilt</u>
<u>$|\Omega| = 1 + k \cdot p$ für ein $k \geq 0$.</u>

<u>Beweis</u> Sei $P \in \Omega$. Dann ist P der einzige Fixpunkt der Wirkung von P auf Ω.

<u>Denn:</u> Für $g \in P$ ist $gPg^{-1} = P \Rightarrow P$ Fixpunkt.
Ist $Q \in \Omega$ auch ein Fixpunkt, so $gQg^{-1} = Q$ für alle $g \in P \Rightarrow P \leq Nor_G(Q) \Rightarrow PQ$ ist Untergruppe nach § 2.12. Nach dem 1. Isomorphiesatz § 1.23 gilt $P/_{P \cap Q} \cong PQ/_Q$ $(Q \trianglelefteq Nor_G(Q))$

$\Rightarrow \left| P/_{P \cap Q} \right| = \left| PQ/_Q \right| = p^l$ für ein $l \geq 0$

$\Rightarrow$ PQ ist p-Gruppe, $PQ \supseteq P \Rightarrow PQ = P$
Lagrange
$\Rightarrow Q \subseteq P \Rightarrow Q = P$ wegen Maximalität. □

Jetzt folgt Beh A aus § 2.13. □

Beh. B $\quad \Omega = Syl_p(G)$.

Sei $P \in \Omega$, $|P| = p^l$. Es gilt

$$|G| = |Nor_G(P)| \cdot |\Omega| \qquad \text{(Lagrange)}$$

weil $Nor_G(P)$ genau der Stabilisator von P ist ($gPg^{-1} = P \Leftrightarrow g \in Nor_G(P)$). Folglich ist

$|Nor_G(P)| = p^m \cdot s$ für ein $s \geq 1$ (weil $|\Omega| = 1 + kp$ teilerfremd zu p ist).

$\boxed{\text{Angenommen, } l < m.}$ Betrachte $K = Nor_G(P)/P$

$\Rightarrow |K| = p^{m-l} \cdot s$ (Lagrange) sowie

$$f : Nor_G(P) \to K, \quad g \mapsto gP.$$

Nach Cauchys Satz § 2.11 gibt es eine p-Gruppe $R \leq K$.

Dann ist auch $f^{-1}(R) = H$ eine p-Gruppe und

$|H| = |P| \cdot |R| > |P|$ ↯ Also ist $l = m$.

Es folgt $\Omega = Syl_p(G)$. □

Wir haben (1), (2), (3) gezeigt und (4) gilt, weil $\Omega = Syl_p(G)$. □

15. Eine Anwendung.

<u>Satz</u> Seien p, q Primzahlen, $p < q$, p <u>kein</u> Teiler von $q-1$. Ist G eine Gruppe mit $|G| = p \cdot q$, so ist G abelsch.

<u>Beweis</u> Wir schreiben
$$|Syl_p(G)| = 1 + k \cdot p$$
$$|Syl_q(G)| = 1 + l \cdot q$$

$\rightsquigarrow$ $q = s(kp+1)$.

<u>1. Fall</u> $s = 1$ $\rightsquigarrow$ $q - 1 = k \cdot p$ ↯

<u>2. Fall</u> $s \geq 2$ $\Rightarrow$ $k = 0$ (weil q Primzahl)

$\rightsquigarrow$ $Syl_p(G) = \{P\}$ $\Rightarrow$ $G = Nor_G(P)$, d.h. $P \trianglelefteq G$.

Schreibe $p = s' \cdot (lq + 1)$ $\rightsquigarrow$ $l = 0$ wegen $p < q$

$\Rightarrow$ $Syl_q(G) = \{Q\}$ $\Rightarrow$ $Q \trianglelefteq G$.

$|Q| = q$, $|P| = p$ $\Rightarrow$ $P \cap Q = \{e\}$

Betrachte
$$\begin{tikzcd} G \arrow[r, "\beta"] \arrow[d, "\alpha"'] & G/P \cong Q \\ G/Q \cong P & \end{tikzcd}$$

$\rightsquigarrow$ Homomorphismus $G \to G/P \times G/Q$ mit Kern $\{e\}$
$$g \longmapsto (gP, gQ)$$

$\Rightarrow$ Isomorphismus $\rightsquigarrow$ $G \cong P \times Q$ ist abelsch, denn P, Q sind zyklisch nach § 1.12 Korollar B. $\square$

16. Die alternierenden Gruppen $\mathrm{Alt}(n)$. Sei $n \geq 2$.

Für $\alpha \in \mathrm{Sym}(n)$ definieren wir die Signatur

$$\mathrm{sign}(\alpha) = \prod_{1 \leq i < j \leq n} \frac{\alpha(i) - \alpha(j)}{i - j}.$$

Da in Zähler und Nenner bis auf Vorzeichen die gleichen Zahlen stehen, gilt $\mathrm{sign}(\alpha) \in \{\pm 1\} = C_2$.

Lemma Die Abbildung $\mathrm{sign}: \mathrm{Sym}(n) \to C_2$ ist ein surjektiver Homomorphismus.

Bew: Sei $\alpha, \beta \in \mathrm{Sym}(n)$. Dann gilt $\mathrm{sign}(\alpha \circ \beta)$

$$= \prod_{i<j} \frac{\alpha(\beta(i)) - \alpha(\beta(j))}{i-j} = \prod_{i<j} \frac{\alpha(\beta(i)) - \alpha(\beta(j))}{\beta(i) - \beta(j)} \cdot \frac{\beta(i) - \beta(j)}{i-j}$$

$$= \prod_{i<j} \frac{\alpha(\beta(i)) - \alpha(\beta(j))}{\beta(i) - \beta(j)} \, \mathrm{sign}(\beta) = \mathrm{sign}(\alpha) \cdot \mathrm{sign}(\beta).$$

Sei τ die Permutation $\tau: \begin{cases} 1 \longmapsto 2 \\ 2 \longmapsto 1 \\ j \longmapsto j \text{ sonst} \end{cases} \rightsquigarrow \mathrm{sign}(\tau) = -1$ $\square$

Folglich ist sign surjektiv.

Die alternierende Gruppe ist der Kern von sign,

$$\mathrm{Alt}(n) = \{\alpha \in \mathrm{Sym}(n) \mid \mathrm{sign}(\alpha) = 1\} \trianglelefteq \mathrm{Sym}(n).$$

Aus dem Homomorphiesatz folgt $\mathrm{Sym}(n)/\mathrm{Alt}(n) \cong C_2$,

damit $|\mathrm{Alt}(n)| = \frac{n!}{2}$.

17. <u>Semidirekte Produkte</u> Sei $\varphi: G \to K$ ein surjektiver Gruppenhomomorphismus mit Kern $N \trianglelefteq G$. Damit haben wir eine kurze exakte Sequenz

$$1 \to N \hookrightarrow G \xrightarrow{\varphi} K \to 1 \qquad (*)$$

Wir sagen, diese kurze exakte Sequenz <u>zerfällt</u>, wenn es einen Homomorphismus $s: K \to G$ gibt mit $\varphi \circ s = id_K$.

<u>Beispiel</u> Für $n \geq 2$ haben wir

$$1 \to Alt(n) \hookrightarrow Sym(n) \xrightarrow{sign} C_2 \to 1$$

Setze $s(-1) = \tau = \begin{cases} 1 \longmapsto 2 \\ 2 \longmapsto 1 \\ j \longmapsto j \text{ sonst} \end{cases}$, $s(1) = id$

$\Rightarrow$ $s: C_2 \to Sym(n)$ ist Homomorphismus mit $sign \circ s = id_{C_2}$.

<u>Lemma</u> (ÜA 3.2) Sei $\varphi: G \to K$ ein surjektiver Homomorphismus. Dann sind äquivalent:

(i) Die exakte Sequenz $(*)$ zerfällt

(ii) Es gibt eine Untergruppe $H \leq G$ mit $G = NH$ und $N \cap H = \{e\}$.

Dann sagen wir, G ist das <u>semidirekte Produkt</u> von N und H und schreiben $G = N \rtimes H$. Die Abbildung $N \times H \to G$, $(n, h) \longmapsto nh$ ist dann bijektiv, aber nicht unbedingt ein Homomorphismus.

<u>Beweis</u> (i) $\Rightarrow$ (ii): Setze $H = s(K) \leq G$. Wegen $\mathrm{id}_K = \varphi \circ s$ ist s injektiv und $\ker(\varphi) \cap H = \{e\}$.

Für $g \in G$ ist $h = s(\varphi(g)) \in H \Rightarrow \varphi(h) = \varphi(g)$

$\Rightarrow g \in hN = Nh \Rightarrow G = NH$ □

(ii) $\Rightarrow$ (i): $H \cap N = \{e\} \Rightarrow \varphi$ bildet H bijektiv auf $\varphi(H) \leq K$ ab. Wegen $G = NH$ ist $\varphi(H) = \varphi(NH) = K$, also ist die Einschränkung $\varphi|_H : H \to K$ ein Isomorphismus. Sei $s : K \to H$ sein Inverses. □

Für $g \in G = NH$, $g = nh$ ist $h = s(\varphi(g))$ eindeutig, damit auch $n = gh^{-1}$. □

Für $n = 3$ ist $\mathrm{Sym}(n) \not\cong \mathrm{Alt}(3) \times C_2$, denn $|\mathrm{Alt}(3)| = 3 \Rightarrow$ die rechte Seite ist abelsch. □

18. <u>Ein Beispiel: Gruppen der Ordnung 21</u> Sei G eine Gruppe, $|G| = 21$. Was lässt sich über G sagen?

$21 = 3 \cdot 7 \rightsquigarrow |\mathrm{Syl}_7(G)| = 1 + k \cdot 7$ teilt $3 \rightsquigarrow$ es gibt genau eine Sylow-7-Gruppe $P \leq G$, $|P| = 7$ und $P \trianglelefteq G$. Weiter enthält G ein Element t der Ordnung 3 (Satz von Cauchy § 2.11). Setze $H = \langle t \rangle$ und $P = \langle u \rangle$ (P ist zyklisch nach § 1.12).

Weiter ist $P \cap H = \{e\}$ und $\varphi : G \to G/P$ bildet H isomorph ab auf G/P, weil $|G/P| = 3$.

Also ist G ein semidirektes Produkt, $G = NH$.

Betrachte $\gamma_t \in Aut(G)$, $\gamma_t(g) = tgt^{-1}$. Es gilt

$\gamma_t(u) \in P \Rightarrow \gamma_t(u) = u^m$ für ein $1 \leq m \leq 6$.

Weiter ist $\gamma_t^3 = id_G \Rightarrow u^{(m^3)} = u \Rightarrow 7$ teilt $m^3 - 1$

$\Rightarrow m = 1, 2, 4$ (nachrechnen)

<u>1. Fall</u>: $m = 1 \Rightarrow \gamma_t(u) = u$ d.h. $tu = ut$. Dann

ist $P \times H \to G$ $(u^a, t^b) \longmapsto u^a t^b$ ein Isomorphismus,

$G \cong P \times H$ ist abelsch.

<u>2. Fall</u>: $m = 2$ $tut^{-1} = u^2$, d.h. $tu = u^2 t$. Dann

ist G nicht abelsch, aber eindeutig festgelegt. Denn

$$(u^a t^b)(u^c t^d) = u^a \underbrace{(t^b u^c t^{-b})}_{= \gamma_t^b(u^c)} t^{d+b} = u^{a + c(2^b)} t^{d+b}$$

<u>3. Fall</u>: $m = 4$ $\gamma_{t^2}(u) = u^{(4^2)} = u^2$, ersetze t

durch $t^{-1} = t^2 \Rightarrow$ Fall 2. $\square$

Bleibt noch zu zeigen: Fall 2 kommt wirklich vor.

19. <u>Konstruktion</u> Seien N, H Gruppen, sei $\alpha : H \to Aut(N)$

ein Homomorphismus. Wir definieren eine Gruppe

$$G = N \rtimes_\alpha H \quad \text{wie folgt.}$$

$G = \{(n, h) \mid n \in N, h \in H\}$ mit folgender Verknüpfung.

$$(n_1, h_1) \cdot (n_2, h_2) = (n_1 \alpha(h_1)(n_2), h_1 h_2)$$

Man rechnet nach: das ist eine assoziative Verknüpfung,

Neutralelement ist (e_N, e_H) und das Inverse von

(n,h) ist $(\alpha(h^{-1})(n^{-1}), h^{-1})$. Weiter ist

$N \cong \tilde{N} = \{(n, e_H) \mid n \in N\} \trianglelefteq G$

$H \cong \tilde{H} = \{(e_N, h) \mid h \in H\} \leq H$

und $G = \tilde{N}\tilde{H}$, $\tilde{N} \cap \tilde{H} = \{(e_N, e_H)\}$.

Im Beispiel oben: $P = \langle u \rangle$ zyklisch der Ordnung 7

$H = \langle t \rangle$ zyklisch der Ordnung 3

$\alpha : H \to \mathrm{Aut}(P)$, $t \mapsto [u^a \mapsto u^{2a}]$

also $\alpha(t)(u) = u^2$.

↯

~~ff~~