§2 Gruppenwirkungen und Sylow-Sätze

1. **Gruppenwirkungen** Sei G eine Gruppe und X eine nicht leere Menge. Eine **Wirkung von G auf X** (auch: **G-Wirkung**, "**G-Aktion**") ist ein Homomorphismus $\alpha: G \to \mathrm{Sym}(X)$.

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

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

(wenn klar ist, welches α gemeint ist). Die Abbildung

$$\begin{aligned} G \times X &\longrightarrow X \\ (g, x) &\longmapsto g(x) \end{aligned}$$

erfüllt folgende Eigenschaften:

(W1) $e(x) = x$ für alle $x \in X$ ($e \in G$ Neutralelement)

(W2) $(a \circ b)(x) = a(b(x))$ für alle $a, b \in G$, $x \in X$.

Ist umgekehrt eine Abbildung $G \times X \to X$ gegeben, die (W1) und (W2) erfüllt, so erhalten wir eine Wirkung $\alpha: G \to \mathrm{Sym}(X)$ durch

$$\alpha(g) = [x \longmapsto g(x)]$$

denn aus (W2) folgt: $\alpha(g^{-1})$ ist Inverse zu $\alpha(g)$, also ist die Abbildung $\alpha(g): X \to X$ bijektiv, und $\alpha: G \to \mathrm{Sym}(X)$ ist ein Homomorphismus nach (W2).

2. Def Gegeben sei eine G-Wirkung $G \times X \to X$.

Für $x \in X$ ist der Stabilisator (die Standgruppe)

$$G_x = \{ g \in G \mid g(x) = x \} \leq G$$

Die Bahn (der Orbit) von x ist

$$G(x) = \{ g(x) \mid g \in G \} \subseteq X$$

Der Kern der Wirkung ist $\bigcap_{x \in X} G_x \leq G$.

Satz Der Stabilisator G_x ist eine Untergruppe und der Kern ist ein Normalteiler.

Beweis Es gilt $e(x) = x \Rightarrow e \in G_x$ Für $a, b \in G_x$ gilt $(ab)(x) = a(\underbrace{b(x)}_{=x}) = a(x) = x \Rightarrow ab \in G_x$

$a^{-1}(x) = a^{-1}(\underbrace{a(x)}_{=x}) = (a^{-1}a)(x) = e(x) = x \Rightarrow a^{-1} \in G_x$ □

Also ist $G_x \leq G$ Untergruppe.

Es gilt: $\bigcap_{x \in X} G_x = \{ g \in G \mid g(x) = x \text{ für alle } x \in X \}$

Das ist genau der Kern des zugehörigen Homomorphismus

$\alpha : G \to \mathrm{Sym}(X)$, also ein Normalteiler.

□

3. Beispiel (a) Sei G eine Gruppe. Für $g \in G$ definiere eine Abbildung $\lambda_g : G \to G$ durch $\lambda_g(x) = gx$. Es folgt

$$\lambda_g \circ \lambda_h = \lambda_{gh} \qquad \lambda_e = id_G \Rightarrow \lambda_g \lambda_{g^{-1}} = id_G = \lambda_{g^{-1}} \lambda_g$$

also $\lambda_g \in Sym(G)$. Die Gruppe G wirkt also auf der Menge $G = X$. Es gilt für die Wirkung: $G_x = \{ g \in G \mid \lambda_g(x) = x \} = \{ g \in G \mid gx = x \} = \{e\}$.

Zu $x, y \in G$ gibt es genau ein $g \in G$ mit $\lambda_g(x) = y$, nämlich $g = yx^{-1}$.

Man nennt das die Linksreguläre Wirkung von G auf sich.

(b) Sei G eine Gruppe und $H \leq G$ Untergruppe. Sei $X = G/H = \{ aH \mid a \in G \}$. Die Gruppe G wirkt auf X durch

$$\lambda_g : G/H \to G/H$$
$$aH \longmapsto gaH$$

Es gilt wieder $\lambda_g \lambda_h = \lambda_{gh}$, $\lambda_e = id_{G/H}$

Der Stabilisator von $x = H \in X$ ist

$G_x = \{ g \in G \mid gH = H \} = H$.

Zu $x = aH$, $y = bH \in X$ gibt es wieder $g \in G$ mit $g(x) = y$, nämlich $g = ba^{-1}$. Anders als im Bsp (a) ist g nicht eindeutig, falls $H \neq \{e\}$ gilt (für $H = \{e\}$ erhalten wir wieder Beispiel (a)).

4. Korollar (Satz von Cayley). Zu jeder Gruppe G gibt es eine Menge X und eine injektive Homomorphismus $\chi : G \to \mathrm{Sym}(X)$.

Beweis: Setze $G = X$ und $\lambda : G \to \mathrm{Sym}(X)$ wie in Beispiel §2.3 (a) □

Eine Untergruppe von $\mathrm{Sym}(X)$ nennt man auch eine Permutationsgruppe. Der Satz von Cayley wird auch so formuliert: jede Gruppe "ist" (bis auf Isomorphie) eine Permutationsgruppe.

5. Def Ein G-Wirkung $G \times X \longrightarrow X$ heißt transitiv, wenn es für alle $x, y \in X$ ein $g \in G$ gibt mit $g(x) = y$.

Die in Bsp. §2.3 (a),(b) betrachtete Wirkung

sind also transitiv.

Satz Gegeben sei eine transitive G-Wirkung $G \times X \to X$. Sei $x \in X$ und $H = G_x$. Dann ist die Abbildung

$$\begin{aligned} G/H &\longrightarrow X \\ gH &\longmapsto g(x) \end{aligned}$$

wohldefiniert und bijektiv. Für jedes $y \in X$ mit $y = g(x)$ gilt $G_y = g G_x g^{-1}$.

Beweis Betrachte die Abbildung $\varepsilon : G \to X$, $\varepsilon(g) = g(x)$. Es gilt $\varepsilon(g) = \varepsilon(g') \Leftrightarrow$ $g(x) = g'(x) \Leftrightarrow g^{-1}g'(x) = x \Leftrightarrow g^{-1}g' \in G_x = H$ $\Leftrightarrow$ $g'H = gH$. Damit ist die erste §1.13 Behauptung gezeigt.

Für $y = g(x)$ gilt $a(y) = y \Leftrightarrow ag(x) = g(x)$ $\Leftrightarrow$ $g^{-1}ag(x) = x \Leftrightarrow g^{-1}ag \in G_x$ $\Leftrightarrow$ $a \in gG_xg^{-1}$ □

6. Bahnen Gegeben sei ein G-Wirkung $G \times X \to X$.

Lemma Für Bahnen $G(x), G(y) \subseteq X$ gilt stets:
Ist $G(x) \cap G(y) \neq \emptyset$, so gilt $G(x) = G(y)$,
Bahnen sind entweder disjunkt oder gleich.

Beweis Annahme, $G(x) \cap G(y) \ni z$, also
$z = a(x) = b(y)$ für $a, b \in G$. Es folgt
$b^{-1}a(x) = y$, also $y \in G(x)$, also $G(y) \subseteq G(x)$.
Genauso folgt auch $G(y) \supseteq G(x)$, also $G(x) = G(y)$. □

Bem Für jedes $x \in X$ wirkt G transitiv auf der Bahn $G(x) \subseteq X$. Denn: $y, z \in G(x)$,
$y = a(x)$ und $z = b(x)$ $\rightsquigarrow$ $x = a^{-1}(y)$ $\rightsquigarrow$ $z = ba^{-1}(y)$.
Weiter gilt $g(y) = ga(x) \in G(x)$. <36½

Def Die Menge der Bahnen bezeichnen wir mit

$$G\backslash X = \{ G(x) \mid x \in X \} \quad \text{"Bahnraum"}$$

Bem Das passt zur Notation für Nebenklassen:
Gegeben sei eine Untergruppe $H \subseteq G$. Setze $X = G$,
dann wirkt H auf $G = X$ durch

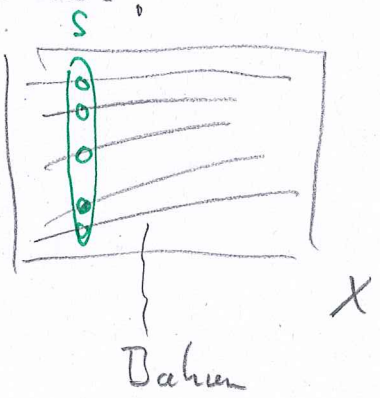
$$\begin{aligned} H \times X &\longrightarrow X \\ (h, x) &\longmapsto hx. \end{aligned}$$

Die Länge einer Bahn $G(x)$ ist $\#G(x)$.
Ist $\{x\} = G(x)$ (Bahn der Länge 1),
so sagt man, dass $x \in X$ ein Fixpunkt
der G-Wirkung auf X ist. Für alle $g \in G$
gilt dann $gx = x$.

Die Bahnen der Wirkung von H auf G sind dann genau die Rechtsnebenklassen, $H(x) = Hx$ für $x \in X = G$, die Bahnenmenge ist also $H\backslash G = \{Hx \mid x \in G\}$

7. <u>Die Bahnengleichung</u> Gegeben sei eine G-Wirkung $G \times X \to X$. Ein <u>Schnitt</u> (ein <u>Transversale</u>) ist eine Teilmenge $S \subseteq X$ mit folgender Eigenschaft: Für jedes $x \in X$ gilt $\#(S \cap G(x)) = 1$, jede Bahn trifft S genau einmal. Es folgt $\#S = \#(G\backslash X)$.

Mit Hilfe des Auswahlaxioms sieht man, dass Schnitte stets existieren.



<u>Satz</u> Sei $S \subseteq X$ ein Schnitt der G-Wirkung $G \times X \to X$. Wenn X endlich ist, dann gilt

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

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

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

$$\#G(s_i) = \#G/G_{s_i} = [G : G_{s_i}]$$

(links: §2.5; rechts: §1.14)

8. Automorphismen und Konjugationswirkung

Sei G eine Gruppe. Ein bijektiver Homomorphismus $\alpha: G \to G$ heißt Automorphismus von G. Die Menge

$$\mathrm{Aut}(G) = \{\alpha: G \to G \mid \alpha \text{ Automorphismus}\}$$

ist eine Gruppe, mit der Komposition von Automorphismen als Verknüpfung und id_G als Neutralelement.

Beispiel Sei $a \in G$. Dann ist die Abbildung

$$\gamma_a: G \to G,\quad g \mapsto aga^{-1}$$

ein Automorphismus. Denn:

$$\gamma_a(gh) = agha^{-1} = aga^{-1}aha^{-1} = \gamma_a(g)\gamma_a(h)$$

$\Rightarrow \gamma_a$ Homomorphismus

$$\gamma_a(g) = e \iff aga^{-1} = e \iff g = a^{-1}ea = e$$

$\Rightarrow \gamma_a$ Monomorphismus, $\ker(\gamma_a) = \{e\}$

Gegeben $g \in G$ Folgt $\gamma_a(a^{-1}ga) = g$

$\Rightarrow \gamma_a$ Epimorphismus.

$\Rightarrow \gamma_a$ Automorphismus.

oder: $\gamma_a \circ \gamma_{a^{-1}} = \mathrm{id}_G = \gamma_{a^{-1}} \circ \gamma_a$

Satz Die Abbildung $G \xrightarrow{\tau} \mathrm{Aut}(G)$, $a \longmapsto \tau_a$ ist ein Homomorphismus.

Beweis Es gilt

$$\tau_a \circ \tau_b(g) = abgb^{-1}a^{-1} = abg(ab)^{-1} = \tau_{ab}(g)$$

also $\tau_a \circ \tau_b = \tau_{ab}$. □

Weil $\mathrm{Aut}(G) \leq \mathrm{Sym}(G)$ eine Untergruppe ist, ist $\tau: G \to \mathrm{Aut}(G)$ eine Wirkung von G auf G, die **Konjugationswirkung**.

Beachte den Unterschied zu §2.3(a)

$$\lambda_a(g) = ag \qquad \tau_a(g) = aga^{-1}$$

λ_a ist **kein** Homomorphismus (für $a \neq e$)

$$\lambda_a(gh) = agh \neq \lambda_a(g)\lambda_a(h) = agah$$!

Der **Kern** von $\tau: G \to \mathrm{Aut}(G)$ ist

$$Z(G) = \{a \in G \mid \text{für alle } g \in G \text{ gilt } aga^{-1} = g\}$$
$$= \{a \in G \mid \text{für alle } g \in G \text{ gilt } ag = ga\}$$

Man nennt diesen Normalteiler das **Zentrum**

von G. Das Zentrum von G ist also abelsch (und G ist genau dann abelsch, wenn $Z(G) = G$ gilt).

Beim Im Allgemein ist die Abbildung

$\gamma : G \to Aut(G)$ weder injektiv noch surjektiv.

Das Bild $\gamma(G) \leq Aut(G)$ ist die Gruppe der innere Automorphismen, $\gamma(G) = Inn(G) \leq Aut(G)$.

Mit dem Homomorphiesatz also:

$$G/Z(G) \cong Inn(G)$$

Wie sehen die Stabilisatoren in der Konjugationswirkung aus? Der Stabilisator von $g \in G$ ist der Zentralisator von g (vgl §1.6)

$$Z_G(g) = \{ a \in G \mid aga^{-1} = g \}$$
$$= \{ a \in G \mid ag = ga \}$$

Beachte: es gilt stets $\langle g \rangle \leq Z_G(g)$, denn

$$ggg^{-1} = g \Rightarrow g \in Z_G(g) \Rightarrow \langle g \rangle \leq Z_G(g).$$

Die Bahnen $G(g) = \{ aga^{-1} \mid a \in G \}$ nennt man Klassen oder Konjugiertenklassen in G.

9. Satz (Die Klassengleichung) Sei G eine endliche Gruppe, sei $S \subseteq G$ ein Schnitt der Konjugation wirkung γ. Sei $\mathcal{K} = S - Z(G)$. Dann gilt

$$\#G = \#Z(G) + \sum_{s \in \mathcal{K}} [G : Z_G(s)]$$

Beweis Nach der Bahngleichung gilt

$$\#G = \sum_{s \in S} [G : Z_G(s)]$$

Für jedes $z \in Z(G)$ gilt $G(z) = \{a z a^{-1} \mid a \in G\} = \{z\}$

also $Z(G) \subseteq S$ und $\#G(z) = 1$ für alle $z \in Z(G)$. □

10. Korollar Sei p eine Primzahl und G eine endliche Gruppe mit $\#G = p^m$, $m \geq 1$.

Dann gilt $Z(G) \neq \{e\}$.

Beweis Für $g \in G - Z(G)$ ist $Z_G(g) \neq G$. Nach dem Satz von Lagrange §1.14 folgt $\#Z_G(g) = p^l$, $l < m$.

Insbesondere ist dann p ein Teiler von $[G : Z_G(g)] = p^{m-e} \neq 1$. Folglich ist p ein Teiler von $\#Z(G)$, also $\#Z(G) \geq p$. □

#

42 1/2

Def Eine endliche Gruppe G heißt **p-Gruppe**, für eine Primzahl p, wenn gilt $\#G = p^m$ für ein $m \geq 1$. Das vorige Korollar besagt also: jede p-Gruppe hat ein nichttriviales Zentrum.

Bsp $G = \left\{ \begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix} \in K^{3\times 3} \right\}$ mit $K = \mathbb{F}_p$

(Körper mit p Elem.) $\#G = p^3 \Rightarrow G$ ist p-Gruppe. Das Zentrum ist $\left\{ \begin{pmatrix} 1 & 0 & z \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \in K^{3\times 3} \right\}$.

Unser nächstes Ziel ist der Beweis der Sylow-Sätze. Das braucht etwas Vorbereitung.

11, **Def** Sei G eine Gruppe und $H \leq G$ eine Untergruppe. Der **Normalisator** von H in G ist

$$N_G(H) = \{ n \in G \mid nHn^{-1} = H \}$$

Wenn G eine endliche Gruppe ist, dann nennt man ihre Kardinalität $\#G$ die Ordnung von G. Das passt zu §1.11: die Ordnung eines Elements $g \in G$ ist die Ordnung der von g erzeugten zyklischen Gruppe, $o(g) = \#\langle g \rangle$, vgl. §1.12

Satz Der Normalisator $N_G(H)$ ist eine Untergruppe von G und es gilt

$$H \trianglelefteq N_G(H) \qquad \text{(daher der Name).}$$

Insbesondere gilt $H \subseteq N_G(H)$.

Beis Sei $X = \{ aHa^{-1} \mid a \in G \}$. Dann wird G auf der Menge X durch Konjugation,

$$G \times X \longrightarrow X$$
$$(g, aHa^{-1}) \longmapsto gaHa^{-1}g^{-1} = (ga)H(ga)^{-1}$$

operiert. Der Stabilisator von $H \in X$ ist genau $N_G(H)$, also eine Untergruppe.

Wir gilt $H \subseteq N_G(H)$ (klar) und nach Definition gilt für alle $n \in N_G(H)$, dass

$nHn^{-1} = H$, also $H \trianglelefteq N_G(H)$. □

Die Menge $X = \{ aHa^{-1} \mid a \in G \}$ nennt man die Konjugiertenklasse der Untergruppe H in G.

Folgerung aus dem Satz: Ist $K \subseteq N_G(H)$ eine Untergruppe, dann ist $KH \subseteq N_G(H)$ eine Untergruppe, denn $H \trianglelefteq N_G(H)$, das folgt aus § 1.23 Lemma

12. Satz (Cauchys Satz). Sei G eine endliche Gruppe und sei p eine Primzahl. Wenn p ein Teiler von $\#G$ ist, dann enthält G (mindestens) ein Element der Ordnung p.

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

Da $g_1, \dots, g_{p-1} \in G$ frei gewählt werden können und $g_p = (g_1 \cdots g_{p-1})^{-1}$, gilt, $\#X = (\#G)^{p-1}$ und p teilt $\#X$. Gesucht ist ein Element $g \in G$ mit $g \neq e$ und $(g, g, g, \dots, g) \in X$ (d.h. $g^p = e \neq g$).

Setze $K = \mathbb{Z}/p\mathbb{Z}$. Diese Gruppe K wirkt auf X wie folgt: sei $\bar{k} \in K$, sei

$$\bar{k}(g_1, \dots, g_p) = (g_{1+k}, g_{2+k}, \dots, g_{p+k}) \qquad (*)_{44\frac{1}{2}}$$

(Indizes mod p). Die Fixpunkte dieser K-Wirkung sind genau die Tupel $(g, \dots, g) \in X$. Also ist $(e, \dots, e)$ ein Fixpunkt. Da $\#K = p$ hat jede K-Bahn $K(x)$ Länge $\#K(x) = [K : K_x] \in \{1, p\}$ und die Bahn der Länge 1 sind die Fixpunkte. Nach der Bahnengleichung gilt (für ein Schnitt $S \subseteq X$)

$$\#X = \#G^{p-1} = \sum_{s \in S} [K : K_s]$$

(*) Das ist wirklich ein $\mathbb{K}$- Witz:

$0 < k \leq p$ wirkt durch

$\overline{k} : (g_1, \dots, g_p) \longmapsto (g_{1+k}, \dots, g_p, g_1, \dots, g_k)$

$g_1 \cdots g_k = a$ $\qquad ab = e$ nach Voraussetzung

$g_{k+1} \cdots g_p = b$ $\qquad \Rightarrow b = a^{-1}$

$g_{1+k} \cdot g_{2+k} \cdots g_p \cdot g_1 g_2 \cdots g_k = ba = e$

$\Rightarrow (g_{1+k}, \dots, g_k) \in X$

Die Primzahl p teilt hier Sinn, es gilt $[K:K_s] \in \{1, p\}$ und für $s = (e, e, \dots e)$ gilt $[K:K_s] = 1$. Also gibt es ein $s \neq (e, \dots, e)$ mit $[K:K_s] = 1$ □

Wir brauchen noch das folgende technische Hilfsmittel.

13. Lemma Sei $G \times X \to X$ eine Wirkung einer endlichen Gruppe G auf einer endlichen Menge X. Sei p eine Primzahl. Angenommen, es gilt folgendes:

(*) zu jedem $x \in X$ gibt es eine p-Gruppe $P \subseteq G$ mit $P(x) = \{x\}$.

Dann gilt $\#X = kp + 1$ für ein $k \geq 0$ und G wirkt transitiv auf X.

Beweis: Sei $S \subseteq X$ ein Schnitt. Für jedes $s \in S$ wirkt G also transitiv auf $G(s)$. Sei $s \in S$. Sei $P \subseteq G$ p-Gruppe mit $P(s) = \{s\}$. Für jedes $x \in X - \{s\}$ teilt p die Länge der Bahn $P(x)$ (weil P p-Gruppe ist und $P(x) \neq \{x\}$ nach (*)). Es folgt $\#G(s) = kp + 1$. Angenommen, $S \neq \{s\}$. Für $t \in S - \{s\}$ folgt $\#G(t) = lp$, weil P in $G(t)$ keinen Fixpunkt hat. Andererseits folgt aus gleichem Argument, dass $\#G(t) = mp + 1$ ↯

Es folgt $S = \{s\}$ und $X = G(s)$ □

Jetzt beweisen wir Sylows Sätze. Peter Sylow war ein norwegischer Mathematiker und Lehrer. Seine Sätze sind in der endlichen Gruppentheorie ganz wesentlich.

14. Definition Sei G eine endliche Gruppe, sei p eine Primzahl mit $\#G = p^m \cdot r$, wobei $m \geq 1$ sei und p kein Teiler von r ist. Eine Untergruppe $U \subseteq G$ heißt Sylow-p-Gruppe in G, wenn gilt $\#U = p^m$.

Die Menge aller Sylow-p-Gruppen in G wird mit $Syl_p(G)$ bezeichnet.

(Im Moment ist nicht klar, dass $Syl_p(G) \neq \emptyset$, aber das beweisen wir gleich.)

Theorem (Sylows Sätze) Sei G eine endliche Gruppe, sei p eine Primzahl mit $\#G = p^m \cdot r$, $m \geq 1$, p kein Teiler von r. Dann gilt folgendes.

(1) $Syl_p(G) \neq \emptyset$

(2) G wirkt transitiv auf $Syl_p(G)$: zu $U, V \in Syl_p(G)$ gibt es stets $g \in G$ mit $gUg^{-1} = V$.

(3) $\# Syl_p(G) = k \cdot p + 1$ für ein $k \geq 0$

(4) Ist $P \subseteq G$ eine p-Gruppe, so gibt es $U \in Syl_p(G)$ mit $P \subseteq U$.

//

Beweis Sei Γ die Menge aller p-Gruppen in G. Nach Cauchys Satz ist $\Gamma \neq \emptyset$.

Sei $\Omega \subseteq \Gamma$ die Menge aller maximalen p-Gruppen in Γ (weil G endlich ist, ist jede p-Gruppe $P \subseteq G$ in einer maximalen p-Gruppe enthalten).

Die Gruppe G wirkt durch Konjugation auf den Mengen Γ und Ω. Nach Definition gilt $Syl_p(G) \subseteq \Omega$.

1. Schritt G wirkt transitiv auf Ω und es gilt $\#\Omega = kp+1$ für ein $k \geq 0$.

Beweis 1. Schritt. Wir benutzen das Lemma §2.13.

Beh Für $U \in \Omega$ ist U der einzige Fixpunkt der Wirkung von U auf der Menge Ω.

Denn: Wenn U das Element $V \in \Omega$ fixiert, so folgt $U \leq N_G(V) \underset{\S 2.11}{\Rightarrow} UV \leq G$ Untergruppe, $V \trianglelefteq UV$

Es gilt $\#UV = \#V \cdot [UV:V] = \#V \cdot \#U/V$ sowie
$\uparrow$ Lagrange §1.14

$UV/V \overset{\uparrow}{\cong} U/U\cap V$ (1. Isomorphiesatz §1.23) $= \frac{\#U}{\#(U\cap V)}$ also ist $\#UV/V$ eine p-Potenz,

denn $\#U$ und $\#U\cap V$ sind p-Potenzen. Folglich ist $UV \leq G$ eine p-Gruppe. Da U und V maximale p-Gruppen sind und $U, V \leq UV$ folgt $U = UV = V$.

Mit Lemma §2.13 folgt nun: G wirkt transitiv auf Ω und $\#\Omega = kp+1$ □

2. Schritt Es gilt $\Omega = Syl_p(G)$

Beweis 2. Schritt Sei $U \in \Omega$, $\#U = p^l$. Wir müssen zeigen, dass $p^l = p^m$ gilt.

Wegen Schritt 1 gilt jedenfalls

$$(*) \quad \#G = p^m \cdot r = \#N_G(U) \cdot \#\Omega = \#N_G(U) \cdot (kp+1)$$

und Folglich

$$(**) \quad \#N_G(U) = p^m \cdot s \qquad \text{für ein } s \geq 1.$$

Angenommen, es gilt $\ell < m$. Betrachte

$$N_G(U) \xrightarrow{\pi_U} N_G(U)/U = K$$

es folgt $\#N_G(U) = p^m \cdot s = \underbrace{\#U}_{=p^\ell} \cdot \#K$, also ist p ein Teiler von $\#K$. Nach Cauchys Satz §2.12. gibt es eine p-Gruppe $P \leq K$. Setze $V = \pi_U^{-1}(P) \leq N_G(U)$. Es folgt mit $P = V/U$, dass

$$\#V = \#U \cdot \#P,$$ also ist V eine p-Gruppe.

Da p ein Teiler von $\#P$ ist, folgt $V \supsetneq U$, ein Widerspruch zur Maximalität von U.

Folglich gilt $\#U = p^m$ für alle $U \in \Omega$ und damit $\Omega = Syl_p(G)$. ⊏

Damit sind (1), (2) und (3) bewiesen.

Wer $Syl_p(G) = \Omega$ folgt (4). □

Addendum zu Sylows Theorem.

Es gilt (mit den Bezeichnungen von oben)

$$r = s \cdot (kp+1)$$

Das folgt aus (*) und (**).

15. Beispiel einer Anwendung.

Lemma Seien p, q Primzahlen mit $p < q$.
Wenn G eine Gruppe ist mit $\# G = p \cdot q$
und wenn p kein Teiler von $q-1$ ist,
dann ist G abelsch.

Beweis Sei $\# Syl_p(G) = k \cdot p + 1$
$\# Syl_q(G) = l \cdot q + 1$

$\Rightarrow q = s \cdot (kp+1)$

1. Fall $s = 1 \Rightarrow q = kp+1$ Widerspruch zur Annahme, dass p kein Teiler von $q-1$ ist

2. Fall $kp+1 = 1 \Rightarrow$ es gibt genau eine Sylow-p-Gruppe $U \leq G \Rightarrow G = N_G(U)$ d.h. $U \trianglelefteq G$.

Jetzt $pq = s' \cdot (lq+1)$ wegen $q > p$ folgt
$s' = p$ und $lq+1 = 1 \Rightarrow$ es gibt genau eine Sylow-q-Gruppe $Q \leq G \Rightarrow Q \trianglelefteq G$.

Wir wiss.: $\#P = p$ $\#Q = q$ und
$\#(P \cap Q)$ teilt nach Lagr. p und q $\Rightarrow$
$P \cap Q = \{e\}$. Weil $P \trianglelefteq G$ und $Q \trianglelefteq G$ gilt
für $a \in P$ und $b \in Q$, dass

$$\underbrace{\underbrace{a}_{\in Q}\, \underbrace{b\, a^{-1}}_{\in Q}\, b^{-1}}_{\in P} \in Q \cap P \quad \text{d.h.} \quad ab = ba$$

Nach § 1.23 haben wir ein Monomorphismus

$$\begin{aligned} P \times Q &\xrightarrow{\varphi} G \\ (a,b) &\longmapsto ab \end{aligned}$$

Wegen $\#(P \times Q) = p \cdot q = \#G$ ist φ surjektiv,
also ein Isomorphismus.
Wenn $\#P = p$ und $\#Q = q$ sind P und Q
abelsch: ist $a \in P$, $a \neq e$, so gilt $o(a) > 1$ und
$o(a)$ teilt p $\Rightarrow$ $o(a) = p$ $\Rightarrow$ $\langle a \rangle = P$ $\Rightarrow$ P zyklisch
$\Rightarrow$ P abelsch vgl. § 1.12. Gleiches gilt für
Q. (Mit Ü4 4.3 folgt jetzt sogar: G ist zyklisch) $\square$

Bsp Die Gruppe $S_{gm}(3)$ ist nicht abelsch,
vgl § 1.7. Es gilt $\#S_{gm}(3) = 2 \cdot 3$
(aber 2 teilt $3-1$!?).
Was sind die Sylowgruppen in $S_{gm}(3)$? (Ü1)

Beim Beweis von Lemma § 2.15 haben wir einige nützliche Fakten bewiesen, die auch sonst hilfreich sein können.

(1) Jede endliche Gruppe, deren Ordnung eine Primzahl ist, ist abelsch.

(2) Wenn $\varphi: K \to G$ ein Homomorphismus von endlichen Gruppen ist, und wenn gilt $\#K = \#G$, dann ist φ ein Isomorphismus.

(3) Wenn $N, M \trianglelefteq G$ Normalteiler sind und wenn gilt $N \cap M = \{e\}$, dann ist die Abbildung

$$\begin{aligned} N \times M &\longrightarrow G \\ (n, m) &\longmapsto n \cdot m \end{aligned}$$

ein Homomorphismus.

(4) Wenn G endlich ist und p eine Primzahl und wenn p ein Teiler von $\#G$ ist mit $\#Syl_p(G) = 1$, dann ist die (eindeutige) Sylow-p-Gruppe $U \in Syl_p(G)$ ein Normalteiler in G, $U \trianglelefteq G$.

Ü 4 Schicken Sie die Beweise für (1) – (4) noch einmal selber sorgfältig auf.

16. Satz Sei G eine endliche Gruppe mit $\#G = p \cdot q$, $p \neq q$ Primzahlen. Dann gibt es einen Normalteiler $N \trianglelefteq G$, $\{e\} \neq N \neq G$.

Beweis: OE $p < q$, $\#Syl_q(G) = l_q + 1$

$\overset{\S 2.14}{\Rightarrow}$ $p = s(l_q+1) \Rightarrow l_q + 1 = 1$ wegen $p < q$

$\Rightarrow$ es gibt genau ein Sylow-q-Gruppe $U \leq G$

$\Rightarrow U \trianglelefteq G$ und $\#U = p$. □ #

Wir betrachten also nächst p-Gruppen genauer.

17. Lemma Sei G eine Gruppe. Dann ist jede Untergruppe $H \leq Z(G)$ Normalteiler in G.

Beweis: Sei $g \in G$ und $h \in H \leq Z(G)$. Es folgt $ghg^{-1} = h$, also $gHg^{-1} = H$ □

Satz Sei p Primzahl und G eine p-Gruppe, $\#G = p^m$, $m \geq 1$. Dann gibt es Normalteiler $G_k \trianglelefteq G$ mit $\#G_k = p^k$ für $0 \leq k \leq m$ und mit

$$G_m \trianglerighteq G_{m-1} \trianglerighteq \dots \trianglerighteq G_1 \trianglerighteq G_0 = \{e\}$$

Beweis: Induktion nach m. Für $m = 1$ ist nichts zu zeigen. Sei jetzt $\#G = p^m$ mit $m > 1$.

Nach §2.10 ist $Z(G) \neq \{e\}$, also $\#Z(G) = p^s$ für ein $s \geq 1$ (Lagrange). Nach Cauchys Satz §2.12

gibt es $g \in Z(G)$ mit $o(g) = p$. Sei $G_1 = \langle g \rangle$

und $G \xrightarrow{\pi} \tilde{G} = G/G_1$ (nach dem Lemma gilt $G_1 \trianglelefteq G$.)

Es folgt $\#\tilde{G} = p^{m-1}$, nach Induktion gibt es auch

$\tilde{G}_k \trianglelefteq \tilde{G}$ mit $\#\tilde{G}_k = p^k$, $\tilde{G} \supseteq \tilde{G}_{m-2} \supseteq \dots \supseteq \tilde{G}_0$.

Sei $G_{k+1} = \pi^{-1}(\tilde{G}_k)$, es folgt nach § 1.22, dass

$G_{k+1} \trianglelefteq G$, sowie $G_m \supseteq G_{m-1} \supseteq \dots \supseteq G_1 \supseteq G_0 = \{e\}$.

Wegen $G_1 \subseteq G_{k+1}$ folgt $\tilde{G}_k \cong G_{k+1}/G_1$, also

$\#G_{k+1} = p \cdot \#\tilde{G}_k = p^{k+1}$. □

— <54½

18. Def Sei G eine Gruppe, sei $G = G_m \supseteq G_{m-1} \supseteq \dots \supseteq G_0 = \{e\}$

Untergruppen. Wenn gilt

$$G_{k-1} \trianglelefteq G_k$$

dann heißt $G_m \supseteq \dots \supseteq G_0$ Normalreihe in

G. Die Quotienten G_k/G_{k-1} heißen Faktoren der

Normalreihe.

Eine Gruppe, die eine Normalreihe mit abelschen

Faktoren hat, heißt auflösbare Gruppe.

Beispiele (a) G abelsch $\Rightarrow$ G auflösbar,

setze $G_1 = G \supseteq G_0 = \{e\}$

Folgerung Ist G eine endliche Gruppe, p eine Primzahl und ist p^k ein Teiler von $\#G$, dann hat G eine Untergruppe der Ordnung p^k.

Beweis. Sei $U \in Syl_p(G)$, $\#U = p^m$.

Dann gilt $k \leq m$ und nach dem vorigen Satz gibt es eine Untergruppe $H \leq U$ mit $\#H = p^k$ □

(b) $G = Sym(3)$, $\#G = 6$, $\tau : \{1,2,3\} \to \{1,2,3\}$

τ: $1 \mapsto 2$, $2 \mapsto 3$, $3 \mapsto 1$

$o(\tau) = 3$, $G_1 = \langle \tau \rangle \trianglelefteq G$ (weil $[G : G_1] = 2$, ü A 3.2 oder § 2.16) $\#\, G/G_1 = 2$ was abelsch, also ist $Sym(3)$ auflösbar.

(c) Nach Satz § 2.17 ist jede p-Gruppe auflösbar.

Wir betrachten jetzt <u>abelsche</u> p-Gruppen.

~~18.~~ 19. <u>Lemma A</u> Sei G abelsche p-Gruppe. Wenn G genau eine Untergruppe $H \leq G$ der Ordnung p hat, dann ist G zyklisch.

<u>Beis</u> Satz $\#G = p^m$, $m \geq 1$. Induktion nach m.

Für $m = 1$ ist nichts zu zeigen. Sei jetzt $m > 1$.

Betrachte den Homomorphismus $\varphi : G \to G$, $g \mapsto g^p$ (das ist ein Homomorphismus, weil G abelsch ist: $(gh)^p = g^p h^p$).

Es gilt $ker(\varphi) = \{g \in G \mid g^p = e\} = \{g \in G \mid o(g) \in \{1, p\}\}$

Ist $o(g) = p$, so folgt aus der Annahme $g \in H$, also $H = ker(\varphi)$, denn $h \in H$ was $o(h) \in \{1, p\}$.

Setze $K = \varphi(G)$. Nach dem Homomorphiesatz § 1.20 gilt $K \cong G/H$ also $\#K = p^{m-1}$. Wegen $m > 1$

Folgt aus Cauchys Satz §2.12, dass K ein Elt der Ordng p enthält. Folglich gilt $H \subseteq K$.
Also hat K genau ein Untergrpp der Ordng p und ist das wg. mal Induktionsannahme zyklisch,
$K = \langle k \rangle$ für ein $k \in K = \varphi(G)$. Wähl $g \in G$ mit $\varphi(g) = g^p = k$. Wegen $o(g) = p \cdot r$ folgt $o(g^r) = p$ $\Rightarrow$ $H \subseteq \langle g \rangle$ (wg. der Eindeutigkeit von H)
also $\langle g \rangle / H \cong K \Rightarrow \# \langle g \rangle = \# K \cdot \# H = \# G$
$\Rightarrow G = \langle g \rangle$ □

Lemma B Sei G zyklisch mit $\# G = k \cdot l$. Dann hat G genau ein Untergrpp $H \subseteq G$ mit $\# H = k$
(ü A 4.1)

Bew: Betrachte $\varphi : G \to G$, $g \mapsto g^k$, das ist ein Homomorphismus. Der Kern ist $K = \{ g \in G \mid g^k = e \}$.
Ist $H \subseteq G$ Untergrpp mit $\# H = k$, so folgt $H \subseteq K$.
Sei $u \in G$ Erzeuger, $G = \langle u \rangle$. Das Bild von φ ist dann $\varphi(G) = \langle u^k \rangle$ mit $o(u^k) = l$. Also folgt
$l = \# \varphi(G) = \frac{\# G}{\# K} \Rightarrow \# K = k \Rightarrow H = K$. □

Lemma G Sei G eine endliche p-Gruppe, sei $u \in G$ ein Element maximaler Ordnung in G und sei $U = \langle u \rangle$. Dann gibt es eine Untergruppe $H \leq G$ mit $H \cap U = \{e\}$ und $G = HU$, d.h. $H \times U \cong G$.

Beweis Sei $\#G = p^m$. Für $m = 1$ ist G zyklisch, also $G = U$ und $H = \{e\}$ $\rightsquigarrow$ fertig.
Sei jetzt $m > 1$, Induktion nach m.
1. Fall G zyklisch, $G = U$, $H = \{e\}$ fertig.
2. Fall G nicht zyklisch. Da U genau eine Untergruppe der Ordnung p hat (Lemma B) gibt es nach Lemma A und Cauchys Satz ein Element $w \in G - U$ mit $o(w) = p$. Sei $W = \langle w \rangle$. Es folgt $U \cap W = \{e\}$, mit $w \notin U$ ($\#U \cap W$ ist p-Potenz). Betrachte $\pi : G \to G/W$. Wegen $\ker(\pi) = W$ ist die Einschränkung von π auf U injektiv, d.h. $o(\pi(u)) = o(u)$. Folglich ist $\pi(u)$ ein Element maximaler Ordnung in $L = G/W$, und $\#G/W = p^{m-1}$.
Nach Induktionsannahme gibt es eine Untergruppe $H' \leq L$ mit $H' \cap \pi(U) = \{e_L\}$ und $L = \pi(U)H' \cong \pi(U) \times H'$.
Sei $H = \pi^{-1}(H')$. Es folgt $H \cap U = \{e\}$, denn: $h \in H$, $\pi(h) \in \pi(U) \rightsquigarrow \pi(h) = e_L \rightsquigarrow h \in W$.

Weiter gilt für $g \in G$, dass $\pi(g) = \pi(u^k)\pi(h)$ für ein $k \geq 0$ und $h \in H$. Es folgt

$$g = \underbrace{u^k}_{\in U} \underbrace{h w^\ell}_{\in H} \quad \text{für ein } \ell \geq 0$$

also $G = UH$ □ ⊣

Korollar Sei G eine abelsche p-Gruppe, $\#G = p^m$ mit $m \geq 1$. Dann gibt es eindeutig bestimmte Zahlen $n_1 \geq \dots \geq n_r \geq 1$ mit $m = n_1 + n_2 + \dots + n_r$

$$G \cong \mathbb{Z}/p^{n_1}\mathbb{Z} \times \mathbb{Z}/p^{n_2}\mathbb{Z} \times \dots \times \mathbb{Z}/p^{n_r}\mathbb{Z}.$$

Beweis Wähle $u_1 \in G$ mit maximaler Ordnung $o(u_1) = p^{n_1}$

$U_1 = \langle u_1 \rangle \cong \mathbb{Z}/p^{n_1}\mathbb{Z}$ und eine Untergruppe

$G_1 \subseteq G$ wie in Lemma 6 mit $U_1 \cap G_1 = \{e\}$,

$G = U_1 G_1 \cong U_1 \times G_1$. Wähle $u_2 \in G_1$ mit maximaler Ordnung $o(u_2) = p^{n_2}$, $U_2 = \langle u_2 \rangle \cong \mathbb{Z}/p^{n_2}\mathbb{Z}$,

$G_1 = U_2 G_2$ usw. Nach endlich vielen Schritten

$G = U_1 U_2 U_3 \dots U_r \cong U_1 \times \dots \times U_r$

Zur Eindeutigkeit der Zahlen $n_1, n_2, \dots, n_r$.

Für $\ell \geq 1$ sei $\varphi_\ell : G \to G$, $g \mapsto g^{p^\ell}$

Da G abelsch ist, ist φ_ℓ ein Homomorphismus mit

$h_r(\varphi_e) = \{ g \in G \mid o(g) \text{ teilt } p^e \}$, insbesondere

$$\left.\begin{array}{ll} \varphi_e(u_i) = e & \text{für } e \geq n_i \\ \varphi_e(u_i) \neq e & \text{für } e < n_i \end{array}\right\} \Rightarrow \#\varphi_e(u_i) = \begin{cases} \{1\} & e \geq n_i \\ \mathbb{Z}/p^{n_i - e}\mathbb{Z} & e < n_i \end{cases}$$

$$\Rightarrow \#\varphi_e(G) = \prod_{n_i > e} p^{n_i - e} = p^{N_e}, \text{ aus dem Zahl}$$

$N_1, N_2, \ldots$ lassen sich die n_i berechnen,

$$N_e = \sum_{n_i > e} (n_i - e)$$

□

20. Theorem Sei G eine endliche abelsche Gruppe,

$\#G = p_1^{l_1} \cdots p_s^{l_s}$ $\quad 2 \leq p_1 < p_2 < \ldots < p_s$ Primzahl,

$l_1, l_2, \ldots, l_s \geq 1$. Dann gilt

$$G \cong P_1 \times \ldots \times P_s$$

wobei P_j eine abelsche p_j-Gruppe der Ordnung $p_j^{l_j}$ ist wie im vorigen Korollar.

Insbesondere ist jede endliche abelsche Gruppe ein Produkt von zyklischen Gruppen.

Beweis Da G abelsch ist, ist jede Sylow-p_j-Gruppe in G normal, also gibt es (vgl. §2.14 (2)) genau eine Sylow-p_j-Gruppe $P_j \leq G$, und P_j enthält alle Elemente $g \in G$, deren Ordnung eine p_j-Potenz ist.

Betrachte

$$\varphi: P_1 \times P_2 \times \dots \times P_s \longrightarrow G$$
$$(g_1, \dots, g_2) \longmapsto g_1 g_2 \cdots g_s$$

Weil G abelsch ist, ist φ ein Homomorphismus (oder: weil für alle $i<j$ gilt $P_i \cap P_j = \{e\} \rightsquigarrow$ *-Aufgabe auf Blatt 6 ...). Es genügt zu zeigen, dass φ injektiv ist, dann folgt aus Kardinalitätsgründen, dass φ bijektiv ist. Zeige also $\ker(\varphi) = \{e\}$.

Angenommen, $g_1 \cdots g_s = e$ $\quad g_i \in P_i$

Setze $r_i = \dfrac{\#G}{P_i^{l_i}}$. Für $j \neq i$ folgt $g_j^{r_i} = e$, weil $\#P_j$ ein Teiler von r_i ist. Also gilt

$$(g_1 \cdots g_s)^{r_i} \overset{\uparrow}{=} g_1^{r_i} \cdots g_s^{r_i} = g_i^{r_i} = e^{r_i} = e$$

(↑ o.B.d.A.)

Also ist $o(g_i)$ ein Teiler von r_i. Weil $o(g_i)$ ein P_i-Potenz ist, folgt $o(g_i) = 1$, d.h. $g_i = 1$.

Es folgt $\ker(\varphi) = \{(e, \dots, e)\}$. □

21. Satz Sei G eine endliche auflösbare Gruppe mit einer Normalreihe $G = G_m \trianglerighteq \dots \trianglerighteq G_0$ mit abelschen Faktoren. Dann gibt es für jedes $1 \le k \le m$ Untergruppen H_j mit

$$G_k \trianglerighteq H_\ell \trianglerighteq H_{\ell-1} \dots \trianglerighteq H_0 = G_{k-1}$$

mit $H_j / H_{j-1} \cong \mathbb{Z}/p_j\mathbb{Z}$ p_j Primzahl.

Insbesondere hat jede endliche auflösbare Gruppe eine Normalreihe, in der alle Faktoren zyklisch von Primzahlordnung sind.

Beis Betrachte die abelsche Gruppe $A = G_k / G_{k-1}$.

Nach Theorem §2.19 und §2.17, angewandt auf die Sylowgruppen von A, gibt es Untergruppen

$$A = A_\ell \supseteq \dots \supset A_0 = \{e_A\}$$

mit $A_j / A_{j-1} \cong \mathbb{Z}/p_j\mathbb{Z}$ p_j Primzahl.

Sei $\pi : G_k \to G_k/G_{k-1} = A$ kanonische Epimorphismus.

und $H_0 = \pi^{-1}(A_j)$ $\Rightarrow$ $H_j \le G_k$,

$$G_k \trianglerighteq H_\ell \trianglerighteq H_{\ell-1} \dots \trianglerighteq H_0 = G_{k-1}$$

$$H_j / H_{j-1} \cong A_j / A_{j-1} \cong \mathbb{Z}/p_j\mathbb{Z}$$

↑ 2. Isomorphiesatz

□

22. Kommutatoren

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

Der Kommutator von a und b ist

$$[a,b] = aba^{-1}b^{-1} = ab(ba)^{-1} \quad \rightsquigarrow \quad ab = [a,b]ba$$

Offensichtlich gilt $[a,b]^{-1} = [b,a]$ und

$$[a,b] = e \iff a \text{ zentralisiert } b \iff b \text{ zentralisiert } a$$
$$\iff a \text{ und } b \text{ vertauschen.}$$

Die Kommutatorgruppe von G ist

$$DG = \langle [a,b] \mid a,b \in G \rangle$$

, die von allen Kommutatoren erzeugte Gruppe.

Satz Sei G eine Gruppe. Dann gilt

(i) $DG \trianglelefteq G$

(ii) G/DG ist abelsch

(iii) Ist A abelsche Gruppe und $\varphi: G \to A$ ein Homomorphismus, so gilt $DG \leq \ker(\varphi)$.

Beweis (i) Für $g, a, b \in G$ gilt $g[a,b]g^{-1} = [gag^{-1}, gbg^{-1}]$ (nachrechnen), also gilt für alle $g \in G$, $a_1, \dots a_s, b_1, \dots b_s \in G$

dass $g[a_1,b_1] \cdots [a_s,b_s]g^{-1} \in DG$

also ist $gDGg^{-1} \leq DG$ für alle $g \in G \Rightarrow DG \trianglelefteq G$.

(ii) Sei $g, h \in G$. Es folgt wegen $gh = [g,h]hg$

$$ghDG = \underbrace{[g,h]}_{\in e DG} hgDG = hgDG \quad , \text{ dass}$$

G/DG abelsch ist.

(iii) Für alle $g, h \in G$ gilt

$$\varphi([g,h]) = [\varphi(g), \varphi(h)] = e_A$$

↑ weil A abelsch ist

also $[g,h] \in \ker(\varphi) \Rightarrow DG \subseteq \ker(\varphi)$ □

Man definiert rekursiv $D^0G = G$ $D^1(G) = DG$

$D^{k+1}G = D(D^kG) \subseteq D^kG$.

Es folgt $D^{k+1}G \trianglelefteq G$ mit Induktion, denn:

$a, b \in D^kG \rightsquigarrow g[a,b]g^{-1} = [\underbrace{gag^{-1}}_{\in D^kG}, \underbrace{gbg^{-1}}_{\in D^kG}] \in D^{k+1}G$ ← Induktionsannahme

$g \in G$

also $g(D^{k+1}G)g^{-1} \subseteq D^{k+1}G$

23. Satz Eine Gruppe G ist auflösbar genau dann, wenn für ein $m \geq 0$ gilt $D^mG = \{e\}$. #

Beweis Angenommen, $D^mG = \{e\}$. Dann ist

$$G = D^0G \supseteq D^1G \supseteq D^2G \supseteq \dots \supseteq D^mG = \{e\}$$

eine Normalreihe und $D^kG / D^{k+1}G = D^kG / D(D^kG)$

ist abelsch nach §2.23(ii)

Ist umgekehrt $G = G_m \trianglerighteq \dots \trianglerighteq G_0 = \{e\}$ eine Normalreihe mit abelschen Faktoren, so folgt

$DG_k \subseteq G_{k-1} \rightsquigarrow D^kG_k \subseteq D^{k-1}G_{k-1} \subseteq D^{k-2}G_{k-2} \dots$

$\Rightarrow D^mG \subseteq D^{m-1}G_m \subseteq D^{m-1}G_{m-1} \subseteq \dots \subseteq D^0G_0 = \{e\}$ □

Korollar Bilder und Untergruppen von auflösbaren Gruppen sind auflösbar.

Beis. Sei G auflösbar, mit $D^m G = \{e_G\}$.

Sei $G \xrightarrow{\varphi} K$ ein Homomorphismus. Es folgt

$D^m(\varphi(G)) = \varphi(D^m G) = \varphi(\{e_G\}) = \{e_K\}$.

Sei $H \leq G$ Untergruppe, es folgt $DH \leq DG$

$\Rightarrow D^k H \leq D^k G \Rightarrow D^m H \leq D^m G = \{e\}$ □

24 **Def** Eine Gruppe G heißt **perfekt**, wenn gilt $DG = G$. ($\Rightarrow D^m G = G$ für alle m)

Abs.: Eine Gruppe, die gleichzeitig perfekt und auflösbar ist, ist trivial

25. Die Symmetrischen und Alternierenden Gruppen

$\mathrm{Sym}(n) = \mathrm{Sym}(\{1,2,\dots,n\})$ Gruppe aller Permutationen der Menge $\{1,\dots,n\} = X$

Es gilt $\#\mathrm{Sym}(n) = n! = n\cdot(n-1)\cdot(n-2)\cdots 2\cdot 1$,

denn: $\mathrm{Sym}(n)$ operiert transitiv auf der n-elem. Menge X. Der Stabilisator von $n \in X$ ist $\mathrm{Sym}(n-1)$, also

$$n = \frac{\#\mathrm{Sym}(n)}{\#\mathrm{Sym}(n-1)} \Rightarrow \#\mathrm{Sym}(n) = n!$$

Ergänzung zu Lin. Algebra II § 4.6 (online)

$\pi \in Sym(n)$ $\quad sign(\pi) = \prod_{i<j} \frac{\pi(i)-\pi(j)}{i-j} \in \{\pm 1\}$

$Sym(n) \xrightarrow[\text{(die alternierende Gruppe)}]{sign} C_2 = \{\pm 1\}$ ist Homomorphismus, der Kern ist $Alt(n) = \{\pi \in Sym(n) \mid sign(\pi) = 1\}$

Ist τ_{ij} : $\begin{cases} i \to j \\ j \to i \\ k \to k \text{ für } k \neq i,j \end{cases}$ $\quad i \neq j$

so gilt $sign(\tau_{ij}) = -1$. Die Transpositionen τ_{ij}, $i<j$ erzeugen $Sym(n)$ (LA II Ü A 4.3)

Folglich gilt $Alt(n) = \{\pi \in Sym(n) \mid \pi$ läßt sich schreiben als Produkt einer gerade Zahl von Transpositionen$\}$.

Da C_2 abelsch ist, folgt aus § 2.22 (iii), dass $D Sym(n) \subseteq Alt(n)$.

Satz Es gilt $D Sym(n) = Alt(n)$. Für $n \geq 5$ gilt $D Alt(n) = Alt(n)$, d.h. $Alt(n)$ ist perfekt.

Beweis Für paarweise verschiedene Zahlen $i_1, \dots, i_k$ nennt man die Permutation $\pi = i_1 \to i_2 \to i_3 \to \dots \to i_k \to i_1$, $\ell \mapsto \ell$ für $\ell \neq i_1, i_2, \dots, i_k$

ein k-Zykel und schreibt kurz $\pi = (i_1, i_2, \dots, i_k)$

Ein 2-Zykel ist also das gleiche wie eine Transposition.

Beh $Alt(n)$ wird von den 3-Zykeln in $Sym(n)$ erzeugt.

Beweis Seien a,b,c,d paarweise verschiedene Zahlen. Es gilt

$$(a,c)\circ(a,b) = (a,b,c)$$
$$(a,b)\circ(c,d) = (a,d,c)\circ(a,b,c)$$ □

Nun gilt $[(a,b,c),(b,c)] = (b,a,c)$, es folgt

$D\,\mathrm{Sym}(n) = \mathrm{Alt}(n)$ (Für $n=2$ ist $\mathrm{Sym}(n)$ abelsch!)

Sei jetzt $n \geq 5$ und a,b,c,d,e paarweise verschiedene Zahlen.

Es folgt $[(a,b,c),(c,d,e)] = (d,c,a)$ □

Bem Die Gruppen $\mathrm{Alt}(3)$ und $\mathrm{Alt}(4)$ sind auflösbar (nachrechnen)

Ausblick (1) Jede endliche Gruppe ungerader Ordnung ist auflösbar. (!) Der Beweis dafür wurde von Feit-Thompson in den 60'er Jahren gefunden und ist sehr lang und kompliziert.

(2) Eine nicht triviale Gruppe heißt einfach, wenn $\{e\}$ und G die einzigen Normalteiler von G sind. Die endlichen Einfachen Gruppen sind:

- $\mathbb{Z}/p\mathbb{Z}$ p Primzahl
- $\mathrm{Alt}(n)$ $n \geq 5$
- Gewisse Matrizengruppen wie $PSL_n(\mathbb{F})$, $\mathbb{F}$ ein endlicher Körper ("Gruppen vom Lie-Typ")
- 26 sporadisch endliche einfache Gruppen, von denen die größte, das "Monster", mehr Elemente hat als das Universum Atome ...

Diese Klassifikation der endlichen Einfachen Gruppen ist eines der wichtigsten und tiefsten Ergebnisse der Mathematik des 20. Jhd. Der Beweis ist viele tausend Seiten lang und auf viele Artikel verteilt.