Gruppentheorie

Markus Junker

Sommersemester 2002

1 Grundlagen

$G = (G, \cdot, ^{-1}, e)$ ist eine *Gruppe*, falls $\cdot$ eine assoziative zweistellige Verknüpfung auf G (*Halbgruppe*) mit neutralem Element $e \in G$ ist (*Monoid*), bei der jedes Element $g \in G$ ein inverses Element g^{-1} besitzt. Die Abbildung $^{-1} : G \to G$ und das Element $e \in G$ sind durch $\cdot$ eindeutig bestimmt, d.h. eine Halbgruppe kann auf höchstens eine Art eine Gruppe sein.
[Wohingegen z.B. eine additive Gruppe auf viele Arten zu einem Ring gemacht werden kann, etwa gilt $(\mathbb{R}, +) \cong (\mathbb{C}, +)$. Beide sind sogar als $\mathbb{Q}$-Vektorräume isomorph, also als Gruppen isomorph zu $\bigoplus_{2^{\aleph_0}} \mathbb{Q}$. Auch legt $^{-1}$ die Gruppenstruktur natürlich nicht fest: jede Permutation von $\mathbb{N} \setminus \{0\}$ kann man $^{-1}$-erhaltend auf $\mathbb{Z}$ fortsetzen.]

Das Element g^{-1} ist sogar eindeutiges Rechts- und Linksinverses von g. Es folgt $(g^{-1})^{-1} = g$ und $(gh)^{-1} = h^{-1}g^{-1}$.

Eine Gruppe heißt *kommutativ* oder *abelsch*, falls $g_1 g_2 = g_2 g_1$ für alle $g_1, g_2 \in G$ gilt.

Das Multiplikationszeichen $\cdot$ wird oft weggelassen; für e steht manchmal 1. Kommutative Gruppen werden zuweilen additiv als $(G, +, -, 0)$ geschrieben. Die Anzahl der Elemente von G heißt die *Ordnung von* G.

Beispiele Die *triviale Gruppe* $E = \{e\}$.

Die *zyklischen Gruppen* $\mathbb{Z} = (\mathbb{Z}, +)$ und $Z_n := (\{0, \dots, n-1\}, +\bmod n) \cong \mathbb{Z}/n\mathbb{Z}$ (auch C_n oder $\mathbb{Z}_n$ geschrieben).

Geometrische Gebilde im $\mathbb{R}^n$ besitzen eine *Symmetrie–* und eine *Drehgruppe*. Zum Beispiel ist Z_n die Drehgruppe des regelmäßigen n-Ecks; seine Symmetriegruppe heißt die *Diëdergruppe* D_n. Die unendliche Diëdergruppe D_∞ ist die Symmetriegruppe von $\mathbb{Z}$ als Teilmenge von $\mathbb{R}$.

Die Automorphismen einer Struktur bilden stets eine Gruppe. Zum Beispiel kann man D_n (bzw. Z_n) auch als die Automorphismengruppe eines (gerichteten) Graphen ansehen, nämlich eines (gerichteten) Kreises der Länge n. Die Automorphismen eines Vektorraums V bilden die *allgemeine lineare Gruppe* $GL(V)$. Im Falle $V = K^n$ schreibt man dafür auch $GL(n, K)$.

Die Automorphismen einer Menge Ω sind einfach nur deren Permutationen: sie bilden die *symmetrische Gruppe* S_Ω. Falls $|\Omega| = n$, schreibt man kurz S_n. Untergruppen einer S_Ω heißen *Permutationsgruppen*: man darf dann Elemente nur nach gewissen Regeln vertauschen. Zu einer Permutationsgruppe gehört die Information, wie die Gruppenelemente als Permutation wirken.

Alle diese Beispiele sind Gruppen von Bijektionen, d.h. treten natürlicherweise als Permutationsgruppen auf. Man kann tatsächlich jede Gruppe als Permutationsgruppe auffassen, allerdings

gibt es dazu in der Regel verschiedene Möglichkeiten (z.B. kann Z_2 als Permutationsgruppe auf 4 Elementen entweder ein Paar oder zwei Paare vertauschen).

Manche Gruppen treten nicht natürlicherweise als Permutationsgruppen auf (man spricht dann von „abstrakten Gruppen“). Etwa die *additiven* und *multiplikativen Gruppen* von Körpern (wie $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{F}_q$). Die *Fundamentalgruppe* eines topologischen Raumes ist ein weiteres Beispiel. Manchmal tauchen Gruppen an ungewohnter Stelle auf: zum Beispiel bilden für einen Körper K gewisse K-Algebren unter dem Tensorprodukt eine Gruppe, die *Brauer–Gruppe* von K.

Homomorphismen Ein Homomorphismus zwischen Strukturen ist stets eine strukturerhaltende Abbildung. Ein Gruppenhomomorphismus zwischen zwei Gruppen G und H ist also eine Abbildung $\varphi : G \to H$, die $\varphi(g_1 \cdot g_2) = \varphi(g_1) \cdot \varphi(g_2)$, $\varphi(g^{-1}) = \varphi(g)^{-1}$ und $\varphi(e) = e$ erfüllt.

Es reicht, die erste Bedingung nachzuprüfen, d.h. ein Halbgruppenhomomorphismus zwischen Gruppen ist bereits ein Gruppenhomomorphismus. Mehr noch: ist G Gruppe, H Halbgruppe und $\varphi : G \twoheadrightarrow H$ ein surjektiver Halbgruppenhomomorphismus, so ist H bereits eine Gruppe.

Ein paar Beispiele für Gruppenhomomorphismen sind: Modulorechnen $\bmod n : \mathbb{Z} \to Z_n$; Determinante $\det : \mathrm{GL}(n, K) \to K^\times$; Signum $\mathrm{sgn} : S_n \to Z_2$; Auswertungshomomorphismen $K[X] \to A$, $P(X) \mapsto P(a)$ für Körper K und K-Algebren A, $a \in A$.

Untergruppen Eine *Untergruppe* U von G, in Zeichen $U \leqslant G$, ist eine unter allen Verknüpfungen abgeschlossene Teilmenge von G; insbesondere enthält sie e und ist daher nicht leer. Die Untergruppen von G sind genau die Bilder von Homomorphismen nach G.

Jede Untergruppe U induziert zwei Äquivalenzrelationen auf G: $g_1 \sim_l g_2 :\iff g_2^{-1} g_1 \in U$ und $g_1 \sim_r g_2 :\iff g_1 g_2^{-1} \in U$. Die Äquivalenzklassen von $\sim_l$ sind die *Linksnebenklassen* $gU := \{gu \mid u \in U\}$; die Äquivalenzklassen von $\sim_r$ sind die *Rechtsnebenklassen* $Ug := \{ug \mid u \in U\}$.

[Man kann die Verknüpfungen $\cdot$ und $^{-1}$, später auch ^{g} und $[\ ,\ ]$ durch elementweise Anwendung auf Teilmengen von G fortsetzen. Man schreibt dabei in der Regel g statt $\{g\}$.]

Beachte: $gU = U \iff g \in U$.

Je zwei Nebenklassen stehen in Bijektion zueinander: U mit gU bzw. Ug mittels der Abbildungen $u \mapsto gu$ bzw. $u \mapsto ug$. Also ist zum einen der *Index* $|G : U|$ von U in G, das ist die Anzahl der Rechts– bzw. Linksnebenklassen von U, wohlbestimmt. Zum andern folgt der

Satz 1 (von Lagrange) *Die Ordnung einer Untergruppe teilt die Gruppenordnung: es gilt* $|G| = |U| \cdot |G : U|$ *(bzw.* $|G : U| = \frac{|G|}{|U|}$*, falls* $|G|$ *endlich).*

Untergruppen von Untergruppen sind selbst Untergruppen, und aus $V \leqslant U \leqslant G$ folgt $|G : V| = |G : U| \cdot |U : V|$. Der Schnitt von Untergruppen ist wieder ein Untergruppe; insbesondere gibt es zu jeder Teilmenge X von G eine kleinste, X enthaltende Untergruppe: die *von* X *erzeugte Untergruppe* $\langle X \rangle$. Es gilt $\langle X \rangle = \{x_1^{\pm 1} \cdots x_k^{\pm 1} \mid k \in \mathbb{N}, x_i \in X\}$. Der Schnitt zweier Untergruppen U und V ist die größte in beiden enthaltene Untergruppe. Umgekehrt ist $\langle U \cup V \rangle$ die kleinste U und V enthaltende Untergruppen. Die Untergruppen von G bilden daher einen Verband.

Beispiel: Untergruppenverband von Z_{30} („Würfel“ mit Z_d für $d|30$) und S_3 ($A_3 = Z_3$ und dreimal $Z_2 = S_2$).

Übung: Sind $U, V \leqslant G$, so ist genau dann $UV \leqslant G$, wenn $UV = VU$. [Achtung: dies bedeutet nicht $uv = vu$ für $u \in U, v \in V$!]

Normalteiler Eine Untergruppe N heißt *normal* oder *Normalteiler* von G, in Zeichen $N \trianglelefteq G$, falls $gN = Ng$ für alle $g \in G$ gilt. Man schreibt h^g für $g^{-1}hg$; dann lautet die Normalteilerbedingung $N^g = N$ für alle $g \in G$.

In kommutativen Gruppen ist jede Untergruppe normal.

Im Falle eines Normalteilers N schreibt man G/N für die Menge der (Rechts- wie Links-) Nebenklassen. Man kann darauf repräsentantenweise die Gruppenoperation fortsetzen, also durch $g_1N \cdot g_2N := (g_1g_2)N$. Das neutrale Element ist dann $N = eN$, und es gilt $(gN)^{-1} = g^{-1}N$.

[Schon wegen $(gN)^{-1} = Ng^{-1}$ ist die Bedingung notwendig; ebenso, weil N in G/N als neutrales Element kommutieren muß.]

Normalteiler sind genau die Kerne von Homomorphismen aus G: Zu jedem Normalteiler existiert die kanonische Surjektion $G \twoheadrightarrow G/N$, $g \mapsto \bar{g} = gN$. Ist umgekehrt $\varphi : G \to H$ ein Homomorphismus, so gilt $\varphi(\ker(\varphi)^g) = \varphi(g^{-1})\varphi(\ker(\varphi))\varphi(g) = \varphi(g^{-1})e\varphi(g) = e$.

Schnitte von Normalteilern sind normal. Das Produkt von Normalteilern ist wieder ein Normalteiler. Das Produkt eines Normalteilers mit einer Untergruppe ist wieder eine Untergruppe. Normalteiler von Normalteilern sind nicht notwendig selbst normal!

Zu jeder Teilmenge $X \leqslant G$ gibt es

- einen kleinsten, X enthaltenden Normalteiler $X^G := \langle X^g \mid g \in G\rangle$;
- einen größten, in X enthaltenen Normalteiler $X_G := \bigcap_{g\in G} X^g$;
- eine maximale Untergruppe von G, in der X normal ist, den *Normalisator* $\mathbb{N}_G(X) = \{g \in G \mid X^g = X\}$ von X in G.

Homomorphiesätze Ein Gruppenhomomorphismus $\varphi : G \to H$ induziert einen Isomorphismus $\overline{\varphi} : G/\ker(\varphi) \to \text{Bild}(\varphi)$, $g\ker(\varphi) \mapsto \varphi(g)$. Der Homomorphismus φ zerfällt in $G \twoheadrightarrow G/\ker(\varphi) \xrightarrow{\cong} \text{Bild}(\varphi) \hookrightarrow H$.

Beispiele: $\mathbb{Z}/n\mathbb{Z} \cong Z_n$, $GL(n,K)/SL(n,K) \cong K^\times$, $S_n/A_n \cong Z_2$, $\mathbb{R}[X]/(X^2+1) \cong \mathbb{C}$.

Satz 2 (Noethersche Isomorphiesätze)

(a) *Sei* $H \leqslant G$ *und* $N \trianglelefteq G$. *Dann ist* $H \cap N \trianglelefteq N$ *und* $H/(H\cap N) \cong HN/N$

(b) *Seien* $N \leqslant M \trianglelefteq G$, $N \trianglelefteq G$. *Dann ist* $M/N \trianglelefteq G/N$ *und* $(G/N)/(M/N) \cong G/M$.

Beweis: (a) $H \to HN/N$, $h \mapsto hN$ ist ein Epimorphismus mit Kern $H \cap N$.
(b) $G/N \to G/M$, $gN \mapsto gM$ ist ein Epimorphismus mit Kern M/N. ∎

Direkte Produkte Das (mengentheoretische) *direkte Produkt von Gruppen* $G_1, \ldots, G_n$ wird durch die komponentenweisen Verknüpfungen zu einer Gruppe, die mit $G_1 \times \cdots \times G_n$ bezeichnet wird.

[Kategorientheoretisch ist $G_1 \times \cdots \times G_n$ ein Koprodukt, also gleich der direkten Summe $G_1 \oplus \cdots \oplus G_n$. Für unendlich viele Faktoren stimmt dies nicht mehr: die direkte Summe $\bigoplus_{i\in I} G_i$ ist die Untergruppe des direkten Produktes $\prod_{i\in I} G_i$, die aus den Elementen mit endlichem Träger besteht. Das kategorientheoretische Produkt ist das *freie Produkt*]

Sind U und V zwei kommutierende Untergruppen von G, dann ist die Abbildung $\varphi : U\times V \to G$, $(u,v) \mapsto uv$ ein Homomorphismus mit Bild UV und Kern $\{(u,v) \mid uv = e\} = \{(u,u^{-1}) \mid u \in U\cap V\}$. Es ist also φ ein Isomorphismus, falls $G = UV$ und $U \cap V = E$. G heißt dann das *innere direkte Produkt* von U und V. Entsprechend für mehrere kommutierende Untergruppen.

2 Zyklische Gruppen

Eine Gruppe G heißt *zyklisch*, falls sie von einem Element erzeugt wird. Zyklische Gruppen sind daher kommutativ.

Sei G zyklisch, $g \in G$. Man definiert $g^0 := e$, $g^{n+1} := g \cdot g^n$ per Induktion, und $g^{-n} := (g^n)^{-1}$. Dadurch wird die Abbildung $\gamma_g : \mathbb{Z} \to G, n \mapsto g^n$ zu einem Gruppenhomomorphismus. Außerdem gilt $(g^n)^m = g^{nm}$. $\text{Bild}(\gamma_g) = \langle g \rangle$ ist die von g erzeugte zyklische Untergruppe. Die Größe des Bildes $o(g) := |\langle g \rangle|$ heißt die *Ordnung* von g. Der *Exponent* von G, $\exp G$, ist das kleinste gemeinsame Vielfache der Ordnungen aller Elemente, also die kleinste Zahl n mit $g^n = e$ für alle $g \in G$, falls eine solche existiert, ∞ sonst.

Satz 3 *Die zyklischen Gruppen sind $\mathbb{Z}$ und Z_n für $n \geqslant 1$. Zwei zyklische Gruppen gleicher Ordnung sind isomorph. Untergruppen und homomorphe Bilder zyklischer Gruppen sind zyklisch.*

Beweis: Aus der Homomorphieeigenschaft von φ folgt, daß $\varphi(\langle g \rangle) = \langle \varphi(g) \rangle$. Für $X \subseteq \mathbb{Z}$ liegt $\text{ggT}(X) \in \langle X \rangle$ (denn der ggT schreibt sich als $\mathbb{Z}$-Linearkombination von X), und es gilt $\langle \text{ggT}(X) \rangle = \langle X \rangle$. Eine Untergruppe U von Z_n ist damit als homomorphes Bild des Urbildes von U unter der natürlichen Projektion $\mathbb{Z} \to Z_n$ ebenfalls zyklisch.

Für zyklisches $G = \langle g \rangle$ gilt nun $\mathbb{Z}/\ker(\gamma_g) \cong G$.
1. Fall: $\ker(\gamma_g) = \{0\}$, $\langle g \rangle \cong \mathbb{Z}$, alle g^n sind verschieden und $o(g) = \infty$.
2. Fall: $\ker(\gamma_g) = n\mathbb{Z}$, $\langle g \rangle = \{g^0, g^1, \ldots, g^{n-1}\} \cong Z_n$ und $o(g) = n$. ■

Ein Homomorphismus von einer zyklischen Gruppe ist durch das Bild eines Erzeugers eindeutig bestimmt. Es gibt genau dann einen Homomorphismus $\gamma_h : Z_n \to H$ mit $\gamma_h(1) = h$, falls $o(h) | n$.

Untergruppenverbände und Automorphismengruppen der zyklischen Gruppen

$\mathbb{Z}$: Die Untergruppen sind $n\mathbb{Z}$ für $n \in \mathbb{Z}$, die für $n \neq 0$ jeweils zu $\mathbb{Z}$ isomorph sind. Es gilt $m\mathbb{Z} \leqslant n\mathbb{Z} \iff n | m$. $\mathbb{Z}$ hat zwei Erzeugende: 1 und -1. Daher gilt $\text{Aut}(\mathbb{Z}) = Z_2$.

Z_n: In Z_n erzeugt m eine Untergruppe der Ordnung $\frac{n}{\text{ggT}(m,n)}$. Insbesondere gibt es $\varphi(n)$ viele Erzeugende von Z_n und zu jedem $d | n$ hat Z_n eine zu Z_d isomorphe Untergruppe, und zwar genau eine (da es in Z_n nur d Elemente gibt, deren Ordnung d teilt, oder da $\sum_{d|n} \varphi(d) = n$). Diese Untergruppe ist $\left\{0, \frac{n}{d}, 2\frac{n}{d}, \ldots, (d-1)\frac{n}{d}\right\}$.
Für $\text{ggT}(k, n) = 1$ definiert $x \mapsto kx$ einen Automorphismus von Z_n, und jeder Automorphismus ist von dieser Form. Also gilt $\text{Aut}(Z_n) = ((\mathbb{Z}/n\mathbb{Z})^*, \cdot)$.

Satz 4 *Das direkte Produkt zweier nicht-trivialer zyklischer Gruppen ist genau dann wieder zyklisch, wenn beide Gruppen endlich von teilerfremder Ordnung sind.*

Beweis: Ist $Z_m = \langle g \rangle$ und $Z_n = \langle h \rangle$, so gilt $o((g, h)) = \exp(Z_m \times Z_n) = \text{kgV}(m, n)$.
$\mathbb{Z} \times \mathbb{Z} \ncong \mathbb{Z}$, da z.B. $|\text{Aut}(\mathbb{Z} \times \mathbb{Z})| \geqslant 3$, und $\mathbb{Z} \times Z_n \ncong \mathbb{Z}$ für $n > 1$, da $Z_n \leqslant \mathbb{Z} \times Z_n$. ■

Eine Gruppe heißt *einfach*, wenn sie nicht trivial ist und außer E und sich selbst keine Normalteiler besitzt.

Satz 5 *Die kommutativen einfachen Gruppen sind genau die zyklischen Gruppen von Primzahlordnung.*

BEWEIS: Da G kommutativ, sind alle Untergruppen Normalteiler, insbesondere $\langle g\rangle$ für $g \in G$. Also ist G zyklisch. Aus der Untergruppenstruktur oben ersieht man, daß genau die zyklischen Gruppen von Primzahlordnung keine nicht-trivialen Untergruppen besitzen. ■

3 Freie Gruppen

Sei X eine Menge, dann bezeichnet X^* die Menge der *Wörter* über X, d.h. der endlichen Folgen von Elementen von X. Unter der *Konkatenation* (Hintereinanderschreibung) bildet X^* ein Monoid (mit dem leeren Wort als neutralem Element).

Dieses Monoid kann man in eine Gruppe einbetten, die *freie Gruppe über* X. Dazu nimmt man eine Bijektion $^{-1}$ zwischen X und einer zu X disjunkten, gleichmächtigen Menge X^{-1} und bildet $F := (X \cup X^{-1})^*$. Auf F sei $\sim$ die kleinste Äquivalenzrelation, so daß für Wörter $v, w \in F$ und $x \in X$ sowohl $vxx^{-1}w \sim vw$ als auch $vx^{-1}xw \sim vw$ gilt. (Zwei Wörter in F sind also äquivalent, wenn man sie in endlich vielen solchen Schritten ineinander überführen kann). Falls $v \sim v'$ und $w \sim w'$, so gilt $vw \sim v'w'$, daher ist $F_X := F/\sim$ ein Monoid. Tatsächlich ist F_X eine Gruppe, denn durch elementweises Anwenden von $^{-1}$ erhält man Inverse. Die Elemente von X heißen *freie Erzeugende* von F_X.

Als Trägermenge von F_X kann man auch die *reduzierten Wörter* betrachten: in jeder $\sim$-Klasse gibt es genau einen Repräsentanten minimaler Länge (das muß bewiesen werden!), in dem kein x und x^{-1} aufeinander folgen. Die Gruppenoperation besteht dann aus Konkatenation und anschließender Reduktion, d.h. sukzessives Entfernen von xx^{-1} und $x^{-1}x$.

Falls $X \subseteq G$, so gibt es den Auswertungshomomorphismus $X^* \to G$, der jedem Wort den Wert des Wortes in G zuordnet. X erzeugt genau dann frei eine freie Untergruppe von G, wenn kein nicht-leeres reduziertes Wort in $X \cup X^{-1}$ den Wert e erhält.

Satz 6 *Jede Abbildung $f : X \to G$ setzt sich eindeutig zu einem Homomorphismus $\hat{f} : F_X \to G$ fort. Insbesondere setzt sich jede Abbildung (Bijektion) $X \to Y$ eindeutig zu einem Homo-(Iso-) morphismus $F_X \to F_Y$ fort. Ferner gilt $F_X \cong F_Y \iff |X| = |Y|$.*

BEWEIS: $\hat{f}(x_1^{\pm 1} \cdots x_n^{\pm 1}) = f(x_1)^{\pm 1} \cdots f(x_n)^{\pm 1}$ ist die einzige Möglichkeit, f zu einem Homomorphismus fortzusetzen. $\hat{f}$ ist dadurch wohldefiniert, denn jede Reduktion auf der F_X-Seite ermöglicht die entsprechende Reduktion auf der G-Seite. Die Homomorphie ist dann per Definition gegeben.

Ist $f : X \to Y$ bijektiv, so gilt $\widehat{f^{-1}} = \hat{f}^{-1}$. Daraus folgt $F_X \cong F_Y$, falls $|X| = |Y|$.

Sei $H_X := \langle w^2 \mid w \in F_X\rangle \trianglelefteq F_X$. In F_X/H_X hat jedes Element die Ordnung 2, ist also selbstinvers. Daher ist die Faktorgruppe kommutativ, denn $\bar{x}\bar{y} = (\bar{x}\bar{y})^{-1} = \bar{y}^{-1}\bar{x}^{-1} = \bar{y}\bar{x}$. Also ist F_X/H_X ein $\mathbb{F}_2$-Vektorraum, mit Basis X. Aus $F_X \cong F_Y$ folgt nun $F_X/H_X \cong F_Y/H_Y$ (als Vektorräume), also $|X| = |Y|$. ■

Eine Gruppe heißt *frei*, falls sie zu einem F_X isomorph ist. $|X| = \kappa$ heißt der Rang von F_X; man schreibt dafür auch einfach F_κ. [Tarskis Problem: sind alle freien, nicht-kommutativen Gruppen elementar äquivalent zueinander? Stimmt für unendlich viele freie Erzeugende.]

Beispiele: (1) $F_0 = E$; $F_1 \cong \mathbb{Z}$.

(2) F_2: $\left(\begin{smallmatrix}1 & 2\\ 0 & 1\end{smallmatrix}\right)$ und $\left(\begin{smallmatrix}1 & 0\\ 2 & 1\end{smallmatrix}\right)$ erzeugen frei eine freie Untergruppe von $\mathrm{SL}(2,\mathbb{Z})$.

BEWEIS: Betrachte das Bild von 0 unter den zugehörigen Möbiustransformationen $\alpha(z) = z+2$

und $\beta(z) = \frac{z}{2z+1}$ auf $\hat{\mathbb{C}}$. Für $n \neq 0$ verschiebt α^n den offenen Einheitskreis außerhalb des Einheitskreises und läßt ∞ fest. Beachte $\beta(z) = \alpha(z^{-1})^{-1}$, also $\beta^n(z) = \alpha^n(z^{-1})^{-1}$, damit wirft β^n für $n \neq 0$ das Äußere des Einheitskreises samt ∞ in den Einheitskreis. Damit lassen nur die reduzierten Wörter in α und β, in denen β nicht vorkommt, ∞ fest. ■

Satz 7 (Schreier) *Untergruppen freier Gruppen sind frei.* [schwer, ohne Beweis]

(3) Falls F_2 von x, y frei erzeugt wird, so bilden die $z_n := y^{-n}xy^n$ ein freies System.

BEWEIS: Ein nicht-triviales Wort in den z_n ist der Form $w = z_{n_1}^{k_1} \cdots z_{n_j}^{k_j}$ mit $n_i \neq n_{i+1}$, $k_i \neq 0$ und $j > 0$. Wegen $z_n^k = y^{-n}x^k y^n$ folgt $w = y^{-k_1}x^{k_1}y^{n_2-n_1} \cdots y^{n_j-n_{j-1}}x^{k_j}y^{n_j}$. Dies ist die reduzierte Form, also $w \neq e$. ■

Also gilt $F_{\aleph_0} \leqslant F_2$.[1] (Es gilt natürlich auch $F_2 \leqslant F_{\aleph_0}$!) Daher:

- Der Rang kann bei Untergruppen zunehmen.
- Von zwei Elementen erzeugte Gruppen sind bereits beliebige kompliziert.
- Alle freien Gruppen sind linear, d.h. Untergruppe von einem $\mathrm{GL}(n, K)$.
  [Das folgt für überabzählbaren Rang aus modelltheoretischen Überlegungen, denn die Klasse der linearen Gruppen ist unter elementarer Äquivalenz abgeschlossen.]

Freie Erzeugendensysteme freier Gruppen ähneln Basen von Vektorräumen insofern ihre Mächtigkeit festgelegt ist. Es gibt aber freie Systeme größeren Ranges (es gilt also kein Ergänzungssatz!)

Satz 8 **(a)** *Für $n \in \mathbb{N}$ gilt: wird F_n von $g_1, \ldots, g_n$ erzeugt, so sind $g_1, \ldots, g_n$ frei.*

(b) *F_κ kann nicht von weniger als κ Elementen erzeugt werden.*

κ Erzeugende sind natürlich bei unendlichem κ in der Regel nicht frei.

BEWEIS: (a) ist schwer: ohne Beweis. (b) ist für endliches κ klar aus (a). Für unendliches κ enthält ein kleineres Erzeugendensystem weniger als κ Buchstaben. ■

Im Einklang mit der bisherigen Definition sei der *Rang* einer beliebigen Gruppe die minimale Anzahl von Erzeugenden.

$Z(G) := \{g \in G \mid gh = hg \text{ für alle } h \in G\}$ heißt das *Zentrum* von G; dies ist stets ein Normalteiler. G ist genau dann kommutativ, wenn $G = Z(G)$.

Satz 9 *Für $\kappa > 1$ gilt $Z(F_\kappa) = E$.*

BEWEIS: Falls das reduzierte Wort v weder mit $x \in X$ noch mit x^{-1} beginnt, so gilt $xv \neq vx$. ■

[Es gilt sogar mehr: die einzigen kommutativen Untergruppen sind die (unendlichen) zyklischen; „kommutieren“ ist eine Äquivalenzrelation auf $G \setminus \{e\}$.]

Präsentationen von Gruppen Jede Gruppe ist homomorphes Bild einer freien Gruppe. Sei nämlich X ein Erzeugendensystem von G. Dann setzt sich die Identität auf X zu einem (surjektiven) Homomorphismus $\widehat{\mathrm{id}_X} : F_X \to G$ fort.

Sei $\pi : F_X \to G$ eine Surjektion und R erzeuge $\ker(\varphi)$ als Normalteiler, d.h. $\ker(\varphi) = R^{F_X}$. Dann heißt $\langle X, R\rangle$ eine *Präsentation* von G: X ist ein Erzeugendensystem mit *Relationen* R und G ist die „größte“ von X erzeugte Gruppe, in der alle Wörter aus R der Wert e annehmen.

[1] $\aleph_0$ steht für „abzählbar–unendlich“, $2^{\aleph_0}$ für „kontinuumsgroß“ (d.h. so groß wie $\mathbb{R}$).

Beispiel: (1) $\langle d \mid d^n \rangle$ ist eine Präsentation von Z_n.
(2) $\langle s, d \mid s^2, d^n, s^{-1}dsd \rangle$ ist eine Präsentation von D_n. Ohne die Relation d^n erhält man eine Präsentation von D_∞.

Satz 10 (Dyck) *Ist $R \subseteq S$, so setzt sich id_X zu einem eindeutig bestimmten surjektiven Homomorphismus $\langle X \mid R \rangle \to \langle X \mid S \rangle$ fort.*

Eine Gruppe $\langle X, R \rangle$ heißt *endlich präsentiert*, falls sowohl X als auch R endlich sind. Jede endliche Gruppe ist endlich präsentiert; jede endlich präsentierte Gruppe ist endlich erzeugt – die Umkehrungen gelten jeweils nicht.

Das *Wortproblem* für eine endlich präsentierte Gruppe $G = \langle X, R \rangle$ fragt, ob es einen Algorithmus gibt, welcher für Wörter in X^* entscheidet, ob sie in G der Wert e annehmen. Es gibt endlich präsentierte Gruppen mit unlösbarem Wortproblem. In F_n ist dagegen das Wortproblem lösbar, indem man einfach zum reduzierten Wort übergeht und prüft, ob es gleich e ist.

Es ist auch nicht entscheidbar, ob eine Präsentation die triviale Gruppe liefert.

Freie Gruppen in Varietäten Ist W eine Menge von Wörtern in den Variablen $X = \{x_1, x_2, \dots\}$ und X^{-1} und G eine Gruppe, so sei $W(G)$ die Menge aller Auswertungen der Wörter in G, d.h. die Menge der Bilder von W unter allen Homomorphismen $X^* \to G$. Die Klasse der Gruppen G, für die $W(G) = \{e\}$ gilt, heißt die von W bestimmte *Varietät von Gruppen.*

Zum Beispiel ist die Varietät der abelschen Gruppen durch das Wort $x_1x_2x_1^{-1}x_2^{-1}$ bestimmt, die Varietät der Gruppen vom Exponenten 2 durch das Wort x^2.

Ist $\mathfrak{V}$ die durch W definierte Varietät, dann heißt $F_\kappa/\langle W(F_\kappa)\rangle$ eine *in $\mathfrak{V}$ freie Gruppe.* Ist $X \subseteq G \in \mathfrak{V}$, dann setzt sich id_X eindeutig zu einem Homomorphismus $F_\kappa/\langle W(F_\kappa)\rangle \to G$ fort; insbesondere ist jede Gruppe in $\mathfrak{V}$ homomorphes Bild einer in $\mathfrak{V}$ freien Gruppe.

Beispiel: Für $W = \{x_1x_2x_1^{-1}x_2^{-1}\}$ ist $F'_\kappa := \langle W(F_\kappa)\rangle$ und $F_\kappa/F'_\kappa \cong \bigoplus_\kappa \mathbb{Z}$ die *freie abelsche Gruppe.*

Beweis: : Für $\langle x_i \rangle \cong \mathbb{Z}$ erfüllt $\bigoplus_{i\in\kappa}\langle x_i\rangle$ die Präsentation $\langle (x_i)_{i\in\kappa} \mid x_ix_jx_i^{-1}x_j^{-1}\rangle$, mit dem Satz von Dyck erhält man also eine Surjektion $F_\kappa/F'_\kappa \to \bigoplus_{i\in\kappa}\langle x_i\rangle$. Umgekehrt kann man einem Element $n_1x_{i_1}\cdots n_kx_{i_k} \in \bigoplus_{i\in\kappa}\langle x_i\rangle$ mit $i_1 \leqslant \cdots \leqslant i_k$ das Wort $x_{i_1}^{n_1}\cdots x_{i_k}^{n_k}$ zuordnen, was eine surjektive Umkehrung auf F_κ/F'_κ ergibt. ∎

Freie Produkte Seien G und H zwei Gruppen. Dann ist ihr freies Produkt $G * H$ definiert als $\langle G \cup H \mid R\rangle$, wobei R alle Wörter über G und über H enthält, die in G bzw. in H trivial werden. Das freie Produkt von G und H kann man auch als die Folgen von Elementen, die abwechselnd aus G und aus H kommen, beschreiben, wobei die Gruppenoperation die Konkanetation mit den naheliegenden Reduktionen ist.

Beispiel: (1) $F_\kappa * F_\lambda \cong F_{\kappa+\lambda}$
(2) $Z_2 * Z_2 \cong D_\infty$ ($x \mapsto -x$ und $x \mapsto 1 - x$ sind freie Erzeuger der Ordnung 2).
(3) $Z_2 * Z_3 \cong \mathrm{PSL}(2, \mathbb{Z})$ [siehe Robinson 6.2]

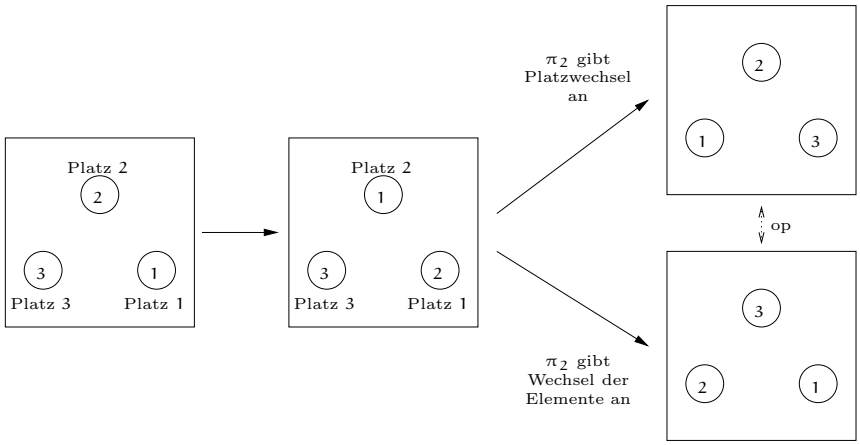
Satz 11 *Man kann jede Gruppe vom Rang $\leqslant \aleph_0$ in eine vom Rang 2 einbetten.*

Es gibt also $2^{\aleph_0}$ viele Gruppen vom Rang 2, im Gegensatz zu $\aleph_0$ vielen zyklischen. [Direkt: man kann in $F_{\{x,y\}}$ gewisse Relationen $o(y^{-n}xy^n) = n$-te Primzahl fordern.]

BEWEIS: [Skizze] $G = \langle e = g_0, g_1, \dots \rangle$ wird zunächst in $G_1 := G * F_{\{a,b\}}$ eingebettet. Betrachte darin die Untergruppen $H_1 = \langle a, a^b, a^{b^2}, \dots \rangle$ und $H_2 = \langle b, g_0 b^a, g_1 b^{a^2}, \dots \rangle$. Beide Erzeugendensysteme sind frei, also ist $\varphi : H_1 \to H_2$, $\varphi(a^{b^n}) = g_n b^{a^n}$ ein Isomorphismus. Nun kann man G_1 nach $G_2 := (G_1 * \langle t \rangle)/K$ abbilden, wobei $o(t) = \infty$ und K besagt, daß φ von der Konjugation mit t induziert wird, also die Abbildung $H \to H$, $x \mapsto x^t$ auf H_1 mit φ übereinstimmt. Es ist nun ein nicht-trivialer Satz, daß dies eine Einbettung ist. Dann sieht man $H = \langle a, t \rangle$. ■

4 Automorphismen und semi-direkte Produkte

Die Gruppe G^{op} Zu jeder Gruppe $(G, \cdot)$ gibt es die Gruppe $G^{op} = (G, *)$ mit $h * g = gh$. Es ist $G \cong G^{op}$ vermöge $g \mapsto g^{-1}$; die Identität dagegen ist kein Homomorphismus. Der Unterschied wird bei Gruppen von Abbildungen deutlich: versteht man die Verknüpfung $f \circ g$ als „erst f, dann g“ oder umgekehrt? Permutationsgruppen illustrieren den Unterschied: Sei $\pi_1 = \binom{123}{213}$ und $\pi_2 = \binom{123}{231}$. Was ist $\pi_1 \circ \pi_2$?



Innere Automorphismen $\gamma_g : x \mapsto x^g := g^{-1}xg$ heißt *Konjugation mit* g und ist ein Automorphismus von G. Man erhält durch $g \mapsto \gamma_{g^{-1}}$ einen Homomorphismus $\varphi : G \to \mathrm{Aut}(G)$ mit $\mathrm{Bild}(\varphi) = \mathrm{Inn}(G)$, den sogenannten *inneren Automorphismen*, und $\mathrm{Kern}(\varphi) = Z(G)$.

BEWEIS: $(\gamma_g)^{-1} = \gamma_{g^{-1}}$ und $\gamma_{gh} = \gamma_h \circ \gamma_g$.
Ferner: $\gamma_g = \mathrm{id} \iff x = x^g$ für alle $x \iff gx = xg$ für alle $x \iff g \in Z(G)$. ■

Beachte: $g \mapsto \gamma_g$ ist ein Homomorphismus $G \to \mathrm{Aut}(G)^{op}$!

Es gilt $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$; der Quotient $\mathrm{Out}(G) := \mathrm{Aut}(G)/\mathrm{Inn}(G)$ heißt die Gruppe der *äußeren Automorphismen*.

BEWEIS: $\alpha^{-1} \circ \gamma_g \circ \alpha = \gamma_{\alpha^{-1}(g)}$ für $g \in G$ und $\alpha \in \mathrm{Aut}(G)$. ■

Eine Untergruppe ist genau dann normal, wenn sie invariant unter $\mathrm{Inn}(G)$ ist. Eine Untergruppe, die sogar unter ganz $\mathrm{Aut}(G)$ invariant ist, heißt *charakteristisch*. Zum Beispiel ist das Zentrum eine charakteristische Untergruppe.

Semidirekte Produkte Angenommen $N \trianglelefteq G$, $H \leqslant G$ mit $HN = G$ und $H \cap N = E$. Dann heißt $G = H \ltimes N = N \rtimes H$ *(inneres) semidirektes Produkt von* H *und* N.

Jedes Element $g \in G$ hat dann eine eindeutige Darstellung $g = hn$ mit $h \in H$ und $n \in N$ (denn

$h_1n_1 = h_2n_2 \Longrightarrow h_2^{-1}h_1 = n_2n_1^{-1} \in H \cap N = E$). Die Abbildung $N \to N$, $n \mapsto n^h$ ist für $h \in H$ ein Automorphismus von N; mit dem zugehörigen Homomorphismus $\alpha : H \to \mathrm{Aut}(N)$ gilt also $(h_1n_1)(h_2n_2) = (h_1h_2)(n_1^{h_2}n_2) = (h_1h_2)(\alpha(h_2)(n_1) \cdot n_2)$.

Seien umgekehrt H, N und $\alpha : H \to \mathrm{Aut}(N)$ gegeben. Dann bildet man das *(äußere) semidirekte Produkt* $G := H \ltimes_\alpha N = N \rtimes_\alpha H$ mit Grundmenge $H \times N$ und Operation $(h_1n_1) \cdot (h_2n_2) = (h_1h_2, \alpha(h_2)(n_1) \cdot n_2)$. Durch $h \mapsto (h, e)$ und $n \mapsto (e, n)$ kann man H und N als Untergruppen von G auffassen; es gilt dann $N \trianglelefteq G$ und $\alpha(h_2)$ wird zur Konjugation mit h_2 (im semidirekten Produkt werden die Automorphismen $\alpha[H]$ von inneren Automorphismen induziert).

Das semidirekte Produkt ist genau dann ein direktes Produkt, wenn $\alpha[H] = \{\mathrm{id}\}$.

Beispiel: $D_n = Z_2 \ltimes Z_n$. Zugrunde liegt ein nicht-trivialer Homomorphismus $Z_2 \to \mathrm{Aut}(Z_n)$.

Das Kranzprodukt Wir betrachten zunächst einen Spezialfall: Die Automorphismengruppe einer Äquivalenzrelation mit n Klassen von jeweils k Elementen heißt das *Kranzprodukt* $S_k \wr S_n$.

Satz 12 *Es ist* $S_k \wr S_n \cong (\underbrace{S_k \times \ldots \times S_k}_{n\text{-}mal}) \rtimes S_n$*; der Homomorphismus* $S_n \to \mathrm{Aut}(S_k \times \cdots \times S_k)$ *ist durch das Vertauschen der Komponenten gegeben. Insbesondere gilt* $|S_k \wr S_n| = n \cdot k^n$.

Beweis: Sei S_k Permutationsgruppe auf X, S_n auf Y. Dann operiert $S_k \wr S_n$ auf $X \times Y$. Als Untergruppen hat man zum einen $S_k^n := S_k \times \cdots \times S_k$ mit komponentenweiser Operation auf den ersten Komponenten, zum andern S_n mit Operation auf der zweiten Komponente, die erste festlassend. Man sieht leicht $S_k^n \cap S_n = E$, $S_k^n \trianglelefteq \langle S_k^n, S_n\rangle = S_k^n \cdot S_n$ und $\langle S_k^n, S_n\rangle = S_k \wr S_n$. ■

Im allgemeinen Fall sei G Permutationsgruppe auf X und H Permutationsgruppe auf Y. Das *Kranzprodukt* $G \wr H$ ist die Permutationsgruppe auf $X \times Y$, die von folgenden Permutationen erzeugt wird:

$$(x, y) \mapsto \begin{cases} (g(x), y) & \text{falls } y = y_0 \\ (x, y) & \text{falls } y \neq y_0 \end{cases} \quad \text{für alle } y_0 \in Y,\ g \in G$$

$$(x, y) \mapsto (x, h(y)) \quad \text{für alle } h \in G$$

Es gilt dann $G \wr H \cong (\underbrace{H \times \ldots \times H}_{|G|\text{-mal}}) \rtimes_\alpha G$, wobei $\alpha : G \to \mathrm{Aut}(H \times \ldots \times H)$ die Operation von G auf den Komponenten angibt. Es folgt $|G \wr H| = |H|^{|G|} \cdot |G|$.

Beispiel (Rubik's Cube):

„Verdrehgruppe“ $\overset{\text{Index 12?}}{\leqslant}$ $\underbrace{(S_3 \wr S_8)}_{\text{Op. auf Ecken}} \times \underbrace{(S_2 \wr S_{12})}_{\text{Op. auf Kanten}}$ mit Ordnung $8 \cdot 3^8 \cdot 12 \cdot 2^{12} \approx 2{,}6 \cdot 10^9$

5 Gruppenoperationen

Sei G eine Gruppe und $\Omega \neq \emptyset$ eine Menge. Dann *operiert* G *auf* Ω und Ω heißt eine G-*Menge*), falls es zu jedem $\omega \in \Omega$ und $g \in G$ ein $\omega.g$ gibt mit

1. $\omega.e = \omega$ für alle $\omega \in \Omega$
2. $(\omega.g).h = \omega.(gh)$ für alle $\omega \in \Omega$ und $g, h \in G$

Eine Abbildung $\alpha : \Omega \to \Omega'$ zwischen G-Mengen heißt G-*äquivariant*, falls $\alpha(\omega.g) = \alpha(\omega).g$ für alle $\omega \in \Omega$ und $g \in G$ gilt. Zwei Operationen von G auf Ω, Ω' heißen *äquivalent*, falls es eine G-äquivariante Bijektion $\alpha : \Omega \to \Omega'$ gibt.

Satz 13 *G-Mengen Ω entsprechen Homomorphismen $\varphi : G \to \mathrm{Sym}(\Omega)$.*

BEWEIS: Setze $\varphi(g)(\omega) = \omega.g$. ■

Operiert G auf Ω, so ist $\omega \sim \omega' :\Longleftrightarrow \exists g \in G\ \omega.g = \omega'$ eine Äquivalenzrelation mit Äquivalenzklassen $\omega^G = \{\omega.g \mid g \in G\}$, den *Bahnen* der Operation.
$G_\omega := \{g \in G \mid \omega.g = \omega\} \leq G$ heißt der *Stabilisator* von ω.
Es gilt $\bigcap_{\omega\in\Omega} G_\omega =$ Kern des Homomorphismus $G \to \mathrm{Sym}(G)$.

Definition: Eine Operation $\varphi : G \to \mathrm{Sym}(\Omega)$ heißt

- *transitiv*, falls es nur eine Bahn gibt.
- *treu*, falls $\mathrm{Kern}(\varphi) = E$. (Dann ist G Permutationsgruppe von Ω, das heißt $G \leq \mathrm{Sym}(\Omega)$.)
- *semiregulär*, falls $G_\omega = E$ für alle $\omega \in \Omega$ gilt.
- *regulär*, falls sie transitiv und semiregulär ist.

Beispiel (1) G operiert regulär auf $\Omega = G$ durch Rechtsmultiplikation, das heißt $\omega.g := \omega g$, mit Homomorphismus $\rho_G : G \to \mathrm{Sym}(G)$. Ebenso operiert G regulär auf $\Omega = G$ durch Linksmultiplikation mit dem Inversen, $\omega.g := g^{-1}\omega$, mit Homomorphismus $\lambda_G : G \to \mathrm{Sym}(G)$.

Als Folgerung ergibt sich:

Satz 14 (Satz von Cayley) *Jede Gruppe G ist Untergruppe von* $\mathrm{Sym}(G)$*; jede Gruppe ist also Permutationsgruppe.*

Satz 15 *Die beiden Operationen ρ_G und λ_G sind äquivalent vermöge $\iota : \omega \mapsto \omega^{-1}$; folglich sind $\rho_G(G)$ und $\lambda_G(G)$ in* $\mathrm{Sym}(G)$ *durch ι konjugiert. Die beiden Operationen sind genau dann isomorph (das heißt: ergeben dieselbe Permutationsgruppe), wenn G kommutativ ist.*

BEWEIS: Die G-Äquivarianz von ι ist $(\omega g)^{-1} = g^{-1}\omega^{-1}$. Ist $\alpha : \Omega \to \Omega$ G-äquivariant und bijektiv, so folgt $\alpha(\alpha^{-1}(\omega)._1 g) = \omega._2 g$ aus $\alpha(\omega._1 g) = \alpha(\omega)._2 g$, also sind beide Operationen durch α konjugiert. Ist G kommutativ, so ergibt sich durch ρ_G und λ_G dieselbe Permutationsgruppe; ist umgekehrt $x \mapsto xg$ von der Form $x \mapsto h^{-1}x$, so folgt $g = h^{-1}$ mit $x = e$, also $xg = gx$ für alle x. ■

Hingegen sind λ_G und $\rho_{G^{op}}$ (bzw. ρ_G und $\lambda_{G^{op}}$) isomorph!

Beispiel (2) Sei $U < G$. Dann operiert U durch Rechtsmultiplikation auf $\Omega = G$. Die Operation ist treu, aber nicht transitiv. Die Bahnen sind die Rechtsnebenklassen $G : U$.

Beispiel (3) G operiert durch Rechtsmultiplikation auf $G : U$, das heißt $Uh.g := Uhg$.
Diese Operation ist transitiv, ihr Kern ist U_G. Sie ist also genau dann treu, wenn U keinen nicht-trivialen Normalteiler enthält; und genau dann regulär, wenn $U = E$.

Beispiel (4) G operiert auf $\Omega = G$ durch Konjugation, das heißt $\omega.g := \omega^g = g^{-1}\omega g$.
Der Kern ist Z(G), die Bahnen sind die Konjugationsklassen $h^G = \{g^{-1}hg \mid g \in G\}$. Im Gegensatz zu den bisherigen Beispielen sind diese im Allgemeinen von verschiedener Größe!

Satz 16 *G operiere auf Ω.*

(a) ω^G *steht in Bijektion mit* $G : G_\omega$ *vermöge* $\omega.g \mapsto G_\omega g$.
Insbesondere ist $|\omega^G| = |G : G_\omega|$*; im endlichen Fall gilt* $|\omega^G| \,\big|\, |G|$.

(b) *Ist* $\omega' \in \omega^G$*, etwa* $\omega' = \omega.g$*, so gilt* $G_{\omega'} = G_\omega^g$.

(c) *Ist* G *transitiv, so gilt* $|G| = |\Omega| \cdot |G_\omega|$ *für jedes* $\omega \in \Omega$.

(d) *Ist* G *regulär, so gilt* $|G| = |\Omega|$.

BEWEIS: (a) Die Abbildung ist offenbar surjektiv und wegen $\omega.g = \omega.h \iff \omega.gh^{-1} = \omega \iff gh^{-1} \in G_\omega \iff G_\omega g = G_\omega h$ wohldefiniert und injektiv.
(b) $h \in G_{\omega'} \iff \omega'.h = \omega' \iff \omega.gh = \omega.g \iff h^{g^{-1}} \in G_\omega \iff h \in G_\omega^g$.
(c),(d) sind klar nach (a). ■

Folgerung 17

(a) *Sei* G *kommutative, transitive Permutationsgruppe auf* Ω*. Dann operiert* G *regulär.*

(b) *Jede transitive Operation ist äquivalent zur Multiplikation auf* $G : G_\omega$ *(beliebiges* $\omega \in \Omega$*).*

(c) *Jede reguläre Operation ist äquivalent zur Rechtsmultiplikation auf* G.

BEWEIS: (a) Seien $\omega, \omega' \in \Omega$. Wegen der Transitivität existiert $g \in G$ mit $\omega' = \omega g$, also $G_{\omega'} = G_\omega^g = G_\omega$, da $G_\omega \trianglelefteq G$ (G kommutativ). Also $E = \bigcap_{\omega' \in \Omega} G_{\omega'} = G_\omega$.
(b) Direkt aus Teil (a) des Satzes.
(c) G operiere regulär durch Rechtsmultiplikation auf $G = G_\omega$. Dann ist $G_{G_\omega} = G_\omega = E$. ■

Falls G transitiv operiert und $G_\omega = E$ für ein $\omega \in \Omega$ gilt, so bereits $G_\omega = E$ für alls $\omega \in \Omega$!

Lemma 18 G *operiere durch Rechtsmultiplikation auf* $G : U$ *und* $G : V$.
Beide Operationen sind genau dann äquivalent, wenn U *und* V *konjugiert sind.*

BEWEIS: Gegeben sei $\alpha : (G : U) \xrightarrow{\sim} (G : V)$ mit $\alpha(U) = Vh$. Dann gilt:

$$g \in U \overset{*}{\iff} Vgh \underbrace{= \alpha(U)g = \alpha(Ug) \overset{*}{=} \alpha(U)}_{**} = Vh \overset{**}{\iff} hgh^{-1} \in V \iff g \in V^h$$

■

Folgerung 19 *Operiert* G *auf* Ω*, so gilt* $|\Omega| = \sum_{i \in I} |G : G_{\omega_i}|$*, wobei* $(\omega_i)_{i \in I}$ *ein Repräsentantensystam der Bahnen ist.*

Spezialfall: G operiere durch Konjugation auf Ω. Die einelementigen Konjugationsklassen werden genau durch die Elemente des Zentrums gebildet. Dabei ist G_ω gleich dem *Zentralisator* $C_G(\omega) = \{g \in G \mid g\omega = \omega g\}$ von ω in G. Es gilt nun die *Klassengleichung:*

$$|G| = |Z(G)| + \sum_{i \in I} |G : G_{g_i}|,$$

wobei $(g_i)_{i \in I}$ ein Repräsentantensystem der nicht-trivialen Konjugationsklassen ist.

Definition: G operiert durch Konjugation auf $\mathfrak{P}(G)$. Für $X \subseteq G$ ist der Stabilisator hierbei der *Normalisator* $N_G(X) := \{g \in G \mid X^g = X\}$ von X in G. Dadurch wird X zur $N_G(X)$-Menge unter Konjugation, der Kern ist der *Zentralisator* $C_G(X) := \{g \in G \mid xg = gx \text{ für alle } x \in X\}$.
Es gilt also $C_G(X) \trianglelefteq N_G(X)$, $N_G(X)/C_G(X) \hookrightarrow \mathrm{Sym}(X)$ und ferner $C_G(X) = \bigcap_{x \in X} C_G(x)$.

Falls $X \leqslant G$, so $X \leqslant N_G(X)$ und $N_G(X)/C_G(X) \hookrightarrow \mathrm{Aut}(X)$; weiter gilt $Z(N_G(X)) \leqslant C_G(X)$ und $Z(X) \leqslant C_G(X)$.

G heißt p-Gruppe (p Primzahl), falls $|G| = p^n$ für ein $n \geqslant 1$.

Satz 20 **(a)** *Ist* G *eine* p*-Gruppe, so ist* $Z(G) \neq E$ *und* $Z(G)$ *ist* p*-Gruppe.*

(b) $|G| = p^2$, p *Primzahl* $\Rightarrow$ G *abelsch.*

Beweis: (a) Klassengleichung: $|G| = |Z(G)| + \sum_{i \in I} |G : C_G(g_i)|$. Es gilt $p \,\big|\, |G : C_G(g_i)|$ und $p \,\big|\, |G|$, also auch $p \,\big|\, |Z(G)|$.
(b) Sei $Z := Z(G)$. Da $1 < |Z| \,\big|\, |G|$, gilt $|Z| = p$ oder $|Z| = p^2$. Also ist $G/Z = \langle gZ \rangle$ zyklisch. Somit gilt $G = \langle Z, g \rangle$. Da g mit Z kommutiert, ist G abelsch. ■

p-Gruppen sind daher nilpotent, d.h. $G, G/Z(G), (G/Z(G))/Z(G/Z(G)), \ldots$ erreicht E.

6 Symmetrische Gruppen

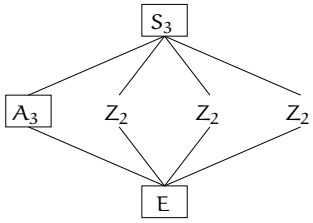
Zwei Elemente in S_n sind genau dann konjugiert zueinender, wenn sie in der Zykelzerlegung dieselbe Anzahl Zykel derselben Länge besitzen: $(i_{11} \ldots i_{1k_1}) \cdots (i_{n1} \ldots i_{nk_n})$ ist konjugiert zu $(j_{11} \ldots j_{1k_1}) \cdots (j_{n1} \ldots j_{nk_n})$ durch die Permutation $i_{lm} \mapsto j_{lm}$.

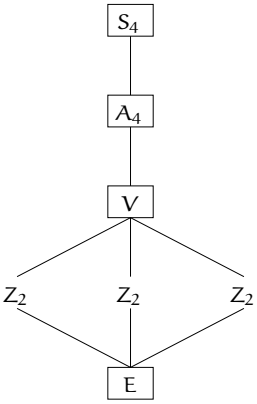
Satz 21 S_n *wird von den Transpositionen,* A_n *von den* 3*-Zykeln erzeugt.*

Beweis: Durch höchstens $n-1$ Transpositionen kann man jede Permutation darstellen: man versetzt zunächst das erste Element an die richtige Stelle, dann das zweite, usw. Da $(ab)(ac) = (abc)$ und $(ab)(cd) = (abc)(adc)$, ist ferner jedes Produkt geradzahlig vieler Transpositionen ein Produkt von 3-Zykeln. ■

Beispiele (Normalteiler sind in den Bildern umrahmt)**:**

$S_1 = E$, $A_1 = E$;
$S_2 \cong Z_2$, $A_2 = E$





S_4 hat zwei nicht-triviale Normalteiler: A_4, der Kern der Signumfunktion, und die Kleinsche Vierergruppe $V \cong Z_2 \times Z_2$, der Kern der Operation der Würfelgruppe auf den 3 Achsen. Es gilt $S_4/A_4 \cong Z_2$; $S_4/V \cong S_3$; $A_4/V \cong Z_3$.

Betrachtet man die Konjugationsklassen der S_4, so sieht man schnell, daß es bereits aus „arithmetischen“ Gründen keinen weiteren nicht-trivialen Normalteiler geben kann: Jeder Normalteiler ist Vereinigung vollständiger Konjugationsklassen und die Anzahl der Elemente muß 24 teilen.

Identität	1
Transpositionen	6
3-Zykel	8
4-Zykel	6
Doppeltranspositionen	3

Satz 22 A_n *ist einfach für* $n \neq 4$.

Beweis: Es gilt sicher für $n \leqslant 3$. Sei $n \geqslant 5$ und $E \neq N \trianglelefteq A_n$. Die Permutationen werden hier von links verknüpft.

- N darf keinen 3-Zykel enthalten: je zwei 3-Zykel $(abc), (a'b'c')$ sind zunächst in S_n konjugiert, etwa durch π. Dann sind sie auch in A_n konjugiert, denn falls π ungerade ist, so finde (d, e) mit $d, e \notin \{a, b, c\}$ ($n \geqslant 5$!). Es gilt dann weiterhin $((ef)\pi)(abc)((ef)\pi)^{-1} = (a'b'c')$.
- N darf keine Permutation enthalten, die einen Zykel der Länge $\geqslant 4$ besitzt: Falls $\sigma \in N$ mit $\sigma = (abcd\ldots)(\ldots)\ldots$, so ist $(abc)^{-1}\sigma(abc) = (bcad\ldots)\ldots =: \sigma'$ und $\sigma^{-1}\sigma' = (abc)$.

Also haben alle Elemente aus N nur Zykel der Länge 2 und 3.

- Falls zwei disjunkte Zykel der Länge 3 vorkommen, etwa $\sigma = (abc)(a'b'c')\ldots$, so ist $(a'b'c)^{-1}\sigma(a'b'c) = (abc')(cc'b')\ldots =: \sigma'$ und damit $\sigma\sigma' = (aa'cbc')\ldots$ im Widerspruch zur Zykellänge $\leqslant 3$. Also bestehen alle Elemente von N Zykellänge 2.
- Ist $\sigma = (ab)(a'b') \in N$, so ist $\sigma' = (acb)^{-1}\sigma(acb) = (ac)(a'b') \in N$ für alle $c \notin \{a, b, a'b'\}$ und somit auch $\sigma\sigma' = (abc) \in N$.
- Ist $\sigma = (a_1b_1)(a_2b_2)(a_3b_3)(a_4b_4) \in N$, so auch $\sigma' = (a_3b_2)(a_2b_1)\sigma(a_2b_1)(a_3b_2) = (a_1a_2)(a_3b_1)(b_2b_3)(a_4b_4)\ldots$ und damit auch $\sigma\sigma' = (a_1a_3b_2)(a_2b_3b_1)$ ∎

Folgerung 23 *Sei* $n \geqslant 4$. *Die Normalteiler von* S_n *sind* E, A_n, S_n.

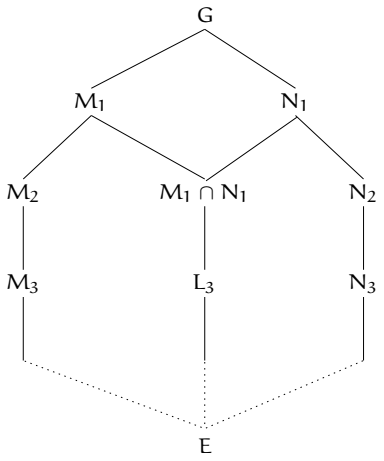
Beweis: Sei $N \trianglelefteq S_n$. Dann ist $N \cap A_n \trianglelefteq A_n$. Falls $N \cap A_n = A_n$, so hat N höchstens Index 2 in S_n, also $N = A_n$ oder $N = S_n$. Andernfalls $N \cap A_n = E$, also $|N| \leqslant 2$, da $|S_n| = |NA_n| = \frac{|N| \cdot |A_N|}{|N \cap A_n|}$, das heißt $N = \langle (ab) \rangle$. Dies ist ein Widerspruch, da alle Transpositionen konjugiert sind. ∎

Eine Untergruppenreihe $E = N_k \lhd N_{k-1} \lhd \ldots \lhd N_0 = G$ heißt *Kompositionsreihe* von G, falls alle N_j/N_{j+1} einfach sind. Die Faktoren N_j/N_{j+1} heißen *Kompositionsfaktoren* von G. Es ist klar, daß Kompositionsreihen in endlichen Gruppen stets existieren und daß sich jede „Subnormalreihe“ $E = N_k \lhd N_{k-1} \lhd \ldots \lhd N_0 = G$ zu einer Kompositionsreihe verfeinert.

Satz 24 (Jordan-Hölder) *Sei* G *endlich. Zwei Kompositionsreihen von* G *haben die gleiche Länge und bis auf Permutution dieselben Kompositionsfaktoren.*

Beweis:
Seien zwei Kompositionsreihen $N_k \lhd N_{k-1} \lhd \ldots \lhd N_0$ und $M_l \lhd M_{l-1} \lhd \ldots \lhd M_0$ gegeben. Falls $N_1 = M_1$, so fertig nach Induktion. Andernfalls gilt $M_1N_1 = G$, $G/M_1 \cong N_1/(N_1 \cap M_1)$ und $G/N_1 \cong M_1/(N_1 \cap M_1)$. Sei $L_m \lhd L_{m-1} \lhd \ldots \lhd L_2$ Kompositionsreihe von $N_1 \cap M_1$. Die Eigenschaft im Satz definiert eine Äquivalenzrelation $\sim$ auf Kompositionsreihen. Es gilt per Induktion und aus obigen Überlegungen:

$$\begin{aligned} M_l \lhd \ldots \lhd M_1 \lhd G &\sim L_m \lhd \ldots L_3 \lhd M_1 \cap N_1 \lhd M_1 \lhd G \\ &\sim L_m \lhd \ldots L_3 \lhd M_1 \cap N_1 \lhd N_1 \lhd G \\ &\sim N_k \lhd \ldots \lhd N_1 \lhd G \end{aligned}$$



∎

S_n hat für $n \neq 4$ genau eine Kompositionsreihe: $E \lhd A_n \lhd S_n$ mit Faktoren A_n und Z_2. Die S_4 hat genau drei (isomorphe) Kompositionsreihen $E \lhd Z_2 \lhd V \lhd A_4 \lhd S_4$ mit Faktoren Z_2, Z_2, Z_3, Z_2.

Automorphismentürme und vollständige Gruppen Eine Gruppe G mit $Z(G) = E$ heißt *vollständig*, falls die Einbettung $G \hookrightarrow \mathrm{Aut}(G)$, $g \mapsto \gamma_g$ ein Isomorphismus ist, also falls $G \cong \mathrm{Inn}(G) = \mathrm{Aut}(G)$.

Lemma 25 *Falls* $Z(G) = E$*, so gilt* $C_{\mathrm{Aut}(G)}(\mathrm{Inn}(G)) = E$*, insbesondere* $Z(\mathrm{Aut}(G)) = E$.

Beweis: Sei $\alpha \circ \gamma_g = \gamma_g \circ \alpha$. Dann gilt für alle $x \in G$: $\alpha(x)^g = (\gamma_g \circ \alpha)(x) = (\alpha \circ \gamma_g)(x) = \alpha(x^g) = \alpha(x)^{\alpha(g)}$, also $\alpha(x)^{\alpha(g)g^{-1}} = \alpha(x)$ oder $\alpha(g)g^{-1} \in Z(G) = E$, d.h. $\alpha(g) = g$. ■

Falls $Z(G) = E$, kann man also den *Automorphismenturm* von G konsruieren, nämlich $G \leqslant \mathrm{Aut}(G) \leqslant \mathrm{Aut}(\mathrm{Aut}(G)) \cdots$.

Satz 26 (ohne Beweis) *(Wielandt) Ist* G *endlich, so wird der Automorphismenturm nach endlich vielen Schritten stationär.*
(Thomas) Ist G *unendlich, so wird der Automorphismenturm nach* $(2^{|G|})^+$ *vielen Schritten stationär.*

Automorphismen der S_n

Satz 27 *Es bestehen folgende eins–zu–eins–Entsprechungen:*

- *Äquivalenzklassen treuer Operationen von* S_n *auf* $\{1, \ldots, n\}$
- *Konjugationsklassen von Untergruppen von Index* n *der* S_n
- *Äußere Automorphismen der* S_n

Beweis:

- Eine treue Operation von $G = S_n$ auf $\{1, \ldots, n\}$ entspricht einer Injektion (also einem Isomorphismus) $G = S_n \hookrightarrow S_n$. Jede andere (äquivalente) Operation erhält man durch Vorschalten eines (inneren) Automorphismus.
- S_n operiert treu auf $\{1, \ldots, n\} \iff S_n$ operiert transitiv:
  „$\Rightarrow$“ ist klar.
  „$\Leftarrow$“ ist klar für $n \leqslant 2$. Ansonsten operiert S_n/Kern immer noch transitiv und enthält mehr als 2 Elemente, der Kern kann also nicht die A_n sein. Zusätzlich überlege man sich, daß $S_4/V \cong S_3$ nicht transitiv auf 4 Elementen operieren kann.
  Transitive Operationen sind aber äquivalent zur Rechtsmultiplikation auf den Nebenklassen eines Stabilisators, der dann Index n hat.
- Äquivalente Operationen entsprechen dabei konjugierten Untergruppen, also inneren Automorphismen. ■

S_n als Permutationsgruppe von $\{1, \ldots, n\}$ aufzufassen, bedeutet, jedem $g \in S_n$ eine Permutation zuzuweisen. Innere Automorphismen der S_n vertauschen die Elemente $\{1, \ldots, n\}$, weisen somit $g \in S_n$ eine andere Permutation mit gleicher Zykelzerlegung zu. Äußere Automorphismen dagegen vertauschen einige Konjugationsklassen, weisen also manchen Elementen $g \in S_n$ andere Typen von Permutationen zu. Dies muß konjugationsklassenweise erfolgen, natürlich die Ordnung der Permutationen erhalten und auch die Parität, da A_n charakteristisch in S_n ist.

Außerdem dürfen nicht-triviale aüßere Automorphismen die Transpositionen nicht enthalten, da diese alle anderen Permutationen erzeugen, genauer:

Lemma 28 *Ist* S_n *als Permutationsgruppe von* $\{1, \ldots, n\}$ *gegeben und* α *ein Automorphismus, welcher Transpositionen auf Transpositionen abbildet, so ist* $\alpha \in \mathrm{Inn}(S_n)$.

BEWEIS: Die Transposition (12) wird auf (ab) und (13) auf (cd) abgebildet. Da $o((12)(13)) = 3$, gilt $|\{a, b, c, d\}| = 3$, etwa $d = a$. Mit demselben Argument wird (14) entweder auf (ae) für ein e oder auf (bc) geworfen. Letzteres führt zum Widerspruch, da $o((12)(13)(14)) = 4$, aber $o((ab)(ac)(bc)) = 2$. Also ist $1 \mapsto a$ usw. eine wohldefinierte Abbildung σ und man sieht leicht, daß α der Konjugation mit σ entspricht. ■

Satz 29 *Ist* $n \neq 2, 6$*, so ist* S_n *vollständig, also* $\mathrm{Aut}(S_n) = \mathrm{Inn}(S_n) = S_n$.
Weiter ist $\mathrm{Aut}(S_2) = E$*,* $\mathrm{Inn}(S_6) = S_6$ *und* $\mathrm{Out}(S_6) = Z_2$.

BEWEIS: $n = 2$ ist klar; für $n \geqslant 3$ gilt $Z(S_n) = E$, also $S_n \cong \mathrm{Inn}(S_n) \hookrightarrow \mathrm{Aut}(S_n)$.
S_6 hat zwei Konjugationsklassen von Untergruppen von Index 6 (alle $\cong S_5$!):

- die Einpunktstabilisatoren
- es gibt 24 5-Zykel in der S_5, also 6 Untergruppen der Ordnung 5. Darauf operiert S_5 transitiv durch Konjugation; da der Kern nicht die A_5 sein kann, operiert sie auch treu. Man erhält also eine Einbettung $S_5 \hookrightarrow S_6$, deren Bild wegen der Transitivität kein Einpunktstabilisator sein kann.

Daß es keine weiteren Untergruppen von Index 6 gibt, bleibt ohne Beweis!

Ein äußerer Automorphismus muß die Transpositionen auf eine andere Konjugationsklasse von ungeraden Elementen der Ordnung 2 werfen, also Produkten von k disjunkten Transpositionen, k ungerade. Für $n \leqslant 5$ gibt es das nicht; für $n \geqslant 7$ und $1 < k < \frac{n}{2}$ gibt es davon

$$\binom{n}{2}\binom{n-2}{2} \cdot \ldots \cdot \binom{n-2k+2}{2} \cdot \frac{1}{k!} = \frac{n!}{k!(n-2k)!2^k}$$

viele, und $\binom{n}{2}$ viele Transpositionen. Gleichheit bedeutet $(n-2) \cdot \ldots \cdot (n-2k+1) = 2^{k-1}k!$, also $(n-2) \cdot \ldots \cdot (n-k+1) \leqslant 2^{k-1}$, aber $n-2 > 4$ und $n-k+1 \geqslant 2$; Widerspruch! ■

Die Vollständigkeit der S_n bedeutet, daß die Zuordnung Konjugationsklasse $\leftrightarrow$ Zykelzerlegung eindeutig ist. Im Falle der S_6 gibt es folgende Möglichkeit:

Ordnung	Parität	Zykelzerlegung	Anzahl		
1	+	()	1		
2	−	(..)	15	}	
	+	(..)(..)	45	}	
	−	(..)(..)(..)	15	} ↖	
3	+	(...)	40	} ←	nicht-triviale
	+	(...)(...)	40	} ←	äußere Auto-
4	−	(....)	90		morphismen
	+	(....)(..)	90		vertauschen
5	+	(.....)	144		diese Klassen
6	−	(.....)	120	} ↙	
	−	(...)(..)	120	} ↙	

Bemerkung:

(a) Für $n \geqslant 4$ gilt $Z(A_n) = E$, also $A_n \cong \mathrm{Inn}(A_n) \hookrightarrow \mathrm{Aut}(A_n)$.
(Hölder) $\mathrm{Aut}(A_n) = S_n$ für $n \neq 6$ (also $\mathrm{Out}(A_n) = Z_2$) und $|\mathrm{Out}(A_6)| = 4$.
Ferner natürlich $\mathrm{Aut}(A_3) = Z_2$ und $\mathrm{Aut}(A_2) = E$.

(b) Es gilt $S_n = A_n \rtimes S_2$. Für S_2 kann man die von einer beliebigen Permutation σ der Ordnung 2 erzeugte Untergruppe nehmen. Der Homomorphismus ergibt sich aus $\langle\sigma\rangle \hookrightarrow S_n \hookrightarrow \mathrm{Aut}(A_n)$ und somit, falls A_n als Permutationsgruppe auf $\{1,\ldots,n\}$ gegeben ist, aus der Vertauschung der Elemente gemäß σ.

7 Die Polyedergruppen

Würfel und Oktaeder (beziehungsweise Dodekaeder und Ikosaeder) sind zueinender dual: die Mittelpunkte der Flächen des einen sind die Eckpunkte des anderen. Also haben sie gleiche Dreh- und Symmetriegruppen.

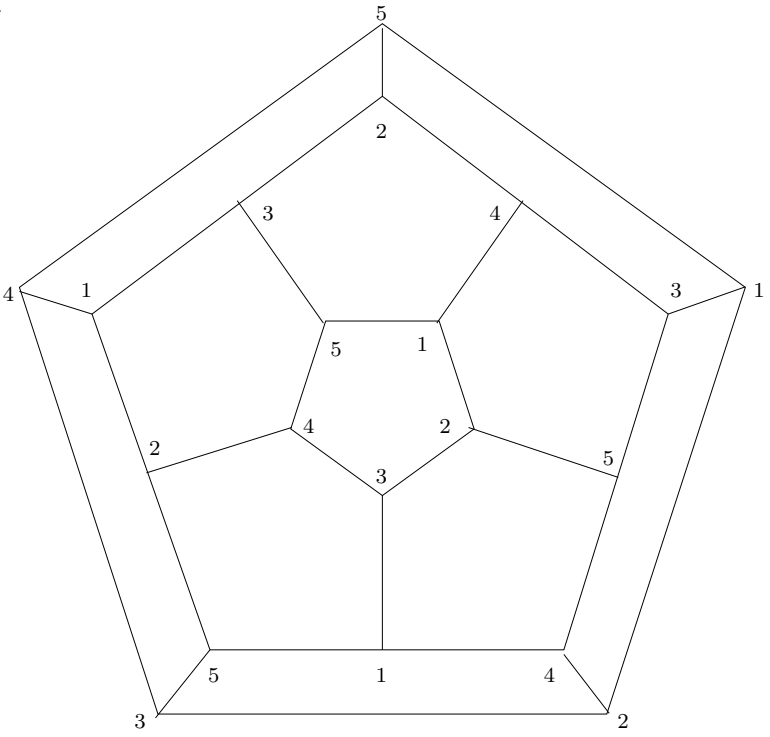
Satz 30 *Die Dreh- und Symmetriegruppen der regulären Polyeder sind:*

	Drehgruppe	*Symmetriegruppe*
Tetraeder	A_4	S_4
Würfel/Oktaeder	S_4	$S_4 \times S_2$
Dodekaeder/Ikosaeder	A_5	$A_5 \times S_2$

Beweis: Sei Σ jeweils die Symmetriegruppe, Δ die Drehgruppe. Σ operiert transitiv auf den beiden Orientierungen des Raumes mit Kern $\mathtt{Delta}$. Es gilt also $\Delta \trianglelefteq \Sigma$ vom Index 2.

Tetraeder: Δ und Σ operieren treu und transitiv auf den 4 Ecken. Δ besteht aus 12, Σ aus 24 Elementen, also gilt $\Sigma = S_4$ und $\Delta = A_4$.

Würfel: Δ operiert treu auf den 4 Hauptdiagonalen; da Δ 24 Elemente enthält (transitiv auf den 6 Flächen und der Stabilisator einer Fläche besteht aus 4 Drehungen)), ist $\Delta = S_4$. Die Symmetrie σ, welche jeder Ecke die gegenüberliegende zuordnet, hat Ordnung 2 und ist charakteristisch. Also gilt $\langle\sigma\rangle \trianglelefteq \Sigma$ bzw. $\sigma \in Z(\Sigma)$ und insbesondere $\sigma \notin \Delta$. Es folgt $\Sigma = \Delta \times \langle\sigma\rangle \cong S_4 \times S_2$.
(Wegen $Z(\Delta) = E$ folgt auch $Z(\Sigma) = \langle\sigma\rangle$. Durch die treue Operation von Σ auf den 6 Flächen erhält man die Symmetriegruppe als Untergruppe der S_6.)



Dodekaeder: Die 20 Ecken bilden 5 maximale Tetraeder (dafür gibt es 2 Möglichkeiten, die durch Symmetrie ineinander übergehen; die Tetraeder sind jeweils um 72 Grad zueinander gedreht). Dual kann man den Ikosaeder als Schnitt von 5 Tetraedern darstellen. Δ operiert treu auf den 5 Tetraedern, denn jede Ecke eines Tetraeders ist mit Ecken je drei verschiedener

anderer Terateder benachbart. Somit gilt $\Delta \hookrightarrow S_5$. Wegen $|\Delta| = 60$ (transitiv auf 12 Flächen, Einpunktstabilisator der Größe 5) folgt $\Delta = A_5$. Sei σ wiederum die Spiegelung, die jeder Ecke ihr gegenüber zuordnet. Wie im Falle des Würfels überzeugt man sich von $\sigma \in Z(\Sigma)$, damit $\Sigma = \Delta \times \langle\sigma\rangle \cong A_5 \times S_2$. ■

$\Delta_{\text{Würfel}}$ operiert auf den 3 Paaren gegenüberliegender Flächen (beziehungsweise der Achsen dadurch), dies ergibt den Homomorphismus $S_4 \twoheadrightarrow S_3$ mit Kern V. Ferner bilden die 4 Ecken des Würfels 2 regelmäßige Tetraeder. Die Operation von Δ darauf ergibt $S_4 \twoheadrightarrow S_2$ mit Kern A_4.

8 Die Sylow–Sätze

Sei in diesem Abschnitt G stets eine endliche Gruppe, p eine Primzahl und $|G| = p^a n$ mit $p \nmid n$. Eine p-*Sylowgruppe von* G ist eine Untergruppe $U \leqslant G$ der Ordnung p^a (also eine p-Untergruppe mit $p \nmid |G : U|$). Die Menge der p-Sylowgruppe von G wird mit $\mathrm{Syl}_p(G)$, ihre Anzahl mit $N_p(G)$ bezeichnet.

Satz 31 (Sylow) **(a)** *Sei* $|G| = p^b m$ *und* $\#(p^b)$ *die Anzahl der Untergruppen von* G *der Ordnung* p^b*. Dann gilt* $\#(p^b) \equiv 1 \pmod p$*. Insbesondere existieren* p*-Sylowgruppen stets.*

(b) *Je zwei* p*-Sylowgruppen sind zueinander konjugiert und es gilt* $N_p(G) = |G : N_G(P)| \equiv 1 \pmod p$ *für eine* p*-Sylowgruppe* P*, insbesondere* $N_p(G) \mid n$*.*

(c) *Jede* p*-Untergruppe von* G *ist in einer* p*-Sylowgruppe enthalten.*

Folgerung 32 (Cauchy) *Falls* $p \mid |G|$*, so existiert* $g \in G$ *mit* $o(g) = p$*.*

Beweis: (a) $\Omega := \{M \subseteq G \mid |M| = p^b\}$ ist G-Menge unter Rechtsmultiplikation mit Bahnen $\Omega_j = \{M_j g \mid g \in G\}$, $j = 1, \ldots, k$. Sei $U_j = \{g \in G \mid M_j g = M_j\}$ der Stabilisator von M_j der eingeschränkten Operation auf Ω_j. Also gilt $M_j = M_j U_j = \bigcup_{g \in M_j} gU_j$, mithin $|U_j| \mid |M_j| = p^b$, d.h. U_j ist p-Gruppe. Wegen $|\Omega_j| = |G : U_j|$ gilt $pm \mid |\Omega_j| \iff |U_j| < p^b$. Ferner $|U_j| = p^b \iff |\Omega_j| = m \iff M_j = g_j U_j$ für ein $g_j \iff \Omega_j = \{g_j U_j g \mid g \in G\} = \{Vg \mid g \in G\}$, wobei $V := U_j^{g_j^{-1}}$ eine Untergruppe der Ordnung p^b ist. Also entsprechen Bahnen der Größe m genau Untergruppen in Ω. Es folgt

$$\binom{mp^b}{p^b} = |\Omega| \equiv \sum_{|\Omega_j| = m} |\Omega_j| = \#(p^b) \cdot m \pmod{pm}.$$

Dies gilt auch für $G = Z_{|G|}$, wo $\#(p^b) = 1$ ist, was $\binom{mp^b}{p^b} \equiv m \pmod{pm}$ ergibt. Zusammen folgt $m \equiv \binom{mp^b}{p^b} \equiv \#(p^b)m \pmod{pm}$, also $1 \equiv \#(p^b) \pmod p$.

(b,c) Sei $P \in \mathrm{Syl}_p(G)$ und Q eine p-Untergruppe von G, dann operiert Q auf $\{P^g \mid g \in G\}$ durch Konjugation. Alle Bahnen haben p-Potenzgröße. Ist $\{P^g\}$ eine einelementige Bahn, so folgt $Q \leqslant N_G(P^g)$, also $P^g \trianglelefteq \langle Q, P^g\rangle = QP^g$, welches eine p-Gruppe der Ordnung $\frac{|Q| \cdot |P^g|}{|Q \cap P^g|}$ ist, die $p^a = |P^g|$ nicht überschreiten darf. Daher $Q \leqslant P^g$.

Falls $Q = P$, so folgt daraus $P = P^g$, d.h. $\{P\}$ ist die einzige einelementige Bahn, woraus sich $|G : N_G(P)| = |\{P^g \mid g \in G\}| \equiv 1 \pmod p$ ergibt.

Für beliebiges Q muß es daher eine einelementige Bahn $\{P^g\}$ geben, mithin $Q \leqslant P^g \in \mathrm{Syl}_p(G)$ und Gleichheit aus Größengründen, falls $Q \in \mathrm{Syl}_p(G)$. ■

Ist $|G| = p_1^{k_1} \dots p_n^{k_n}$ die Primfaktorzerlegung und $P_i \in \mathrm{Syl}_{p_i}(G)$, so gilt $P_i \cap P_j = E$ für $i \neq j$ und $G = \langle P_1, \dots, P_n \rangle$, da $p_i^{k_i} \mid \langle P_1, \dots, P_n \rangle$.

Satz 33 *Sind alle Sylowgruppen* $P_1, \dots, P_n$ *normal in* G*, so ist* $G = P_1 \times \cdots \times P_n$.

Beweis: Wegen der Konjugiertheit gehören dann alle Sylowgruppen zu verschiedenen Primzahlen. Per Induktion über k beweist man (a) $(P_1 \cdots P_{k-1}) \cap P_k = E$; (b) $|P_1 \cdots P_k| = |P_1| \cdots |P_k|$ und (c) $P_1 \cdots P_k = P_1 \times \cdots \times P_k$. Die Induktionsschritte für (a) und (b) ergeben sich direkt aus den Induktionsvoraussetzungen für (b) und (a). Für (c) muß man nur noch nachweisen, daß die P_i elementeweise kommutieren: für $h \in P_i$ gilt $h^{-1}g^{-1}hg \in P_i P_i^g = P_i$, analog $\in P_j$ für $g \in P_j$, also $h^{-1}g^{-1}hg = e$. Damit folgt $P_1 \cdots P_k = (P_1 \cdots P_{k-1}) \times P_k$ aus (a). ■

Satz 34 *Sei* $N \trianglelefteq G$ *und* $P \in \mathrm{Syl}_p(G)$*. Dann gilt* $P \cap N \in \mathrm{Syl}_p(N)$ *und* $PN/N \in \mathrm{Syl}_p(G/N)$.

Beweis: $P \cap N$ und $PN/N \cong P/(P \cap N)$ sind p-Gruppen und jeweils maximale p-Untergruppen, da $|N : P \cap N| = \frac{|NP|}{|P|} \mid \frac{|G|}{|P|}$ sowie $|G/N : PN/N| = |G : PN| \mid |G : P|$. ■

Satz 35 *(Frattini–Argument) Sei* $N \trianglelefteq G$ *und* $P \in \mathrm{Syl}_p(N)$*. Dann* $G = N_G(P) \cdot N$.

Beweis: Sei $g \in G$. Dann ist $P^g \in \mathrm{Syl}_p(N)$, also gibt es $h \in N$ mit $P^g = P^h$. Damit $gh^{-1} \in N_G(P)$, also $g \in N_G(P) \cdot N$. ■

Eine beispielhafte Anwendung

Satz 36 *Ist* G *einfach der Ordnung 60, so* $G \cong A_5$.

Beweis: Angenommen es gibt $U < G$ mit $|G : U| \leqslant 5$. Rechtsmultiplikation auf $G : U$ liefert einen nicht-trivialen Homomorphismus $\varphi : G \to S_{G:U}$. Da G einfach, ist φ eine Einbettung, aus Größengründen folgt $|G : U| = 5$ und $\mathrm{Bild}(\varphi) = A_5$.

Angenommen $|G : U| > 5$ für alle $U < G$. Dann:

$$\begin{aligned} 5 < N_5(G) &\equiv 1 \pmod 5 \text{ und } N_5 \mid 12, \text{ also } N_5 = 6 \\ 5 < N_3(G) &\equiv 1 \pmod 3 \text{ und } N_3 \mid 20, \text{ also } N_3 = 10 \\ 5 < N_2(G) &\equiv 1 \pmod 2 \text{ und } N_2 \mid 15, \text{ also } N_2 = 15 \end{aligned}$$

Seien $P_1, P_2 \in \mathrm{Syl}_2(G)$ mit $|P_1 \cap P_2| = 2$. Da $P_1 \cap P_2 \trianglelefteq P_i$ $(i = 1, 2)$, ist $P_1 \cap P_2 \trianglelefteq \langle P_1, P_2 \rangle =: Q$, folglich $Q \neq G$. Da außerdem $|Q| > 4$, ist $|G : Q|$ ein echter Teiler von 15, also 3 oder 5: Widerspruch, 2-Sylowgruppen sind paarweise disjunkt über E. Es ergibt sich:

$$\left.\begin{aligned} \left|\{g \in G \mid o(g) = 5\}\right| &= 6 \cdot 4 = 24 \\ \left|\{g \in G \mid o(g) = 3\}\right| &= 10 \cdot 2 = 20 \\ \left|\{g \in G \mid o(g) = 2 \text{ oder } 4\}\right| &= 15 \cdot 3 = 45 \end{aligned}\right\} \geqslant 90 \text{ Elemente: Widerspruch!}$$

■

9 Auflösbare Gruppen

Eine endliche Gruppe G heißt *auflösbar*, falls alle Kompositionsfaktoren abelsch sind (bzw. zyklisch sind oder von Primzahlordnung).

Beispiele:

- Alle abelschen Gruppen sind auflösbar.
- $D_n = Z_n \rtimes Z_2$ ist auflösbar.
- S_n ist genau dann auflösbar, wenn $n \leqslant 4$.
- p-Gruppen sind auflösbar (denn die Subnormalreihe $E \lhd Z(G) \lhd \cdots$ hat abelsche Faktoren).
- G ist auflösbar, falls $|G| = pq$ mit Primzahlen $p \neq q$:
  O.b.d.A. gilt $p < q$. Da $N_q \equiv 1 \pmod q$ und $N_q \mid p$, folgt $N_q = 1$. Für $Q \in \mathrm{Syl}_q(G)$ ist also $E \lhd Q \lhd G$ Kompositionsreihe mit zyklischen Faktoren.

Kommutatoren Für $g, h \in G$ ist $[g,h] := g^{-1}h^{-1}gh \in G$ der *Kommutator* von g und h. Die Untergruppe $G' := \langle [g,h] \mid g,h \in G\rangle$ heißt die *Kommutatorgruppe* von G.

Setze $G^{(0)} := G$ und $G^{(n+1)} := (G^{(n)})'$. Alle $G^{(n)}$ sind charakteristische Untergruppen von G; $\cdots \trianglelefteqslant G^{(2)} \trianglelefteqslant G^{(1)} \trianglelefteqslant G^{(0)}$ heißt die *Kommutatorreihe* von G.

Lemma 37 *Sei $N \trianglelefteqslant G$. Dann ist G/N genau dann abelsch (bzw. auflösbar), wenn $G' \leqslant N$ (bzw. $G^{(k)} \leqslant N$ für ein k).*

Insbesondere ist also G/G' maximaler abelscher Quotient von G.

Beweis: G/N abelsch $\iff [g,h]N = [gN, hN] = N$ für alle $g,h \in G \iff [g,h] \in N$ für alle $g,h \in G \iff G' \leqslant N$.

Per Induktion sieht man $(G/N)^{(k)} = G^{(k)}N/N$, folglich $N = (G/N)^{(k)} = G^{(k)}N/N \iff G^{(k)} \leqslant N$. Man schließt mit dem folgenden Satz. ■

Satz 38 *Äquivalent sind:*

(a) *G ist auflösbar.*

(b) *Es gibt eine Subnormalreihe $E = N_k \lhd \cdots \lhd N_0 = G$ mit abelschen Faktoren.*

(c) *Es gibt ein k mit $G^{(k)} = E$.*

Beweis: (a)⇒(b) per Definition.
(b)⇒(a): verfeinere die Subnormalreihe zu einer Kompositionsreihe.
(b)⇒(c): Per Induktion zeigt man $G^{(j)} \leqslant N_j$:
Trivial für $j = 0$; im Induktionsschritt folgt $G^{(j+1)} = (G^{(j)})' \leqslant N_j' \leqslant N_{j+1}$ mit dem Lemma.
(c)⇒(b): Die Kommutatorreihe ist eine solche Reihe laut dem Lemma. ■

Eine unendliche Gruppe heißt auflösbar, falls Bedingung (c) des Satzes erfüllt ist. Das kleinste k mit $G^{(k)} = E$ heißt *Auflösbarkeitsstufe* von G. In unendlichen, nicht auflösbaren Gruppen kann man natürlich die Kommutatorreihe transfinit fortführen, indem man $G^{(\lambda)} := \bigcap_{\alpha<\lambda} G^{(\alpha)}$ für Limeszahlen λ setzt. Eine Gruppe heißt *hypo–abelsch*, falls $G^{(\alpha)} = E$ für ein $\alpha \in \mathrm{Ord}$.

Sätze über auflösbare Gruppen

Satz 39 **(a)** *Untergruppen und homomorphe Bilder auflösbarer Gruppen sind auflösbar.*

(b) *Sei $N \trianglelefteqslant G$. Sind N und G/N auflösbar, so auch G.*

(c) *Sind alle G/N_i auflösbar ($i = 1, \ldots, n$), so auch $G/\bigcap_{i=1}^n N_i$.*

(d) *Sind $U \leqslant G$ und $N \trianglelefteqslant G$ auflösbar, so auch UN.*

BEWEIS: (a) $U \leqslant G \Rightarrow U^{(n)} \leqslant G^{(n)}$.
$N \trianglelefteq G \Rightarrow (G/N)^{(n)} = G^{(n)}N/N$.
(b) Sei $N^{(k)} = E$ und $(G/N)^{(n)} = G^{(n)}N/N = N$, also $G^{(n)} \leqslant N$. Dann $G^{(n+k)} \leqslant N^{(k)} = E$.
(c) Sei $G^{(k_i)} \leqslant N_i$ für $i = 1, \ldots, n$. Setze $k := \max\{k_i\}$, dann $G^{(k)} \leqslant \bigcap_i N_i$.
(d) $UN/N \cong U/(U \cap N)$ ist auflösbar nach (a), N nach Voraussetzung, mithin UN nach (b). ■

Satz 40 *Alle endlichen Gruppen mit Ordnung* p^a, pqr, p^aq *oder* p^2q^2 *sind auflösbar, wobei* p, q, r *Primzahlen sind und* $a, b \in \mathbb{N}$.

BEWEIS: Fall p^a ist bereist abgehandelt.

Fall p^aq: Sei G minimales Gegenbeispiel; dann ist $p \neq q$ und G einfach (sonst wären $N \lhd G$ und G/N auflösbar, also auch G). Insbesondere folgt $N_p(G) = q$ aus $N_p(G) > 1$ und $N_p(G) \mid q$. Falls $P_1 \cap P_2 = E$ für alle $P_1, P_2 \in \mathrm{Syl}_p(G)$, $P_1 \neq P_2$, so

$$\left|\left\{g \in G \;\middle|\; o(g) = p^k, k \in \mathbb{N}\right\}\right| = N_p(G) \cdot (p^a - 1) + 1 = |G| - (q - 1)$$

und die verbleibenden Elemente reichen gerade für eine q-Sylowgruppe aus: Widerspruch.
Sei daher $E \neq D := P_1 \cap P_2$ maximal. Dann $D \trianglelefteq \langle N_{P_1}(D), N_{P_2}(D)\rangle =: N$.

- Falls N eine p-Gruppe ist, so $N \leqslant P_3 \in \mathrm{Syl}_p(G)$, o.B.d.A. $P_3 \neq P_2$ und $P_2 \cap P_3 \geqslant P_2 \cap N \geqslant N_{P_1}(D) > D$, da P_1 p-Gruppe, damit nilpotent ist und die Normalisator–Eigenschaft besitzt (kommt im Kapitel über nilpotente Gruppen): Widerspruch zur Maximalität von D.
- Also gilt $|N| = p^bq$. Sei $Q \in \mathrm{Syl}_q(N)$. Da $|QP_1| = \frac{|Q|\cdot|P_1|}{|Q\cap P_1|} = \frac{qp^a}{1} = |G|$, gilt $QP_1 = G$. Sei $g \in G$, $g = xy$ mit $x \in Q, y \in P_1$. Dann $D^g = D^{xy} = D^y$ (da $x \in Q \leqslant N \leqslant N_G(D)$) und $D^y \leqslant P_1^y = P_1$. Folglich ist $E \neq D^G$ ein echter Normalteiler von G: Widerspruch.

Fall pqr: Sei $p > q > r$. Falls G eine normale Sylowgruppe N besitzt, so ist N auflösbar und der Quotient ebenfalls nach dem vorherigen Fall. Also mit $k, l, m \in \mathbb{N}$:

$$1 + p \leqslant N_p(G) = 1 + kp \mid qr, \text{ also } N_p = qr$$
$$1 + q \leqslant N_q(G) = 1 + lq \mid pr, \text{ also } N_q \geqslant p$$
$$1 + r \leqslant N_r(G) = 1 + mr \mid pq, \text{ also } N_r \geqslant q$$

Es folgt

$$\begin{aligned} pqr = |G| &\geqslant 1 + \left|\left\{g \in G \;\middle|\; o(g) = p\right\}\right| + \left|\left\{g \in G \;\middle|\; o(g) = q\right\}\right| + \left|\left\{g \in G \;\middle|\; o(g) = r\right\}\right| \\ &\geqslant 1 + qr(p-1) + p(q-1) + q(r-1) = pqr + 1 + pq - p - q \end{aligned}$$

Also $1 + pq - p - q \leqslant 0$, d.h. $p(q-1) \leqslant q - 1$ und $p \geqslant 1$: Widerspruch.

Fall p^2q^2: Sei G minimales Gegenbeispiel; dann ist $p \neq q$ und G einfach. O.b.d.A. $p > q$. Wegen $N_p(G) \equiv 1 \pmod p$ und $N_p(G) \mid q^2$ folgt $N_p(G) = q^2$.

- Angenommen es gibt $P_1, P_2 \in \mathrm{Syl}_p(G)$ mit $D := P_1 \cap P_2$ der Ordnung p. Da die P_i abelsch sind (Ordnung p^2!), gilt $D \trianglelefteq \langle P_1, P_2\rangle =: N$. Es folgt $|N| = p^2q$ und $|G : N = q$. Die Rechtsmultiplikation von G auf $G : N$ ergibt eine Einbettung $G \hookrightarrow S_q$: Widerspruch, da $p \nmid q!$.
- Also schneiden sich verschiedene p-Sylowgruppen in E. Damit

$$\left|\left\{g \in G \;\middle|\; o(g) | p^2\right\}\right| = N_p(p^2 - 1) + 1 = q^2(p^2 - 1) + 1 = |G| - (q^2 - 1)$$

und es bleiben wiederum nur Elemente für eine q-Sylowgruppe: Widerspruch. ■

Satz 41 (ohne Beweis) (Burnside) *Alle Gruppen der Ordnung* p^aq^b *sind auflösbar.*

(Feit, Thompson) *Alle Gruppen ungerader Ordnung sind auflösbar (sehr schwer).*

Eine Liste kleiner nicht-auflösbarer bzw. einfacher nicht-abelscher Gruppen

- Sei G eine Gruppe mit $|G| < 200$. Dann ist G auflösbar außer für $|G| = 60, 120, 168, 180$.
- Falls $|G| = 60$, so $G \cong A_5$.
  Falls $|G| = 120$, so $G \cong S_5 \cong A_5 \rtimes Z_2$, $G \cong A_5 \times Z_2$ oder $G \cong \mathrm{SL}(2,5)$, wobei $Z_2 \cong Z(\mathrm{SL}(2,5))$ und $\mathrm{PSL}(2,5) = \mathrm{SL}(2,5)/Z_2 \cong A_5$.
  Falls $|G| = 180$, so $G \cong A_5 \times Z_3$.
  Falls $|G| = 168$, so $G \cong \mathrm{PSL}(2,7)$.
- Eine Liste der einfachen, nicht-abelschen Gruppen der Ordnung $\leqslant 5000$:

$\lvert G\rvert =$		$G \cong$		$\lvert G\rvert =$		$G \cong$	
	60		$A_5 = \mathrm{PSL}(2,5)$		1092		$\mathrm{PSL}(2,13)$
	168		$\mathrm{PSL}(2,7)$		2248		$\mathrm{PSL}(2,17)$
	360		$A_6 = \mathrm{PSL}(2,9)$		2520		A_7
	504		$\mathrm{PSL}(2,8)$		3420		$\mathrm{PSL}(2,19)$
	660		$\mathrm{PSL}(2,11)$		4080		$\mathrm{PSL}(2,16)$

Die Hallschen Sätze Sei π eine Menge von Primzahlen. Eine endliche Gruppe heißt π-Gruppe, falls alle Primteiler der Gruppenordnung aus π stammen. U ist π-Hallgruppe von G, falls U π-Gruppe ist und alle Primteiler von $|G : U|$ nicht aus π stammen.

Im Allgemeinen existieren π-Hallgruppen nicht: z.B. hätte eine $\{3,5\}$-Hallgruppe der A_5 Index 4, womit sich eine Einbettung $A_5 \hookrightarrow S_4$ ergäbe.

In auflösbaren Gruppen dagegen gilt die Verallgemeinerung der Sylowschen Sätze:

Satz 42 (Hall, ohne Beweis) *Sei G auflösbar. Dann existieren π-Hallgruppen zu jeder Primzahlmenge π; π-Hallgruppen sind zueinander konjugiert und jede π-Untergruppe von G ist in einer π-Hallgruppe enthalten.*

Umgekehrt ist G auflösbar, wenn G zu jeder Primzahl p eine $\mathbb{P}\setminus\{p\}$-Hallgruppe besitzt.

10 Nilpotente Gruppen

Eine Gruppe G heißt *nilpotent*, wenn es eine *Zentralreihe* in G gibt, das heißt Normalteiler $N_i \trianglelefteqslant G$ mit $E = N_0 \lhd N_1 \lhd \cdots \lhd N_c = G$ und $N_{i+1}/N_i \leqslant Z(G/N_i)$. Die minimale Länge c einer Zentralreihe von G heißt *Nilpotenzklasse* von G.

$E = Z_0(G)$ und induktiv $Z_{i+1}(G) \geqslant Z_i(G)$ so, daß $Z_{i+1}(G)/Z_i(G) = Z(G/Z_i(G))$ definiert die sogenannte *aufsteigende Zentralreihe*

$$E = Z_0(G) \lhd Z_1(G) \lhd \cdots$$

Man kann sie durch $Z_{\alpha+1}(G)/Z_\alpha(G) = Z(G/Z_\alpha(G))$ und $Z_\lambda(G) := \bigcup_{\alpha<\lambda} Z_\alpha(G)$ für Limeszahlen λ transfinit fortsetzen. Klarerweise sind alle $Z_\alpha(G)$ charakteristische Untergruppen. $Z_\infty(G) := \bigcup_{\alpha\in\mathrm{Ord}} Z_\alpha(G)$ heißt das *Hyperzentrum* von G; G heißt *hyperzentral*, falls $G = Z_\infty(G)$.

Für $X, Y \in G$ setzt man $[X,Y] := \langle [x,y] \mid x \in X, y \in Y\rangle$.
Also ist $G' = [G,G]$. Man definiert nun $K_1(G) := G$ und induktiv $K_{n+1}(G) := [K_n(G), G]$. Es gilt also $G' = K_2(G)$ und $G^{(n)} \leqslant K_{n+1}(G)$. Definiert man induktiv die *n-fach Kommutatoren* $[g_1, \ldots, g_n] := [[g_1, \ldots, g_{n-1}], g_n]$ und beachtet, daß wegen $[xy, z] = [x^y, z^y][y, z]$ jeder Kommutator von Produkten Produkt von Kommutatoren ist, so sieht man leicht $K_n(G) = \langle [g_1, \ldots, g_n] \mid g_i \in G\rangle$, was die von der bisherigen Praxis abweichende Indizierung erklärt.

Die *absteigende Zentralreihe* ist nun:

$$G = K_1(G) \geqslant K_2(G) \geqslant \cdots$$

Dies ist tatsächlich eine Zentralreihe: $K_\alpha(G)$ ist offenbar charakteristisch in G, und ist $N \trianglelefteq G$, so $N/[N,G] \leqslant Z(G/[N,G])$, denn $[g[N,G], h[N,G]] = [g,h] \cdot [N,G] = [N,G]$.

Auch die absteigende Zentralreihe ist transfinit fortsetzbar durch $K_{\alpha+1}(G) := [K_\alpha(G), G]$ und $K_\lambda(G) := \bigcap_{\alpha<\lambda} K_\alpha(G)$ für Limeszahlen λ. Dann heißt $K_\infty(G) := \bigcap_{\alpha\in \mathrm{Ord}} K_\alpha(G)$ das *Hypozentrum* von G, und G *hypozentral*, falls $K_\infty(G) = E$.

Achtung: Bei manchen Autoren ist Hyperzentrum $= Z_\omega(G)$ und Hypozentrum $= K_\omega(G)$!

Lemma 43 *Seien* $U, V \leqslant G$ *Dann gilt:*

(a) $[U,V] = [V,U]$

(b) *Für* $U_0 \leqslant U$ *und* $V_0 \leqslant V$ *gilt* $[U_0, V_0] \leqslant [U,V]$

(c) $[U,V] \trianglelefteq \langle U, V\rangle$

(d) $[U,V] \leqslant U \iff V \leqslant N_G(U)$

(e) $U, V \trianglelefteq G \Rightarrow [U,V] \trianglelefteq G$ *und* $[U,V] \subseteq U \cap V$

Beweis: (a) $[x,y] = [y,x]^{-1}$; (b) ist klar.

(c) Wegen $[x,y]^z = [xz,y][z,y]^{-1}$ für $z \in U$ und $[x,y]^z = [x,z]^{-1}[x,yz]$ für $z \in V$.

(d) $[x,y] = x^{-1}x^y \in X \iff x^y \in X$.

(e) $[x,y]^g = [x^g, y^g]$; dann mit (d) $[U,V] \subseteq U \cap V$. ■

Satz 44 *Äquivalent sind:*

- G *ist nilpotent der Klasse* c *mit Zentralreihe* $E = N_0 < \cdots < N_c = G$.
- $G = K_1(G) > \cdots > K_{c+1}(G) = E$.
- $E = Z_0(G) < \cdots < Z_c(G) = G$.

Weiter gilt $K_i(G) \leqslant NZ_{c-i+1}(G)$.

Beweis: (a) $\Rightarrow$ (b),(c): Sei $E = N_0 = M_{c+1} < \cdots < N_1 = M_1 < G$ eine Zentralreihe. Zeige $N_i \leqslant Z_i(G)$ und $K_i(G) \leqslant M_i$ per Induktion:
$N_{i+1}/N_i \leqslant Z(G/N_i) \Longrightarrow [N_{i+1}, G] \subseteq N_i \subseteq Z_i \overset{(*)}{=} [Z_{i+1}, G]$; die Behauptung folgt, da per Definition $Z_{i+1}(G)$ maximal mit der Eigenschaft $(*)$ ist.
$M_i/M_{i+1} \leqslant Z(G/M_{i+1}) \Longrightarrow [M_i/M_{i+1}, G/M_{i+1}] = E$ in G/M_{i+1}, das heißt $[M_i, G] \leqslant M_{i+1}$.
Per Induktion: $K_{i+1}(G) = [K_i(G), G] \leqslant [M_i, G] \leqslant M_{i+1}$.

(b),(c)$\Rightarrow$(a) ist klar mit „höchstens der Klasse c“; Gleichheit folgt aus der Umkehrrichtung! ■

Also ist bewiesen, daß die aufsteigende die „maximale“ und die absteigende die „minimale“ mögliche Zentralreihe ist.

Beispiele:

(a) Abelsche Gruppen sind nilpotent.

(b) p-Gruppen sind nilpotent.

(c) $U(n,K)$, die oberen $n \times n$-Dreiecksmatrizen mit Einsen auf der Diagonale und Koeffizienten aus K sind nilpotent.

(d) S_3 ist auflösbar, aber nicht nilpotent. Also sind Erweiterungen einer nilpotenten Gruppe durch eine nilpotente Gruppe nicht notwendigerweise nilpotent.

(e) Sei $G = D_\infty = \langle d, s\rangle$ mit $o(d) = \infty$, $o(s) = 2$ und $d^s = d^{-1}$. Dann
$$\left.\begin{array}{l} K_2(G) = G' = \langle [d,s]\rangle = \langle d^2\rangle \\ K_{j+1}(G) = \langle [d^{2^{j-1}}, s]\rangle = \langle d^{2^j}\rangle \end{array}\right\} \Rightarrow K_\omega(G) = E;\ \text{ferner } G'' = E \text{ und } Z(G) = E.$$
Also ist G auflösbar der Stufe 2, nicht nilpotent, hypozentral, aber die aufsteigende Zentralreihe bleibt trivial.

(f) Sei Z_{p^∞} = die „p^n-ten Einheitswurzeln in $\mathbb{C}$ für alle n“ $= \langle a_0, a_1, \ldots\rangle$ mit $a_0 = e$, $a_j^p = a_{j-1}$ und abelsch. Setze $G = Z_{p^\infty} \rtimes \langle b\rangle$ mit $b^p = 1$ und $a_j^b = a_j a_{j-1}$. Dann ist G/Z_{p^∞} zyklisch, also $G' \leqslant Z_{p^\infty}$ und $G'' = E$, also ist G auflösbar der Stufe 2. Wegen $[a_j, b] = a_j^{-1} a_j a_{j-1} = a_{j-1} \in [Z_{p^\infty}, G]$ gilt $K_j(G) = Z_{p^\infty}$ für alle $j \geqslant 2$ und G ist nicht nilpotent. Andererseits gilt $a_1 \in Z(G)$ und $[a_{i+1}, b] = a_i$, also folgt mit Induktion $a_i \in Z_i$. Daher $Z_{p^\infty} \leqslant Z_\omega(G)$, $G = Z_{\omega+1}(G)$ und G ist hyperzentral.

Satz 45 **(a)** *Untergruppen und homomorphe Bilder nilpotenter Gruppen der Klasse* c *sind nilpotent der Klasse* $\leqslant c$.

(b) G_i *nilpotent für* $i = 1, \ldots, n \Longrightarrow G_1 \times \ldots \times G_n$ *ist nilpotent der Klasse* $\max\{c_i\}$.

(c) G/N_j *nilpotent für* $i = 1, \ldots, n \Longrightarrow G/\bigcap_{i=1}^n N_i$ *nilpotent der Klasse* $\leqslant c$.

(d) *Sind* $M, N \trianglelefteq G$ *nilpotent der Klassen* c_M, c_N, *so ist* $M \cdot N$ *nilpotent der Klasse* $\leqslant c_M + c_N$.

(e) *(Hall)* $N \trianglelefteq G$ *und* G/N' *nilpotent* $\Longrightarrow G$ *nilpotent.*

Beweis: (a) $K_i(U) \leqslant K_i(G)$, $K_i(G/N) = K_i(G)N/N$

(b) $K_i(G_1 \times \ldots \times G_n) = K_i(G_1) \times \ldots \times K_i(G_n)$.

(c) Mit (a) und (b), denn $G/\bigcap_{i=1}^n N_i \hookrightarrow G/N_1 \times \ldots \times G/N_n$, denn $G \to G/N_1 \times \ldots \times G/N_n$, $g \mapsto (gN_1, \ldots, gN_n)$ hat Kern $\bigcap_{i=1}^n N_i$.

(d) Aus Kommutatorrechnung sieht man $[UV, W] = [U, V][V, W]$. Per Induktion folgt:
$K_{i+1}([M, N]) = \prod_{X_i \in \{M,N\}} [X_1, \ldots, X_i]$, also

$$K_{i+1}([M,N]) = \Big[\prod_{X_i\in\{M,N\}} [X_1,\ldots,X_i], MN\Big] = \prod_{X_i\in\{M,N\}} [X_1,\ldots,X_i,M]\cdot \prod_{X_i\in\{M,N\}} [X_1,\ldots,X_i,N]$$

Mit dem Lemma (d) und $M \trianglelefteq G$ folgt $[X_1, \ldots, X_i] \leqslant \underbrace{[M, \ldots, M]}_{k \text{ mal}}$, wobei k die Anzahl von M unter den X_i ist. Also $[X_1, \ldots, X_{c_M + c_N + 1}] \leqslant K_{c_M+1}(M) = E$ oder $\leqslant K_{c_N+1}(N) = E$.

(e) Folgt am Ende des Kapitels. ■

Satz 46 *Für eine endliche Gruppe* G *sind äquivalent:*

(a) G *ist nilpotent.*

(b) G *erfüllt die* Normalisator-Bedingung, *das heißt* $U < G \Longrightarrow U < N_G(U)$.

(c) *Jede maximale Untergruppe ist normal in* G.

(d) *Jede Sylowgruppe ist normal in* G.

(e) G *ist direktes Produkt ihrer Sylowgruppen.*

(f) *Falls* $(o(g), o(h)) = 1$, *so* $gh = hg$.

BEWEIS: (b) $\Rightarrow$ (c) ist trivial; (d) $\Rightarrow$ (e) bereits gezeigt und (e) $\Rightarrow$ (f) klar.

(a) $\Rightarrow$ (b): Sei j so, daß $K_{j+1}(G) \leqslant U$, $K_j(G) \not\leqslant U$. Dann $[K_j(G), U] \leqslant [K_j(G), G] = K_{j+1}(G) \leqslant U$, also $K_j(G) \leqslant N_G(U)$ mit Teil (d) des Lemmas.

(c) $\Rightarrow$ (d): Sei $P \in \mathrm{Syl}_p(G)$, $N_G(P) \neq G$ und $N_G(P) \leqslant U <_{\max} G$. Für $g \in G$ gilt dann nach Voraussetzung $P^g \leqslant U^g = U$, also $P, P^g \in \mathrm{Syl}_p(U)$ und es existiert $u \in U$ mit $P^g = P^u$. Damit $gu^{-1} \in N_G(P) \leqslant U$, daß heißt $g \in uU = U$: Widerspruch!

(f) $\Rightarrow$ (d): Seien $P_1 \in \mathrm{Syl}_{p_1}(G), \ldots, P_n \in \mathrm{Syl}_{p_n}(G)$ zu den verschiedenen Primzahlteilern $p_1, \ldots, p_n$ von $|G|$. Dann $P_i \trianglelefteq \langle P_1, \ldots, P_n \rangle = G$.

(e) $\Rightarrow$ (a) Sylowgruppen sind als p-Gruppen nilpotent, damit auch ihr direktes Produkt. ■

In unendlichen Gruppen sind die Bedingungen (b), (c) und (f) schwächer als Nilpotenz!

Satz 47 *Sei* G *nilpotent und* $E < N \trianglelefteq G$. *Dann ist* $[N, G] < N$ *und* $N \cap Z(G) \neq E$.

BEWEIS: Sei $N_1 := N$ und $N_{i+1} := [N_i, G]$. G habe Nilpotenzklasse $c > 0$. Dann ist $N_{c+1} \leqslant K_{c+1}(G) = E$, also ist $N_1 > N_2$ echt absteigend. Sei $N_m = E \neq N_{m-1}$. Dann ist $E = [N_m, G]$, also $E \neq N_{m-1} \leqslant Z(G) \cap N$. ■

Die Fitting–Gruppe Die *Fitting-Gruppe* $F(G)$ von G ist die von alles nilpotenten Normalteilern erzeugte (charakteristische) Untergruppe.

Sei nun G endlich. $O_p(G) := \bigcap\{P \mid P \in \mathrm{Syl}_p(G)\} \trianglelefteq G$ ist als p-Gruppe nilpotent und maximale normale p-Untergruppe von G: ist N normale p-Untergruppe, so $N \leqslant P \in \mathrm{Syl}_p(G)$ und $N = N^g \leqslant P^g$, mithin $N \leqslant O_p(G)$. Falls N nilpotenter Normalteiler von G ist, so $N = P_1 \times \ldots \times P_n$ mit $P_i \in \mathrm{Syl}_{p_i}(N)$ und die P_i sind als charakteristische Untergruppen von N normal in G. Also gilt $P_i \leqslant O_p(G)$ und $N \leqslant \prod_{p \in PZ} O_p(G)$. Folglich ist $\prod_{p \in PZ} O_p(G) = F(G)$ der maximale nilpotente Normalteiler von G.

Die Frattini–Gruppe Die *Frattini-Untergruppe* $\Phi(G) := \bigcap\{U \mid U <_{\max} G\}$ ist offenbar ebenfalls eine charakteristische Untergruppe von G. Sie hat als wesentliche Eigenschaft, die Untergruppe aller „Nichterzeuger“ von G zu sein. Genauer heißt dies: Falls $G = H\Phi(G)$ für $H \leqslant G$, so gilt $H = G$ (denn andernfalls $H \leqslant U_{\max}$ und per Definition auch $\Phi(G) \leqslant U$).

Sei nun wieder G endlich.

Lemma 48 **(a)** $\Phi(G)$ *ist nilpotent.*

(b) *Ist* $G/\Phi(G)$ *ist nilpotent, so auch* G.

BEWEIS: (a) Sei $P \in \mathrm{Syl}_p(\Phi(G))$. Mit dem Frattini-Argument gilt $G = N_G(P) \cdot \Phi(G)$, also $N_G(P) = G$.

(b) Sei $P \in \mathrm{Syl}_p(G)$. Dann ist $P\Phi(G)/\Phi(G) \in \mathrm{Syl}_p(G/\Phi(G))$, also $P\Phi(G)/\Phi(G) \trianglelefteq G/\Phi(G)$ und somit auch $N := P\Phi(G) \trianglelefteq G$. Wieder mit dem Frattini-Argument: $G = N_G(P \cap N) \cdot N = N_G(P) \cdot N = N_G(P) \cdot P \cdot \Phi(G) = N_G(P) \cdot \Phi(G)$, also $G = N_G(P)$. ■

Sei M maximale Untergruppe von G. Ist $M \trianglelefteq G$, so ist $|G/M| = p$ eine Primzahl. (Andernfalls: Sei $P/M \in \mathrm{Syl}_p(G/M)$ für einen Teiler p von $|G/M|$, dann $P = G$, also G p-Gruppe. In p-Gruppen G/M mit $|G/M| = p^l$ existiert Untergruppe U/M mit $|U| = p^{l-1}$, also $U = M$.)
Also ist G/M abelsch, das heißt $G' \leqslant M$. Umgekehrt folgt $M \trianglelefteq G$ aus $G' \leqslant G$. Folglich gilt:

Satz 49 G *ist nilpotent* $\iff$ $G' \leqslant M$ *für alle maximalen* M $\iff$ $G' \leqslant \Phi(G)$.

Es folgt nun der offengebliebene Beweis des Satzes von Hall: sind $N \trianglelefteq G$ und G/N' nilpotent, so auch G:

BEWEIS: Für $N \trianglelefteq G$ gilt $\Phi(N) \leqslant \Phi(G)$: denn angenommen $\Phi(N) \nleqslant M <_{\max} G$. Dann folgt $G = \Phi(N)M$, also $N = \Phi(N)(N \cap M)$ und $N = N \cap M$: Widerspruch. Ferner, falls $N \leqslant \Phi(G)$, so $\Phi(G/N) = \bigcap \{U/N \mid U/N <_{\max} G/N\} = \bigcap \{U \mid N \leqslant U <_{\max} G\}/N = \Phi(G)/N$.
Nun $(G/N')' = G'/N' \overset{G/N' \text{ nilpotent}}{\leqslant} \Phi(G/N') = \Phi(G)/N'$, da $N' \overset{N \text{ nilpotent}}{\leqslant} \Phi(G)$; also $G' \leqslant \Phi(G)$. ■

11 Abelsche Gruppen

Alle Gruppen in diesem Abschnitt sind kommutativ und werden daher in der Regel additiv $(G, 0, +, -)$ geschrieben; insbesondere schreibt man ng für g^n. Dadurch werden abelsche Gruppen zu $\mathbb{Z}$-Moduln. Ein großer Teil der Theorie abelscher Gruppen gilt allgemeiner für Moduln über Hauptidealringen.

Da $n(g+h) = ng + nh$, gilt $o(g+h) \mid \mathrm{kgV}(o(g), o(h))$. Es folgt, daß $G[n] := \{g \in G \mid ng = 0\} = \{g \in G \mid o(g) | n\}$ eine Untergruppe von G ist (wohingegen z.B. $S_n[2]$ ganz S_n erzeugt).

Für eine Primzahl p setzt man ferner die p-*Komponente* G_p als die Menge aller p-*Elemente*, d.h. $G_p := \bigcup_{n \in \mathbb{N}} G[p^n] = \{g \in G \mid \exists n \in \mathbb{N}\, p^n g = 0\}$. Die p-Komponente G_p ist die maximale p-Untergruppe von G und somit charakteristisch in G; G/G_p enthält keine p-Elemente mehr. Im endlichen Fall ist G_p also die p-Sylowgruppe von G.

$G[p]$ ist auf natürliche Weise ein $\mathbb{F}_p$-Vektorraum (die Modulmultiplikation $\mathbb{Z} \times G[p] \to G[p]$ faktorisiert durch $p\mathbb{Z}$), insbesondere sind die Gruppenautomorphismen genau die Vektorraumautomorphismen. Ferner sind Untergruppen auch Unterräume.

Torsionsgruppen Elemente endlicher Ordnung heißen auch *Torsionselemente*; sie bilden die *Torsionsgruppe* $\mathrm{Tor}(G) := \{g \in G \mid \exists n \in \mathbb{N}\, ng = 0\}$ von G. Eine Gruppe G heißt Torsionsgruppe, falls $G = \mathrm{Tor}(G)$, und *torsionsfrei*, falls $\mathrm{Tor}(G) = E$. Es ist $G/\mathrm{Tor}(G)$ maximale torsionsfreie Faktorgruppe von G (falls $n \cdot g\mathrm{Tor}(G) = E$, so $ng \in \mathrm{Tor}(G)$, also existiert ein m mit $mng = 0$, womit $g \in \mathrm{Tor}(G)$).

Satz 50 *Sei* G *Torsionsgruppe. Dann gilt* $G \cong \bigoplus_{p \in \mathbb{P}} G_p$.

BEWEIS: $G_p \cap G_q = E$ für $p \neq q$ ist klar.

Sei $g \in G$ und $o(g) = p_1^{k_1} \cdots p_l^{k_l}$ die Primzahlzerlegung. Setze $n_i := \frac{o(g)}{p_i^{k_i}}$ und $g_i := n_i g \in G_{p_i}$, da $o(g_i) = p_i^{k_i}$. Wegen $\mathrm{ggT}(n_1, \ldots, n_l) = 1$ gibt es $a_1, \ldots, a_l$ mit $a_1 n_1 + \cdots + a_l n_l = 1$. Es folgt $g = (a_1 n_1 + \cdots + a_l n_l)g = a_1 g_1 + \cdots + a_l g_l \in \bigoplus_{i=1}^{l} G_{p_i}$. ■

Beispiele:

- Alle endlichen Gruppen sind Torsionsgruppen; Z_{p^∞} und alle unendlich-dimensionalen Vektorräume über $\mathbb{F}_q$ sind unendliche Torsionsgruppen.
- $\mathbb{Z}$ und $\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}$ sind Beispiele torsionsfreier Gruppen.
- $\mathrm{Tor}(\mathbb{C}^\times) =$ alle Einheitswurzeln.
- $\mathrm{Tor}(\mathbb{R}^\times) = \{\pm 1\}$.

Lemma 51 *Die endlich erzeugten Torsionsgruppen sind genau die endlichen Gruppen.*

BEWEIS: Sei $G = \langle g_1, \ldots, g_n \rangle$ Torsionsgruppe. Dann sind die zyklischen Gruppen $\langle g_i \rangle$ endlich und $G = \langle g_1 \rangle + \cdots + \langle g_n \rangle$. Die Umkehrrichtung ist klar. ■

Lemma 52 *Sei* G *abelsche* p*-Gruppe vom Exponenten* p^m *und* g *ein Element maximaler Ordnung. Dann gilt* $G = \langle g \rangle \oplus H$.

BEWEIS: Sei M maximal mit $M \cap \langle g \rangle = \emptyset$ (existiert nach Zorns Lemma). Falls $G \neq M + \langle g \rangle$, so sei $x \in G \setminus (M + \langle g \rangle)$ von minimaler Ordnung. Dann ist $px \in M + \langle g \rangle$, das heißt $px = y + l \cdot g$ mit $y \in M$. Es gilt $0 = p^m x = p^{m-1} y + p^{m-1} l \cdot g$, folglich $p^{m-1} l \cdot g \in M \cap \langle g \rangle$ und somit $p^m \mid p^{m-1} l$, also $p \mid l$. Sei $l = pj$, also $p(x - jg) = y \in M$ und $x - jg \notin M$, da $x \notin M + \langle g \rangle$. Aus der Maximalität von M folgt nun $\langle x - jg, M \rangle \cap \langle g \rangle \neq \emptyset$, das heißt es existieren k, k' und $y' \in M$ mit $0 \neq kg = k'(x - jg) + y'$. Also ist $k'x \in M + \langle g \rangle$.
Angenommen $p \mid k'$: Da $p(x - jg) \in M$ und $y' \in M$, folgt $k'(x - jg) \in M$, somit $kg = 0$.
Also $p \nmid k'$, das heißt $\mathrm{ggT}(p, k') = 1$. Da $px, k'x \in M + \langle g \rangle$ erhält man $x \in M + \langle g \rangle$: Widerspruch!
Mithin $G = M + g$ und somit $G = M \oplus g$. ■

Satz 53 *Jede endliche abelsche Gruppe ist direkte Summe zyklischer Gruppen.*

BEWEIS: Zerlege G in die direkte Summe seiner p-Komponenten und zerlege dann induktiv mit Hilfe des Lemmas jede p-Komponente. ■

Mit diesem Struktursatz kann man nun einfach sämliche abelschen Gruppe einer gegebenen Ordnung bestimmen. Für $360 = 2^3 \cdot 3^2 \cdot 5$ sind dies zum Beispiel:

$$\begin{array}{rr} Z_2 \oplus Z_2 \oplus Z_2 \ \oplus\ Z_3 \oplus Z_3 \ \oplus\ Z_5 & Z_2 \oplus Z_2 \oplus Z_2 \ \oplus\ Z_9 \ \oplus\ Z_5 \\ Z_2 \oplus Z_4 \ \oplus\ Z_3 \oplus Z_3 \ \oplus\ Z_5 & Z_2 \oplus Z_4 \ \oplus\ Z_9 \ \oplus\ Z_5 \\ Z_8 \ \oplus\ Z_3 \oplus Z_3 \ \oplus\ Z_5 & Z_8 \ \oplus\ Z_9 \ \oplus\ Z_5 \end{array}$$

Folgerung 54 *Sei* K *ein Körper,* G *endlich* $\leqslant K^\times$*. Dann ist* G *zyklisch. Insbesondere ist* $\mathbb{F}_q^\times$ *zyklisch.*

BEWEIS: Es reicht zu zeigen, daß G_p zyklisch ist. Sei $G_p = Z_{p^{n_1}} \times \ldots \times Z_{p^{n_k}}$. Dann gilt $|G[p]| = p^k$. Die Elemente von $G[p]$ sind aber Lösungen von $x^p = 1$, wovon es in einem Körper nur p viele geben kann. Also $k = 1$. ■

Beispiele

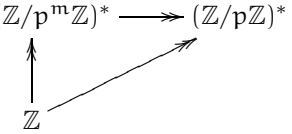
(a) $\mathbb{F}_{p^n}$ ist Vektorraum der Dimension n über $\mathbb{F}_p$, somit ist die additive Gruppe $(\mathbb{F}_{p^n}, +) \cong \underbrace{Z_p \oplus \cdots \oplus Z_p}_{n \text{ mal}}$; die multiplikative Gruppe $(\mathbb{F}_{p^n}^\times, \cdot) \cong Z_{p^n - 1}$.

(b) Sei $n = p_1^{m_1} \cdots p_k^{m_k}$ die Primfaktorzerlegung. Dann gilt

$$\left((\mathbb{Z}/n\mathbb{Z})^*, \cdot\right) \cong (\mathbb{Z}/p_1^{m_1}\mathbb{Z})^* \times \ldots \times (\mathbb{Z}/p_k^{m_k}\mathbb{Z})^*$$

da (chinesischer Restsatz!) $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{m_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_k^{m_k}\mathbb{Z}$ als Ring. Weiter
für $p > 2$: $(\mathbb{Z}/p^m\mathbb{Z})^* \cong Z_{p^{m-1}(p-1)}$
für $m \geqslant 2$: $(\mathbb{Z}/2^m\mathbb{Z})^* \cong Z_{2^{m-2}} \times Z_2$ und $(\mathbb{Z}/2\mathbb{Z})^* \cong E$.

BEWEIS: (b) $(\mathbb{Z}/p\mathbb{Z})^* = \mathbb{F}_p^\times \cong Z_{p-1}$. Betrachte die Surjektion $\varphi : (\mathbb{Z}/p^m\mathbb{Z})^* \to (\mathbb{Z}/p\mathbb{Z})^*$, $x + p^m\mathbb{Z} \mapsto x + p\mathbb{Z}$, mit Kern $\{\overline{x} \mid x \equiv 1 \bmod p\}$ der Größe p^{m-1}.



Behauptung: $\mathrm{Kern}(\varphi) = \langle\overline{1+p}\rangle$. Dann folgt daß $(\mathbb{Z}/p^m\mathbb{Z})^* = Z_{p-1} \times \mathrm{Kern}(\varphi)$ zyklisch ist. Dazu zeigt man per Induktion nach k zunächst $(1+p)^{p^k} \equiv 1+p^{k+1} \pmod{p^k}$. Daraus gewinnt man $(1+p)^{p^{m-2}} \equiv 1 + p^{m-1} \not\equiv 1 \pmod{p^m}$, also hat $\overline{1+p}$ die Ordnung p^{m-1} in $\mathrm{Kern}(\varphi)$.

Sei nun $\psi : (\mathbb{Z}/2^m\mathbb{Z})^* \twoheadrightarrow (\mathbb{Z}/4\mathbb{Z})^* = \{\overline{1}, \overline{-1}\}$. Wie oben zeigt man mit Induktion nach k zunächst: $(1+4)^{2^k} = 1+2^{k+2} (\mathrm{mod} 2^{k+3})$, also hat $\overline{5}$ die maximale Ordnung 2^{m-2} in $\mathrm{Kern}(\psi)$. Außerdem ist $\overline{-1} \notin \mathrm{Kern}(\psi)$ und hat Ordnung 2, somit $\langle\overline{5}\rangle \cap \langle\overline{-1}\rangle = E$. Es folgt $(\mathbb{Z}/2^m\mathbb{Z})^* \cong \langle\overline{5}\rangle \times \langle\overline{-1}\rangle \cong Z_{2^{m-2}} \times Z_2$. ■

Die Gleichung $x^2 \equiv 1 \pmod{2^m}$ hat 4 Lösungen: $1, -1, 1+2^{m-1}, -1+2^{m-1}$.

Freie abelsche Gruppen

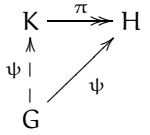
Satz 55 (a) *Seien $\overline{F_1}, \overline{F_2}$ freie abelsche Gruppen über X_1 bzw. X_2. Dann ist $\overline{F_1} \cong \overline{F_2} \iff |X_1| = |X_2|$.*

(b) *Echte Untergruppen freier abelscher Gruppen sind wieder frei abelsch (von kleinerem Rang, falls dieser endlich ist).*

BEWEIS: (a): „⇒“ ist klar; „⇐“: $F_i/2F_1$ ist $\mathbb{F}_2$-Vektorraum mit Basis X_i.

(b) für endlichen Rang: Sei $X = \{x_1, \ldots, x_n\}$ und $H < F$. Setze $F_i = \langle x_1\rangle \oplus \cdots \oplus \langle x_i\rangle$ und $H_i = H \cap F_i$. Dann gilt $H_{i+1}/H_i \cong H_{i+1}F_i/F_i \leqslant F_{i+1}/F_i \cong \langle x_{i+1}\rangle$. Entweder ist $H_{i+1} = H_i$, oder $H_{i+1}/H_i = \langle y_{i+1} + H_i\rangle$ und $H_{i+1} = H_i \oplus \langle y_{i+1}\rangle$ mit $y_{i+1} \in \langle x_{i+1}\rangle$. Also ist H direkte Summe der y_i, wobei gegenüber F mindestens ein Index i ausfällt.
Bei beliebigem Rang funktioniert der gleiche Beweis mit transfiniter Induktion. ■

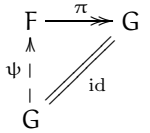
Eine abelsche Gruppe heißt *projektiv*, falls für alle Gruppen K, H, für alle Epimorphismen $\pi : K \to H$ und für alle Homomorphismen $\varphi : G \to H$ ein Homomorphismus $\psi : G \to K$ existiert mit $\varphi = \pi \circ \psi$.



Satz 56 (MacLane) *Die projektiven abelschen Gruppen sind genau die freien abelschen Gruppen.*

Mit dem gleichen Beweis gilt dies für alle Varietäten $\mathfrak{V}$, in denen Untergruppen von $\mathfrak{V}$-freien Gruppen wieder $\mathfrak{V}$-frei sind. Dies sind nur die Varietäten aller Gruppen, aller abelschen Gruppen und der abelschen Gruppen von Exponenten p.

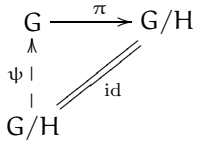
BEWEIS: „⇐“: Sei G freie abelsche Gruppe über X. Zu $x \in X$ existiert $a_x \in K$ mit mit $\pi(a_x) = \varphi(g)$. Setze $x \mapsto a_x$ zu Homomorphismus $\psi : G \to K$ fort.



„⇒“: Sei G projektiv, Quotient der frei abelschen Gruppe F wie rechts. Man erhält $\psi : G \to F$ und $\pi \circ \psi = \mathrm{id}_G$, also ist ψ injektiv, G Untergruppe einer freien abelschen Gruppe und damit selbst frei abelsch. ■

Folgerung 57 *Falls G abelsch, $H \leqslant G$ und G/H frei abelsch, so ist $G \cong H \oplus K$ mit $G/H \cong K$.*

BEWEIS: Sei $\pi : G \to G/H$ die natürliche Surjektion, ψ der Schnitt dazu, den man aus der Projektivität gewinnt. Dann gilt $G = \mathrm{Kern}(\pi) \oplus \mathrm{Bild}(\psi)$:



Wegen $\pi(g - \psi(\pi(g))) = \pi(g) - (\pi \circ \psi)(\pi(g)) = \pi(g) - \pi(g) = 0$ für $g \in G$ gilt $G = \mathrm{Kern}(\pi) + \mathrm{Bild}(\psi)$.
Ferner ist für $g = \psi(g' + H) \in \mathrm{Kern}(\pi) + \mathrm{Bild}(\psi)$: $g' + H = \pi(\psi(g' + H)) = 0$. ■

Endlich erzeugte abelsche Gruppen

Satz 58 **(a)** *Die endlich erzeugten Torsionsgruppen sind genau die endlichen Gruppen, d.h. die endlichen direkten Summen endlicher zyklischer Gruppen.*

(b) *Die endlich erzeugten torsionsfreien Gruppen sind genau die freien abelschen Gruppen endlichen Ranges, d.h. die endlichen direkten Summen unendlicher zyklischer Gruppen.*

(c) *Die endlich erzeugten abelschen Gruppen sind genau die endlichen direkten Summen beliebiger zyklischer Gruppen.*

$\mathbb{Q}$ ist torsionsfrei, aber weder frei noch endlich erzeugt!

BEWEIS: (a): bereits gezeigt.

(b) „⇐“: $\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}$ ist offenbar torsionsfrei und endlich erzeugt.

„⇒“: Sei $G = \langle g_1, \ldots, g_n \rangle$ torsionsfrei. Zeige per Induktion $G \cong \mathbb{Z}^k$ für ein $k \leqslant n$:
Sei $H := \{ g \in G \mid \exists n\, ng \in \langle g_1 \rangle \} \leqslant G$. Falls $mx \in H$, so $mnx \in \langle g_1 \rangle$, also $x \in H$, das heißt G/H ist torsionsfrei. $G/H = \langle g_2 + H, \ldots, g_n + H \rangle \cong \mathbb{Z}^k$ per Induktion und G/H ist frei abelsch, also existiert $K \leqslant G$ mit $G = K \oplus H$. Nun ist H als direkter Summand von G endlich erzeugt, $H/\langle g_1 \rangle$ ist Torsionsgruppe, also ist $H/\langle g_1 \rangle$ endlich und es gibt ein $m \in \mathbb{N}$ mit $mH \leqslant \langle g_1 \rangle$. Also ist $H \to \langle g_1 \rangle$, $h \mapsto mh$ injektiver Homomorphismus ($mh_1 = mh_2 \Longrightarrow m(h_1 - h_2) = 0 \Longrightarrow h_1 = h_2$, da G torsionsfrei). Da $H \neq E$ ist $H \cong \mathbb{Z}$ und somit $G = H \oplus K \cong \mathbb{Z} \oplus \mathbb{Z}^k = \mathbb{Z}^{k+1}$.

(c) „⇒“: $G/\mathrm{Tor}(G)$ ist endlich erzeugt und torsionsfrei, also frei abelsch und $\cong \mathbb{Z}^k$. Somit ist $G \cong \mathrm{Tor}(G) \oplus \mathbb{Z}^k$. Dann ist $\mathrm{Tor}(G)$ eine endlich erzeugte Torsionsgruppe, also direkte Summe zyklischer Gruppen nach (a).

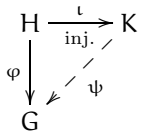
„⇐“ ist klar. ■

Divisible Gruppen Eine abelsche Gruppe G heißt *divisibel* (oder *teilbar*), falls es für alle $g \in G$ und alle $m \in \mathbb{N}/\{0\}$ ein $h \in G$ mit $mh = g$ gibt (mit anderen Worten: die Homomorphismen $G \to G$, $g \mapsto mg$ sind alle surjektiv, bzw. $G = mG$ für alle $m \in \mathbb{N}/\{0\}$).

Beispiele:

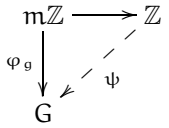
- $\mathbb{Q}$ und die Prüfergruppen Z_{p^∞}.
- E ist die einzige endliche divisible Gruppe.
- Homomorphe Bilder und beliebige direkte Summen divisibler Gruppen sind divisibel.
- Untergruppen divisibler Gruppen sind im Allgemeinen nicht divisibel ($\mathbb{Z} \leqslant \mathbb{Q}$).

Eine abelsche Gruppe G heißt *injektiv*, falls für alle Gruppen H, K, alle injektiven Homomorphismen $\iota : H \to K$ und Homomorphismen $\varphi : H \to G$ ein Homomorphismus $\psi : K \to G$ existiert mit $\varphi = \psi \circ \iota$.

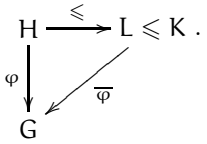


Satz 59 (Baer) *Die injektiven abelschen Gruppen sind genau die divisiblen Gruppen.*

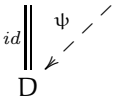
BEWEIS: „⇒“: Sei $g \in G$. Betrachte den Homomorphismus $\varphi_g : m\mathbb{Z} \to G$, $m \mapsto g$. Dann existiert $\psi_g : \mathbb{Z} \to G$ mit $m\psi_g(1) = \psi_g(m) = \varphi_g(m) = g$.



„⇐“: Sei ohne Einschränkung $H \leqslant K$, sei $\overline{\varphi} : L \to G$ mit $H \leqslant L \leqslant K$ maximale Fortsetzung von φ (existiert mit Zorns Lemma).
Sei nun $x \in K \setminus L$.



Falls $L \cap \langle x \rangle =$, so setze $\overline{\varphi}$ fort auf $L \cap \langle x \rangle$ durch $\overline{\varphi}(x) = 0$.
Falls $L \cap \langle x \rangle = \langle mx \rangle$. Sei $g = \overline{\varphi}(mx)$ und $g = mg'$ mit $g' \in G$. Setze $\overline{\varphi}$ fort auf $L + \langle x \rangle$ durch $h + nx \mapsto \overline{\varphi}(l) + ng'$ (nachrechnen, daß dies ein Homomorphismus ist!). ■

Folgerung 60 **(a)** *Ist* G *abelsch und* $D \leqslant G$ *divisibel, so gilt* $G \cong D \oplus K$.
(Denn 

, also $G = \mathrm{Bild}(\iota) \oplus \mathrm{Kern}(\psi) \cong D \oplus \mathrm{Kern}(\psi)$ *wie oben.)*

(b) *Jede abelsche Gruppe* G *zerlegt sich in* $G = D \oplus K$*, wobei* D *die eindeutig bestimmte maximale divisible Untergruppe ist und* K *keine unendlichen divisiblen Untergruppen enthält.*

Freie abelsche Gruppen verhalten sich dual zu den divisiblen Gruppen:

- Die freien abelschen Gruppen sind die projektiven, die divisiblen die injektiven.
- Untergruppen freier ablescher Gruppen sind frei abelsch; homomorphe Bilder divisibler Gruppen sind divisibel.
- Jede abelsche Gruppe ist homomorphes Bild einer freien abelschen Gruppe und Untergruppe einer divisiblen Gruppe.
- Rang 1: Die nicht-trivialen Untergruppen von $\mathbb{Z}$ sind zu $\mathbb{Z}$ isomorph; die homomorphen Bilder sind alle zyklischen Gruppen. Die echten Untergruppen von Z_{p^∞} sind die zyklischen p-Gruppen (die endlich erzeugten Untergruppen von $\mathbb{Q}$ sind von der Form $\mathbb{Z}^n$); einziges nicht-triviales homorphes Bild ist Z_{p^∞} (bzw. $\mathbb{Q}$).

BEWEIS: Sei F frei abelsch mit $F \xrightarrow{\text{surj.}} G$ mit Kern K. Dann ist $F \cong \bigoplus_k \mathbb{Z} \leqslant \bigoplus_k \mathbb{Q} = D$ (divisibel), also $G \cong F/K \leqslant D/K$ divisibel. ■

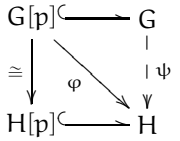
Es gibt sogar eine bis auf Isomorphie eine eindeutig bestimmte kleinste divisible Obergruppe, die *divisible Hülle*.

Divisible torsionsfreie Gruppen sind auf natürliche Weise $\mathbb{Q}$-Verktorräume (torsionsfrei impliziert, daß die Division durch n eindeutig wird).

Satz 61 *Divisible Gruppen sind genau beliebige direkte Summen von* $\mathbb{Q}$ *und* Z_{p^∞}.

BEWEIS: $G/\mathrm{Tor}(G)$ ist divisibel und torsionsfrei; also ist $G/\mathrm{Tor}(G) = \bigoplus_k \mathbb{Q}$ und $G = \bigoplus_k \mathbb{Q} \oplus \mathrm{Tor}(G) = \bigoplus_k \mathbb{Q} \oplus \bigoplus_{p \in \mathbb{P}} \mathrm{Tor}(G)_p$. Nun ist $\mathrm{Tor}(G)$ als homomorphes Bild von G divisibel, ebenso seine p-Komponenten $\mathrm{Tor}(G)_p$.

Also sei ohne Einschränkung G eine divisible p-Gruppe. Dann ist $G[p]$ ein $\mathbb{F}_p$-Vektorraum der Dimension d. Setze $H = \bigoplus_d Z_{p^\infty}$ und $\varphi : G[p] \to H[p]$ ein Isomorphismus. H ist divisibel, also injektiv und es existiert $\psi : G \to H$ mit $\psi(G[p]) = H[p]$.



Kern(ψ) ist eine p-Gruppe, also folgt aus Kern(ψ) $\cap\, G[p] = 0$ bereits Kern(ψ) $= 0$. Ebenso folgt Bild(ψ) $= H$ aus Bild(ψ) $\cap\, H[p] = H[p]$, da in jeder Komponente von H eine divisible Untergruppe von Z_{p^∞} erreicht werden muß, also E oder ganz Z_{p^∞}. ■

12 Matrixgruppen

Ein n-dimensionaler Vektorraum V über einem Körper K führt zu drei verschiedenen „Geometrien“:

- V als Vektorraum (mit 0 als ausgezeichnetem Element);
- V als *affiner Raum* $\mathbb{A}(V)$, dem homogenen Raum zu V, in dem alle Punkte gleichberechtigt sind;
- und schließlich zum *projektiven Raum* $\mathbb{P}(V)$, dem Raum der eindimensionalen Unterräume von V, den man auch durch Ergänzen eines $(n-1)$-dimensionalen Vektorraums über K um „unendliche Punkte“ (= Parallelitätsklassen von Geraden) erhalten kann.

Zu diesen drei Räumen gehören jeweils Automorphismengruppen. Man beachte, daß der Körper K in den Geometrien beinhaltet ist, (z.B. als Streckungen um einen festen Punkt – für $n \geqslant 2$ kann man K explizit aus der Inzidenzstruktur zwischen Punkten und Geraden in $\mathbb{A}(V)$ wiedergewinnen). Also kann man sowohl die Automorphismen betrachten, welche K punktweise festlassen, als auch jene, welche einen Automorphismus von K induzieren. Schlielich kann man Zusatzstruktur erhalten wollen, insbesondere interessiert hier das durch die Determinante bestimmte Volumen. Diese Automorphismengruppen erhalten folgende Namen:

	K beweglich	K fest	volumenerhaltend
affiner Raum	AΓL(V)	AGL(V)	ASL(V)
Vektorraum	ΓL(V)	GL(V)	SL(V)
projektiver Raum	PΓL(V)	PGL(V)	PSL(V)

Für $V = K^n$ schreibt man auch $\square\square L(n, K)$ statt $\square\square L(V)$, und schließlich $\square\square L(n, q)$, falls $K = \mathbb{F}_q$. Es gelten nun folgende Beziehungen zwischen den Gruppen (wobei $\square$ je nach Position für A, P und nichts bzw. Γ, G und S steht):

- $\square SL(V) \leqslant \square GL(V) \leqslant \square\Gamma L(V)$; $\square L(V) \leqslant A\square L(V)$ und $\square L(V) \twoheadrightarrow P\square L(V)$.
- $\square\Gamma L(V) = \square GL(V) \rtimes \mathrm{Aut}(K)$.
- $AGL(V) = GL(V) \ltimes V$ (V als Gruppe der Translationen), ebenso $ASL(V) = SL(V) \ltimes V$.
- $\det : GL(V) \twoheadrightarrow K^\times$ mit Kern $SL(V)$.
- $PGL(V) = GL(V)/K^\times$, wobei $K^\times$ hier die Gruppe der zentralen Streckungen ist, ebenso $PSL(V) = SL(V)/\{x \in K^\times \mid x^n = 1\}$.

Sei $I = I_n$ die Identitätsmatrix in $GL(n, K)$ und E_{ij} die Matrix mit Eintrag 1 an der Position (i, j) und 0 sonst. Eine *Transvektion* ist eine Matrix $T_{ij}(a) := I + aE_{ij}$ für $i \neq j$. Alle Transvektionen liegen in $SL(n, K)$.

Lemma 62 *Es gilt* $C_{GL(n,K)}(SL(n, K)) = \{aI \mid a \in K^\times\}$.

Folgerung 63 $Z(GL(n, K)) = \{aI \mid a \in K^\times\}$
$Z(SL(n, K)) = Z(GL(n, K)) \cap SL(n, K) = \{aI \mid a \in K^\times, a^n = 1\}$.

Beweis: Aus $[A, T_{ij}(1)] = I$ folgt $AE_{ij} = E_{ij}A$, also $a_{ii} = a_{jj}$ und $a_{ki} = a_{jk} = 0$ für $k \neq i, j$. ■

Nun ermöglichen die Beziehungen oben die Ordnungen der Gruppen $\square\square L(n,q)$ auszurechnen:

Zunächst gibt es q^k viele $\mathbb{F}_q$-Linearkombinationen von k-Vektoren (der Nullvektor ist Linearkombintion aus null Vektoren!). Baut man eine Matrix zeilenweise auf, liegt sie genau dann in $GL(n,q)$, wenn für alle k der k-te Zeilenvektor nicht Linearkombination der vorangehenden ist. Also folgt $g(n,q) := |GL(n,q)| = (q^n-1)(q^n-q)\cdots(q^n-q^{n-1})$.

Sei $q = p^k$ mit $p = \mathrm{char}(\mathbb{F}_q)$. Dann gilt $\mathrm{Aut}(\mathbb{F}_q) \cong Z_k$ (erzeugt durch den Frobenius). Ferner ist $\{x \in \mathbb{F}_q \mid x^n = 1\}$ eine Untergruppe der multiplikativen Gruppe $\mathbb{F}_q^\times \cong Z_{q-1}$ der Ordnung $\mathrm{ggT}(q-1,n)$. Für die anderen Gruppen ergeben sich damit als Mächtigkeiten folgende Vielfache von $g(n,q)$ (mit der Anordnung von oben):

	Γ	allgemeine	spezielle
affine Gruppen	kq^n	q^n	$\frac{q^n}{q-1}$
lineare Gruppen	k	1	$\frac{1}{q-1}$
projektive Gruppen	$\frac{k}{q-1}$	$\frac{1}{q-1}$	$\frac{1}{(q-1)\mathrm{ggT}(q-1,n)}$

Zu bemerken ist, daß einzig bei der PSL die Gruppenordnung nicht notwendig monoton mit n und q wächst.

Üblich sind noch folgende Bezeichnungen:

$T(n,K)$ bezeichnen die oberen Dreiecksmatrizen, also die regulären Matrizen (a_{ij}) mit $a_{ij} = 0$ für $i > j$. Sie bilden eine auflösbare Untergruppe von $GL(n,K)$ (im Falle eine algebraisch abgeschlossenen Körpers K eine sogenannte *Borel–Gruppe*: eine maximale zusammenhängende auflösbare Untergruppe von $GL(n,K)$. Alle Borel–Gruppen sind untereinander konjugiert).

$U(n,K)$ steht für die oberen Dreiecksmatrizen mit $a_{ii} = 1$ für alle $i = 1,\ldots,n$. Sie bilden eine nilpotente Untergruppe von $GL(n,K)$. Wegen $|U(n,q)| = q^{\frac{n(n-1)}{2}}$ und $GL(n,q) = q^{\frac{n(n-1)}{2}} \cdot \prod_{i=1}^{n}(q^i-1)$ ist $U(n,q)$ offenbar eine p-Sylowgruppe von $GL(n,q)$.

Permutationsmatrizen Jede endliche Gruppe G läßt sich in $GL(|G|,R)$ einbetten für einen beliebigen Ring R mit $0 \neq 1$. Dazu genügt es, S_n in $GL(n,R)$ einzubetten. Dies geschieht durch $\Pi : S_n \to GL(n,R)$, $\sigma \mapsto \sum_{i=1}^{n} E_{i\sigma(i)}$, welches ein Gruppenhomomorphismus ist, falls man für S_n die Verknüpfung von links nimmt. Für die bei Abbildungen übliche Verknüpfung von rechts müßte man $\Pi^{op} : \sigma \mapsto \sum_{i=1}^{n} E_{\sigma(i)i}$ benutzen.

Das Bild von Π besteht aus den sogenannten *Permuationsmatrizen*: Matrizen, die pro Zeile und Spalte genau einen Eintrag 1 und sonst stets 0 enthalten. Durch $\sigma \mapsto \sum_{i=1}^{n} E_{i\sigma(i)} + \sum_{i=1}^{n} E_{i+n\,\sigma(i)+n}$ erhält man auch Einbettungen in $SL(2|G|,R)$ und $PSL(2|G|,K)$.

Sei p Primzahl. Da man jede endliche Gruppe in ein $GL(n,p)$ einbetten kann, wo die Existenz von Sylowgruppen oben konkrt aufgezeigt wurde, erhält man einen Alternativbeweis der Existenz von Sylowgruppen, wenn man zeigen kann, daß sie sich auf Untergruppen überträgt.

Sei also $H \leqslant G$ und $P \in \mathrm{Syl}_p(G)$. Aus der Doppelnebenklassenzerlegung $G = \bigcup_{i\in I} Hx_iP$ erhält man

$$|G| = \sum_{i\in I} \frac{|H|\cdot|P|}{|H^{x_i} \cap P|} = |P| \cdot \sum_{i\in I} \frac{|H|}{|H^{x_i} \cap P|}$$

Folglich gibt es ein i mit $p \nmid \frac{|H|}{|H^{x_i}\cap P|}$, also ist die p-Gruppe $H^{x_i} \cap P$ eine Sylowgruppe von H^{x_i} bzw. $H \cap P^{x_i^{-1}} \in \mathrm{Syl}_p(H)$.

Die Einfachheit von PSL

Satz 64 $\mathrm{PSL}(n, q)$ *ist einfach für* $n > 2$ *oder* $q > 3$.

Lemma 65 *Die Transvektionen erzeugen* $\mathrm{SL}(n, K)$.

BEWEIS: Für $n = 1$ ist das Lemma trivial; sei also $n > 1$. Multiplikation mit $T_{ij}(a)$ (von rechts bzw. links) bedeutet Addition des a-fachen der i-ten Spalte zur j-ten bzw. der j-ten Zeile zur i-ten.

Die erste Spalte ist nicht der Nullvektor, etwa $a_{k1} \neq 0$. Durch eventuelle Addition der k-ten Zeile zur n-ten kann man $a_{n1} \neq 0$ annehmen; durch Addition des $\frac{1-a_{11}}{a_{n1}}$-fachen der n-ten Zeile zur ersten erhält man $a_{11} = 1$. Nun bewirkt Addition des $(-\frac{a_{k1}}{a_{11}})$-fachen der ersten Zeile zur k-ten und Addition des $(-\frac{a_{1k}}{a_{11}})$-fachen der ersten Spalte zur k-ten, daß man $a_{1k} = a_{k1} = 0$ für $k \neq 0$ annehmen kann. Dann schließt man per Induktion nach n. ■

Lemma 66 *Alle Transvektionen sind in* $\mathrm{GL}(n, K)$ *konjugiert; für* $n > 2$ *sogar in* $\mathrm{SL}(n, K)$.

BEWEIS: Sei A Diagonalmatrix mit $a_{ii} = 1$, $a_{jj} = \frac{b}{a}$; falls $n > 2$ sei ein anderes Diagonalelement $a_{kk} = a_{jj}^{-1}$ und alle anderen Diagonalelement $a_{kk} = 1$. Dann gilt $A^{-1}T_{ij}(a)A = T_{ij}(b)$. Sei B wie I_n bis auf vier Einträge: $b_{ii} = b_{kk} = 0$, $b_{ik} = 1$ und $b_{ki} = -1$. Dann $B^{-1}T_{ij}(a)B = T_{kj}(a)$. Im Falle $n = 2$ fehlt noch $J^{-1}T_{12}(a)J = T_{21}(a)$, wobei $J = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$. ■

Der Beweis des Satzes kann nun mit längerer Matrixrechnung erfolgen: man zeigt zunächst, daß ein nicht im Zentrum enthaltener Normalteiler eine Transvektion enthalten muß. Im Falle $n = 2$ müssen die Transvektionen zwar keine Konjugationsklasse in $\mathrm{SL}(2, q)$ bilden, man kann aber auf direktem Wege nachrechen, daß die von einer Transvektion erzeugte normale Untergruppe bereits ganz $\mathrm{SL}(2, q)$ ist. (Details können im Buch von Robinson nachgelesen werden.)

Einen strukturelleren Beweis erhält man, indem man $\mathrm{SL}(n, K)$ auf dem projektiven Raum operieren läßt. Wichtig ist dann, daß $\mathrm{SL}(n, K)$ zweifach transitiv operiert und (für $n > 23$ oder $|K| > 3$) eine perfekte Gruppe ist.

- $\mathrm{PSL}(2, 2) \cong \mathrm{GL}(2, 2) \cong S_3$ (operiert auf den 3 eindimensionalen Unterräumen von $\mathbb{F}_2^2$).
  $\mathrm{PSL}(2, 3) \cong A_4$ (operiert auf den 4 Punkten der projektiven Geraden über $\mathbb{F}_3$).
  $\mathrm{PSL}(2, 4) \cong \mathrm{PSL}(2, 5) \cong A_5$ (bis auf Isomorphie einzige einfache Gruppe der Ordnung 60).
  $\mathrm{PSL}(4, 2) \cong A_8$
  $\mathrm{PSL}(2, 9) \cong A_6$
  Es gibt keine weiteren Isomorphien zwischen $\mathrm{PSL}(n, q)$ und symmetrischen oder alternierenden Gruppen.
- $\mathrm{PSL}(2, 7) \cong \mathrm{PSL}(3, 2)$ ist bis auf Isomorphie die einzige einfache Gruppe der Ordnung 168.
  Es gilt $|\mathrm{PSL}(4, 2)| = |\mathrm{PSL}(3, 4)$, aber $A_8 \cong \mathrm{PSL}(4, 2) \ncong \mathrm{PSL}(3, 4)$: hier liegen zwei nichtisomorphe einfache Gruppen gleicher Ordnung vor!.

Man erkennt eine gewisse Analogie zwischen S_n, A_n, sgn, 3-Zykel einerseits und $\mathrm{GL}(n, K)$, $\mathrm{SL}(n, K)$, det, Transvektionen andererseits. Mit Ausnahme kleiner Werte gilt zum einen $S_n' = A_n' = A_n$ und $A_n \cong A_n/Z(A_n)$ ist einfach, zum andern $\mathrm{GL}(n, K)' = \mathrm{SL}(n, K)' = \mathrm{SL}(n, K)$ und $\mathrm{SL}(n, q)/Z(\mathrm{SL}(n, q))$ ist einfach.

13 Anhang

Eine vollständige Liste der Gruppen der Ordnung $\leqslant 15$

Ein Strich $-$ bedeutet eine triviale Sylowgruppe, ein Eintrag 1 eine normale, nicht-triviale Sylowgruppe; p steht für den eventuellen Primteiler $\geqslant 5$ der Gruppenordnung.

$\lvert G\rvert$	Gruppe G	$\exp(G)$	Art	N_2	N_3	N_p	G'	$Z(G)$	$\mathrm{Aut}(G)$
1	$E = Z_1 = S_1$	1	trivial	–	–	–	E	E	E
2	$Z_2 = S_2 = D_1$	2	zykl. einfach	1	–	–	E	G	E
3	$Z_3 = A_3$	3	zykl. einfach	–	1	–	E	G	Z_2
4	Z_4	4	zyklisch	1	–	–	E	G	Z_2
	$Z_2 \times Z_2 = D_2$	2	abelsch	1	–	–	E	G	S_3
5	Z_5	5	zykl. einfach	–	–	1	E	G	Z_4
6	Z_6	6	zyklisch	1	1	–	E	G	Z_2
	$S_3 = D_3$	6	auflösbar	3	1	–	A_3	E	S_3
7	Z_7	7	zykl. einfach	–	–	1	E	G	Z_6
8	Z_8	8	zyklisch	1	–	–	E	G	$Z_2 \times Z_2$
	$Z_4 \times Z_2$	4	abelsch	1	–	–	E	G	$Z_2 \times Z_2$
	$Z_2 \times Z_2 \times Z_2$	2	abelsch	1	–	–	E	G	$\mathrm{GL}(3,2)$
	D_4	4	nilpotent	1	–	–	Z_2	Z_2	D_4
	Q_8	4	nilpotent	1	–	–	Z_2	Z_2	S_4
9	Z_9	9	zyklisch	–	1	–	E	G	Z_6
	$Z_3 \times Z_3$	3	abelsch	–	1	–	E	G	$\mathrm{GL}(2,3)$
10	Z_{10}	10	zyklisch	1	–	1	E	G	Z_4
	D_5	10	auflösbar	5	–	1	Z_5	E	$Z_4 \ltimes Z_5$
11	Z_{11}	11	zykl. einfach	–	–	1	E	G	Z_{10}
12	Z_{12}	12	zyklisch	1	1	–	E	G	$Z_2 \times Z_2$
	$Z_6 \times Z_2$	6	abelsch	1	1	–	E	G	S_3
	$Z_4 \ltimes Z_3$	12	auflösbar	3	1	–	Z_2	Z_3	S_3
	D_6	6	auflösbar	3	1	–	Z_3	Z_2	D_6
	A_4	6	auflösbar	1	4	–	$Z_2 \times Z_2$	E	S_4
13	Z_{13}	13	zykl. einfach	–	–	1	E	G	Z_{12}
14	Z_{14}	14	zyklisch	–	–	1	E	G	Z_7
	D_7	14	auflösbar	7	–	1	Z_7	E	$Z_6 \ltimes Z_7$
15	Z_{15}	15	zyklisch	–	–	1	E	G	$Z_2 \times Z_4$
24	S_4	12	auflösbar	3	4	–	A_4	E	S_4
60	A_5	30	einfach	5	10	6	A_5	E	A_5

60 ist die kleinste Gruppenordnung, für die es eine nicht-auflösbare Gruppe gibt, die dann die kleiste nicht-abelsche einfache Gruppe ist.
24 ist die kleinste Gruppenordnung, in der es keine normalen Sylowgruppen geben muß. Ein Beispiel hierfür ist die S_4. Alle Gruppen kleinerer Ordnungen sind also p-Gruppen oder semidirekte Produkte ihrer Sylowgruppen. Exemplarisch sei vorgeführt, wie man im Fall der Gruppenordnungen 8 und 12 sämtliche Gruppen bis auf Isomorphie bestimmt.

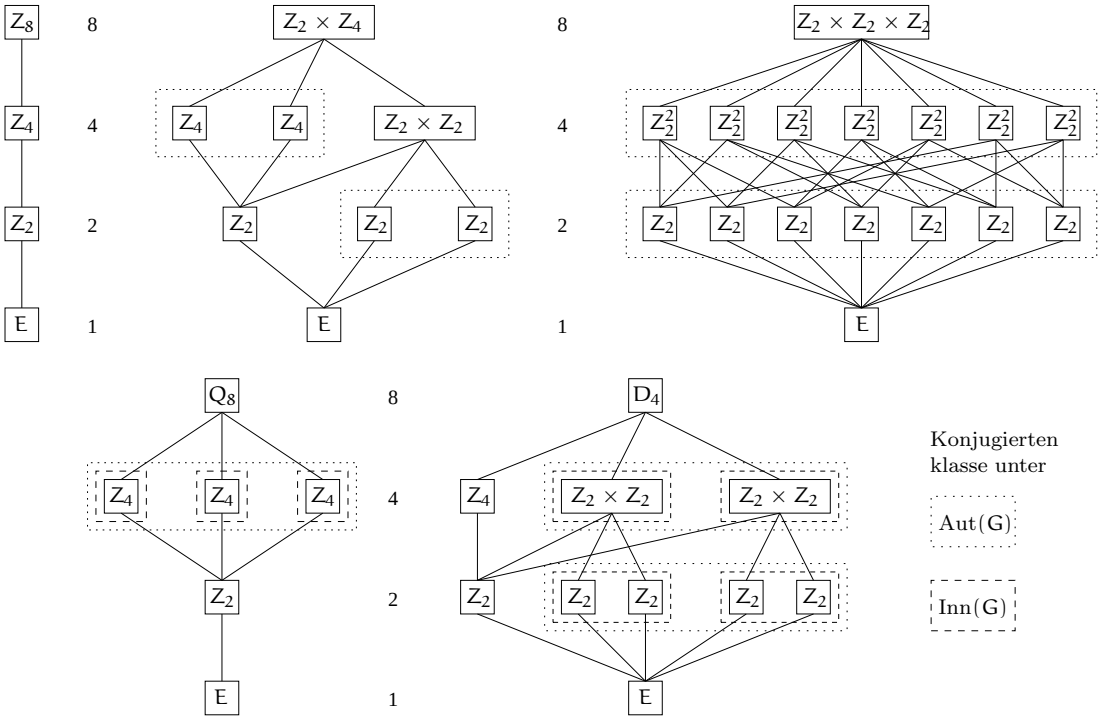
Die Gruppen der Ordnung 8 Sei G eine Gruppe der Ordnung 8.

1. Fall: G ist abelsch. Dafür gibt es die drei Möglichkeiten Z_8, $Z_4 \times Z_2$ und $Z_2 \times Z_2 \times Z_2$.

2. Fall: G ist nicht abelsch. Dann ist der Exponente von G gleich 4 (denn Gruppen vom Exponent 2 sind $\mathbb{F}_2$-Vektorräume). Insbesondere gibt es Elemente der Ordnung 4; alle davon erzeugten zyklischen Untergruppen sind normal (da Index 2). Da aus zyklischem $G/Z(G)$ folgt, daß G abelsch ist, gilt $Z(G) \cong Z_2$ und $G/Z(G) \cong Z_2 \times Z_2$.

Unterfall a): es gibt mehr als ein Element der Ordnung 2. Dann gibt es eine zyklische Untergruppe U der Ordnung 4 und ein Element $g \notin U$ der Ordnung 2. Es folgt, daß $G = U \rtimes \langle g \rangle \cong D_4$.

Unterfall b): es gibt nur ein Element der Ordnung 2, also drei zyklische Untergruppen der Ordnung 4, die sich gemeinsam in Z_2 schneiden. Es folgt $G \cong Q_8$.



Die Gruppen der Ordnung 12 Sei G eine Gruppe der Ordnung 12, $P \in \mathrm{Syl}_2(G)$ und $Q \in \mathrm{Syl}_3(G)$. Es gilt dann $P \cong Z_4$ oder $P \cong Z_2 \times Z_2$ und $Q \cong Z_3$. Ferner

$$N_2(G) \equiv 1 \ (\mathrm{mod} 2) \text{ und } N_2 \mid 3, \text{ also } N_2 = 1 \text{ oder } N_2 = 3$$
$$N_3(G) \equiv 1 \ (\mathrm{mod} 3) \text{ und } N_3 \mid 4, \text{ also } N_3 = 1 \text{ oder } N_3 = 4$$

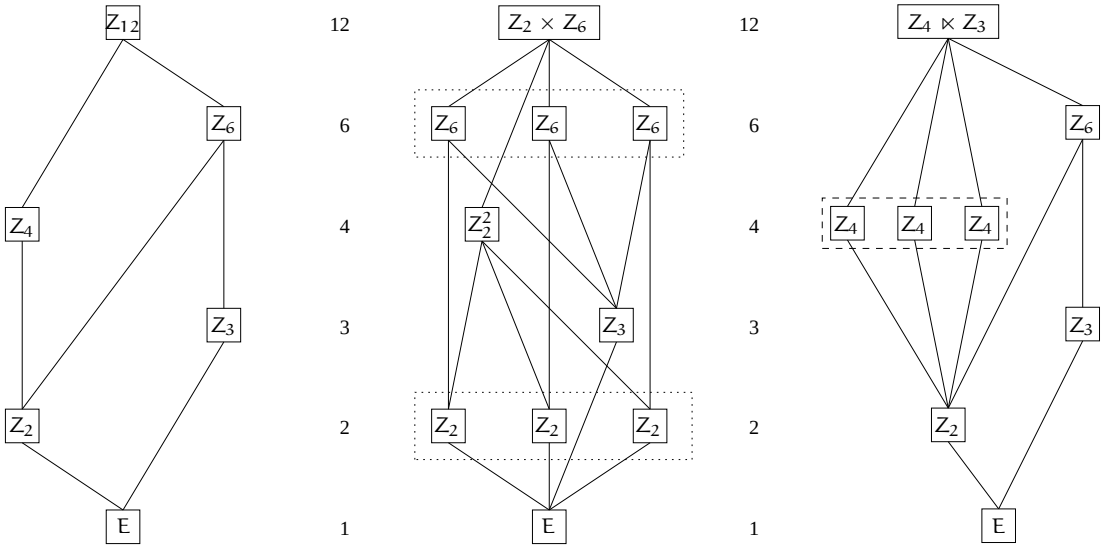
Angenommen $N_3 = 4$. Dann $\left|\left\{g \in G \;\middle|\; o(g) \mid 4\right\}\right| = 12 - N_3(G) \cdot (3-1) = 4$, also $N_2 = 1$. Folglich ist eine der Sylowgruppen normal, somit G ein semidirektes Prordukt aus P und Q.

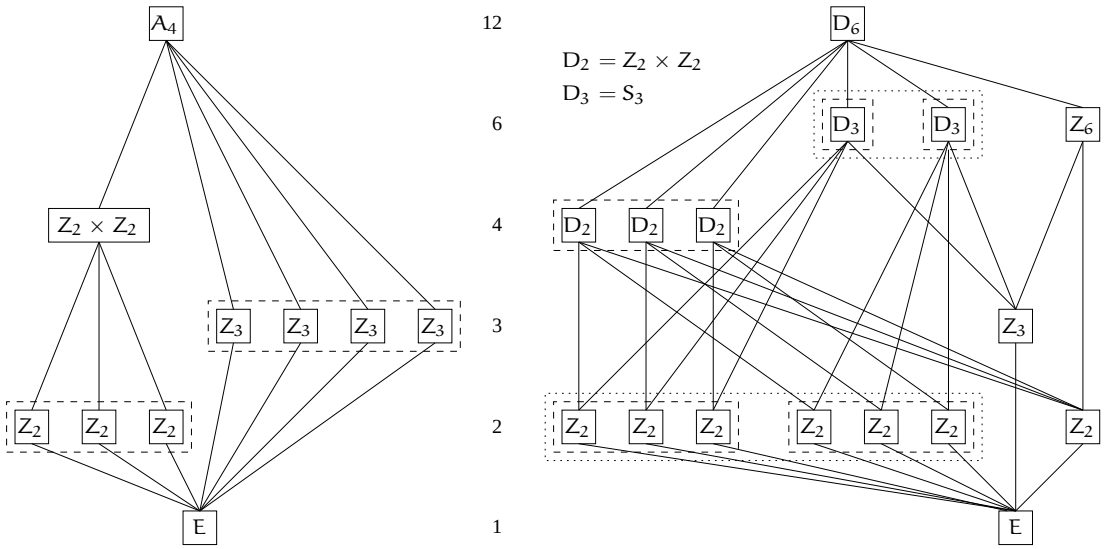
1. Fall: Beide Sylowgruppen sind normal und G ist kommutativ. Es folgt (a) $G \cong Z_4 \times Z_3 \cong Z_{12}$ oder (b) $G \cong (Z_2 \times Z_2) \times Z_3 \cong Z_2 \times Z_6$.

2. Fall: $P \trianglelefteq G$ und $N_3(G) = 4$. Falls $P = Z_4$, so gibt es keinen nicht-trivialen Homomorphismus $Q = Z_3 \to \mathrm{Aut}(P) = Z_2$. Falls $P = Z_2 \times Z_2$, so gibt es zwei nicht-triviale, zueinander konjugierte Homomorphismen $Q \to \mathrm{Aut}(P) = Z_3$. Es folgt (c) $G \cong (Z_2 \times Z_2) \rtimes Z_3 \cong A_4 \cong \mathrm{PSL}(2,3)$.

3. Fall: $N_2(G) = 3$, $N_3(G) = 1$, d.h. nur P ist normal in G. Falls $P = Z_4$, so gibt es einen nicht-trivialen Homomorphismus $P \to \mathrm{Aut}(Q) = Z_2$. Es folgt (d) $G \cong Z_4 \ltimes Z_3$.

Falls $P = Z_2 \times Z_2$, so gibt es drei nicht-triviale, zueinander konjugierte Homomorphismen $P \to \mathrm{Aut}(Q) = Z_2$. Es folgt (e) $G \cong (Z_2 \times Z_2) \ltimes Z_3 \cong Z_2 \ltimes Z_6 \cong Z_2 \times S_3 \cong D_6$.





Ein paar Strukturaussagen:

- Sei $|G| = p$ für eine Primzahl p:
  dann ist G zyklisch, abelsch einfach, $G \cong Z_p$.
- Sei $|G| = p^2$ für eine Primzahl p:
  dann ist G abelsch, $G \cong Z_{p^2}$ oder $G \cong Z_p \times Z_p$.
- Sei $|G| = pq$ für Primzahlen $p < q$:
  dann ist die q-Sylowgruppe Z_q normal in G, also $G \cong Z_p \ltimes Z_q$. Es gibt den trivialen Homomorphismus $Z_p \to \mathrm{Aut}(Z_q) \cong Z_{q-1}$ mit $G \cong Z_p \ltimes Z_q \cong Z_{pq}$. Ein nicht-trivialer Homomorphismus existiert genau dann, wenn $q \mid p-1$; er ist dann eindeutig bestimmt. Falls $p = 2$, ist dann $G \cong D_q$. Kleinstes anderes Beispiel ist $Z_3 \ltimes Z_7$ der Ordnung 21. Für viele Paare (p, q) gibt es also nur eine Gruppe der Ordnung pq.
- 24 ist die kleinste Gruppenordnung, in der es keine normalen Sylowgruppen geben muß. Ein Beispiel hierfür ist die S_4.

Symmetrische Gruppen:

$\|G\|$	Gruppe G	Art	G'	$Z(G)$	$\mathrm{Aut}(G)$
1	$S_1 = A_1 = A_2$	trivial	E	E	E
2	S_2	zykl. einfach	E	S_2	E
3	A_3	zykl. einfach	E	A_3	S_2
6	S_3	auflösbar	A_3	E	S_3
12	A_4	auflösbar	$Z_2 \times Z_2$	E	S_4
24	S_4	aufösbar	A_4	E	S_4
60	A_5	einfach	A_5	E	S_5
120	S_5	$A_5 \backslash Z_2$	A_5	E	S_5
360	A_6	einfach	A_6	E	$S_6 \backslash Z_2$
720	S_6	$A_6 \backslash Z_2$	A_6	E	$S_6 \backslash Z_2$
$\frac{n!}{2}$	A_n	einfach	A_n	E	S_n
$n!$	S_n	$A_n \backslash Z_2$	A_n	E	S_n

Der Untergruppenverband der S_4