Gruppentheorie
Vorlesungsnotizen

Stilianos Louca

April 2009

Inhaltsverzeichnis

1 Einführung

Anwendungsgebiete der Gruppentheorie und typische Gruppen:

Zahlbereiche

1. $(\mathbb{Z},+),\ (\mathbb{Q},+),\ (\mathbb{R},+),\ (\mathbb{C},+)$
2. $(\mathbb{Q}\setminus\{0\},\cdot),\ (\mathbb{R}\setminus\{0\},\cdot),\ (\mathbb{C}\setminus\{0\},\cdot)$
3. $\mathbb{Z}/n\mathbb{Z} := \{0+n\mathbb{Z},...,n-1+n\mathbb{Z}\}$: Restklassengruppe modulo n (mit "+").
4. $(\mathbb{Z}/n\mathbb{Z})^* := \{a+n\mathbb{Z} : \mathrm{ggT}(a,n)=1\}$: Prime Restklassengruppe modulo n (mit "$\cdot$").

Lineare Algebra

Sei $\mathbb{K}$ ein Körper und V ein $\mathbb{K}$-Vektorraum, $n\in\mathbb{N}$.

1. $\mathrm{GL}(n,\mathbb{K}) := \{A\in\mathbb{K}^{n\times n} : \det(A)\neq 0\}$ mit Matrixmultiplikation : Allgemeine lineare Gruppe des Grades n über $\mathbb{K}$.
2. $\mathrm{GL}(V) := \{f : V\to V \mid f \text{ linear, bijektiv}\}$ mit Verkettung $\circ$: Allgemeine lineare Gruppe von V.
3. $\mathrm{SL}(n,\mathbb{K}) := \{A\in\mathbb{K}^{n\times n} : \det(A)=1\}$: Spezielle lineare Gruppe des Grades n über $\mathbb{K}$.

Sei nun V ein euklidischer $\mathbb{K}$-Vektorraum mit Skalarprodukt $\langle\cdot,\cdot\rangle$.

1. $O(V) := \{f : V\to V \mid f \text{ Isometrie}\}$ mit Verkettung $\circ$: Orthogonale Gruppe von V.
   Bemerke: $f : V\to V$ ist eine *Isometrie* $:\Leftrightarrow f$ ist linear und $\langle fx,fy\rangle = \langle x,y\rangle$ für $x,y\in V$.
2. $O(n) := O(n,\mathbb{R}) := \left\{A\in\mathbb{R}^{n\times n} : A^TA = 1_n\right\}$: Orthogonale Gruppe des Grades n.

Nun sei V unitär mit Skalarprodukt $\langle\cdot,\cdot\rangle$.

1. $U(V) := \{f : V\to V \mid f \text{ Isometrie}\}$: Unitäre Gruppe von V.
2. $U(n) := U(n,\mathbb{C}) := \left\{A\in\mathbb{C}^{n\times n} : \overline{A^T}A = 1_n\right\}$: Unitäre Gruppe des Grades n.

Kombinatorik

Sei $\Omega\neq\emptyset$ eine Menge.

1. $\mathrm{Sym}(\Omega) := \{f : \Omega\to\Omega \mid f \text{ bijektiv}\}$ mit Verkettung $\circ$: Symmetrische Gruppe auf Ω.
2. $\mathrm{Alt}(\Omega) := \{f\in\mathrm{Sym}(\Omega) : f \text{ gerade}\}$: Alternierende Gruppe auf Ω (Ω endlich).

Geometrie

1. $\mathrm{AO}(\mathbb{R}^n) := \{f : \mathbb{R}^n\to\mathbb{R}^n \mid \|fx-fy\| = \|x-y\|\ \forall\ x,y\in\mathbb{R}^n\}$: Bewegungsgruppe.
2. Gegeben beliebige Menge im $\mathbb{R}^n$, z.B. regelmäßiges n-Eck $P_n\subset\mathbb{R}^n$. Dann bezeichnet
$$D := \left\{f\in\mathrm{AO}(\mathbb{R}^2) : f(P_n)=P_n\right\}$$
die so genante *Symmetriegruppe* von P_n.
Bemerke: Im Falle eines regelmäßigen n-Ecks heißt $D =: D_n$ n-te *Diedergruppe*. Es ist dann $|D_n| = 2n$.
3. Friesgruppen : Symmetriegruppen unendlich ausgedehnter Objekte im $\mathbb{R}^2$.

Algebra

Es sei $\mathbb{L} \mid \mathbb{K}$ eine Körpererweiterung von $\mathbb{K}$.

1. $\mathrm{Gal}(\mathbb{L} \mid \mathbb{K}) := \left\{ f : \mathbb{L} \to \mathbb{L} \mid f \text{ Automorphismus in } \wedge \ f\big|_{\mathbb{K}} = \mathrm{Id}_{\mathbb{K}} \right\}$: Galoisgruppe.

Topologie

Fundamentalgruppen, Homologiegruppen.

Zahlentheorie

Es sei $\mathbb{K}$ ein algebraischer Zahlenkörper und $O_{\mathbb{K}}$ der Ganzheitsring von $\mathbb{K}$.

1. $O_{\mathbb{K}}^{\times} := \left\{ a \in O_{\mathbb{K}} \setminus \{0\} : \frac{1}{a} \in O_{\mathbb{K}} \right\}$: Einheitsgruppe.
2. Die Klassengruppe {gebrochene Ideale} / {gebrochene Hauptideale}

2 Halbgruppen

2.1 Einführung

2.1.1 Definition: Monade

Es sei M eine beliebige Menge, und $\circ : M \times M \to M$ eine beliebige Abbildung:

$$(a, b) \mapsto a \circ b$$

Dann heißt das Paar $(M, \circ)$ *Monade*.
Man schreibt auch: $a * b,\ a \cdot b,\ a + b,\ ab$.

Beispiele:

- $+, -, \cdot$ auf $\mathbb{R}, \mathbb{N}, \mathbb{C}$
- $\cap, \cup$ auf der Potenzmenge $\mathscr{P}(X)$ irgendeiner Menge X.
- ggT, kgV auf $\mathbb{N}$.
- $\circ$ auf $\mathrm{Abb}(X) := \{f : X \to X \mid f \text{ Abbildung}\}$

2.1.2 Definition: Neutrales Element

Es sei $(M, \circ)$ eine Monade. Dann heißt $e \in M$:

Linksneutral: $:\Leftrightarrow\ \forall\, a \in M : e \circ a = a$

Rechtsneutral: $:\Leftrightarrow\ \forall\, a \in M : a \circ e = a$

Neutral: $:\Leftrightarrow$ e ist links- und rechtsneutral.

Bemerkungen:

- Ist e links- und f rechtsneutral, dann ist $e = f$. Somit kann insbesondere maximal ein neutrales Element in M existieren.
- Das neutrale Element wird oft mit 1 bezeichnet, bzw. mit 0 falls "+" die Verknüpfung ist.

Beispiel: 0 ist neutral in $(\mathbb{Z}, +)$ und 1 neutral in $(\mathbb{Z}, \cdot)$.

2.1.3 Definition: Kommutativität, Monoid

Es sei $(M, \circ)$ eine Monade. Dann heißen $a, b \in M$ *vertauschbar* $:\Leftrightarrow\ ab = ba$.
$(M, \circ)$ heißt *kommutativ* (*abelsch*) $:\Leftrightarrow\ \forall x, y : x \circ y = y \circ x$ (Kommutativgesetz).
$(M, \circ)$ heißt *Halbgruppe* $:\Leftrightarrow\ \forall\, x, y \in M : (x \circ y) \circ z = x \circ (y \circ z)$.
$(M, \circ)$ heißt *Monoid* $:\Leftrightarrow$ $(M, \circ)$ ist Halbgruppe mit neutralem Element.

Beispiele:

- $(\mathbb{N}, +)$ ist Halbgruppe, $(\mathbb{N}_0, +)$ ist Monoid.
- Für beliebige Menge $X \neq \emptyset$, ist $\mathrm{Abb}(X)$ ein Monoid, mit neutralem Element die Identität Id_X.
- Für beliebige Menge $A \neq \emptyset$ (*Alphabet*) bezeichne *Buchstabe* ein Element aus A. Ein *Wort* über A ist eine beliebige endliche Folge
$$w = (a_1, .., a_n) := a_1 \dots a_n\ ,\ n \in \mathbb{N},\ a_i \in A$$
Die Menge
$$\mathcal{W} := \{w : w \text{ Wort über } A\}$$

heißt *freie Halbgruppe* über A, mit der Verknüpfung

$$(a_1, ..., a_n) \circ (b_1, .., b_m) := (a_1, .., a_n, b_1, .., b_m)$$

Bemerke: $(\mathcal{W}, \circ)$ besitzt kein neutrales Element. Führt man das leere Wort $\varepsilon \notin \mathcal{W}$ ein, so heißt

$$\mathcal{W}_0 := \mathcal{W} \cup \{\varepsilon\}$$

freies Monoid über A mit neutralem Element ε.

2.1.4 Definition: Invertierbarkeit

Es sei $(M, \circ)$ ein Monoid. Ein Element $a \in M$ heißt:

Rechtsinvertierbar: $:\Leftrightarrow\ \exists\, b \in M : a \circ b = 1$

Linksinvertierbar: $:\Leftrightarrow\ \exists\, b \in M : b \circ a = 1$

Man sagt b ist *rechts-* bzw. *linksinvers* zu a. Ist b links- und c rechtsinvers zu a, so muss $b = c$ sein. In dem Falle schreibt man $b = a^{-1}$, nennt a^{-1} *invers* zu a und a *invertierbar*.

Bemerkungen:

- Ist a invertierbar, so ist auch a^{-1} invertierbar, und $(a^{-1})^{-1} = a$.
- Sind x, y invertierbar, so ist auch xy invertierbar, mit $(xy)^{-1} = y^{-1}x^{-1}$.

Beispiel: Für beliebigen Körper $\mathbb{K}$ und $n \in \mathbb{N}$, ist $\mathbb{K}^{n\times n}$ ein Monoid bzgl. Matrixmultiplikation, mit neutralem Element die Einheitsmatrix 1_n. $A \in \mathbb{K}^{n\times n}$ ist invertierbar im obigen Sinne, genau dann wenn $\det(A) \neq 0$. Bemerke dass die Linksinvertierbarkeit einer Matrix äquivalent zu deren Rechtsinvertierbarkeit ist (Besonderheit!).

2.1.5 Definition: Potenzen

Es sei $(H, \circ)$ ein Halbgruppe und $h \in H,\ n \in \mathbb{N}$. Dann nennt man

$$h^n := \underbrace{h \circ \cdots \circ h}_{n \text{ mal}}$$

die n-te Potenz von a. Ist H ein Monoid, so definiert man $a^0 := 1$. Ist ferner a invertierbar, so schreibt man

$$a^{-n} := (a^{-1})^n = (a^n)^{-1}$$

Rechenregeln:

- $a^m \circ a^n = a^{m+n}$
- $(a^m)^n = a^{m\cdot n}$
- Falls $ab = ba$, dann ist $(ab)^n = a^n b^n$

Bemerke: Ist "+" die Verknüpfung, so schreibt man auch $n \cdot a := a^n$. Die Rechenregeln lauten dann

- $(m + n)a = ma + na$
- $(mn)a = m(na)$
- $n(a + b) = na + nb$ falls $a + b = b + a$

2.2 Homomorphismen

2.2.1 Definition: Homomorphismus

Es seien M, N Monaden und $f : M \to N$ eine Abbildung. Dann heißt f:

Homomorphismus: $:\Leftrightarrow \ \forall\, a, b \in M : f(ab) = f(a)f(b)$

Monomorphismus: $:\Leftrightarrow f$ ist ein injektiver Homomorphismus.

Epimorphismus: $:\Leftrightarrow f$ ist ein surjektiver Homomorphismus.

Isomorphismus: $:\Leftrightarrow f$ ist ein bijektiver Homomorphismus.

Endomorphismus: $:\Leftrightarrow f$ ist ein Homomorphismus und $(M, \circ) = (N, \circ)$.

Automorphismus: $:\Leftrightarrow f$ ist ein bijektiver Endomorphismus.

Man schreibt

$$\mathrm{Hom}(M, N) := \{f : M \to N \mid f \text{ homomorph}\}$$

$$\mathrm{End}(M) := \mathrm{Hom}(M, M)$$

$$\mathrm{Aut}(M) := \{f \in \mathrm{End}(M) : f \text{ bijektiv}\}$$

Beispiele:

- Für Körper $\mathbb{K}$ und $n \in \mathbb{N}$ ist $\det : (\mathbb{K}^{n\times n}, \cdot) \to (\mathbb{K}, \cdot)$ ein Homomorphismus.
- Die Exponentialfunktion $\exp : (\mathbb{R}, +) \to (\mathbb{R}, \cdot)$ ist ein Homomorphismus.
- Es sei $(\mathcal{W}, \circ)$ die freie Halbgruppe über das Alphabet A und

  $$l(a_1...a_n) := n$$

  die *Länge* jedes Wortes $(a_1..a_n) \in \mathcal{W}$. Dann ist $l : (\mathcal{W}, \circ) \to (\mathbb{N}, +)$ Homomorph.

2.2.2 Lemma über Homomorphismen

- Sind L, M, N Monaden und $f \in \mathrm{Hom}(L, M),\ g \in \mathrm{Hom}(M, N)$, dann ist auch $g \circ f \in \mathrm{Hom}(L, N)$.
- Ist $f : M \to N$ ein Isomorphismus, so ist auch $f^{-1} : N \to M$ ein Isomorphismus.

2.2.3 Definition: Isomorphe Monaden

Zwei Monaden $(M, \circ),\ (N, \circ)$ heißen *isomorph* $(M \cong N)$, falls ein Isomorphismus $f : M \to N$ existiert.

Beispiel: $(\{w, f\}, \vee) \cong (\{0, 1\}, \cdot)$ mit $w \mapsto 0,\ f \mapsto 1$.

2.2.4 Satz über Isomorphie

Die Isomorphie ist eine Äquivalenzrelation über alle Monaden, das heißt:

- $M \cong M$ (Reflexivität)
- $M \cong N \ \Rightarrow \ N \cong M$ (Symmetrie)
- $L \cong M \ \wedge \ M \cong N \ \Rightarrow \ L \cong N$ (Transitivität)

3 Gruppen

3.1 Einführung

3.1.1 Definition: Gruppe

Eine *Gruppe* ist eine Halbgruppe $(G, \circ)$ mit einem linksneutralen Element, in der jedes Element linksinvertierbar ist.

3.1.2 Lemma über Gruppen

Eine Gruppe $(G, \circ)$ ist ein Monoid in dem jedes Element invertierbar ist.

Beispiele:

- $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ sind (abelsche) Gruppen, $(\mathbb{N}, +)$, $(\mathbb{N}_0, +)$ nicht.
- $(\mathbb{Q} \setminus \{0\}, \cdot)$, $(\mathbb{R} \setminus \{0\}, \cdot)$, $(\mathbb{C} \setminus \{0\}, \cdot)$ sind (abelsche) Gruppen, $(\mathbb{Z} \setminus \{0\}, \cdot)$ nicht.
- Für Monoid $(M, \circ)$, ist die *Einheitsgruppe von M* (*unit-group*)

  $$\mathcal{U}(M) := \{a \in M : a \text{ invertierbar}\}$$

  eine Gruppe.
- Für beliebige Menge X ist die *symmetrische Gruppe auf X*

  $$\mathrm{Sym}(X) := \mathcal{U}(\mathrm{Abb}(X)) := \{f : X \to X \mid f \text{ bijektiv}\}$$

  aller *Permutationen* eine Gruppe. Für $X = \{1, .., n\}$ schreibt man auch $\mathrm{Sym}(X) =: \mathrm{Sym}(n)$ und nennt die Elemente in $\mathrm{Sym}(n)$ *Permutationen* des Grades n. Man schreibt:

  $$f = \begin{pmatrix} 1 & 2 & .. & n \\ f(1) & f(2) & \dots & f(n) \end{pmatrix}$$

  Somit ist

  $$f^{-1} = \begin{pmatrix} f(1) & f(2) & \dots & f(n) \\ 1 & 2 & \dots & n \end{pmatrix}$$
- Für Körper $\mathbb{K}$ und $n \in \mathbb{N}$ ist

  $$\mathcal{U}(\mathbb{K}^{n\times n}, \cdot) = \left\{A \in \mathbb{K}^{n\times n} : \det(A) \neq 0\right\} = \mathrm{GL}(n, \mathbb{K})$$
- Für jede nicht-leere Familie $(G_i)_{i\in I}$ von Gruppen G_i ist auch das *direkte Produkt*

  $$\bigtimes_{i\in I} G_i := \left\{(g_i)_{i\in I} : g_i \in G_i,\ i \in I\right\}$$

  mit der Verknüpfung

  $$(g_i)_{i\in I} \circ (h_i)_{i\in I} := (g_i \circ h_i)_{i\in I}$$

  eine Gruppe. Im Fall $I = \{1, .., n\}$ schreibt man

  $$\bigtimes_{i=1}^{n} G_i =: G_1 \times \cdots \times G_n$$

  mit

  $$(g_1, .., g_n) = (g_i)_{i\in I}$$

3.1.3 Definition: Ordnung einer Gruppe

Die *Ordnung* $|G|$ einer Gruppe $(G, \circ)$ ist die Anzahl ihrer Elemente.

3.1.4 Lemma: Ordnung von $\mathrm{Sym}(n)$ und $\mathrm{GL}(n,\mathbb{K})$

1. Für $n \in \mathbb{N}$ ist $|\mathrm{Sym}(n)| = n!$
2. Für Körper $\mathbb{K}$ mit $|\mathbb{K}| =: q$ und $n \in \mathbb{N}$ ist $|\mathrm{GL}(n,\mathbb{K})| = (q^n-1)(q^n-q)\dots(q^n-q^{n-1})$

3.1.5 Satz über Gruppenhomomorphismen

Es sei $f : G \to H$ ein Homomorphismus zwischen den Gruppen $(G,\circ)$ und $(H,\circ)$. Dann gilt:

$$f(1_G) = 1_H \quad \wedge \quad f\left(g^{-1}\right) = f(g)^{-1} \ \forall \ \in G$$

Beispiel: Für Körper $\mathbb{K}$ und $n \in \mathbb{N}$ ist $\det : \mathrm{GL}(n,\mathbb{K}) \to (\mathbb{K}\setminus\{0\},\cdot)$ ein Homomorphismus. Demnach ist $\det(1_n) = 1$ und

$$\det(A^{-1}) = \det(A)^{-1}\ ,\ A \in \mathrm{GL}(n,\mathbb{K})$$

3.2 Untergruppen

3.2.1 Definition: Untergruppe

Eine Teilmenge $U \subseteq G$ einer Gruppe $(G,\circ)$ heißt *Untergruppe* von G, falls gilt:

1. $1_G \in U$
2. Für $a,b \in U$ ist $a \circ b,\ a^{-1} \in U$

Bemerkung: U ist mit der entsprechend eingeschränkten Verknüpfung selbst eine Gruppe. Wir schreiben $U \leq G$ (bzw. $U < G$ im Fall $U \neq G$). Ist $U < G$, so heißt U eine *echte Untergruppe* von G.

Beispiele:

- $(\mathbb{Z},+) < (\mathbb{Q},+) < (\mathbb{R},+) < (\mathbb{C},+)$
- $(\mathbb{Q}\setminus\{0\},\cdot) < (\mathbb{R}\setminus\{0\},\cdot) < (\mathbb{C}\setminus\{0\},\cdot)$
- In jeder beliebigen Gruppe G sind G selbst und die *triviale Untergruppe* $\{1_G\} =: 1$ Untergruppen.
- Für jede nicht-leere Familie $(G_i)_{i\in I}$ von Gruppen bildet

  $$\left\{(g_i)_{i\in I} \in \bigtimes_{i\in I} G_i \middle| \ |\{i \in I : g_i \neq 1\}| < \infty\right\}$$

  eine Untergruppe von $\bigtimes_{i\in I} G_i$. Diese heißt *eingeschränktes direktes Produkt* von $(G_i)_{i\in I}$. Man schreibt $\coprod_{i\in I} G_i$. Für $|I| < \infty$ ist

  $$\coprod_{i\in I} G_i = \bigtimes_{i\in I} G_i$$

- Für jede Monade M ist die *Automorphismengruppe* $\mathrm{Aut}(M)$ mit Verkettung $\circ$ eine Untergruppe von $(\mathrm{Sym}(M),\circ)$.

3.2.2 Satz: Charakterisierung von Untergruppen

Eine nicht-leere Teilmenge $U \subseteq G$ einer Gruppe $(G,\circ)$ ist genau dann eine Untergruppe von G, wenn gilt:

$$a \circ b^{-1} \in U \ \ \forall\, a,b \in U$$

3.2.3 Definition: Produkte von Teilmengen

Für Teilmengen $X, Y \subseteq G$ einer Gruppe $(G, \circ)$ setzt man

$$XY := \{xy : x \in X,\ y \in Y\}$$

und

$$X^{-1} := \left\{x^{-1} : x \in X\right\}$$

Bemerkungen: Für $X, Y, Z \subseteq G$ gilt:

- $(X^{-1})^{-1} = X$
- $(XY)^{-1} = Y^{-1}X^{-1}$
- $(XY)Z = X(YZ)$
- Satz 3.2.2 besagt: $X \leq G \ \Leftrightarrow\ X \neq \emptyset \ \wedge\ XX^{-1} \subseteq X$

3.2.4 Satz: Eigenschaften von Untergruppen

Es sei $(G, \circ)$ eine Gruppe. Dann gilt stets:

1. $U \cup V \leq G \ \Leftrightarrow\ U \subseteq V \ \vee\ V \subseteq U$ für Untergruppen $U, V \leq G$.
2. $UV \leq G \ \Leftrightarrow\ UV = VU$ für Untergruppen $U, V \leq G$.
3. $U \subseteq W \ \Rightarrow\ UV \cap W = U(V \cap W)$ (Dedekind-Identität) für Untergruppen $U, V, W \leq G$.
4. Für jede nicht-leere Menge $\{U_i\}_i$ von Untergruppen $U_i \leq G$ ist auch $\bigcap_i U_i$ eine Untergruppe.

3.2.5 Satz über Gruppenhomomorphismen und Untergruppen

Seien G, H Gruppen und $f \in \mathrm{Hom}(G, H)$. Dann gilt:

1. Ist $U \leq G$, so ist $f(U) \leq H$. Insbesondere ist $\mathrm{image}(f) := f(G) \leq H$.
2. Ist $V \leq H$, so ist $f^{-1}(H) \leq G$. Insbesondere ist $\ker(f) := f^{-1}(\{1_H\}) \leq G$.
3. Ist $U \leq G$, so ist $f^{-1}\left(f(U)\right) = U \ker(f) = \ker(f)U$.
4. Ist $V \leq H$, so ist $f\left(f^{-1}(V)\right) = V \cap f(G)$.
5. Der Zusammenhang zwischen $\mathscr{U} := \{U \leq G : \ker(f) \subseteq U\}$ und $\mathscr{V} := \{V \leq H : V \subset f(G)\}$, gegeben durch

$$U \mapsto f(U)\ ,\ V \mapsto f^{-1}(V)\ \ ,\ U \in \mathscr{U},\ V \in \mathscr{V}$$

   ist bijektiv.

Notationen:

- $f(U)$ heißt *Bild* von U unter f.
- $f^{-1}(V)$ heißt *Urbild* von V unter f.
- $\mathrm{image}(f) := f(G)$ heißt *Bild* von f.
- $\ker(f) := f^{-1}(\{1_H\})$ heißt *Kern* von f.

Beispiel: Für Körper $\mathbb{K}$ und $n \in \mathbb{N}$ ist

$$\mathrm{SL}(n,\mathbb{K}) = \{A \in \mathrm{GL}(n,\mathbb{K}) : \det(A) = 1\} = \ker\left(\det : \mathrm{GL}(n,\mathbb{K}) \to \mathbb{K} \setminus \{0\}\right)$$

3.2.6 Satz: Charakterisierung injektiver Homomorphismen

Für jeden Gruppenhomomorphismus $f : G \to H$ gilt:

$$f \text{ injektiv} \quad \Leftrightarrow \quad \ker(f) = \{1_G\}$$

3.2.7 Definition: Innerer Automorphismus, Zentrum

Für jedes $a \in G$ einer Gruppe G ist

$$\mathrm{ad}_a : G \to G \quad , \quad x \mapsto axa^{-1}$$

ein Automorphismus auf G, und heißt der *von a induzierte, innere Automorphismus von G*. Die Abbildung

$$\mathrm{ad} : G \to \mathrm{Aut}(G) \quad , \quad a \mapsto \mathrm{ad}_a$$

ist Homomorph, das heißt insbesondere

$$\mathrm{ad}_{ab} = \mathrm{ad}_a \circ \mathrm{ad}_b \quad , \quad \mathrm{ad}_{a^{-1}} = \mathrm{ad}_a^{-1}$$

Nach Satz 3.2.5 ist

$$\mathrm{Inn}(G) := \mathrm{image}(\mathrm{ad}) := \mathrm{ad}(G) \leq \mathrm{Aut}(G)$$

Man nennt $\mathrm{Inn}(G)$ die *innere Automorphismengruppe* von G. Man nennt

$$\underbrace{Z(G)}_{\leq G} := \ker(\mathrm{ad}) = \left\{a \in G : axa^{-1} = x \ \ \forall\, x \in G\right\}$$

$$= \{a \in G : ax = xa \ \ \forall\, x \in G\}$$

das *Zentrum* von G.

3.2.8 Lemma: Innere Automorphismen und Produktgruppen

Sei G eine Gruppe und $H, K \leq G$ mit $G = HK$. Dann gilt

$$G = \mathrm{ad}_x(H)\,\mathrm{ad}_y(K) \ \ \forall\, x, y \in G$$

3.2.9 Lemma über triviale Zentren

Sei G eine Gruppe mit $Z(G) = 1$. Dann ist auch $Z(\mathrm{Aut}(G)) = 1$.

3.2.10 Definition: Erzeuger einer Gruppe

Für beliebige Untermenge $X \subseteq G$ einer Gruppe $(G, \circ)$ heißt der Durchschnitt

$$\langle X \rangle := \bigcap_{\substack{U_i \leq G \\ X \subseteq U_i}} U_i$$

die *von X erzeugte Untergruppe* in G. Sie ist die *kleinste* Untergruppe von G die X enthält. Für $X = \{a_1, .., a_n\}$ schreibt man

$$\langle X \rangle =: \langle a_1, .., a_n \rangle$$

Ist $X \subseteq G$ so dass $\langle X \rangle = G$, so heißt X ein *Erzeugendensystem* von G. Hat G ein endliches Erzeugendensystem, so heißt G *endlich erzeugt*.

Bemerkungen:

- Jede Gruppe besitzt ein Erzeugendensystem, nämlich G selbst.
- Jede endliche Gruppe ist endlich erzeugt.

3.2.11 Satz: Charakterisierung von erzeugten Gruppen

Für Teilmenge $X \subseteq G$ einer Gruppe $(G, \circ)$ besteht $\langle X \rangle$ aus den Elementen der Form

$$x_1^{\varepsilon_1} \circ \cdots \circ x_n^{\varepsilon_n} \quad , \quad n \in \mathbb{N}_0,\ x_i \in X,\ \varepsilon_i \in \{\pm 1\}$$

wobei man im Fall $n = 0$ das Produkt als 1_G interpretiert.

Bemerkungen:

(i) Vergleiche $\langle X \rangle$ mit dem span(X) einer Untermenge $X \subseteq V$ eines Vektorraumes V.

(ii) Für $X \subseteq G$ und Gruppenhomomorphismus $\alpha : G \to H$ ist

$$\langle \alpha(X) \rangle = \alpha\left(\langle X \rangle\right)$$

denn

$$\langle \alpha(X) \rangle = \{\alpha(x_1)^{\varepsilon_1} \circ \cdots \circ \alpha(x_n)^{\varepsilon_n} : n \in \mathbb{N}_0,\ \varepsilon_i \in \{\pm 1\},\ x_i \in X\}$$

$$= \{\alpha\left(x_1^{\varepsilon_1} \circ \cdots \circ x_n^{\varepsilon_n}\right) : n \in \mathbb{N}_0,\ \varepsilon_i \in \{\pm 1\},\ x_i \in X\} = \alpha\left(\langle X \rangle\right)$$

3.2.12 Definition: Zyklische Gruppe

Sei G eine Gruppe und $x \in G$. Dann heißt

$$\langle x \rangle := \langle \{x\} \rangle = \{x^n : n \in \mathbb{Z}\}$$

die von x *erzeugte zyklische Gruppe*. Ist $G = \langle a \rangle$ für irgendein $a \in G$, so heißt G *zyklisch*.

Bemerkung: Zyklische Gruppen sind immer abelsch.

3.3 Nebenklassen

3.3.1 Definition: Linkskongruenz, Rechtskongruenz

Sei G eine Gruppe, $H \leq G$ und $a, b \in G$.

- Ist $a^{-1}b \in H$, so heißt a *linkskongruent zu* b *modulo* H. Man schreibt

$$a \equiv_l b \ (\mathrm{mod} H)$$

- Ist $ab^{-1} \in H$, so heißt a *rechtskongruent zu* b *modulo* H. Man schreibt

$$a \equiv_r b \ (\mathrm{mod} H)$$

3.3.2 Lemma über Links- und Rechtskongruenz

Links- und Rechtskongruenz $\equiv_l \pmod H$, $\equiv_r \pmod H$ sind Äquivalenzrelationen auf G, das heißt

Reflexivität: $a \equiv_l a \pmod H \ \ \forall\, a \in G$

Symmetrie: $a \equiv_l b \pmod H \ \Leftrightarrow\ b \equiv_l a \pmod H \quad \forall\, a, b \in G$

Transitivität: $a \equiv_l b \pmod H \ \wedge\ b \equiv_l c \pmod H \quad \Rightarrow \quad a \equiv_l c \pmod H \quad \forall\, a, b, c \in G$

Analog auch für $\equiv_r \pmod H$.

3.3.3 Lemma: Charakterisierung von Links- und Rechtskongruenz

Sei G eine Gruppe und $H \leq G$. Dann gilt für $a, b \in G$:

$$a \equiv_l b \pmod H \quad \Leftrightarrow \quad b \in aH$$

und

$$a \equiv_r b \pmod H \quad \Leftrightarrow \quad b \in Ha$$

3.3.4 Definition: Links- und Rechtsnebenklasse

Sei G eine Gruppe und $H \leq G$. Die Äquivalenzklasse von $a \in G$ bzgl. $\equiv_l \pmod H$ heißt *Linksnebenklasse von a modulo (nach) H*, und ist nach Lemma 3.3.3 gegeben durch

$$[a]_l = aH$$

Die Äquivalenzklasse von a bzgl. $\equiv_r \pmod H$ heißt *Rechtsnebenklasse von a modulo (nach) H*, und ist analog gegeben durch

$$[a]_r = Ha$$

Wir setzen

$$G/H := \{aH : a \in G\} \quad , \quad H \setminus G := \{Ha : a \in G\}$$

Bemerkung: Die Zuordnungen

$$H \to aH \ , \ h \mapsto ah$$

und

$$H \to Ha \ , \ h \mapsto ha$$

sind beide bijektiv, so dass insbesondere gilt

$$|aH| = |Ha| = |H|$$

3.3.5 Definition: Index einer Untergruppe

Sei G eine Gruppe und $H \leq G$. Für $Ha \in H \setminus G$ ist $(Ha)^{-1} = a^{-1}H^{-1} = a^{-1}H \in G/H$. Analog ist $(aH)^{-1} \in H \setminus G$ für $aH \in G/H$. So erhält man eine Bijektion $G/H \to H \setminus G$. Mann nennt

$$|G : H| := |G/H| = |H \setminus G|$$

den *Index* von H in G.

Beispiel: Seien $S, N \leq G$ Untergruppen der Gruppe G. Dann gilt nach 3.2.4 die Äquivalenz

$$\langle S, N \rangle = SN \quad \Leftrightarrow \quad SN = NS \ .$$

Ist dies der Fall und noch dazu $S \cap N = \{1\}$, dann ist $\langle S, N \rangle = \biguplus_{s \in S} sN$ und N besitzt in $\langle S, N \rangle$ den Index $|S|$.

3.3.6 Satz von Lagrange

Für jede Untergruppe $H \leq G$ einer Gruppe G gilt:

$$|G| = |G : H| \cdot |H|$$

Insbesondere sind $|H|\,,\ |G : H|$ im Fall $|G| < \infty$ Teiler von $|G|$.

Beweis: G ist die disjunkte Vereinigung der Linksnebenklassen modulo H. Es gibt $|G : H|$ Nebenklassen, jede enthält $|H|$ Elemente. Bemerke dass die Kardinalitäten im Falle unendlicher Gruppen entsprechend zu deuten sind.

Beispiel: Gruppen der Ordnung 24 können keine Untergruppe der Ordnung 7 enthalten.

3.3.7 Korollar über Gruppen mit Primzahlordnungen

Gruppen von Primzahlordnung sind immer zyklisch.

3.3.8 Definition: Ordnung eines Elementes

Für jedes Element $a \in G$ einer Gruppe G heißt $|\langle a\rangle|$ *Ordnung* von a.

Bemerkung: Bekanntlich ist

$$\langle a\rangle = \{a^n : n \in \mathbb{Z}\}$$

Man unterscheidet zwischen zwei Fällen. Im ersten, trivialen Fall sind alle $a^n,\ n \in \mathbb{Z}$ paarweise verschieden. Dann ist $|\langle a\rangle| = |\mathbb{Z}|$.

Im zweiten Fall ist $a^n = a^m$ für irgendwelche $m < n \in \mathbb{Z}$, also insbesondere $a^{n-m} = 1$ mit $(n - m) \in \mathbb{N}$. Sei nun $k \in \mathbb{N}$ das kleinste k, so dass $a^k = 1$. Dann sind

$$1, a^1, a^2, ..., a^{k-1}$$

paarweise verschieden, denn wäre $a^i = a^j$ mit $0 \leq i \leq j \leq k - 1$ so wäre $a^{j-i} = 1$ also $j - i = 0$ nach Wahl von k. Im Falle $i \geq k$ ist $a^{i-k} = a^i$, also

$$a^i \in A := \left\{1, a^1, .., a^{k-1}\right\} \quad \forall\ i \in \mathbb{N}_0$$

Analog ist $(a^i)^{-1} = a^{-i} = a^{-i+k}$, das heißt $a^i \in A\ \ \forall\ i \in \mathbb{Z}$. Daher

$$\langle a\rangle = \left\{1, a^1, .., a^{k-1}\right\}$$

und

$$|\langle a\rangle| = k$$

In beiden Fällen ist

$$|\langle a\rangle| = \inf\left\{k \in \mathbb{N} : a^k = 1\right\} \tag{3.3.8.1}$$

wobei $\inf \emptyset := \infty$.

3.3.9 Satz von Fermat-Euler

Für jedes Element $a \in G$ einer endlichen Gruppe G gilt $a^{|G|} = 1$.

Beweis: Nach Lagrange (3.3.6) ist

$$|G| = \underbrace{|G : \langle a\rangle|}_{l} \cdot |\langle a\rangle|$$

Sei $k \in \mathbb{N}$ minimal so dass $a^k = 1$, d.h. $k = |\langle a\rangle|$ (vgl. vorige Bemerkung). Also

$$a^{|G|} = a^{kl} = (a^k)^l = 1^l = 1$$

□

3.3.10 Satz über Element-Ordnungen

Sei G eine Gruppe und $g \in G$ mit Ordnung $|\langle g \rangle| =: n \in \mathbb{N}$. Dann gilt:

1. Ist $k \in \mathbb{Z}$ mit $g^k = 1$, so gilt $n \mid k$.
2. Für $k \in \mathbb{Z}$ hat g^k die Ordnung $\frac{n}{\mathrm{ggT}(n,k)}$.

3.3.11 Korollar für zyklische Gruppen

Sei G eine zyklische, endliche Gruppe.

1. Für jedes $n \in \mathbb{N}_0$ gilt:
$$|\{g \in G : g^n = 1\}| = \mathrm{ggT}(n, |G|)$$
2. Zu jedem Teiler n von $|G|$ enthält G genau eine Untergruppe der Ordnung n.

3.3.12 Satz über Untergruppen von $(\mathbb{Z}, +)$

Für jede Untergruppe $U \leq \mathbb{Z}$ existiert ein $n \in \mathbb{N}_0$ mit

$$U = n\mathbb{Z} := \{nz : z \in \mathbb{Z}\}$$

Bemerkung: Es ist $|\mathbb{Z} : n\mathbb{Z}| = n$ für $n \in \mathbb{N}$, denn:
Für $z \in \mathbb{Z}$ existieren $q, r \in \mathbb{Z}$ mit $z = qn + r,\ 0 \leq r < n$ und daher $z \in r + n\mathbb{Z}$. Folglich:

$$\mathbb{Z} = (0 + n\mathbb{Z}) \cup (1 + n\mathbb{Z}) \cup \cdots \cup (n - 1 + n\mathbb{Z})$$

Da $0, 1, .., n-1$ in paarweise verschiedenen Linksnebenklassen modulo $n\mathbb{Z}$ liegen, folgt die Behauptung.

Dabei besitzt $\mathbb{Z}$ für $n \in \mathbb{N} \cup \{\infty\}$ genau eine Untergruppe vom Index n.

3.3.13 Satz über Untergruppen zyklischer Gruppen

Jede Untergruppe V einer zyklischen Gruppe $G = \langle g \rangle,\ g \in G$ ist ebenfalls zyklisch.

Beweis: Betrachten den Epimorphismus

$$f : (\mathbb{Z}, +) \to (G, \circ) \quad , \quad n \mapsto g^n$$

Dann ist $V = f(f^{-1}(V))$. Da $f^{-1}(V) \leq \mathbb{Z}$ ist nach vorigem Satz 3.3.12 $f^{-1}(V) = n\mathbb{Z}$ für irgendein $n \in \mathbb{N}_0$. Daher ist

$$V = f(n\mathbb{Z}) = \langle g^n \rangle$$

zyklisch.
□

3.3.14 Definition: Modulo H, K

Seien G eine Gruppe, $H, K \leq G$ und $a, b \in G$. Wir schreiben

$$a \equiv b \pmod{H, K}$$

falls $h \in H,\ k \in K$ existieren mit $b = hak$.

3.3.15 Lemma über die Relation $\equiv \pmod{H,K}$

Seien G eine Gruppe und $H, K \leq G$. Dann ist die Relation "$\equiv \pmod{H,K}$" eine Äquivalenzrelation auf G.

Bemerkung: Für $a \in G$ ist die Äquivalenzklasse von a bzgl. $\equiv \pmod{H,K}$ die *Doppelnebenklasse*

$$HaK := \{hak : h \in H,\ k \in K\}$$

von a *modulo (nach)* H, K. Man setzt

$$H \setminus G/K := \{HaK : a \in G\} \tag{3.3.15.1}$$

Als Spezialfall ist dann

$$H \setminus G = H \setminus G/1 \quad , \quad G/K = 1 \setminus G/K$$

Beachte: $|HaK|$ ist im allgemeinen **kein** Teiler von $|G|$. Als Beispiel betrachte

$$G := \mathrm{Sym}(3)\ ,\ a := 1\ ,\ b := \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\ ,\ c := \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

mit

$$H := \langle b \rangle = \{1, b\}\ ,\ K := \langle c \rangle = \{1, c\}\ ,\ HaK = \{1, b, c, bc\}$$

Dann ist $|HaK| = 4$, kein Teiler von $|G| = 6$.

3.3.16 Lemma über Doppelnebenklassen

Seien G eine Gruppe, $H, K \leq G$ und $a \in G$. Dann enthält HaK genau $\left|H : H \cap (aKa^{-1})\right|$ Linksnebenklassen modulo K und genau $\left|K : (a^{-1}Ha) \cap K\right|$ Rechtsnebenklassen modulo H. Insbesondere ist

$$|HaK| = \left|H : H \cap (aKa^{-1})\right| \cdot |K| = \left|K : (a^{-1}Ha) \cap K\right| \cdot |H|$$

Bemerke: Nach Satz 3.2.5 ist

$$aKa^{-1} = \mathrm{ad}_a(K) \leq G \ \Rightarrow\ H \cap aKa^{-1} \leq G$$

Analog ist auch $a^{-1}Ha \cap K \leq G$.

Beispiel: Für $a = 1$ ist $HaK = HK$. Nach obigem Satz enthält $|HK|$ genau $|H : H \cap K|$ Linksnebenklassen modulo K und genau $|K : H \cap K|$ Rechtsnebenklassen modulo H. Insbesondere:

(i) $|HK| = |H : H \cap K| \cdot |K| = |K : H \cap K| \cdot |H|$.

(ii) Ist $|K \cap H| < \infty$, dann $|HK| = \frac{|H| \cdot |K|}{|H \cap K|}$.

(iii) $|H : H \cap K| \leq |G : K|$

(iv) Aus $|H : H \cap K| = |G : K| < \infty$ folgt $G = HK = KH$.

3.3.17 Verallgemeinerung des Satzes von Lagrange

Den Satz von Lagrange (3.3.6) kann man folgendermaßen verallgemeinern: Ist G eine Gruppe und $K \leq H \leq G$, so gilt:

$$|G : K| = |G : H| \cdot |H : K|$$

Bemerke: Dies ist tatsächlich eine Verallgemeinerung, denn mit

$$G = \biguplus_{i \in I} g_i H \quad , \quad H = \biguplus_{j \in J} h_j K$$

$(|I| = |G : H|\,,\ |J| = |H : K|)$ folgt

$$G = \biguplus_{\substack{i \in I \\ j \in J}} g_i h_j K$$

3.3.18 Lemma über Indizes von Untergruppen

Für Untergruppen $H, K \leq G$ einer Gruppe G gilt stets:

(i) $|G : H \cap K| \leq |G : H| \cdot |G : K|$

(ii) Ist $|G : H \cap K| = |G : H| \cdot |G : K| < \infty$, so ist $G = HK = KH$.

(iii) Sind $|G : H|$, $|G : K|$ endlich und teilerfremd, so ist

$$|G : H \cap K| = |G : H| \cdot |G : K|$$

also insbesondere $G = HK = KH$.

4 Zerlegung von Gruppen

4.1 Normalgruppen und Faktorgruppen

4.1.1 Satz: Charakterisierung von Normalgruppen

Für Untergruppe $N \leq G$ einer Gruppe G sind äquivalent:

1. $gNg^{-1} \subseteq N \ \ \forall\, g \in G$
2. $gNg^{-1} = N \ \ \forall\, g \in G$
3. $gN = Ng \ \ \forall\, g \in G$
4. G/N ist eine Gruppe mit der Verknüpfung $(gN)(hN) = ghN$ für $g, h \in G$ (vgl. 3.2.3).
5. Es existiert eine Gruppe H und Homomorphismus $f : G \to H$ mit $N = \ker(f)$.

4.1.2 Definition: Normalgruppe

Es sei $N \leq G$ eine Untergruppe von G die eine (bzw. alle) der Eigenschaften in Satz 4.1.1 erfüllt. Dann heißt N *normal* (*Normalteiler*) in G. Man schreibt: $N \trianglelefteq G$, im Falle $N \neq G$ auch $N \triangleleft G$. Die Menge $G/N = N \setminus G$ heißt *Faktorgruppe* (*Quotientengruppe*) von G modulo (nach) N.

Bemerkungen:

(i) Für Normalteiler $N \trianglelefteq G$ ist

$$f : G \to G/N, \quad g \mapsto gN$$

ein Epimorphismus, und heißt *kanonischer (natürlicher) Epimorphismus von G auf G/N*. Dabei ist

$$1_{G/N} = f(1) = 1N = N$$

und

$$(gN)^{-1} = f(g)^{-1} = f(g^{-1}) = g^{-1}N$$

für $g \in G$. Ferner gilt für $a, b \in G$:

$$a \equiv_l b (\mathrm{mod} N) \ \Leftrightarrow \ aN = bN \ \Leftrightarrow \ Na = Nb \ \Rightarrow \ a \equiv_r b (\mathrm{mod} N) \ .$$

Man schreib daher kurz: $a \equiv b (\mathrm{mod} H)$ und sagt a ist *kongruent* zu b modulo N.

(ii) Für Teilmenge $X \subseteq G$ und $U \trianglelefteq G$ gilt:

$$\{xU : x \in \langle X \rangle\} = \langle xU : x \in X \rangle \tag{4.1.2.1}$$

denn

$$\langle xU : x \in X \rangle = \{(x_1^{\varepsilon_1} U) \dots (x_n^{\varepsilon_n} U) : n \in \mathbb{N}_0,\ \varepsilon_i \in \{\pm 1\},\ x_i \in X\}$$

$$= \{(x_1^{\varepsilon_1} \dots x_n^{\varepsilon_n})\, U : n \in \mathbb{N}_0,\ \varepsilon_i \in \{\pm 1\},\ x_i \in X\}$$

$$= \{gU : g \in \langle X \rangle\}$$

Spezialfall: Für Teilmenge $X \subseteq G$ und $U \trianglelefteq \langle X \rangle$ ist

$$\langle X \rangle / U = \langle xU : x \in X \rangle$$

(setze $G := \langle X \rangle$).

(iii) Ist $N \trianglelefteq G$ und $g \in G$, so ist

$$|\langle gN\rangle| \leq |\langle g\rangle|$$

denn

$$(gN)^{|\langle g\rangle|} = \underbrace{g^{|\langle g\rangle|}}_{1} N = 1_{G/N}$$

(iv) In jeder Gruppe G sind $\{1\}$ und G normal. Sind $\{1\}$ und G die einzigen Normalteiler von G und ist $G \neq \{1\}$, so heißt G *einfach*. Nach Lagrange (3.3.6) sind z.B. Gruppen mit Primzahlordnung stets einfach.

Eine nicht-einfache Gruppe $G \neq \{1\}$ stellt man sich aus Normalteiler N und Faktorgruppe G/N zusammengesetzt vor. So werden einfache Gruppen zu Bausteinen für beliebige Gruppen. Die Bestimmung aller endlichen, einfachen Gruppen war eines der größten Projekte der Mathematik überhaupt. Beteiligt waren ca. 50-100 Mathematiker. Die entsprechenden Arbeiten haben einen Umfang von ca. 10 000 Seiten. Das Projekt wurde ca. 2000 erfolgreich abgeschlossen.

(v) In jeder Gruppe G ist jede Untergruppe $U \leq Z(G)$ normal, denn

$$\forall\ g \in G,\ u \in U : gug^{-1} = ugg^{-1} = u \in U \quad .$$

Insbesondere ist $Z(G) \trianglelefteq G$. Ferner gilt: Ist G abelsch, so ist $G = Z(G)$. Daher ist in einer abelschen Gruppe G jede Untergruppe normal.

(vi) Seien G eine Gruppe, $H \leq G$ und $|G : H| = 2$. Dann ist $H \trianglelefteq G$, denn H und $G \setminus H$ sind die einzigen Linksnebenklassen (Rechtsnebenklassen) nach H, also gilt Punkt (3) in 4.1.1.

(vii) Für $n \in \mathbb{N}$ und Körper $\mathbb{K}$ ist

$$\mathrm{SL}(n, \mathbb{K}) = \ker(\det) \trianglelefteq \mathrm{GL}(n, \mathbb{K})$$

(viii) Für jeden Gruppen-Homomorphismus $f : G \to H$ und $N \trianglelefteq H$ ist $f^{-1}(N) \trianglelefteq G$, denn für $g \in G, x \in f^{-1}(N)$ ist

$$f\left(gxg^{-1}\right) = f(g)\underbrace{f(x)}_{\in N} f(g)^{-1} \in N \quad \Rightarrow \quad gxg^{-1} \in f^{-1}(N)$$

(ix) Für jeden Gruppen-Homomorphismus $f : G \to H$ und $M \trianglelefteq G$ ist $f(M) \trianglelefteq f(G)$, denn für $g \in G, m \in M$ ist

$$f(g)f(m)f(g)^{-1} = f(gmg^{-1}) \in f(M)$$

Beachte dass $f(M) \trianglelefteq H$ allgemein **nicht** gilt.

(x) Für jede Familie $(N_i)_{i\in I} \neq \emptyset$ von Normalteilern N_i einer Gruppe G sind auch

$$\bigcap_{i\in I} N_i$$

und

$$\langle N_i : i \in I\rangle := \left\langle \bigcup_{i\in I} N_i \right\rangle$$

normal in G.

(xi) Für jede Gruppe G, Automorphismus $A \in \mathrm{Aut}(G)$ und $a, x \in G$ gilt:

$$(A \circ \mathrm{ad}_a \circ A^{-1})(x) = A(aA^{-1}(x)a^{-1}) = A(a)A(A^{-1}(x))A(a)^{-1} = \mathrm{ad}_{A(a)}\, x$$

das heißt

$$A \circ \mathrm{ad}_a \circ A^{-1} = \mathrm{ad}_{A(a)} \in \mathrm{Inn}(G)$$

Somit ist insbesondere

$$\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$$

Die Quotientengruppe

$$\mathrm{Out}(G) := \mathrm{Aut}(G)/\mathrm{Inn}(G)$$

heißt *äußere Automorphismengruppe* von G.

(xii) Aus $K \trianglelefteq H \trianglelefteq G$ folgt im allgemeinen **nicht** $K \trianglelefteq G$, das heißt $\trianglelefteq$ ist nicht transitiv!

4.1.3 Lemma: Normalität von Untergruppen mit kleinstem Primzahlindex

Sei H eine Untergruppe einer endlichen Gruppe G, deren Index der kleinste Primfaktor von $|G|$ ist. Dann ist $H \trianglelefteq G$.

4.1.4 Lemma über Faktorgruppen zyklischer Gruppen

Ist G eine zyklische Gruppe und $N \trianglelefteq G$, so ist auch G/N zyklisch.
Beweis: Für $G = \langle g \rangle$ ist $G/N = \langle gN \rangle$.

4.1.5 Lemma über zyklische innere-Automorphismengruppen

Ist G eine Gruppe mit $G/Z(G)$ zyklisch, so ist G abelsch.

4.1.6 Lemma über Potenzen und Normalteiler

Sei G eine Gruppe, $N \trianglelefteq G$ und $|G : N|$ endlich. Dann ist

$$g^{|G:N|} \in N \quad \forall\, g \in G$$

Beweis: Die Faktorgruppe G/N hat Ordnung $|G : N|$. Nach Fermat-Euler 3.3.9 ist

$$\underbrace{(gN)^{|G:N|}}_{g^{|G:N|}N} = \underbrace{1_{G/N}}_{N}$$

also $g^{|G:N|} \in N$.
□

4.1.7 Lemma: Erzeugung durch Normalteiler

Es seien $H_1, .., H_n$ Normalteiler der Gruppe G. Dann gilt:

$$\Big\langle \bigcup_{i=1}^{n} H_i \Big\rangle = H_1 \cdot .. \cdot H_n$$

4.1.8 Homomorphiesatz

Für jeden Gruppenhomomorphismus $f : G \to H$ ist

$$F : G/\ker(f) \to f(G) \quad , \quad g\ker(f) \mapsto f(g)$$

wohldefiniert und ein Isomorphismus. Insbesondere ist

$$G/\ker(f) \cong f(G)$$

Beispiele:

(i) Sei $H = \langle h \rangle$ zyklisch. Dann ist

$$f : \mathbb{Z} \to H \ , \ z \overset{f}{\mapsto} h^z$$

ein Epimorphismus. Nach Satz 3.3.12 ist

$$\ker(f) = n\mathbb{Z}$$

für irgendein $n \in \mathbb{N}_0$. Daher

$$H \cong \mathbb{Z}/n\mathbb{Z}$$

das heißt jede zyklische Gruppe ist zu $(\mathbb{Z}/n\mathbb{Z}, +)$ für ein $n \in \mathbb{N}_0$ isomorph.

(ii) Für jede Gruppe G ist $\mathrm{ad} : G \to \mathrm{Aut}(G),\ a \mapsto \mathrm{ad}_a$ ein Homomorphismus mit

$$\ker(f) = Z(G) \quad , \quad \mathrm{Inn}(G) = \mathrm{image}(\mathrm{ad}) \quad .$$

Daher

$$G/Z(G) \cong \mathrm{Inn}(G) \quad .$$

(iii) Für $n \in \mathbb{N}$ und Körper $\mathbb{K}$ ist

$$\det : \mathrm{GL}(n, \mathbb{K}) \to \mathbb{K} \setminus \{0\}$$

ein Epimorphismus mit $\ker(\det) = \mathrm{SL}(n, \mathbb{K})$. Daher

$$\mathrm{GL}(n, \mathbb{K}) / \mathrm{SL}(n, \mathbb{K}) \cong \mathbb{K} \setminus \{0\} \quad .$$

Insbesondere ist $\mathrm{GL}(n, \mathbb{K}) / \mathrm{SL}(n, \mathbb{K})$ abelsch.

(iv) Für jede Familie $(N_i)_{i \in I}$ von Normalteilern N_i einer Gruppe G ist

$$f : G \to \bigtimes_{i \in I} G/N_i \ , \ g \mapsto (gN_i)_{i \in I}$$

ein Homomorphismus mit Kern

$$N := \bigcap_{i \in I} N_i$$

Nach dem Homomorphiesatz ist also

$$G/N \to \bigtimes_{i \in I} G/N_i \ , \ gN \mapsto (gN_i)_{i \in I}$$

ein Monomorphismus.

4.1.9 1. Isomorphiesatz

Seien G eine Gruppe, $H \leq G$ und $N \trianglelefteq G$. Dann ist

$$HN \leq G \ , \ N \trianglelefteq HN \ , \ H \cap N \trianglelefteq H$$

und

$$H/(H \cap N) \cong (HN)/N$$

Bemerkung: Im Fall $H \trianglelefteq G$ ist auch $HN \trianglelefteq G$, denn

$$aHNa^{-1} = \underbrace{aHa^{-1}}_{H} \underbrace{aNa^{-1}}_{N} = HN \quad \forall\ a \in G$$

4.1.10 2. Isomorphiesatz

Sei G eine Gruppe, $N \trianglelefteq G$ und $N \leq H \leq G$. Dann gilt die Äquivalenz:

$$H/N \trianglelefteq G/N \quad \Leftrightarrow \quad H \trianglelefteq G$$

Gegebenfalls ist dann

$$(G/N)/(H/N) \cong G/H$$

4.1.11 3. Isomorphiesatz

Sei G eine Gruppe, $U_0 \trianglelefteq U \leq G$ und $V_0 \trianglelefteq V \leq G$. Dann gilt:

$$(U \cap V_0)U_0 \trianglelefteq (U \cap V)U_0$$
$$(V \cap U_0)V_0 \trianglelefteq (V \cap U)V_0$$
$$(U_0 \cap V)(V_0 \cap U) \trianglelefteq U \cap V$$

und

$$(U \cap V)U_0/(U \cap V_0)U_0 \cong (V \cap U)V_0/(V \cap U_0)V_0 \cong (U \cap V)/(U_0 \cap V)(V_0 \cap U)$$

4.1.12 Satz über quasi-disjunkte Normalteiler

Seien G eine Gruppe und $M, N \trianglelefteq G$ mit $M \cap N = \{1\}$. Dann ist

$$mn = nm \quad \forall\ m \in M,\ n \in N$$

Beweis: Mit

$$\underbrace{\underbrace{m}_{\in M}\underbrace{(nm^{-1}n^{-1})}_{\in M}}_{\in M} = \underbrace{\underbrace{(mnm^{-1})}_{\in N}\underbrace{n^{-1}}_{\in N}}_{\in N}$$

folgt $mnm^{-1}n^{-1} = 1$. $\square$

4.1.13 Definition: Charakteristische, vollinvariante Untergruppen

Eine Untergruppe U einer Gruppe G mit der Eigenschaft

$$f(U) \subseteq U \quad \forall\ f \in \mathrm{Aut}(G)$$

bzw.

$$f(U) \subseteq U \quad \forall\ f \in \mathrm{End}(G)$$

heißt *charakteristisch* bzw. *vollinvariant* in G.

Bemerkungen:

(i) Für $U \leq G$ gilt: $U \trianglelefteq G \ \Leftrightarrow\ f(U) \subseteq U \quad \forall\ f \in \mathrm{Inn}(G)$.

(ii) Daher gilt für Untergruppen die Implikationskette: Vollinvariant $\Rightarrow$ Charakteristisch $\Rightarrow$ Normal.

(iii) Für jede charakteristische Untergruppe $U \leq G$ und alle $f \in \mathrm{Aut}(G)$ ist

$$U = f\Big(\ \underbrace{f^{-1}(U)}_{\substack{\subseteq U \\ \text{da} \\ f^{-1} \in \mathrm{Aut}(G)}}\ \Big) \subseteq f(U)$$

das heißt tatsächlich $f(U) = U$.

Beispiele:

(i) Für jede Gruppe G ist $Z(G)$ charakteristisch in G, denn für $z \in Z(G),\ g \in f(G) = G,\ f \in \mathrm{Aut}(G)$ gilt

$$f(z)g = f(zf^{-1}(g)) = f(f^{-1}(g)z) = gf(z) \quad .$$

Im allgemeinen ist jedoch $Z(G)$ **nicht** vollinvariant in G.

(ii) Für jede Gruppe G ist $U := \langle g^2 : g \in G \rangle$ vollinvariant in G, denn für $g \in G,\ f \in \mathrm{End}(G)$ ist $f(g^2) = f(g)^2$.

4.1.14 Satz über charakteristische und vollinvariante Untergruppen

Für jede Gruppe G und $K \leq H \leq G$ gilt:

1. Ist K charakteristisch in H und H charakteristisch in G, so ist auch K charakteristisch in G.
2. Ist K vollinvariant in H und H vollinvariant in G, so ist auch K vollinvariant in G.
3. Ist K charakteristisch in H und $H \trianglelefteq G$, so ist auch $K \trianglelefteq G$.

4.1.15 Lemma: Untergruppen von Faktorgruppen

Sei G eine Gruppe. Dann gilt:

1. Für $N \trianglelefteq G,\ U \leq G$ ist
$$V := \{uN : u \in U\} = \{unN : u \in U,\ n \in N\} = \underbrace{(UN)/N}_{\substack{U/N \\ \text{falls } N \leq U}}$$
eine Untergruppe von G/N.
2. Sind $N \trianglelefteq U, \tilde{U} \leq G$ mit $U/N = \tilde{U}/N$, so ist $U = \tilde{U}$.
3. Sei $N \trianglelefteq G$. Dann lässt sich auch jede Untergruppe $V \leq G/N$ mit einem (eindeutigen) $N \trianglelefteq U \leq G$ so darstellen:
$$V = \underbrace{\{u \in G : uN \in V\}}_{U} /N$$
4. Sei $N \trianglelefteq G$ und $N \trianglelefteq U \leq G$. Dann ist $U/N < G/N$ genau dann wenn $U < G$.
5. Sei $N \trianglelefteq G$ und $N \trianglelefteq U \leq G$. Dann ist $U/N \trianglelefteq G/N$ genau dann wenn $U \trianglelefteq G$ ist.
6. Für $N \trianglelefteq V_1, V_2 \leq G$ ist $V_1/N \leq V_2/N$ genau dann wenn $V_1 \leq V_2$.
7. Sei $N \trianglelefteq G$ und $N \trianglelefteq U \leq G$. Sind $N \leq G$ und $U/N \leq G/N$ charakteristisch, so ist auch $U \leq G$ charakteristisch.

Beweis:

1. Klar.
2. Es sei $\tilde{U}/N = U/N$. Es genügt zu zeigen $U \subseteq \tilde{U}$. Für $u \in U$ gilt $uN \in \tilde{U}/N$, also $uN = \tilde{u}N$ für ein $\tilde{u} \in \tilde{U}$. Demnach $\tilde{u}^{-1}u \in N \subseteq \tilde{U}$, also $u \in \tilde{u}\tilde{U} = \tilde{U}$.
3. U ist tatsächlich eine Untergruppe, denn für $a, b \in U$ ist $abN = \underbrace{(aN)}_{\in V}\underbrace{(bN)}_{\in V} \in V$ also $ab \in U$. Analog ist auch $a^{-1} \in U$, und offensichtlich $U \neq \emptyset$. Per Konstruktion ist $N \subseteq U$ und $U/N = V$.
   Eindeutigkeit folgt aus Teil (2).
4. Nach Darstellung in (3) ist $gN \notin U/N$ äquivalent zu $g \notin U$.
5. Siehe 2. Isomorphiesatz 4.1.10.
6. Richtung "$\Leftarrow$" ist klar.
   Richtung "$\Rightarrow$" : Nach (3) existiert eine Untergruppe $U \leq V_2$ mit $V_1/N = U/N$. Wegen Eindeutigkeit (2) ist $V_1 = U$.

7. Seien N und $U/N \leq G/N$ charakteristisch und $\alpha \in \mathrm{Aut}(G)$. Dann induziert α einen Automorphismus $\overline{\alpha} \in \mathrm{Aut}(G/N)$ durch
$$\overline{\alpha}(gN) := \alpha(g)N$$
Dabei ist $\overline{\alpha}$ wohldefiniert und injektiv, denn
$$gN = hN \;\Leftrightarrow\; g^{-1}h \in N \;\Leftrightarrow\; \underbrace{\alpha(g)^{-1}\alpha(h)}_{\alpha(g^{-1}h)} \in N \;\Leftrightarrow\; \alpha(h)N = \alpha(g)N$$
(beachte dass auch $\alpha^{-1}(N) \subseteq N$ ist). Homomorphie ist klar, Surjektivität folgt aus Surjektivität von α. Da U/N charakteristisch ist, ist
$$\alpha(U)/N \subseteq \overline{\alpha}(U/N) \subseteq U/N$$
Nach Teil (6) also $\alpha(U) \subseteq U$.

□

4.2 Ω-Gruppen

4.2.1 Definition: Ω-Gruppe

Sei Ω eine Menge. Eine Ω-*Gruppe* ist ein Paar, das aus einer Gruppe G und einer Abbildung
$$\Omega \times G \to G \;\;,\;\; (\omega, g) \mapsto {}^{\omega}g$$
mit
$${}^{\omega}(g \circ h) = {}^{\omega}g \circ {}^{\omega}h \;\;,\;\; \omega \in \Omega,\; g, h \in G$$
besteht. Die Elemente von Ω heißen *Operatoren*. Man sagt kurz: G ist eine Ω-Gruppe.

Bemerkung: Zu $\omega \in \Omega$ gehört dann $G \to G,\; g \mapsto {}^{\omega}g$ zu $\mathrm{End}(G)$. Dabei können verschiedene Elemente von Ω durchaus den gleichen Endomorphismus von G liefern.

Beispiele:

(i) Jeder Vektorraum V über Körper $\mathbb{K}$ lässt sich als $\mathbb{K}$-Gruppe auffassen:
$${}^{\omega}v = \omega \cdot v \;\;,\;\; \omega \in \mathbb{K},\; v \in V$$

(ii) Sei G eine Gruppe, $\Omega = \mathrm{End}(G)$ (bzw. $\Omega = \mathrm{Aut}(G)$ oder $\Omega = \mathrm{Inn}(G)$). Dann wird G mit
$${}^{\omega}g := \omega(g) \;\;,\;\; \omega \in \Omega,\; g \in G$$
zu einer Ω-Gruppe.

(iii) Sei G eine Gruppe und $\Omega \subseteq G$. Dann wird G mit
$${}^{\omega}g := \omega g \omega^{-1} \;\;,\;\; \omega \in \Omega,\; g \in G$$
zu einer Ω-Gruppe.

(iv) Für jede Familie $(G_i)_{i \in I} \neq \emptyset$ von Ω-Gruppen G_i ist auch $\bigtimes_{i \in I} G_i$ wieder eine Ω-Gruppe mit
$${}^{\omega}(g_i)_{i \in I} := ({}^{\omega}g_i)_{i \in I} \;\;,\;\; \omega \in \Omega,\; (g_i)_{i \in I} \in \bigtimes_{i \in i} G_i$$

4.2.2 Definition: Ω-Untergruppe

Seien Ω eine Menge und G eine Ω-Gruppe. Eine Untergruppe $H \leq G$ mit
$${}^{\omega}h \in H \;\; \forall\, \omega \in \Omega,\; h \in H$$
heißt Ω-*Untergruppe* von G. Ist sogar $H \trianglelefteq G$, so heißt H Ω-*Normalteiler* von G.

Bemerkungen:

(i) Jede Ω-Untergruppe von G kann man wieder als Ω-Gruppe auffassen.

(ii) Für jede Ω-Normalgruppe $N \trianglelefteq G$ wird G/N zu einer Ω-Gruppe mit

$$^{\omega}(gN) := (^{\omega}g)N \quad , \quad g \in G,\ \omega \in \Omega$$

Beispiele:

(i) Ist G eine Gruppe und $\Omega = \mathrm{End}(G)$ (bzw. $\Omega = \mathrm{Aut}(G)$ bzw. $\Omega = \mathrm{Inn}(G)$) so sind die Ω-Untergruppen von G genau die vollinvarianten (bzw. charakteristischen bzw. normalen) Untergruppen.

(ii) Zu $\mathbb{K}$-Vektorraum V sind die $\mathbb{K}$-Untergruppen genau die Unterräume von V (vgl. Beispiel (i) in 4.2.1).

4.2.3 Definition: Ω-Homomorphismus

Sei Ω eine Menge und G, H Ω-Gruppen. Ein Homomorphismus $f : G \to H$ mit

$$f\,(^{\omega}g) = {}^{\omega}(f(g)) \quad , \quad g \in G,\ \omega \in \Omega$$

heißt Ω-Homomorphismus. Analog hat man auch Ω-Monomorphismen, Ω-Isomorphismen usw. und entsprechend die Notationen

$$\cong_{\Omega}\ ,\ \mathrm{Hom}_{\Omega}(G)\ ,\ \mathrm{End}_{\Omega}(G)\ ,\ \mathrm{Aut}_{\Omega}(G)$$

Beispiel: Sei G eine Ω-Gruppe. Für jede Ω-Untergruppe $H \leq G$ ist die Inklusionsabbildung $H \to G,\ h \mapsto h$ ein Ω-Monomorphismus. Für jeden Ω-Normalteiler $N \trianglelefteq G$ ist die kanonische Abbildung

$$G \to G/N\ ,\ g \mapsto gN$$

ein Ω-Epimorphismus.

Bemerkung: Viele Aussagen über Gruppen, Untergruppen, Homomorphismen usw. übertragen sich problemlos auf Ω-Gruppen, Ω-Untergruppen, Ω-Homomorphismen usw. Z.B. sind Bild und Kern von Ω-Homomorphismen stets Ω-Untergruppen und jeder Ω-Homomorphismus $f : G \to H$ induziert einen Ω-Isomorphismus

$$G/\ker(g) \to f(G) \quad , \quad g\ker(f) \mapsto f(g)$$

(vgl. Homomorphiesatz 4.1.8). Analog übertragen sich die anderen Isomorphiesätze auf Ω-Gruppen.

4.3 Normalreihen

4.3.1 Definition: Normalreihe

Eine endliche Folge von Untergruppen

$$G = G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_l = \{1\} \tag{4.3.1.1}$$

einer Gruppe G heißt *Subnormalreihe* von G der *Länge* l (beachte: $l+1$ Gruppen) mit *Faktoren* $G_0/G_1, .., G_{l-1}/G_l$. Ist $G_i \trianglelefteq G\ \forall\ i$ dann heißt die Folge *Normalreihe*. Ist $G_{i-1} \neq G_i$ so heißt die Folge *(Sub-)Normalreihe ohne Wiederholungen*. Eine *Verfeinerung* der Subnormalreihe ist eine Subnormalreihe

$$G = H_0 \trianglerighteq H_1 \trianglerighteq \cdots \trianglerighteq H_m = \{1\}$$

derart dass eine Injektion

$$f : \{1, .., l\} \to \{1, .., m\}$$

mit $G_i = H_{f(i)}$ existiert. Im Fall $m > l$ heißt die Verfeinerung *echt*.

Beispiel: Seien

$$a := \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \ , \ b := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in \mathrm{GL}(2, \mathbb{C})$$

und $G := \langle a, b \rangle$. Dann ist $|G| = 8$ und

$$G \trianglerighteq \langle a^2, b \rangle \trianglerighteq \langle b \rangle \trianglerighteq \{1\}$$

eine Subnormalreihe, jedoch wegen $\langle b \rangle \not\trianglelefteq G$ keine Normalreihe. Dagegen ist

$$G \trianglerighteq \langle a^2, b \rangle \trianglerighteq \langle a^2 \rangle \trianglerighteq \{1\}$$

eine Normalreihe, da $\langle a^2 \rangle = Z(\langle a^2, b \rangle)$ das heißt $\langle a^2 \rangle$ charakteristisch in $\langle a^2, b \rangle$ also nach Satz 4.1.14 normal in G.

4.3.2 Definition: Äquivalente Subnormalreihen

Zwei Subnormalreihen

$$G = G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_l = \{1\}$$

$$G = H_0 \trianglerighteq H_1 \trianglerighteq \cdots \trianglerighteq H_m = \{1\}$$

einer Gruppe G heißen *isomorph* (*äquivalent*), wenn $l = m$ und $f \in \mathrm{Sym}(l)$ existiert mit

$$G_{i-1}/G_i \cong H_{f(i)-1}/H_{f(i)}$$

das heißt, sie haben gleiche Länge und ihre Faktoren sind bis auf die Reihenfolge jeweils isomorph.

Beispiel: Die zyklische Gruppe $\mathbb{Z}/6\mathbb{Z}$ hat isomorphe Normalreihen

$$\mathbb{Z}/6\mathbb{Z} \overset{1.}{\trianglerighteq} 2\mathbb{Z}/6\mathbb{Z} \overset{2.}{\trianglerighteq} 6\mathbb{Z}/6\mathbb{Z} \tag{4.3.2.1}$$

und

$$\mathbb{Z}/6\mathbb{Z} \overset{2.}{\trianglerighteq} 3\mathbb{Z}/6\mathbb{Z} \overset{1.}{\trianglerighteq} 6\mathbb{Z}/6\mathbb{Z} \tag{4.3.2.2}$$

4.3.3 Verfeinerungssatz von Schreier

Je zwei Subnormalreihen einer Gruppe G haben isomorphe Verfeinerungen.

4.3.4 Definition: Kompositionsreihe

Eine *Kompositionsreihe* einer Gruppe G ist eine Subnormalreihe von G ohne Wiederholungen, die keine echte Verfeinerung ohne Wiederholungen hat.

Beispiele:

(i) Die Subnormalreihen (4.3.2.1) und (4.3.2.2) von $\mathbb{Z}/6\mathbb{Z}$ sind Kompositionsreihen.

(ii) $\mathbb{Z}$ selbst hat keine Kompositionsreihe, denn jede Subnormalreihe

$$\mathbb{Z} \trianglerighteq n_1\mathbb{Z} \trianglerighteq \cdots \trianglerighteq n_l\mathbb{Z} \trianglerighteq \{0\}$$

kann man zu

$$\mathbb{Z} \trianglerighteq n_1\mathbb{Z} \trianglerighteq \cdots \trianglerighteq n_l\mathbb{Z} \trianglerighteq 2n_l\mathbb{Z} \trianglerighteq \{0\}$$

verfeinern.

(iii) Jede endliche Gruppe G hat eine Kompositionsreihe.

4.3.5 Satz von Jordan-Hölder

Je zwei Kompositionsreihen einer Gruppe sind isomorph.

Beweis: Nach Schreier (4.3.3) haben je zwei Kompositionsreihen von G isomorphe Verfeinerungen. Beide Verfeinerungen haben gleiche Anzahl an Wiederholungen, da eine Wiederholung $G_i = G_{i+1}$ genau dann vorliegt, wenn der entsprechende Faktor $G_i/G_{i+1} = \{1\}$ ist. Man kann also in beiden Verfeinerungen die Wiederholungen streichen, bzw. annehmen dass sie Wiederholungsfrei sind.

Anderseits haben Kompositionsreihen keine echten Verfeinerungen ohne Wiederholungen. Daher sind bereits die ursprünglichen Kompositionsreihen Isomorph.
□

Bemerkung: Nach dem 2. Isomorphiesatz (4.1.10) ist eine Subnormalreihe von G genau dann eine Kompositionsreihe, wenn ihre Faktoren einfache Gruppen sind. Diese heißen dann *Kompositionsfaktoren* von G und die Länge einer Kompositionsreihe heißt *Kompositionslänge* von G (kurz: *Länge* von G).

4.3.6 Definition: Einfache Ω-Gruppe

Sei Ω eine Menge und $G \neq \{1\}$ eine Ω-Gruppe. Dann heißt G *einfach*, wenn $\{1\}, G$ die einzigen Ω-Normalteiler von G sind. Im Fall $\Omega = \mathrm{Aut}(G)$, das heißt $\{1\}, G$ sind die einzigen charakteristischen Normalteiler, heißt G *charakteristisch einfach*.

Bemerkung: Die Definition von Ω-*(Sub-)Normalreihen* und Ω-*Verfeinerungen* ist klar. Eine Ω-*Kompositionsreihe* ist dementsprechend eine Ω-Subnormalreihe ohne Wiederholungen, die keine echte Ω-Verfeinerung ohne Wiederholungen hat.

Die Sätze von Schreier (4.3.3) und Jordan-Holder (4.3.5) übertragen sich. Im Fall $\Omega = \mathrm{Inn}(G)$ heißen Ω-Kompositionsreihen *Hauptreihen*, ihre Faktoren *Hauptfaktoren*, ihre Länge *Hauptlänge*. Nach Satz 4.1.14 (3) ist jeder Hauptfaktor charakteristisch einfach.

4.3.7 Satz über Ω-Subnormalreihen

Sei Ω eine Menge und G eine Ω-Gruppe mit Ω-Subnormalreihe

$$G = G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_l = \{1\}$$

Dann gilt:

1. Für jede Ω-Untergruppe $H \leq G$ ist

   $$H = H \cap G_0 \trianglerighteq H \cap G_1 \trianglerighteq \cdots \trianglerighteq H \cap G_l = \{1\}$$

   eine Ω-Subnormalreihe von H mit

   $$(H \cap G_{i-1})/(H \cap G_i) \cong_\Omega [(H \cap G_{i-1})G_i]/G_i \leq G_{i-1}/G_i \quad .$$

2. Für jeden Ω-Normalteiler $N \trianglelefteq G$ ist

   $$G/N = (G_0N)/N \trianglerighteq (G_1N)/N \trianglerighteq \cdots \trianglerighteq (G_lN)/N$$

   eine Ω-Subnormalreihe von G/N mit

   $$(G_{i-1}N/N)/(G_iN/N) \cong_\Omega (G_{i-1}N)/(G_iN) \cong_\Omega G_{i-1}/(G_{i-1} \cap G_iN) \cong_\Omega (G_{i-1}/G_i)/[(G_{i-1} \cap G_iN)/G_i]$$

   für alle i.

4.3.8 Definition: Normaler Endomorphismus

Ein Endomorphismus $\alpha \in \mathrm{End}(G)$ einer Gruppe G mit

$$\alpha(xyx^{-1}) = x\alpha(y)x^{-1} \quad \forall\ x, y \in G$$

heißt *normal*.

Bemerkung: Mit $\Omega = \mathrm{Inn}(G)$ sind also die normalen Endomorphismen von G genau die Ω-Endomorphismen von G. Ferner ist ein $\alpha \in \mathrm{End}(G)$ genau dann normal, wenn

$$x^{-1}\alpha(x)\alpha(y) = \alpha(y)x^{-1}\alpha(x) \quad \forall\ x, y \in G \quad ,$$

das heißt, wenn $x^{-1}\alpha(x) \quad \forall\ x \in G$ mit jedem $y \in \alpha(G)$ vertauschbar ist. Insbesondere ist ein Automorphismus $\alpha \in \mathrm{Aut}(G)$ genau dann normal, wenn

$$x^{-1}\alpha(x) \in Z(G) \quad \forall\ x \in G$$

ist.

Beispiel: Die Identitätsabbildung

$$\mathrm{Id}_G : G \to G\ ,\ g \mapsto g$$

und die *Nullabbildung*

$$0_G : G \to G\ ,\ g \mapsto 1_G$$

sind stets normal.

4.3.9 Satz (Schur's Lemma)

Für jede Menge Ω, jede einfache Ω-Gruppe G und jedem normalen Ω-Endomorphismus $0_G \neq \alpha \in \mathrm{End}_\Omega(G)$ gilt:

$$\alpha \in \mathrm{Aut}_\Omega(G)$$

4.4 Direkte Zerlegungen

4.4.1 Definition: Direkte Summe

Sei $(G_i)_{i\in I}$ eine Familie von Normalteilern G_i einer Gruppe G mit folgenden Eigenschaften:

(i) $G = \langle G_i : i \in I\rangle$

(ii) $G_i \cap \langle G_j : i \neq j \in I\rangle = \{1\} \quad \forall\ i \in I$

Dann heißt G *direkte Summe* von $(G_i)_{i\in I}$. Man schreibt

$$G = \bigoplus_{i\in I} G_i \quad .$$

Im Fall $I = \{1, .., n\}$ für irgendein $n \in \mathbb{N}$, schreibt man auch

$$G = G_1 \oplus \cdots \oplus G_n \quad .$$

Bemerkungen:

(i) Für verschiedene $i \neq j$ ist $G_i \cap G_j = \{1\}$. Nach Satz 4.1.12 kommutiert also jedes $x_i \in G_i$ mit jedem $x_j \in G_j,\ j \neq i$. Zu jedem $g \in G$ existieren ferner $i_1, .., i_n \in I$, dazu $g_{i_1} \in G_{i_1}, .., g_{i_n} \in G_{i_n}$ mit

$$g = g_{i_1} \dots g_{i_n} \quad .$$

O.B.d.A kann man annehmen dass $i_1, .., i_n$ paarweise verschieden sind, da g_{i_k} aus unterschiedlichen G_{i_k} kommutieren, und so g_{i_k} aus gleichem G_{i_k} *zusammengeschoben* werden können. Auf die Reihenfolge der Faktoren kommt es dabei auch nicht an. Wir setzen $g_i := 1$ für $i \in I \setminus \{i_1, .., i_n\}$ und schreiben auch

$$g = \prod_{i \in I} g_i \quad .$$

Hat man eine Familie $(h_i)_{i \in I}$ von Elementen $h_i \in G_i$ mit

$$|\{i \in I : h_i \neq 1\}| < \infty \quad \wedge \quad g = \prod_{i \in I} h_i \quad ,$$

so ist $g_i = h_i\ \forall\ i$, denn im Fall $g_i \neq h_i$ für irgendein $i \in I$, wäre

$$1 \neq g_i^{-1} h_i = \prod_{i \neq j \in I} g_j h_j^{-1} \in G_i \cap \langle G_j : i \neq j \in I \rangle = \{1\}$$

ein Widerspruch! Jedes Element $g \in G$ lässt sich also in der Form

$$g = \prod_{i \in I} g_i$$

mit eindeutig bestimmten $g_i \in G_i$ beschreiben, von denen nur endlich viele von 1 verschieden sind. Daraus folgt leicht, dass

$$\coprod_{i \in I} G_i \to G \quad , \quad (g_i)_{i \in I} \mapsto \prod_{i \in I} g_i$$

ein Isomorphismus ist. Man identifiziert daher oft

$$G = \bigoplus_{i \in I} G_i \cong \coprod_{i \in I} G_i$$

und schreibt z.B. im Fall $I = \{1, .., n\}$ auch

$$G = G_1 \times \dots \times G_n = G_1 \oplus \dots \oplus G_n = G_1 \cdot .. \cdot G_n$$

In dem Fall ist auch

$$|G| = \prod_{i=1}^{n} |G_i|$$

(ii) Sei umgekehrt $(G_i)_{i \in I}$ eine Familie beliebiger Gruppen. Wir setzen

$$G := \coprod_{i \in I} G_i \quad , \quad \tilde{G}_i := \left\{ (g_j)_{j \in I} \in \coprod_{j \in I} G_j : g_j = 1 \ \ \forall\ i \neq j \in I \right\}$$

Dann folgt leicht

$$G = \bigoplus_{i \in I} \tilde{G}_i$$

und

$$\tilde{G}_j \cong G_j \ \ \forall\ j \in I \quad .$$

Auch hier identifiziert man oft G_j mit $\tilde{G}_j$ und fasst so G_j als Untergruppen von G auf.

4.4.2 Lemma: Assoziativität direkter Summen

Ist $U = \bigoplus_{i\in I} U_i$ $(0 \notin I)$ und $G = U_0 \oplus U$, so ist

$$G = \bigoplus_{i\in I\cup\{0\}} U_i$$

Bemerkung: Dies kann als Assoziativität von $\oplus$ angesehen werden, denn für $U = U_1 \oplus U_2$ wäre dann

$$G = (U_1 \oplus U_2) \oplus U_0 = U_1 \oplus U_2 \oplus U_0 = U_1 \oplus (U_2 \oplus U_0)$$

Beweis: Nennen $V := U_0$. Zeigen zunächst:

$$U_j \cap \langle V,\ U_i : j \neq i \in I\rangle = \{1\} \quad \forall\ j \in I$$

(vgl. Eigenschaft (ii) in 4.4.1). Tatsächlich, wäre $1 \neq u \in U_j \cap \langle V, U_{i\neq j}\rangle$ so besäße u die Darstellung

$$u = g_{i_1} \dots g_{i_n}$$

für irgendwelche $g_{i_l} \in U_{i_l}$ bzw. $g_{i_l} \in V$, dabei muss $1 \neq g_{i_k} =: v \in V$ sein für irgendein $k \in \{1,..,n\}$. Analog zu Bemerkung (ii) in 4.4.1, kann man o.B.d.A annehmen dass g_{i_k} das einzige in V ist und $k = 1$, das heißt $u = v\underbrace{g_{i_2}..g_{i_n}}_{\in\langle U_{i\neq j}\rangle}$ also

$$1 \neq v = \underbrace{u}_{\in U_j}\underbrace{(g_{i_2}..g_{i_n})^{-1}}_{\in\langle U_{i\neq j}\rangle} \in \underbrace{\langle U_i : i \in I\rangle}_{U} \cap V$$

ein Widerspruch. Ferner sind alle U_i Normalteiler von G, denn jedes $h \in G$ besitzt die Darstellung

$$h = \underbrace{h_u}_{\in U}\underbrace{h_v}_{\in V} \quad , \quad h_u = h_{i_1}..h_{i_n} \quad , \quad h_{i_l} \in U_{i_l}$$

wobei o.B.d.A die i_l paarweise verschieden sind, insbesondere also die $h_{i_1}, .., h_{i_n}, h_v$ kommutieren. Somit ist

$$hU_kh^{-1} = hh^{-1}U_k = U_k$$

im Falle $i_l \neq k\ \forall\ l = 1,..,n$ bzw.

$$hU_kh^{-1} = h_{i_1}..h_{i_n}h_vU_kh_v^{-1}h_{i_n}^{-1}..h_{i_1}^{-1} = h_{i_1}U_kh_{i_1}^{-1} = U_k$$

im Falle $k = i_l$ für irgendein $l \in \{1,..,n\}$ (hier o.B.d.A $l = 1$).
□

4.4.3 Lemma über direkte Summen und Isomorphismen

Sei $(G_i)_{i\in I}$ eine Familie von Normalteilern G_i einer Gruppe G mit $G = \bigoplus_{i\in I} G_i$ und $\alpha : G \to H$ ein Gruppenisomorphismus. Dann ist

$$H = \bigoplus_{i\in I} \alpha(G_i)$$

Direkte Summen sind also Isomorphieinvariant.

Beweis: Nach Bemerkung (ix) in Definition 4.1.2 sind $\alpha(G_i) \trianglelefteq H$. Nach Bemerkung (ii) in Satz 3.2.11 ist $H = \langle\alpha(G_i) : i \in I\rangle$. Analog ist auch

$$\alpha(G_i) \cap \langle\alpha(G_j) : i \neq j \in I\rangle = \alpha(G_i) \cap \alpha\left(\langle G_j : i \neq j \in I\rangle\right) = \alpha(\underbrace{G_i \cap \langle G_j : i \neq j \in I\rangle}_{\{1\}}) = \{1\}$$

für $i \in I$.
□

4.4.4 Homomorphiesatz für direkte Summen

Sei G eine Gruppe mit $G = N \oplus M$ für irgendwelche Normalteiler $N, M \trianglelefteq G$. Dann ist

$$G/N \cong M$$

Beweis: Nach Bemerkung (i) in 4.4.1 ist jedes Element $g \in G$ eindeutig zerlegbar in $g = g_n g_m$ mit $g_n \in N,\ g_m \in M$. Die Abbildung

$$f : G \to G \quad , \quad (g_n g_m) \mapsto g_m$$

ist insbesondere ein Homomorphismus, so dass nach Homomorphiesatz 4.1.8 gilt

$$G/\underbrace{\ker(f)}_{N} \cong \underbrace{f(G)}_{M}$$

□

4.4.5 Satz: Hinreichende Bedingung für direkte Summen

Seien $G_1, .., G_n$ Normalteiler der Gruppe G mit

$$G = \underbrace{G_1 \cdot .. \cdot G_n}_{\substack{\langle G_i : i \in I \rangle \\ \text{nach (4.1.7)}}}$$

und

$$G_i \cap (G_1 \cdot .. \cdot G_{i-1}) = \{1\} \quad \forall\ i = 2, .., n \quad .$$

Dann ist

$$G = G_1 \oplus \cdots \oplus G_n \quad .$$

Beispiel: Sind G_1, G_2 Normalteiler einer Gruppe mit $G = G_1 G_2$ und $G_1 \cap G_2 = \{1\}$, dann ist $G = G_1 \oplus G_2$ (vgl. lineare Algebra).

4.4.6 Satz: Hinreichende Bedingung für direkte Summen

Seien $G_1, .., G_n$ Normalteiler einer endlichen Gruppe G mit $|G| = |G_1| \cdot .. \cdot |G_n|$ und

$$\mathrm{ggT}\left(|G_i|, |G_j|\right) = 1 \quad \forall\ i \neq j \quad .$$

Dann ist

$$G = G_1 \oplus .. \oplus G_n$$

4.4.7 Definition: Minimale & maximale Untergruppe

Eine *minimale* (bzw. *maximale*) Untergruppe einer Gruppe G ist eine Untergruppe $U \neq \{1\}$ (bzw. $U \neq G$) von G derart, dass keine Untergruppe $V \leq G$ mit $1 < V < U$ (bzw. $U < V < G$) existiert. Analog definiert man *minimale* bzw. *maximale* Normalteiler.

Bemerkungen:

(i) Ist $N \lhd G$ ein maximaler Normalteiler von G, so ist G/N einfach.
Beweis: Nach Lemma 4.1.15 kann jeder Normalteiler von G/N dargestellt werden als M/N für ein $N \leq M \trianglelefteq G$. Aus $\left\{1_{G/M}\right\} \lhd M/N \lhd G/N$ folgt außerdem $N \lhd M \lhd G$, ein Widerspruch zur Maximalität von N.

(ii) Ist $\{1\} < N$ ein minimaler Normalteiler von G, so ist N einfach.

(iii) Ist $N \lhd G$ ein maximaler Normalteiler von G und $\{1\} < L \trianglelefteq G$ mit $N \cap L = \{1\}$, so ist $G = N \oplus L$.
Beweis: Einerseits ist $N \trianglelefteq NL \trianglelefteq G$. Nach Voraussetzung an L ist jedoch $N < NL$, nach Voraussetzung an N also $NL = G$.

4.4.8 Satz über direkte Summen einfacher Gruppen

1. Sind $G_1, .., G_n$ nicht-abelsche, einfache Normalteiler einer Gruppe G mit $G = G_1 \oplus \cdots \oplus G_n$, so sind die Teilsummen
$$G_{i_1} \oplus \cdots \oplus G_{i_k}$$
die einzigen Normalteiler von G. Insbesondere existiert zu jedem $N \trianglelefteq G$ ein $M \trianglelefteq G$ mit $G = N \oplus M$.

2. Direkte Produkte endlich vieler isomorpher, einfacher Gruppen sind stets charakteristisch einfach.

3. Jede endliche, charakteristisch einfache Gruppe G ist direkte Summe endlich vieler isomorpher, einfacher Gruppen.

4.4.9 Definition: Minimal- & Maximalbedingung für Gruppen

Sei Ω eine Menge. Dann erfüllt eine Ω-Gruppe G die *Minimalbedingung* (bzw. *Maximalbedingung*) für Ω-Gruppen: $:\Leftrightarrow$ Jede nicht-leere Menge $\mathfrak{M} \neq \emptyset$ von Ω-Untergruppen von G enthält ein minimales (bzw. maximales) Element M, das heißt $\nexists\, H \in \mathfrak{M} : H < M$ (bzw. $M < H$).

Bemerkung: Eine Ω-Gruppe G erfüllt die Minimalbedingung genau dann wenn sie keine streng monoton fallende Folge $U_1 > U_2 > \ldots$ von Ω-Untergruppen besitzt.

Sie erfüllt die Maximalbedingung genau dann wenn sie keine streng monoton wachsende Folge $U_1 < U_2 < \ldots$ von Ω-Untergruppen besitzt.

Somit erfüllen insbesondere endliche Gruppen die Minimal- und Maximalbedingung.

4.4.10 Satz von Fitting

Sei Ω eine Menge und G eine Ω-Gruppe mit Minimal- und Maximalbedingung für Ω-Untergruppen erfüllt. Zu jedem normalen $\alpha \in \mathrm{End}_\Omega(G)$ existiert dann ein $k \in \mathbb{N}$ mit:

1. $G \geq \alpha(G) \geq \alpha^2(G) \geq \cdots \geq \alpha^k(G) = \alpha^{k+1}(G) \ldots$

2. $1 \leq \ker(f) \leq \ker(\alpha^2) \leq \cdots \leq \ker(\alpha^k) = \ker(\alpha^{k+1}) = \ldots$

Ferner: Für jedes solche k ist
$$G = \ker(\alpha^k) \oplus \alpha^k(G)$$

Bemerkung: Im Fall $\ker(\alpha^k) = 1$ (d.h. α^k injektiv) ist $G = \alpha^k(G)$ (d.h. α^k surjektiv), also α^k und somit auch α bijektiv.
Im Fall $\ker(\alpha^k) = G$ ist $\alpha^k = 0_G$. Die Abbildung α heißt dann *nilpotent*.

Beispiel: Jeder n-dimensionale $\mathbb{K}$-Vektorraum ($\Omega := \mathbb{K}$) erfüllt die Minimal- bzw. Maximalbedingung, da aus jeder Menge $\mathfrak{M}$ von $\mathbb{K}$-Untergruppen (Unterräume) jedes Element mit minimaler Dimension auch minimal in $\mathfrak{M}$ ist. Da Endomorphismen auf Vektorräumen normal und definitionsgemäß $\mathbb{K}$-Endomorphismen sind, stellt der Fitting-Satz eine Verallgemeinerung des entsprechenden Satzes aus der linearen Algebra dar.

4.4.11 Definition: Unzerlegbare Ω-Gruppe

Sei Ω eine Menge. Eine Ω-Gruppe $G \neq \{1\}$ heißt *unzerlegbar*, falls keine echten Ω-Normalteiler $M, N \lhd G$ existieren, so dass $G = M \oplus N$.

Bemerkung: Jeder normale Ω-Endomorphismus einer unzerlegbaren Ω-Gruppe mit Minimal- und Maximalbedingung für Ω-Untergruppen ist nach Satz 4.4.10 entweder nilpotent oder bijektiv.

4.4.12 Satz über Gruppen mit Minimalbedingung

Sei Ω eine Menge und G eine Ω-Gruppe mit Minimalbedingung für Ω-Untergruppen. Dann existieren endlich viele unzerlegbare Ω-Normalteiler $G_1, .., G_n \trianglelefteq G$ mit $G = G_1 \oplus \cdots \oplus G_n$.

Bemerkung: Falls $G = \{1\}$ setzt man G als direkte Summe von 0 Normalteilern.

Beweis durch Widerspruch: Andernfalls ist die Menge $\mathfrak{M}$ aller Ω-Untergruppen von G, die sich nicht als direkte Summe endlich vieler unzerlegbaren Ω-Untergruppen von G schreiben lassen, nicht-leer ($G \in \mathfrak{M}$). Daher existiert ein minimales Element $M \in \mathfrak{M}$ für das insbesondere gilt: M ist selbst keine unzerlegbare Ω-Untergruppe von G (da sonst $M \notin \mathfrak{M}$). Daher existieren Ω-Untergruppen $M_1, M_2 \lhd M$ mit

$$M = M_1 \oplus M_2$$

Nach Wahl von M (minimal in $\mathfrak{M}$) sind M_1, M_2 direkte Summen endlich vieler unzerlegbaren Ω-Untergruppen von G, also auch M (vgl. Lemma 4.4.2), ein Widerspruch!
□

Beispiele:

(i) Seien

$$a := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix} \ , \ b := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix} \ , \ c := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 5 & 4 \end{pmatrix}$$

in Sym(5) und $G := \langle a, b, c \rangle$. Dann ist

$$G = \underbrace{\langle a, b \rangle}_{\substack{\cong \mathrm{Sym}(3) \\ \text{unzerlegbar}}} \oplus \underbrace{\langle c \rangle}_{\substack{\cong \mathrm{Sym}(2) \\ \text{unzerlegbar}}}$$

aber auch

$$G = \underbrace{\langle a, bc \rangle}_{\cong \mathrm{Sym}(3)} \oplus \langle c \rangle$$

Bemerke die nicht-Eindeutigkeit der Zerlegung von G!

(ii) Ein $\mathbb{K}$-Vektorraum V ist genau dann unzerlegbar, wenn $\dim(V) = 1$.

4.4.13 Definition: Addierbare Endomorphismen

Zwei Endomorphismen $\alpha, \beta \in \mathrm{End}(G)$ einer Gruppe G heißen *addierbar*, falls

$$\alpha + \beta : G \to G \quad , \quad g \mapsto \alpha(g)\beta(g)$$

auch ein Endomorphismus ist.

4.4.14 Charakterisierung von Addierbarkeit

Endomorphismen $\alpha, \beta \in \mathrm{End}(G)$ einer Gruppe G sind genau dann addierbar, wenn jedes $x \in \alpha(G)$ und $y \in \beta(G)$ kommutieren. Gegebenfalls gilt dann

$$\alpha + \beta = \beta + \alpha$$

Bemerkungen:

(i) Sind $\alpha, \beta \in \mathrm{End}(G)$ addierbar so sind auch $\alpha \circ \gamma, \beta \circ \gamma$ bzw. $\gamma \circ \alpha, \gamma \circ \beta$ addierbar für beliebiges $\gamma \in \mathrm{End}(G)$ und es gilt

- $(\alpha + \beta) \circ \gamma = \alpha \circ \gamma + \beta \circ \gamma$
- $\gamma \circ (\alpha + \beta) = \gamma \circ \alpha + \gamma \circ \beta$

denn

$$[(\alpha + \beta) \circ \gamma](g) = (\alpha + \beta)(\gamma(g)) = \alpha(\gamma(g))\beta(\gamma(g)) = (\alpha \circ \gamma + \beta \circ \gamma)(g)$$

$$[\gamma \circ (\alpha + \beta)](g) = \gamma(\alpha(g)\beta(g)) = \gamma(\alpha(g))\gamma(\beta(g)) = (\gamma \circ \alpha + \gamma \circ \beta)(g) \quad , \quad g \in G$$

(ii) Sei Ω eine Menge, G eine Ω-Gruppe und $\alpha, \beta \in \mathrm{End}_\Omega(G)$ addierbar. Dann ist

$$\alpha + \beta \in \mathrm{End}_\Omega(G)$$

denn für $\omega \in \Omega,\ g \in G$ gilt

$${}^\omega((\alpha + \beta)(g)) = {}^\omega(\alpha(g)\beta(g)) = {}^\omega\alpha(g)\,{}^\omega\beta(g) = \alpha({}^\omega g)\beta({}^\omega g) = (\alpha + \beta)({}^\omega g)$$

(iii) Endomorphismen $\alpha_1, .., \alpha_n \in \mathrm{End}(G)$ heißen *paarweise addierbar*, falls α_i, α_j für alle $i \neq j$ addierbar sind (bemerke: man verlangt nicht dass α_i mit sich selber addierbar ist). Gegebenfalls ist dann

$$\alpha_1 + \cdots + \alpha_n : G \to G \quad , \quad g \mapsto \alpha_1(g) \cdot .. \cdot \alpha_n(g)$$

ein Endomorphismus von G, und für $m = 1, .., n-1$ gilt

$$\alpha_1 + \cdots + \alpha_n = (\alpha_1 + \cdots + \alpha_m) + (\alpha_{m+1} + \cdots + \alpha_n)$$

Dabei sind die beiden Summanden rechts, addierbare Endomorphismen von G.

4.4.15 Satz über Projektionen auf direkten Summen

Seien Ω eine Menge und $G_1, .., G_n$ Ω-Normalteiler einer Ω-Gruppe G mit $G = G_1 \oplus .. \oplus G_n$. Für $i = 1, .., n$ sei $\varepsilon_i : G \to G$ definiert durch

$$\varepsilon_i(g_1 \cdot .. \cdot g_n) := g_i \qquad \text{für} \qquad g_1 \in G_1, .., g_n \in G_n$$

Dann sind $\varepsilon_1, .., \varepsilon_n \in \mathrm{End}_\Omega(G)$ normal und paarweise addierbar, mit

$$\varepsilon_i \circ \varepsilon_j = \begin{cases} \varepsilon_i & : i = j \\ 0 & : \text{sonst} \end{cases}$$

und

$$\varepsilon_1 + \cdots + \varepsilon_n = \mathrm{Id}_G$$

4.4.16 Satz über Bijektivität addierbarer Endomorphismen

Seien Ω eine Menge, G eine unzerlegbare Ω-Gruppe mit Minimal- und Maximalbedingung für Ω-Untergruppen und $\alpha, \beta \in \mathrm{End}_\Omega(G)$ normal, addierbar so dass $\alpha + \beta \in \mathrm{Aut}_\Omega(G)$. Dann ist

$$\alpha \in \mathrm{Aut}_\Omega(G) \quad \vee \quad \beta \in \mathrm{Aut}_\Omega(G)$$

4.4.17 Eindeutigkeitssatz von Kroll-Remak-Schmidt

Seien Ω eine Menge, G eine Ω-Gruppe mit Minimal- und Maximalbedingung für Ω-Untergruppen. Ferner sei

$$G = G_1 \oplus \cdots \oplus G_r = H_1 \oplus \cdots \oplus H_s$$

mit unzerlegbaren Ω-Normalteilern $G_1, .., G_r, H_1, .., H_s$. Dann ist:

1. $r = s$
2. Nach geeigneter Umnummerierung von $H_1, ..., H_n$

   $$G = H_1 \oplus \cdots \oplus H_{i-1} \oplus G_i \oplus \cdots \oplus G_r$$

   für beliebiges $i \in \{1, .., r\}$.
3. Es existiert ein $\alpha \in \mathrm{Aut}_\Omega(G)$ so dass $\alpha(G_i) = H_i$ für $i = 1, .., r$.

Bemerkung: Als Spezialfall des Satzes kann der Austauschsatz für Basen aus der linearen Algebra gesehen werden. Dabei sind die unzerlegbaren $\mathbb{K}$-Normalteiler eines $\mathbb{K}$-Vektorraumes V genau die eindimensionalen Unterräume, die wiederum durch einzige Vektoren aufgespannt werden.

Beispiele:

(i) Für endliche Menge $\Lambda = \biguplus_{i=1}^{k} \Lambda_i$ erfüllt die so genannte *Young-Untergruppe*

$$G := \mathrm{Sym}(\Lambda_1) \oplus \cdots \oplus \mathrm{Sym}(\Lambda_k) \leq \mathrm{Sym}(\Lambda)$$

die Bedingungen des Satzes.

(ii) Ähnliches gilt für die *Levi-Untergruppe*

$$G := \underbrace{\left\{ \begin{pmatrix} G_1 & & & 0 \\ & G_2 & & \\ & & \ddots & \\ 0 & & & G_k \end{pmatrix} : G_i \in \mathrm{GL}(n_i, \mathbb{K}) \right\}}_{\cong \mathrm{GL}(n_1,\mathbb{K}) \times \cdots \times \mathrm{GL}(n_k,\mathbb{K})} \leq \mathrm{GL}\left(\sum_{i=1}^{k} n_i, \mathbb{K} \right)$$

für Körper $\mathbb{K}$ und $n_1, .., n_k \in \mathbb{N}$.

5 Abelsche Gruppen

Vorbemerkung: In diesem Abschnitt schreiben wir abelsche Gruppen stets additiv ("+") und "0" für das neutrale Element.

5.1 Basen & Freie Gruppen

5.1.1 Satz: Existenz der Torsionsgruppe

In jeder abelschen Gruppe A bilden die Elemente endlicher Ordnung eine Untergruppe $\mathscr{T}(A)$.

5.1.2 Definition: Torsionsgruppe

Zu abelschen Gruppe A heißt die Untergruppe $\mathscr{T}(A)$ aller Elemente endlicher Ordnung *Torsionsgruppe* (*Torsionsuntergruppe*) von G. Im Fall $\mathscr{T}(A) = A$ heißt A *Torsionsgruppe*, im Fall $\mathscr{T}(A) = \{0\}$ *Torsionsfrei*.

Bemerkungen:

(i) Das Studium abelscher Gruppen teilt sich typischerweise auf in Torsionsgruppen und torsionsfreie Gruppen.

(ii) Jede endliche Gruppe ist eine Torsionsgruppe.

Beispiel: Zur multiplikativen Gruppe $A := \mathbb{C} \setminus \{0\}$ ist

$$\mathscr{T}(A) = \left\{e^{2\pi i \cdot q} : q \in \mathbb{Q}\right\}$$

5.1.3 Satz über Torsionsgruppen

Für abelsche Gruppe A ist $\mathscr{T}(A)$ eine Torsionsgruppe und $A/\mathscr{T}(A)$ torsionsfrei.

5.1.4 Definition: Lineare Unabhängigkeit, Basis, freie Gruppe

Elemente $a_1, .., a_n \in A$ einer abelschen Gruppe A heißen *linear unabhängig*, falls aus

$$0 = z_1 a_1 + \cdots + z_n a_n \quad , \quad z_i \in \mathbb{Z}$$

stets $z_1 = \cdots = z_n = 0$ folgt. Andernfalls heißen $a_1, .., a_n$ *linear abhängig*. Sind $a_1, .., a_n$ linear unabhängig mit $A = \langle a_1, .., a_n \rangle$ so nennt man $a_1, .., a_n$ eine *Basis* von A. Abelsche Gruppen die eine Basis haben, heißen *freie* abelsche Gruppen.

Bemerkungen:

(i) Ist $a_1, .., a_n \in A$ eine Basis der abelschen Gruppe A, so lässt sich nach Satz 3.2.11 jedes Element $x \in A$ schreiben als

$$x = z_1 a_1 + \cdots + z_n a_n$$

für irgendwelche $z_i \in \mathbb{Z}$. Diese Darstellung ist sogar eindeutig, denn aus

$$z_1 a_1 + \cdots + z_n a_n = y_1 a_1 + \cdots + y_n a_n \quad , \quad z_i, y_i \in \mathbb{Z}$$

folgt $(z_1 - y_i) = 0 \ \forall \ i$. Die Abbildung

$$f : \mathbb{Z}^n \to A \ , \ (z_1, .., z_n) \mapsto z_1 a_1 + \cdots + z_n a_n$$

ist also ein Isomorphismus. Umgekehrt ist $\mathbb{Z}^n$ für $n \in \mathbb{N}$ frei mit Basis

$$e_1 := (1, 0, .., 0), .., e_n := (0, .., 0, 1)$$

(ii) Jede freie abelsche Gruppe A ist torsionsfrei, denn für Basis $a_1, .., a_n$ und Element

$$x = z_1 a_1 + \cdots + z_n a_n \in A \ , \ z_i \in \mathbb{Z}$$

mit $|\langle x \rangle| =: k < \infty$ ist

$$0 = k \cdot x = kz_1 \cdot a_1 + \cdots + kz_n \cdot a_n$$

also $kz_i = 0 \ \forall \ i$ bzw. $z_i = 0 \ \forall \ i$.

(iii) Die Umkehrung gilt im allgemeinen nicht! So ist z.B. $(\mathbb{Q}, +)$ torsionsfrei aber nicht frei, denn:

- Sind $x \in \mathbb{Q}$ und $k \in \mathbb{N}$ mit $kx = 0$ so folgt auch $x = 0$.
- Beliebige $x_1, .., x_n \in \mathbb{Q}$ (o.B.d.A $x_i \neq 0, \ n \geq 2$) sind linear abhängig, denn mit $x_i = \frac{p_i}{q_i}, \ p_i \in \mathbb{Z}, \ q_i \in \mathbb{Z} \setminus \{0\}$ ist

$$0 = p_2 q_1 x_1 - p_1 q_2 x_2 + 0x_3 + \cdots + 0x_n$$

(iv) Ist $f : A \to B$ ein Gruppenisomorphismus mit A, B abelsch und $a_1, .., a_n \in A$ eine Basis in A, so sind

$$f(a_1), .., f(a_n)$$

eine Basis in B, denn nach Bemerkung (ii) in 3.2.11 ist $\langle f(a_1), .., f(a_n) \rangle = f\left(\langle a_1, .., a_n \rangle\right) = B$, und aus

$$\underbrace{\sum_{i=1}^{n} z_i f(a_i)}_{f\left(\sum_{i=1}^{n} z_i a_i\right)} = 0 \quad , \quad z_i \in \mathbb{Z}$$

folgt nach Injektivität von f und linearer Unabhängigkeit von $a_1, .., a_n$: $z_i = 0 \ \forall \ i$.

5.1.5 Lemma über Basen direkter Summen

Sei A eine abelsche Gruppe.

1. Für Basis $a_1, .., a_n \in A$ ist
$$A = \langle a_1 \rangle \oplus \cdots \oplus \langle a_n \rangle$$
2. Sind $a_1, .., a_n \in U \leq A$ linear unabhängig, $b_1, .., b_m \in V \leq A$ linear unabhängig und $A = U \oplus V$, so sind
$$a_1, .., a_n, b_1, .., b_m$$
linear unabhängig.
3. Ist $a_1, .., a_n \in U$ eine Basis in $U \leq A$, $b_1, .., b_m \in V$ eine Basis in $V \leq A$ und $A = U \oplus V$, so sind
$$a_1, .., a_n, b_1, .., b_m$$
eine Basis in A.

Bemerke: Aussagen (2) und (3) lassen sich induktiv auf beliebige direkte Summen (mit endlich vielen Summanden) verallgemeinern.

Beweis:

1. Aus $x \in \langle a_k \rangle \cap \langle a_i : i \neq k \rangle$ das heißt
$$x = z_k a_k = z_1 a_1 + \cdots + z_{k-1} a_{k-1} + z_{k+1} a_{k+1} + \ldots z_n a_n \quad , \quad z_i \in \mathbb{Z}$$
folgt
$$z_1 a_1 + \cdots + z_{k-1} a_{k-1} - z_k a_k + z_{k+1} a_{k+1} + \ldots z_n a_n = 0$$
also $z_i = 0 \ \ \forall \ i$ bzw. $x = 0$. Natürlich sind $\langle a_i \rangle \trianglelefteq A$.

2. Es sei
$$\underbrace{\sum_{i=1}^{n} z_i a_i}_{\in U} + \underbrace{\sum_{j=1}^{m} y_j b_j}_{\in V} = 0$$
für irgendwelche $z_i, y_j \in \mathbb{Z}$. Nach Bemerkung (i) in 4.4.1 ist
$$I : U \times V \to A \ , \ (u, v) \mapsto u + v$$
ein Isomorphismus, insbesondere injektiv. Demnach muss
$$\sum_{i=1}^{n} z_i a_i = 0 = \sum_{j=1}^{m} y_j b_j$$
sein, was nach Voraussetzung impliziert $a_i = 0, b_j = 0 \ \ \forall\, i, j$.

3. Nach Voraussetzung sind $U = \langle a_1, .., a_n \rangle$, $V = \langle b_1, .., b_m \rangle$, also
$$A = \langle U, V \rangle = \langle a_1, .., a_n, b_1, .., b_m \rangle$$
Anderseits sind nach (2) die $a_1, .., a_n, b_1, .., b_m$ linear unabhängig.

□

5.1.6 Satz über Epimorphismen nach freien abelschen Gruppen

Seien A eine abelsche Gruppe, B eine freie abelsche Gruppe und $f : A \to B$ ein Epimorphismus. Dann ist $A = U \oplus \ker(f)$ für ein $U \leq A$, insbesondere ist
$$U \cong A/\ker(f) \cong B$$

5.1.7 Satz über torsionsfreie abelsche Gruppen

Jede torsionsfreie, endlich erzeugte, abelsche Gruppe ist frei.

Bemerkung: Es lässt sich sogar zeigen, dass man im Falle $A = \langle a_1, .., a_n \rangle$ eine Basis $b_1, .., b_k$ von A mit $k \leq n$ wählen kann. Jedoch kann man nicht im allgemeinen die $b_1, .., b_k$ aus $\{a_1, .., a_n\}$ wählen. Ein Beispiel ist $\mathbb{Z} = \langle 2, 3 \rangle$ mit $\langle 2 \rangle \neq \mathbb{Z} \neq \langle 3 \rangle$.

5.1.8 Satz: Eindeutigkeit der Basislänge

Sei A eine freie abelsche Gruppe mit Basen $a_1, .., a_k$ und $b_1, .., b_l$. Dann ist $k = l$.

5.1.9 Definition: Rang

Für freie abelsche Gruppe A heißt die (eindeutige) Basislänge $\text{rank}(A)$ *Rang* von A.

Bemerke: Nach Bemerkung (iv) in 5.1.4 ist der Rang einer Gruppe isomorphieinvariant.

5.1.10 Lemma über die Torsionsgruppe

Sei A eine endlich erzeugte abelsche Gruppe. Dann gilt:

1. Die Torsionsgruppe $\mathscr{T}(A)$ ist endlich.
2. Es ist $A = \mathscr{T}(A) \oplus F$ für geeignete freie Untergruppe $F \leq A$.

Bemerkung: Wegen $A/\mathcal{T}(A) \cong F$ (vgl. 4.4.4) ist F durch A bis auf Isomorphie eindeutig bestimmt. Insbesondere ist $\text{rank}(F)$ durch A eindeutig, dagegen F selbst im allgemeinen nicht eindeutig bestimmt.

5.2 Darstellung abelscher Gruppen

5.2.1 Satz: Zerlegung abelscher Gruppen

Sei A eine abelsche Gruppe der Ordnung $n < \infty$ und $n = p_1^{k_1} \cdot .. \cdot p_r^{k_r},\ p_i \in \mathbb{P},\ k_i \in \mathbb{N}$ die Primfaktorzerlegung von n. Dann ist

$$A = A_1 \oplus \cdots \oplus A_r$$

mit

$$A_i := \left\{a \in A : p_i^{k_i} a = 0\right\} \leq A \quad , \quad i = 1, .., r$$

Bemerkung: Nach Lemma 5.2.3 sind $|A_i| = p_i^{l_i}$ für irgendwelche $l_i \in \mathbb{N}_0$. Nach Lagrange 3.3.6 gilt $l_i \leq k_i$ (da $A_i \leq A$), und wegen $|A| = \prod_{i=1}^r |A_i|$ ist sogar $|A_i| = p_i^{k_i}$.

5.2.2 Satz: Darstellung abelscher Gruppen mit Primzahlpotenzordnung

Seien $p \in \mathbb{P},\ k \in \mathbb{N}$ und A eine endliche abelsche Gruppe mit $p^k a = 0\ \forall\ a \in A$. Dann existieren $k_1, .., k_m \in \mathbb{N}$ mit

$$A \cong \left(\mathbb{Z}/p^{k_1}\mathbb{Z}\right) \times \cdots \times \left(\mathbb{Z}/p^{k_m}\mathbb{Z}\right)$$

Bemerkungen:

(i) Offensichtlich ist $p^{k_1+\cdots+k_m} = |A|$.

(ii) Für $l \in \mathbb{N}$ und $p \in \mathbb{P}$ sind

$$\mathbb{Z}/p^l\mathbb{Z},\ p\mathbb{Z}/p^l\mathbb{Z}, \ldots, p^l\mathbb{Z}/p^l\mathbb{Z}$$

die einzigen Untergruppen von $\mathbb{Z}/p^l\mathbb{Z}$. Da

$$\underbrace{p^i\mathbb{Z}/p^l\mathbb{Z}}_{\substack{\text{zyklisch,}\\ \text{Ordnung } p^{l-i}}} \times \underbrace{p^j\mathbb{Z}/p^l\mathbb{Z}}_{\substack{\text{zyklisch,}\\ \text{Ordnung } p^{l-j}}}$$

für $(i,j) \neq (0,0)$ nie zyklisch ist, existieren keine $H_1, H_2 < \mathbb{Z}/p^l\mathbb{Z}$ mit $\mathbb{Z}/p^l\mathbb{Z} = H_1 \oplus H_2$, das heißt $\mathbb{Z}/p^l\mathbb{Z}$ ist unzerlegbar. Nach Kroll-Remak-Schmidt (4.4.17) sind also die $\mathbb{Z}/p^{k_1}\mathbb{Z}, \ldots, \mathbb{Z}/p^{k_m}\mathbb{Z}$ bis auf Isomorphie eindeutig. Insbesondere sind die $k_1, .., k_m$ eindeutig bestimmt.

Beispiel: Bis auf Isomorphie existiert genau eine abelsche Gruppe der Ordnung 2, nämlich $\mathbb{Z}/2\mathbb{Z}$, genau 2 abelsche Gruppen der Ordnung 4, nämlich $\mathbb{Z}/4\mathbb{Z}$ und $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, genau 3 abelsche Gruppen der Ordnung 8, nämlich

$$\mathbb{Z}/8\mathbb{Z}\ ,\ \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}\ ,\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}\ ,$$

genau 5 abelsche Gruppen der Ordnung 16, nämlich

$$\mathbb{Z}/16\mathbb{Z}\ ,\ \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}\ ,\ \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}\ ,\ \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}\ ,\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

usw.

5.2.3 Lemma über abelsche Gruppen mit Primzahlpotenzordnung

Eine endliche, abelsche Gruppe A hat genau dann Primzahlpotenzordnung ($|A| = p^k$ für irgendwelche $p \in \mathbb{P}, k \in \mathbb{N}_0$) falls $p^l a = 0\ \forall\ a \in A$, für irgendein $l \in \mathbb{N}_0$.

Beweis: Richtung "⇒" folgt nach Fermat-Euler (3.3.9).
Richtung "⇐": Induktion über $|G|$. Jedes Element $a \in A$ besitzt p-Potenzordnung (da $|\langle a\rangle| \mid p^l$). Durch Wahl $a \neq 0$ (falls möglich) folgt aus

$$|G| = |\langle a\rangle| \cdot \underbrace{|G/\langle a\rangle|}_{\substack{\text{abelsch,}\\ \text{endlich, mit}\\ p^l(b+\langle a\rangle)=0_{G/\langle a\rangle}\\ \forall\ b\in G}}$$

(wobei $|G/\langle a\rangle| < |G|$) induktiv die Aussage. Alternativ folgt die Behauptung auch aus Satz 5.2.2.
□

Bemerkung: Es kann natürlich sowohl $l < k$ als auch $l > k$ vorkommen. Beispiele sind $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ (mit $p = 2, k = 2$ und $l = 1$) bzw. $\mathbb{Z}/2\mathbb{Z}$ (mit $p = 2, k = 2$ und $l = 2k$).

5.2.4 Satz: Darstellung endlich erzeugter, abelscher Gruppen

Jede endlich erzeugte, abelsche Gruppe ist zu einem direkten Produkt endlich vieler zyklischer Gruppen isomorph, die entweder unendlich sind oder Primzahlordnung haben. Die dabei auftretenden Faktoren sind bis auf Isomorphie und Reihenfolge eindeutig bestimmt.

Beweis: Lemma 5.1.10, Bemerkung (i) in 5.1.4 und Sätze 5.2.1, 5.2.2.

6 Auflösbare Gruppen

6.1 Kommutatorgruppen

6.1.1 Definition: Kommutator

Für Elemente $x, y \in G$ einer Gruppe G heißt

$$[x, y] := xyx^{-1}y^{-1}$$

Kommutator von x und y.

Bemerkungen:

(i) In manchen Büchern definiert man $[x, y] := x^{-1}y^{-1}xy$.

(ii) Wegen $[x, y] = 1 \Leftrightarrow xy = yx$ *misst* der Kommutator die *Abweichung* von der *Umtauschbarkeit* von x, y. Ferner gilt:

$$xy = [x, y]\, yx \ , \ [x, y]^{-1} = [y, x]$$

(iii) Für $x, y, z \in G$ gilt

$$[xy, z] = xyzy^{-1}x^{-1}z^{-1} = x\,[y, z]\,zx^{-1}z^{-1} = x\,[y, z]\,x^{-1}\,[x, z]$$

$$[x, yz] = xyzx^{-1}z^{-1}y^{-1} = xyx^{-1}\,[x, z]\,y^{-1} = [x, y]\,y\,[x, z]\,y^{-1}$$

(schwache Bilinearität).

6.1.2 Definition: Höherer Kommutator

Für Elemente $x_1, .., x_n \in G$ einer Gruppe G definiert man induktiv den sogenannten (*rechtsnormierten*) *höheren Kommutator*:

$$[x_1, .., x_n] := [x_1, [x_2, .., x_n]]$$

wobei $[x] := x$.

Bemerkungen:

(i) Manche Authoren bevorzugen *linksnormierte* Kommutatoren.

(ii) Für $x, y, z \in G$ gilt

$$[xy, z] = [x, y, z]\,[y, z]\,[x, z]$$

$$[x, yz] = [x, y]\,[y, x, z]\,[x, z]$$

(iii) Für jeden Gruppenhomomorphismus $f : G \to H$ gilt:

$$f([x_1, .., x_n]) = [f(x_1), .., f(x_n)] \quad , \quad x_1, .., x_n \in G$$

6.1.3 Lemma über den höheren Kommutator

Für Elemente $x, y, z \in G$ einer Gruppe G gilt:

$$\left(y\left[x, y^{-1}, z\right]y^{-1}\right)\left(z\left[y, z^{-1}, x\right]z^{-1}\right)\left(x\left[z, x^{-1}, y\right]x^{-1}\right) = 1$$

(vgl. Jacobi-Identität für Lie-Algebren).

6.1.4 Definition: Kommutator von Mengen

Für Gruppe G und Teilmengen $A, B \subseteq G$ setzt man

$$[A, B] := \langle [a, b] : a \in A,\ b \in B \rangle$$

Bemerkungen:

(i) Es ist $[A, B] = [B, A]$.

(ii) Für jeden Gruppenhomomorphismus $f : G \to H$ ist

$$f([A, B]) = [f(A), f(B)]$$

Sind A, B normale (charakteristische) Untergruppen von G, so ist auch $[A, B]$ eine normale (charakteristische) Untergruppe von G.

(iii) Es gilt die Äquivalenz:

$$[A, B] = \{1\} \ \Leftrightarrow\ ab = ba \ \forall\ a \in A,\ b \in B$$

6.1.5 Definition: Höherer Kommutator von Mengen

Für Gruppe G und Untermengen $A_1, .., A_n \subseteq G$ definiert man induktiv

$$[A_1, .., A_n] := [A_1, [A_2, .., A_n]]$$

wobei $[A] := A$.

Bemerkungen:

(i) $[A_1, .., A_n]$ enthält alle Elemente der Form $[a_1, .., a_n]$, $a_i \in A_i$, wird aber nicht unbedingt von diesen erzeugt.

(ii) Für jeden Gruppenhomomorphismus $f : G \to H$ ist

$$f([A_1, .., A_n]) = [f(A_1), .., f(A_n)]$$

6.1.6 Satz: Kommutator von Untergruppen

Für Untergruppen $A, B, C \leq G$ einer Gruppe G gilt stets:

1. $[A, B] \trianglelefteq \langle A, B \rangle$
2. Es ist $[A, B] \subseteq A$ genau dann wenn $\forall\ b \in B : \mathrm{ad}_b(A) \subseteq A$ (A wird von B *normalisiert*).
3. Ist $[A, B] \subseteq A$ und $[C, B] \subseteq C$ so folgt $[A, BC] = [A, B]\,[A, C]$.
4. Ist $[A, B, C] = [B, C, A] = 1$, so ist auch $[C, A, B] = 1$ (*3-Untergruppen-Lemma*).

6.1.7 Lemma: Kommutatoren von Faktorgruppen

Sei G eine Gruppe und $N \trianglelefteq G$. Dann:

a) Für $u, v \in G$ gilt

$$[uN, vN]_{G/N} = [u, v]_G\, N$$

b) Für Untermengen $U, V \subseteq G$ ist

$$[\{uN : u \in U\}, \{vN : v \in V\}] = \underbrace{\{gN : g \in [U, V]\}}_{[U,V]N/N}$$

Beweis:

1.
$$[uN, vN]_{G/N} \overset{\text{def.}}{=} (uN)(vN)(uN)^{-1}(vN)^{-1} = (uN)(vN)(u^{-1}N)(v^{-1}N) = \underbrace{(uvu^{-1}v^{-1})}_{[u,v]} N$$

2.
$$[\{uN : u \in U\}, \{vN : v \in V\}] = \left\langle [uN, vN]_{G/N} : u \in U,\ v \in V \right\rangle \overset{(1)}{=} \langle [u,v]\, N : u \in U,\ v \in V \rangle \overset{(4.1.2.1)}{=} \{gN : g \in [U,V]\}$$

□

6.1.8 Definition: Kommutatorgruppe

Für Gruppe G heißt
$$G' := G^{(1)} := [G,G] = \langle [g,h] : g,h \in G \rangle$$
Kommutatorgruppe von G. Ist $G' = G$, so heißt G *perfekt*.

Bemerkung: Für jeden Gruppenhomomorphismus $f : G \to H$ ist $f(G') = f(G)' \leq H$, insbesondere ist $G' \leq G$ vollinvariant.

6.1.9 Satz über die Kommutatorgruppe

Für jede Untergruppe $H \leq G$ einer Gruppe G sind folgende Aussagen äquivalent:

1. $G' \leq H$
2. $H \trianglelefteq G \ \wedge\ G/H$ abelsch.

6.1.10 Definition: Höhere Kommutatorgruppe

Die *höheren Kommutatorgruppen* einer Gruppe G definiert man induktiv:
$$G^{(0)} := G \quad , \quad G^{(i+1)} := \left[G^{(i)}, G^{(i)}\right] \quad , \quad i \in \mathbb{N}_0$$

Bemerkungen:

(i) Für $U \leq G$ und $n \in \mathbb{N}$ ist $U^{(n)} \leq G^{(n)}$.

(ii) Für jeden Gruppenhomomorphismus $f : G \to H$ und $n \in \mathbb{N}$ ist $f(G^{(n)}) = f(G)^{(n)} \leq H^{(n)}$. Insbesondere sind die $G^{(n)} \leq G$ vollinvariant.

(iii) Offenbar sind $G = G^{(0)} \geq G^{(1)} \geq G^{(2)} \geq \ldots$ Setzen dabei
$$G^{(\infty)} := \bigcap_{n \in \mathbb{N}} G^{(n)}$$

6.1.11 Definition: Auflösbare Gruppe

Eine Gruppe G mit $G^{(s)} = \{1\}$ für ein $s \in \mathbb{N}_0$ heißt *auflösbar*. Gegebenfalls heißt das kleinste $s \in \mathbb{N}_0$ mit $G^{(s)} = \{1\}$ die (*Auflösbarkeits-*)*Stufe* von G.

Bemerkungen:

(i) Auflösbarkeit und Auflösbarkeitsstufe sind Isomorphie-invariant.

(ii) Für Gruppe G mit Auflösbarkeitsstufe s gilt:

$$\begin{aligned} s = 0 &\Leftrightarrow G = \{1\} \\ s \leq 1 &\Leftrightarrow G' = \{1\} \Leftrightarrow G \text{ abelsch} \\ s \leq 2 &\Leftrightarrow G'' = \{1\} :\Leftrightarrow G \text{ meta-abelsch} \end{aligned}$$

(iii) Untergruppen und Faktorgruppen (vgl. Lemma 6.1.7 (2)) auflösbarer Gruppen sind auflösbar.

(iv) Gruppen G, H sind genau dann auflösbar, wenn $G \times H$ auflösbar ist, denn

$$(G \times H)^{(n)} = G^{(n)} \times H^{(n)} \quad , \quad n \in \mathbb{N}_0$$

(v) Sind $M, N \trianglelefteq G$ und $G/M, G/N$ auflösbar, so ist auch $G/(M \cap N)$ auflösbar, denn nach Bemerkung (iv) in Homomorphiesatz 4.1.8 ist $G/(M \cap N)$ zu einer Untergruppe von $G/M \times G/N$ isomorph.

(vi) Ist G auflösbar der Stufe s, so ist

$$G = G^{(0)} \trianglerighteq G^{(1)} \trianglerighteq G^{(2)} \trianglerighteq \cdots \trianglerighteq G^{(s)} = \{1\}$$

nach 6.1.9 und 4.1.14 (3) eine Normalreihe mit abelschen Faktoren.

6.1.12 Satz: Charakterisierung von Auflösbarkeit

Für eine Gruppe G sind äquivalent:

1. G ist auflösbar.
2. G hat eine Normalreihe mit abelschen Faktoren.
3. G hat eine Subnormalreihe mit abelschen Faktoren.

Beispiel: Für $n \in \mathbb{N}$ und jeden Körper $\mathbb{K}$ ist die Gruppe $\mathfrak{B}(n, \mathbb{K})$ (*Borelgruppe*) aller oberen Dreiecksmatrizen in $\mathrm{GL}(n, \mathbb{K})$ auflösbar.

6.1.13 Lemma über Auflösbarkeit der Faktorgruppe

Für jede Gruppe G und $N \trianglelefteq G$ gilt: G ist auflösbar $\Leftrightarrow$ $N, G/N$ sind auflösbar.

Bemerkung: Für auflösbare Normalteiler $M, N \trianglelefteq G$ einer Gruppe G ist auch MN ein auflösbarer Normalteiler von G. Dies folgt aus dem Lemma wegen $MN/N \cong M/(M \cap N)$ (vgl. 1. Isomorphiesatz 4.1.9). Ist G endlich, so ist das Produkt aller auflösbaren Normalteiler ein auflösbarer Normalteiler von G. Dieser heißt *auflösbares Radikal* von G.

6.1.14 Satz: Charakterisierung von Auflösbarkeit endlicher Gruppen

Für jede endliche Gruppe G sind äquivalent:

1. G ist auflösbar.
2. Jeder Kompositionsfaktor von G ist zu $\mathbb{Z}/p\mathbb{Z}$ für ein $p \in \mathbb{P}$ isomorph.
3. Jeder Hauptfaktor von G ist zu $(\mathbb{Z}/p\mathbb{Z})^n$ für geeignete $p \in \mathbb{P},\ n \in \mathbb{N}$ isomorph.

Bemerkung: Allgemein hat man folgende Auflösbarkeitskriterien:

(i) Für $p, q \in \mathbb{P},\ a, b \in \mathbb{N}_0$ ist jede Gruppe der Ordnung $p^a q^b$ auflösbar. (Burnsides, 1904)

(ii) Gruppen ungerader Ordnung sind stets auflösbar. (Feit-Thomson, 1963: *Odd order theorem*; Beweis ca. 250 Seiten)

6.2 Nilpotente Gruppen

6.2.1 Definition: Absteigende Zentralfolge

Für Gruppe G und $n \in \mathbb{N}$ definiert man induktiv

$$G_{(1)} := G \ \ , \ \ G_{(2)} := [G, G] \ , \ G_{(n+1)} := \left[G, G_{(n)}\right]$$

Bemerke:

(i) Für $n \in \mathbb{N}$ ist $G_{(n)} = [\underbrace{G, G, ..., G}_{\times n}]$.

(ii) Für $U \leq G$ und $n \in \mathbb{N}$ ist $U_{(n)} \leq G_{(n)}$.

(iii) Für Gruppenhomomorphismus $f : G \to H$ gilt

$$f(G_{(n)}) = f(G)_{(n)} \leq H_{(n)} \ , \ n \in \mathbb{N}$$

Daher sind die $G_{(n)}$ vollinvariant in G, insbesondere jeweils $G_{(n)} \trianglelefteq G$, also $G_{(n+1)} \leq G_{(n)}$ nach Satz 6.1.6 (2). Wir erhalten so eine Folge vollinvarianter Untergruppen

$$G = G_{(1)} \trianglerighteq G_{(2)} \trianglerighteq G_{(3)} \trianglerighteq \dots$$

die sogenannte *absteigende Zentralfolge* von G. Setzen dabei

$$U_{(\infty)} := \bigcap_{n \in \mathbb{N}} G_{(n)}$$

(iv) Für $n \in \mathbb{N}$ ist

$$\left[G/G_{(n+1)},\ G_{(n)}/G_{(n+1)}\right] = \left[G, G_{(n)}\right] G_{(n+1)}/G_{(n+1)} = G_{(n+1)}/G_{(n+1)} = \left\{1_{G/G_{(n+1)}}\right\}$$

das heißt

$$G_{(n)}/G_{(n+1)} \subseteq Z(G/G_{(n+1)})$$

Dies erklärt den Begriff *Zentralfolge*.

6.2.2 Satz: Darstellung von $G_{(n)}$

Für Gruppe G und $n \in \mathbb{N}$ gilt stets:

$$G_{(n)} = \langle [g_1, .., g_n] : g_1, .., g_n \in G \rangle$$

Beachte: Nicht so offensichtlich!

6.2.3 Lemma über $G_{(n)}$

Für Gruppe G und $n, m \in \mathbb{N}$ gilt stets:

1. $\left[G_{(n)}, G_{(m)}\right] \subseteq G_{(n+m)}$
2. $G^{(n)} \subseteq G_{(2^n)}$.

6.2.4 Definition: Aufsteigende Zentralfolge

Für jede Gruppe G definiert man die *aufsteigende Zentralfolge* induktiv durch $Z_0(G) := \{1\}$, $Z_1(G) := Z(G)$ und

$$Z_n(G)/Z_{n-1}(G) := Z\left(G/Z_{n-1}(G)\right) \quad , \quad i \in \mathbb{N}$$

Beachte dass Z_n nach Lemma 4.1.15 wohldefiniert ist.

Bemerkungen:

(i) Für $i \in \mathbb{N}_0$ ist $Z_i(G) \leq G$ charakteristisch. Dies ist für die Fälle $i = 0, 1$ klar. Ist $Z_{i-1}(G)$ charakteristisch für ein $i \in \mathbb{N}_0$, so folgt nach Lemma 4.1.15 (7) dass auch $Z_i(G)$ charakteristisch ist (da $\underbrace{Z(G/Z_{i-1}(G))}_{Z_i(G)/Z_{i-1}(G)} \leq G/Z_{i-1}(G)$ charakteristisch).

(ii) Es ist tatsächlich

$$1 = Z_0(G) \subseteq Z_1(G) \subseteq Z_2(G) \subseteq \dots$$

Setzt man

$$Z_\infty(G) := \bigcup_{i \in \mathbb{N}_0} Z_i(G)$$

so heißt $Z_\infty(G)$ *Hyperzentrum* von G. Dabei ist wieder $Z_\infty(G) \leq G$ charakteristisch.

6.2.5 Definition: Nilpotente Gruppe

Eine Gruppe G mit $Z_c(G) = G$ für ein $c \in \mathbb{N}_0$ heißt *Nilpotent*. Gegebenfalls heißt das kleinste $c \in \mathbb{N}_0$ mit $Z_c(G) = G$ (*Nilpotenz-*)*Klasse* von G.

Bemerke:

$$c = 0 \Leftrightarrow G = \{1\}$$
$$c \leq 1 \Leftrightarrow G \text{ abelsch}$$

6.2.6 Definition: Zentralreihe

Eine Normalreihe

$$G = G_0 \trianglerighteq G_1 \trianglerighteq G_2 \trianglerighteq \cdots \trianglerighteq G_r = \{1\}$$

einer Gruppe G mit

$$G_{i-1}/G_i \subseteq Z(G/G_i) \quad \forall\, i = 1, .., r$$

heißt *Zentralreihe* von G.

Beispiel: Ist G nilpotent der klasse c, so ist

$$G = Z_c(G) \trianglerighteq Z_{c-1}(G) \trianglerighteq \cdots \trianglerighteq Z_0(G) = \{1\}$$

eine Zentralreihe, die (*obere*) *Zentralreihe* von G.

6.2.7 Satz: Charakterisierung von Zentralreihen

Für Untergruppen $G_0, .., G_r$ einer Gruppe G mit

$$G = G_0 \geq G_1 \geq \cdots \geq G_r = \{1\}$$

sind äquivalent:

1. $G = G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_r = \{1\}$ ist eine Zentralreihe.
2. $[G, G_{i-1}] \subseteq G_i, \quad i = 1, .., r$

Bemerkung: Wegen (2) ist jede Verfeinerung einer Zentralreihe wieder eine.

6.2.8 Satz über Zentralreihen

Sei $G = G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_r = \{1\}$ eine Zentralreihe einer Gruppe G. Für $i = 0, .., r$ ist dann

$$G_{r-i} \subseteq Z_i(G) \quad \wedge \quad G_{(i+1)} \subseteq G_i$$

Insbesondere ist $Z_r(G) = G$ und $G_{(r+1)} = \{1\}$, das heißt G ist nilpotent mit Klasse höchstens r.

Bemerkungen:

(i) Nach Beispiel in 6.2.6 und Satz 6.2.8 ist eine Gruppe G genau dann nilpotent, wenn sie eine Zentralreihe hat. Gegebenfalls ist die Nilpotenzklasse c von G durch die Länge $r \geq c$ der Zentralreihe beschränkt.

(ii) Für jede nilpotente Gruppe G der Klasse c ist $G_{(c+1)} = \{1\}$ (Anwendung des Satzes auf die aufsteigende Zentralfolge). Daher ist

$$G = G_{(1)} \trianglerighteq G_{(2)} \trianglerighteq \cdots \trianglerighteq G_{(c+1)} = \{1\}$$

eine Zentralreihe (Satz 6.2.7 (2)), die *absteigende* (*untere* (vgl. 6.2.8)) *Zentralreihe* von G. Nach (i) ist ferner $G_{(c)} \neq \{1\}$.

(iii) Eine Gruppe G ist genau dann nilpotent, wenn $G_{(s)} = \{1\}$ für ein $s \in \mathbb{N}$ ist.

(iv) Untergruppen und Faktorgruppen einer nilpotenten Gruppe G sind wieder nilpotent. Ihre Klasse ist jeweils durch die Klasse von G beschränkt.

(v) Jede nilpotente Gruppe ist auflösbar.

Beachte: Die Umkehrung der Aussage gilt im allgemeinen nicht. So ist z.B. Sym(3) auflösbar, aber wegen $Z(\mathrm{Sym}(3)) = 1$ nicht nilpotent.

(vi) Die Hauptfaktoren einer endlichen, nilpotenten Gruppe haben Primzahlordnung: Durch Verfeinerung der oberen Zentralreihe erhält man nämlich eine Kompositionsreihe, die gleichzeitig Zentralreihe ist (Anwendung des Satzes 6.2.7). Diese ist insbesondere eine Normalreihe und damit eine Hauptreihe[1]. Da G auflösbar ist, haben ihre Faktoren nach Satz 6.1.14 Primzahlordnung.

Beispiel: Eine typische nilpotente Gruppe ist die Untergruppe von $\mathrm{GL}(n, \mathbb{K})$ (für $n \in \mathbb{N}$, $\mathbb{K}$ Körper), die aus allen Matrizen der folgenden Form besteht:

$$\begin{pmatrix} 1 & * & \dots & * \\ 0 & 1 & \dots & * \\ & & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix}$$

6.2.9 Definition: Normalisator

Für jede Teilmenge $X \subseteq G$ einer Gruppe G ist

$$\mathcal{N}_G(X) := \left\{ g \in G : gXg^{-1} = X \right\} \leq G$$

der *Normalisator* von X (in G). Ist $X \leq G$, so ist per Konstruktion $X \trianglelefteq \mathcal{N}_G(X)$.

6.2.10 Satz: Normalizatoren in nilpotenten Gruppen

Für jede echte Untergruppe U einer nilpotenten Gruppe G ist $U < \mathcal{N}_G(U)$.

[1] Kompositionsreihen die Normalreihen sind, sind insbesondere Hauptreihen.

6.2.11 Satz: Normalteiler in nilpotenten Gruppen

Für jeden Normalteiler $\{1\} \neq N \trianglelefteq G$ einer nilpotenten Gruppe G ist $[G, N] < N$ und $Z(G) \cap N \neq \{1\}$.

Folgerung: Insbesondere liegt jeder minimale Normalteiler einer Gruppe im Zentrum, denn

$$1 \neq (N \cap Z(G)) \trianglelefteq N$$

6.2.12 Satz über nilpotente Normalteiler

Für nilpotente Normalteiler $A, B \trianglelefteq G$ einer Gruppe G ist auch AB ein nilpotenter Normalteiler von G. Hat A die Klasse a und B die Klasse b, so hat AB höchstens die Klasse $a + b$.

Bemerkung: Eine Gruppe G die einen nilpotenten Normalteiler $N \trianglelefteq G$ mit nilpotenter Faktorgruppe G/N besitzt, ist **nicht** unbedingt nilpotent. Beispiel:

$$N := \left\langle \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \right\rangle \trianglelefteq \mathrm{Sym}(3)$$

7 Gruppenoperationen

7.0.13 Definition: Gruppenoperation

Eine (*Links-*)*Operation* (*Wirkung*, engl. *action*) einer Gruppe G auf eine Menge Ω ist eine Abbildung

$$G \times \Omega \to \Omega \quad , \quad (g, \omega) \mapsto {}^g\omega$$

mit den Eigenschaften:

$${}^1\omega = \omega \quad , \quad {}^g({}^h\omega) = {}^{gh}\omega \quad \forall\ \omega \in \Omega,\ g, h \in G$$

Man sagt auch: G *operiert* auf Ω, oder Ω ist eine *G-Menge*.

Bemerkungen:

(i) Rechtsoperationen definiert man analog als Abbildungen $\Omega \times G \to \Omega,\ (\omega, g) \mapsto \omega^g$.

(ii) Man beachte die Analogie zur Multiplikation von Vektoren eines $\mathbb{K}$-Vektorraumes mit Skalaren aus einem Körper.

Beispiele:

(i) Für jede Menge Ω operiert $\mathrm{Sym}(\Omega)$ auf Ω durch

$${}^g\omega := g(\omega) \quad , \quad \omega \in \Omega,\ g \in \mathrm{Sym}(\Omega)$$

(ii) Für jeden Körper $\mathbb{K}$ und $\mathbb{K}$-Vektorraum V operiert

$$\mathrm{GL}(V) := \{f : V \to V \mid f \text{ linear, bijektiv}\}$$

auf V durch ${}^g v := g(v),\ g \in \mathrm{GL}(V),\ v \in V$.

(iii) Für $n \in \mathbb{N}$ und jedem Körper $\mathbb{K}$, operiert $\mathrm{GL}(n, \mathbb{K})$ auf $\mathbb{K}^{n\times n}$ durch

$${}^A B := ABA^{-1} \quad , \quad A \in \mathrm{GL}(n, \mathbb{K}),\ B \in \mathbb{K}^{n\times n}$$

(iv) Für $n, m \in \mathbb{N}$ und jeden Körper $\mathbb{K}$ operiert

$$\mathrm{GL}(m, \mathbb{K}) \times \mathrm{GL}(n, \mathbb{K})$$

auf $\mathbb{K}^{m\times n}$ durch

$${}^{(A,B)}C := ACB^{-1} \quad , \quad A \in \mathrm{GL}(m, \mathbb{K}),\ B \in \mathrm{GL}(n, \mathbb{K}),\ C \in \mathbb{K}^{m\times n}$$

(v) Für $n \in \mathbb{N}$ operiert die *orthogonale Gruppe*

$$O(n) := \left\{A \in \mathbb{R}^{n\times n} : AA^T = 1_n\right\}$$

des Grades n auf der Menge S aller reellen, symmetrischen $n \times n$-Matrizen durch

$${}^A B := ABA^T \quad , \quad A \in O(n),\ B \in S$$

(vi) Analog operiert die *unitäre Gruppe*

$$U(n) := \left\{A \in \mathbb{C}^{n\times n} : A\overline{A}^T = 1_n\right\}$$

des Grades n auf die Menge H aller *hermiteschen* $n \times n$ Matrizen $B = \overline{B}^T$ durch

$${}^A B = AB\overline{A}^T \quad , \quad A \in U(n),\ B \in H$$

7.0.14 Lemma über Gruppenoperationen

Für Gruppe G, G-Menge Ω und $g \in G$ ist

$$\tau_g : \Omega \to \Omega \quad , \quad \tau_g(\omega) := {}^g\omega$$

bijektiv mit $\tau_g^{-1} = \tau_{g^{-1}}$. Die Zuordnung

$$\tau : G \to \mathrm{Sym}(\Omega) \quad , \quad g \mapsto \tau_g$$

ist ferner homomorph.

7.0.15 Lemma: Induzierung von Gruppenoperationen

Seien G eine Gruppe, Ω eine Menge und $\tau : G \to \mathrm{Sym}(\Omega)$ ein Homomorphismus. Dann erhält man durch

$${}^g\omega := \tau(g)(\omega) \quad , \quad g \in G,\ \omega \in \Omega$$

eine Operation von G auf Ω.

Bemerkung: Nach Lemmas 7.0.14 und 7.0.15 induziert jede G-Operation auf Ω einen Homomorphismus $G \to \mathrm{Sym}(\Omega)$. Umgekehrt, induziert jeder Homomorphismus $G \to \mathrm{Sym}(\Omega)$ eine Operation von G auf Ω. Es ist klar, dass beide Zuordnungen zu einander invers sind.

7.0.16 Definition: Kern der Gruppenoperation

Die Gruppe G operiere auf der Menge Ω, dazu sei $\tau : G \to \mathrm{Sym}(\Omega)$ der entsprechende Homomorphismus. Dann heißt

$$\ker(\tau) := \{g \in G : \tau_g = \mathrm{Id}_\Omega\} = \{g \in G : {}^g\omega = \omega \ \ \forall\, \omega \in \Omega\}$$

Kern der Operation. Ist $\ker(\tau) = G$, das heißt ${}^g\omega = \omega \ \ \forall\, g \in G,\ \omega \in \Omega$, so heißt die Operation *trivial*. Ist $\ker(\tau) = \{1\}$, das heißt τ injektiv, so heißt die Operation *treu*. Gegebenfalls gilt dann $G \cong \tau(G) \leq \mathrm{Sym}(\Omega)$.

7.0.17 Satz von Caley

Jede Gruppe ist zu einer Untergruppe einer symmetrischen Gruppe isomorph:

$$G \cong U \leq \mathrm{Sym}(G)$$

Beweis: Suchen Ω, so dass G auf Ω operiert. Setzen dazu $\Omega := G$ und

$${}^g\omega := g\omega \quad , \quad g \in G,\ \omega \in \Omega$$

Diese Operation ist treu, denn aus ${}^g g = g$ folgt $g = 1$. Mit den obigen Bezeichnungen gilt dann

$$G \cong \tau(G) \leq \mathrm{Sym}(G)$$

□

7.0.18 Definition: Äquivalenz auf G-Mengen

Die Gruppe G operiere auf der Menge Ω. Für $\alpha, \beta \in \Omega$ schreibt man $\alpha \sim_G \beta \ :\Leftrightarrow$

$$\exists\, g \in G \ : \ {}^g\alpha = \beta$$

Bemerke: Die Relation $\sim_G$ auf Ω ist eine Äquivalenzrelation, das heißt für $\alpha, \beta, \gamma \in \Omega$ gilt:

- Reflexivität: $\alpha \sim_G \alpha$
- Symmetrie: $\alpha \sim_G \beta \;\Leftrightarrow\; \beta \sim_G \alpha$
- Transitivität: $\alpha \sim_G \beta \;\wedge\; \beta \sim_G \gamma \;\Rightarrow\; \alpha \sim_G \gamma$

7.0.19 Definition: Bahn

Die Gruppe G operiere auf Ω. Dann ist für $\alpha \in \Omega$ die *Bahn* (engl. *orbit*)

$$\mathrm{Orb}_G(\alpha) := \{{}^g\alpha : g \in G\}$$

die Äquivalenzklasse von α bzgl. $\sim_G$. Dabei heißt $|\mathrm{Orb}_G(\alpha)|$ *Länge* der Bahn von α.

Bemerkungen: Tatsachen über Äquivalenzklassen folgt, dass Ω die disjunkte Vereinigung der verschiedenen Bahnen von G auf Ω ist. Für beliebiges Repräsentantensystem $\mathscr{R}$ dieser Bahnen gilt also

$$\Omega = \biguplus_{\rho \in \mathscr{R}} \mathrm{Orb}_G(\rho)$$

und

$$|\Omega| = \sum_{\rho \in \mathscr{R}} |\mathrm{Orb}_G(\rho)| \tag{7.0.19.1}$$

(*Bahnengleichung*).

Beispiele:

(i) Für $n \in \mathbb{N}$ und Körper $\mathbb{K}$ liegen zwei Matrizen aus $\mathbb{K}^{n\times n}$ genau dann in der gleichen Bahn der Operation von $\mathrm{GL}(n,\mathbb{K})$ auf $\mathbb{K}^{n\times n}$

$${}^A B := ABA^{-1} \quad , \quad A \in \mathrm{GL}(n,\mathbb{K}),\ B \in \mathbb{K}^{n\times n}$$

wenn sie *ähnlich* sind (Definition).

(ii) Für $m, n \in \mathbb{N}$ und jeden Körper $\mathbb{K}$ liegen zwei Matrizen $\mathbb{K}^{n\times n}$ genau dann in der gleichen Bahn der Operation von $\mathrm{GL}(m,\mathbb{K}) \times \mathrm{GL}(n,\mathbb{K})$ auf $\mathbb{K}^{m\times n}$:

$${}^{(A,B)}C := ACB^{-1} \quad , \quad A \in \mathrm{GL}(m,\mathbb{K}),\ B \in \mathrm{GL}(n,\mathbb{K}),\ C \in \mathbb{K}^{m\times n}$$

wenn sie *äquivalent* sind (Definition).

(iii) In der Theorie konservativer Hamiltonscher Systeme werden Flüsse $(\varphi_t)_{t\in\mathbb{R}}$ von Vektorfeldern (e.g. Bahngleichungen) oft als Operation von $(\mathbb{R}, +)$ auf das System M abstrahiert:

$$\varphi_t \circ \varphi_s := \varphi_{t+s} \in \mathrm{Sym}(M)$$

Die Bahnen $\mathrm{Orb}_{\mathbb{R}}(x_0) = \{\varphi_t(x_0) : t \in \mathbb{R}\}$ sind genau die Bahnen die die Teilchen unter der Wirkung des Vektorfeldes durchlaufen.

7.0.20 Definition: Stabilisator

Die Gruppe G operiere auf Ω. Dann heißt für $\omega \in \Omega$ die Menge

$$\mathrm{St}_G(\omega) := G_\omega := \{g \in G : {}^g\omega = \omega\}$$

Stabilisator von ω in G.

7.0.21 Satz über den Stabilisator

Die Gruppe G operiere auf Ω. Dann gilt:

(i) Für jedes $\omega \in \Omega$ ist $\mathrm{St}_G(\omega) \leq G$ und $\mathrm{St}_G(\omega)$ operiert auf $\Omega \setminus \{\omega\}$.

(ii) Für $g \in G,\ \omega \in \Omega$ gilt
$$\mathrm{ad}_g\left(\mathrm{St}_G(\omega)\right) = \mathrm{St}_G({}^g\omega)$$

(iii) Die Abbildung
$$f : G/\mathrm{St}_G(\omega) \to \mathrm{Orb}_G(\omega) \quad , \quad g\,\mathrm{St}_G(\omega) \mapsto {}^g\omega$$
ist bijektiv. Insbesondere ist
$$|\mathrm{Orb}_G(\omega)| = |G : \mathrm{St}_G(\omega)|$$
Im Fall $|G| < \infty$ ist also jede Bahnlänge ein Teiler von $|G|$.

7.0.22 Definition: Transitivität von Gruppenoperationen

Eine Gruppenoperation von G auf eine Menge $\Omega \neq \emptyset$ heißt *transitiv*, falls Ω nur eine einzige Bahn besitzt.

Bemerkung: Eine G-Menge $\Omega \neq \emptyset$ ist genau dann transitiv, wenn
$$\forall\ \alpha, \beta \in \Omega\ :\ \exists\ g \in G\ :\ {}^g\alpha = \beta$$
Gegebenfalls ist dann nach Satz 7.0.21 (iii):
$$|\Omega| = |G : \mathrm{St}_G(\omega)| \quad , \quad \omega \in \Omega$$
Existiert zu je zwei $\alpha, \beta \in \Omega$ genau ein $g \in G$ mit ${}^g\alpha = \beta$, so heißt die Operation *regulär*. Gegebenfalls ist dann $|\Omega| = |G|$.

Beispiel: Für jede Gruppe G und $H \leq G$ operiert G transitiv auf G/H durch
$${}^g(\omega H) := g\omega H \quad , \quad g, \omega \in G$$
Dabei gilt:
$${}^g(\omega H) = \omega H \ \Leftrightarrow\ \omega^{-1} g \omega H = H \ \Leftrightarrow\ \omega^{-1} g \omega \in H \ \Leftrightarrow\ g \in \omega H \omega^{-1} = \mathrm{ad}_\omega(H)$$
Daher ist $\mathrm{St}_G(\omega H) = \mathrm{ad}_\omega(H)$. Insbesondere also $\mathrm{St}_G(H) = H$ und der Kern der Operation von G auf G/H ist
$$\bigcap_{\omega \in G} \mathrm{St}_G(\omega H) = \bigcap_{\omega \in G} \mathrm{ad}_\omega(H) =: \underbrace{\mathrm{Core}_G(H)}_{\trianglelefteq G} \tag{7.0.22.1}$$
der *Kern* von H in G. Offenbar ist $\mathrm{Core}_G(H)$ der größte Normalteiler $N \trianglelefteq G$ von G mit $N \subseteq H$ und $G/\mathrm{Core}_G(H)$ ist zu einer Untergruppe von $\mathrm{Sym}(G/H)$ isomorph. Auf diese Weise lassen sich oft nicht-triviale Normalteiler von G konstruieren.

7.0.23 Frattini-Argument

Die Gruppe G operiere auf $\Omega \neq \emptyset$, und es sei $H \leq G$. Operiert H auf Ω transitiv, so ist
$$G = H \cdot \mathrm{St}_G(\omega) \quad \forall\ \omega \in \Omega$$

Beweis: Seien $\omega \in \Omega,\ g \in G$. Da H transitiv ist, ist
$$\underbrace{{}^h({}^g\omega)}_{{}^{hg}\omega} = \omega$$
für irgendein $h \in H$, das heißt $hg \in \mathrm{St}_G(\omega)$ bzw.
$$g = h^{-1}(hg) \in H \cdot \mathrm{St}_G(\omega)$$
□

7.0.24 Definition: Fixpunkte

Seien G eine Gruppe, Ω eine G-Menge, $x \in G$ und $Y \subseteq G$. Dann heißen die Elemente in

$$\mathrm{Fix}_\Omega(x) := \{\omega \in \Omega : {}^x\omega = \omega\}$$

bzw.

$$\mathrm{Fix}_\Omega(Y) := \{\omega \in \Omega : {}^y\omega = \omega \ \ \forall\ y \in Y\}$$

Fixpunkte von x bzw. Y.

7.0.25 Burnside's Lemma

Seien G eine endliche Gruppe die auf der endlichen Menge Ω operiere. Dann:

1. Für die Anzahl n der Bahnen von G auf Ω gilt:

$$n = \frac{1}{|G|}\sum_{g\in G} |\mathrm{Fix}_\Omega(g)|$$

   (*durchschnittliche Anzahl von Fixpunkten*).

2. Ist die Operation transitiv und $\omega \in \Omega$, so gilt für die Anzahl m der Bahnen von $\mathrm{St}_G(\omega)$ auf Ω:

$$m = \frac{1}{|G|}\sum_{g\in G} |\mathrm{Fix}_\Omega(g)|^2$$

7.0.26 Definition: n-Transitivität

Die Gruppe G operiere auf der Menge Ω und sei $|\Omega| \geq n \in \mathbb{N}$. Dann heißt die Operation *n-transitiv*, falls zu je zwei n-Tupeln $(\alpha_1, .., \alpha_n),\ (\beta_1, .., \beta_n) \in \Omega^n$ mit jeweils paarweise verschiedenen Elementen (d.h. $\alpha_1, .., \alpha_n$ p.w. und $\beta_1, .., \beta_n$ p.w.) ein $g \in G$ existiert mit ${}^g\alpha_1 = \beta_1, .., {}^g\alpha_n = \beta_n$.

Bemerke: Jede $n \geq 2$-transitive Operation ist auch $(n-1)$-transitiv.

7.0.27 Satz über n-Transitivität

Die Gruppe G operiere auf der Menge Ω. Dann gilt:

1. Ist $n \geq 2$, G n-transitiv auf Ω und $\omega \in \Omega$, so operiert $\mathrm{St}_G(\omega)$ $(n-1)$-transitiv auf $\Omega \setminus \{\omega\}$.
2. Ist $n \geq 2$, G transitiv auf Ω, $\omega \in \Omega$ und $\mathrm{St}_G(\omega)$ $(n-1)$-transitiv auf $\Omega \setminus \{\omega\}$, so operiert G n-transitiv auf Ω.
3. Ist G transitiv auf Ω, $\omega \in \Omega$ und $H := \mathrm{St}_G(\omega)$, so gilt:
   G operiert 2-transitiv $\Leftrightarrow |H \setminus G/H| = 2$ (vgl. 3.3.15.1).
4. Operiert die Gruppe G transitiv auf Ω und sind Ω, G endlich, so gilt:
   G operiert 2-transitiv auf $\Omega \Leftrightarrow \frac{1}{|G|}\sum_{g\in G} |\mathrm{Fix}_\Omega(g)|^2 = 2$.

7.0.28 Satz: Zerlegung transitiver G-Mengen

Für jede Gruppe G und transitive G-Menge Ω mit $|\Omega| \geq 2$ sind äquivalent:

1. $\exists\ \Delta \subsetneq \Omega$ derart, dass $|\Delta| > 1$ und

$$\forall\ g \in G\ :\ ({}^g\Delta) \cap \Delta = \emptyset\ \vee\ {}^g\Delta = \Delta$$

2. $\exists$ eine disjunkte Zerlegung $\Omega = \biguplus_{\Lambda\in\mathcal{L}} \Lambda$, wobei $\Lambda \subsetneq \Omega,\ |\Lambda| > 1$ und ${}^g\Lambda \in \mathcal{L}$ für $g \in G, \Lambda \in \mathcal{L}$.

Bemerke: In der obigen Situation operiert G auch transitiv auf $\mathcal{L}$. Sind nämlich $\Lambda, \Delta \in \mathcal{L}$ so seien $\alpha \in \Lambda, \beta \in \Delta, g \in G$ mit ${}^g\alpha = \beta$. Dann $({}^g\Lambda) \cap \Delta \neq \emptyset \;\Rightarrow\; {}^g\Lambda = \Delta$. Für $\Lambda \in \mathcal{L}$ ist

$$|\mathcal{L}| = |G : \mathrm{St}_G(\Lambda)|$$

und

$$|\Omega| = |\Lambda| \cdot |\mathcal{L}| = |\Lambda| \cdot |G : \mathrm{St}_G(\Lambda)|$$

(da alle $\Lambda \in \mathcal{L}$ gleiche Anzahl an Elementen haben). Für $\lambda \in \Lambda$ ist ferner $\mathrm{St}_G(\lambda) \subseteq \mathrm{St}_G(\Lambda)$ wie man leicht nachrechnet.

7.0.29 Definition: Primitive Operation

Die Gruppe G operiere transitiv auf Ω. Sind die Bedingungen (1), (2) aus Satz 7.0.28 erfüllt, so heißt die Operation *imprimitiv*, sonst *primitiv*.

Bemerke: Die Definition macht nur Sinn, wenn die Operation transitiv ist, da sie sonst ohnehin imprimitiv wäre[2].

Beispiel: Ist $|\Omega| \in \mathbb{P}$, so ist jede transitive Operation auf Ω primitiv, denn die Bedingung $|\Omega| \neq |\Lambda| \neq 1$ und $|\Lambda| \;\big|\; |\Omega|$ widersprechen sich.

7.0.30 Satz: Charakterisierung von Primitivität

Für jede Gruppe G und transitive G-Menge Ω mit $|\Omega| \geq 2$ sind äquivalent:

1. Ω ist primitiv.
2. $\mathrm{St}_G(\omega)$ ist für jedes $\omega \in \Omega$ eine maximale Untergruppe von G.
3. $\mathrm{St}_G(\omega)$ ist für ein $\omega \in \Omega$ eine maximale Untergruppe von G.

7.0.31 Satz über primitive Operationen

Seien G eine Gruppe, $N \trianglelefteq G$ und Ω eine primitive G-Menge. Dann operiert N entweder transitiv oder trivial auf Ω.

7.0.32 Satz: Primitivität 2-transitiver Gruppenoperationen

Jede 2-transitive Operation einer Gruppe G auf einer Menge Ω ist primitiv.

7.0.33 Bemerkung: Operation von Faktorgruppen

Die Gruppe G operiere auf der Menge Ω, dazu der Homomorphismus $\tau : G \to \mathrm{Sym}(\Omega)$. Operiert $U \trianglelefteq G$ trivial auf Ω (d.h. $U \leq \ker(\tau)$), so operiert auch G/U auf Ω durch

$${}^{gU}\omega := {}^g\omega \quad , \quad g \in G,\ \omega \in \Omega$$

Dabei sind n-Transitivität bzw. Primitivität von G äquivalent zur n-Transitivität bzw. Primitivität von G/U. Ferner operiert G/U genau dann treu auf Ω, wenn $U = \ker(\tau)$.

[2] Falls $|\Omega| > 2$.

8 Spezielle Gruppen

8.1 Sylowgruppen

8.1.1 Definition: Konjugation

Jede Gruppe G operiert auf sich selbst durch *Konjugation*:

$$ {}^g x := gxg^{-1} \quad , \quad g, x \in G $$

Dabei heißt

$$ \mathrm{Orb}_G(x) = \{ gxg^{-1} : g \in G \} $$

Konjugationsklasse von x in G. Liegen $x, y \in G$ in der gleichen Konjugationsklasse, das heißt $\exists\, g \in G : y = gxg^{-1}$, so heißen x, y *konjugiert* (in G). Notation $x \sim_G y$ oder $x \sim y$.

Für $x \in G$ heißt

$$ \mathrm{St}_G(x) = \{ g \in G : gxg^{-1} = x \} = \{ g \in G : gx = xg \} =: C_G(x) \tag{8.1.1.1} $$

Zentralisator von x in G. Nach Satz 7.0.21 (iii) enthält die Konjugationsklasse von x in G genau $|G : C_G(x)|$ Elemente. Ist $\mathscr{R}$ ein Repräsentationssystem für die Konjugationsklassen, so erhält die Bahngleichung (7.0.19.1) die Form

$$ |G| = \sum_{x \in \mathscr{R}} |G : C_G(x)| \overset{(3.3.6)}{=} \sum_{x \in \mathscr{R}} \frac{|G|}{|C_G(x)|} \tag{8.1.1.2} $$

(*Klassengleichung*). Die Anzahl $|\mathscr{R}|$ der Konjugationsklassen heißt *Klassenzahl* von G. Die Konjugationsklasse von x in G ist genau dann einelementig, wenn $|G : C_G(x)| = 1$, das heißt $G = C_G(x)$. Dies ist äquivalent zu $x \in Z(G)$.

Bemerkung: Nach Satz 7.0.21 (ii) über Stabilisatoren gilt für beliebige $x, y \in G$:

$$ C_G(\mathrm{ad}_y\, x) = \mathrm{ad}_y(C_G(x)) $$

Beispiel: Jeder Normalteiler $N \trianglelefteq G$ ist Vereinigung von Konjugationsklassen

$$ N = \bigcup_{x \in N} \mathrm{Orb}_G(x) $$

8.1.2 Satz von Landau

Für jede endliche Gruppe G mit Klassenzahl k gilt $|G| \leq k^{2^{k-1}}$.

Beweis: Seien $x_1, x_2, .., x_k = 1$ Repräsentanten für die Konjugationsklassen und sei

$$ n_i := |C_G(x_i)| \quad , \quad i = 1, .., k $$

o.B.d.A. $n_1 \leq n_2 \leq \cdots \leq n_k = |G|$. Wegen (8.1.1.2) ist

$$ \frac{k}{n_1} \geq \frac{1}{n_1} + \frac{1}{n_2} + \ldots \frac{1}{n_k} = 1 $$

das heißt $n_1 \leq k$. Daher

$$ \frac{k}{n_2} \geq \frac{1}{n_2} + \cdots + \frac{1}{n_k} = 1 - \frac{1}{n_1} \geq \frac{1}{n_1} \geq \frac{1}{k} $$

das heißt $n_2 \leq k^2$. Daher

$$ \frac{k}{n_3} \geq \frac{1}{n_3} + \cdots + \frac{1}{n_k} = 1 - \frac{1}{n_1} - \frac{1}{n_2} \geq \frac{1}{n_1 n_2} \geq \frac{1}{k^3} $$

das heißt $n_3 \leq k^4$. Daher

$$ \frac{k}{n_4} \geq \frac{1}{n_4} + \cdots + \frac{1}{n_k} = 1 - \frac{1}{n_1} - \frac{1}{n_2} - \frac{1}{n_3} \geq \frac{1}{n_1 n_2 n_3} \geq \frac{1}{k^7} $$

das heißt $n_4 \leq k^8$. Induktiv zeigt man allgemein $n_i \leq k^{2^{i-1}}$, $i = 1, .., k$. Insbesondere $|G| = n_k = k^{2^{k-1}}$.

Beispiel $k = 1$**:** Dann ist $|G| = 1$.

Beispiel $k = 2$**:** Dann hat $\frac{1}{n_1} + \frac{1}{n_2} = 1$ nur die Lösung $n_1 = n_2 = 2$. Also $|G| = 2$.

Beispiel $k = 3$**:** Aus $\frac{1}{n_1} + \frac{1}{n_2} + \frac{1}{n_3} = 1$ folgt zunächst $n_1 \in \{2, 3\}$.

- Fall $n_1 = 2$. Dann $\frac{1}{n_2} + \frac{1}{n_3} = \frac{1}{2}$, also $n_2 \in \{3, 4\}$.
  - Fall $n_2 = 3$, dann $n_3 = 6$, das heißt $|G| = 6$.
  - Für $n_2 = 4$ ist $n_3 = 4$. Dies ist aber unmöglich (Gruppen der Ordnung 4 sind abelsch, d.h. G hätte 4 Konjugationsklassen).
- Fall $n_1 =$. Dann $\frac{1}{n_2} + \frac{1}{n_3} = \frac{2}{3}$ das heißt $n_2 = 3 = n_3$, also $|G| = 3$.

8.1.3 Definition: p-Gruppe

Sei $p \in \mathbb{P}$. Eine endliche Gruppe deren Ordnung eine p-Potenz ist, heißt p-Gruppe. Ein Gruppenelement, dessen Ordnung eine p-Potenz ist, heißt p-Element.

8.1.4 Satz: Nilpotenz von p-Gruppen

Für $p \in \mathbb{P}$ ist jede endliche p-Gruppe nilpotent.

Spezialfolgerung: Für endliche p-Gruppe G ist insbesondere $Z(G) \neq \{1\}$.

8.1.5 Satz über endliche p-Gruppen

Für $p \in \mathbb{P}$ und jede endliche p-Gruppe G gilt:

1. $|G : Z(G)| \neq p$
2. $|G| = p^2 \;\Rightarrow\; G$ abelsch.

8.1.6 Konjugation auf Gruppen-Potentzmengen

Jede Gruppe G operiert auf $\mathscr{P}(G)$ durch *Konjugation*:

$$^gX := gXg^{-1} := \left\{gxg^{-1} : x \in X\right\} \quad , \quad g \in G,\ X \in \mathscr{P}(G)$$

Dabei heißt

$$\mathrm{Orb}_G(X) := \left\{gXg^{-1} : g \in G\right\}$$

Konjugationsklasse von X in G. Liegen $X, Y \in \mathscr{P}(G)$ in der gleichen Konjugationsklasse, das heißt $\exists\, g \in G$ mit

$$Y = gXg^{-1}$$

so heißen X, Y in G *konjugiert*. Notation: $X \sim_G Y$ oder $X \sim Y$. Für $X \in \mathscr{P}(G)$ ist

$$\mathrm{St}_G(X) = \left\{g \in G : gXg^{-1} = X\right\} = \{g \in G : gX = Xg\} = \mathcal{N}_G(X)$$

Die Konjugationsklasse von X enthält genau $|G : \mathcal{N}_G(X)|$ Elemente.

8.1.7 Definition: p-Sylowgruppe

Seien G eine endliche Gruppe, $p \in \mathbb{P}$ und $|G| = p^a m,\ a \in \mathbb{N}_0$ mit $p \nmid m \in \mathbb{N}$. Dann heißen die Untergruppen der Ordnung p^a von G *p-Sylowgruppen* von G. Die Menge aller p-Sylowgruppen von G sei $\mathrm{Syl}_p(G)$.

8.1.8 Satz von Sylow

Seien G eine endliche Gruppe, $p \in \mathbb{P}$ und $|G| = p^a m$ mit $a \in \mathbb{N}_0,\ p \nmid m$. Dann gilt:

1. Für $b \in \mathbb{N}_0$ mit $b \leq a$ enthält G garantiert eine Untergruppe der Ordnung p^b. Genauer gilt für die Anzahl $\mathcal{Z}_G(p^b)$ dieser Untergruppen:
$$\mathcal{Z}_G(p^b) = 1 (\text{mod } p)$$
das heißt $p \big| \mathcal{Z}_G(p^b) - 1$.
2. Jede Untergruppe $U \leq G$ der Ordnung p^b ist in einer p-Sylowgruppe enthalten.
3. Je zwei p-Sylowgruppen von G sind in G konjugiert. Insbesondere gilt für $P \in \text{Syl}_p(G)$:
$$|G : \mathcal{N}_G(P)| = \big|\text{Syl}_p(G)\big| = \mathcal{Z}_G(p^a) = 1 (\text{mod } p)$$

Beispiel: Seien $p \in \mathbb{P}$, $\mathbb{K}$ ein Körper mit $q := |\mathbb{K}|$ eine Potenz von p, $n \in \mathbb{N}$ und : $G := \text{GL}(n, \mathbb{K})$. Dann:
$$|G| = (q^n - 1)(q^n - q) \dots (q^n - q^{n-1}) = \underbrace{q^{1+2+\dots+n-1}}_{q^{\binom{n}{2}}} \underbrace{(q^n - 1)(q^{n-1} - 1) \dots (q - 1)}_{\text{nicht durch } p \text{ teilbar}}$$

Daher hat jede p Sylowgruppe von G die Ordnung $q^{\binom{n}{2}}$. Anderseits ist die Menge P aller Matrizen der Form
$$\begin{pmatrix} 1 & * & \dots & * \\ & \ddots & \ddots & \vdots \\ & & \ddots & * \\ 0 & & & 1 \end{pmatrix}$$
eine Untergruppe von G mit
$$|P| = q \cdot q^2 \cdot .. \cdot q^{n-1} = \binom{n}{2}$$
das heißt $P \in \text{Syl}_p(G)$. Man kann sich leicht überzeugen, dass $\mathcal{N}_G(P)$ aus allen invertierbaren Matrizen der Form
$$\begin{pmatrix} * & * & \dots & * \\ & \ddots & \ddots & \vdots \\ & & \ddots & * \\ 0 & & & * \end{pmatrix}$$
besteht. Insbesondere:
$$|\mathcal{N}_G(P)| = q^{\binom{n}{2}} (q - 1)^n$$
das heißt nach Sylow
$$\big|\text{Syl}_p(G)\big| \overset{\text{Sylow}}{=} |G : \mathcal{N}_G(P)| = \left(q^{n-1} + \dots + q + 1\right)\left(q^{n-2} + \dots + q + 1\right) \dots (q + 1) = \underbrace{1 (\text{mod } p)}_{\substack{\text{wie} \\ \text{erwartet}}}$$

Offenbar ist auch die Menge Q aller Matrizen der folgenden Form
$$\begin{pmatrix} 1 & & & \\ * & \ddots & & \\ \vdots & \ddots & \ddots & \\ * & \dots & * & 1 \end{pmatrix}$$
eine p-Sylowgruppe von G, also insbesondere konjugiert zu P. Tatsächlich kann man nachweisen:
$$Q = \begin{pmatrix} 0 & & 1 \\ & \iddots & \\ 1 & & 0 \end{pmatrix} P \begin{pmatrix} 0 & & 1 \\ & \iddots & \\ 1 & & 0 \end{pmatrix}^{-1}$$

8.1.9 Korollar: Kompositionsreihen in p-Gruppen

Sei $p \in \mathbb{P}$ und G eine p-Gruppe. Dann existiert zu jeder Untergruppe $U < G$ eine Reihe

$$U =: V_0 \lhd V_1 \lhd \cdots \lhd V_{k-1} \lhd V_k =: G \tag{8.1.9.1}$$

mit $|V_i : V_{i-1}| = p$ für $i = 1, .., k$.

Spezialfall: Für $U = \{1\}$ erhält man so eine Subnormalreihe von G. Wegen $|V_i : V_{i-1}| = p$ kann diese nicht ohne Wiederholungen verfeinert werden, ist also sogar eine Kompositionsreihe.
Insbesondere ist jede Untergruppe $U \leq G$ Teil einer Kompositionsreihe.

Beweis: **Zeigen:** Zu $U < G$ mit $|G : U| > p$ existiert stets ein $U \lhd V < G$.

Nach Satz 8.1.4 ist G nilpotent. Nach Satz 6.2.10 ist daher $U < \mathcal{N}_G(U)$. Im Fall $\mathcal{N}_G(U) < G$ sind wir fertig, denn $U \lhd \mathcal{N}_G(U)$.

Im Fall $\mathcal{N}_G(U) = G$, das heißt $U \lhd G$ ist G/U eine p-Gruppe der Ordnung $> p$. Nach Sylow besitzt sie eine Untergruppe $V/U < G/U$ der Ordnung p, wobei $U \lhd V < G$ (vgl. Satz 4.1.15 über Faktor-Untergruppen).

Hieraus wird ersichtlich: Die Reihe $U < G$ kann sequentiell verfeinert und schließlich (fast) auf die Form (8.1.9.1) gebracht werden, mit einzigem Unterschied dass $V_{k-1} < G$ ist. Doch wegen $|V_k : V_{k-1}| = p$ folgt nach 4.1.3 auch $V_{k-1} \lhd V_k$.
□

8.1.10 Satz von Cauchy

Seien G eine endliche Gruppe und $p \in \mathbb{P}$ mit $p \big| |G|$. Dann enthält G ein Element der Ordnung p.

Beweis: Nach Sylow 8.1.8 enthält G eine Untergruppe U der Ordnung p. Nach Lagrange enthält G $p - 1$ Elemente der Ordnung p.
□

8.1.11 Satz: Frattini Argument für Sylowgruppen

Seien $p \in \mathbb{P}$, G eine endliche Gruppe, $N \trianglelefteq G$ und $Q \in \mathrm{Syl}_p(N)$. Dann ist $G = N \cdot \mathcal{N}_G(Q)$.

Beweis: Die Gruppe G operiert auf $\mathrm{Syl}_p(N)$ durch Konjugation. Nach Sylow 8.1.8 operiert N auf $\mathrm{Syl}_p(N)$ transitiv. Aus dem allgemeineren Frattini Argument 7.0.23 folgt dann

$$G = N \cdot \underbrace{\mathrm{St}_G(Q)}_{\mathcal{N}_G(Q)}$$

□

8.1.12 Satz über p-Sylowgruppen und Normalteiler

Sei G eine endliche Gruppe, $p \in \mathbb{P}$ und $P \in \mathrm{Syl}_p(G)$. Dann gilt:

1. $N \trianglelefteq G \;\Rightarrow\; P \cap N \in \mathrm{Syl}_p(N) \;\wedge\; PN/N \in \mathrm{Syl}_p(G/N)$
2. $\mathcal{N}_G(P) \leq H \leq G \;\Rightarrow\; \mathcal{N}_G(H) = H$. Insbesondere ist $\mathcal{N}_G(\mathcal{N}_G(P)) = \mathcal{N}_G(P)$.

8.1.13 Satz über p-Sylowgruppen und Nilpotenz

Sei G eine endliche Gruppe und $p_1^{a_1} \dots p_r^{a_r}$ die Primfaktorzerlegung von $|G|$. Für $i = 1, .., r$ sei $P_i \in \mathrm{Syl}_{p_i}(G)$. Dann sind äquivalent:

1. G ist nilpotent.
2. $P_i \trianglelefteq G$ für $i = 1, .., r$
3. $G = P_1 \oplus \cdots \oplus P_r$

Bemerke: Für $P \in \mathrm{Syl}_p(G)$ gilt: $P \trianglelefteq G \overset{8.1.8(3)}{\iff} P$ ist die einzige p-Sylowgruppe von G.

8.1.14 Satz über die Auflösbarkeit endlicher Gruppen

Für $p, q, r \in \mathbb{P}$ und Gruppe G gilt:

1. Ist $|G| = p^a q$ für ein $a \in \mathbb{N}_0$, so ist G auflösbar.
2. Ist $|G| = p^2 q^2$ so ist G auflösbar.
3. Ist $|G| = pqr$, so ist G auflösbar.

Beispiel: Es folgt leicht, dass Gruppen der Ordnungen $1, .., 59$ Auflösbar sind.

8.1.15 Satz über einfache p-Gruppen

Für $p \in \mathbb{P}$ hat jede einfache p-Gruppe die Ordnung p.

Beweis: Sei G eine p-Gruppe. Nach 8.1.4 ist $Z(G) \neq \{1\}$, also $1 < Z(G) \trianglelefteq G$. Da G einfach ist muss G abelsch sein. Nach Sylow existiert eine Untergruppe $H \leq G$ der Ordnung p, die nun ein Normalteiler ist. Wegen Einfachheit von G folgt dann $H = G$.
□

8.2 Symmetrische Gruppen

8.2.1 Vorbetrachtung

Sei $n \in \mathbb{N}$. Elemente in $\mathrm{Sym}(n)$ schreibt man in der Form

$$g = \begin{pmatrix} 1 & \dots & n \\ g(1) & \dots & g(n) \end{pmatrix}$$

Existieren paarweise verschiedene $x_1, .., x_k \in \{1, .., n\}$ mit

$$g(x_1) = x_2,\ g(x_2) = x_3,\ \dots g(x_k) = x_1$$

und $g(y) = y$ sonst, so heißt g *k-Zyklus* oder *Zyklus der Länge k*. Man schreibt

$$g = (x_1, x_2, \dots, x_k) = (x_2, \dots, x_k, x_1) = \cdots = (x_k, x_1, \dots, x_{k-1})$$

Zyklen $(x_1, .., x_k)$, $(y_1, .., y_k)$ mit $\{x_1, .., x_k\} \cap \{y_1, .., y_l\} = \emptyset$ heißen *disjunkt*. Gegebenfalls sind dann $(x_1, .., x_k)$, $(y_1, .., y_l)$ vertauschbar. Offenbar kann man jedes $g \in \mathrm{Sym}(n)$ als Produkt disjunkter Zyklen schreiben, z.B.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 8 & 4 & 9 & 5 & 2 & 6 & 3 & 1 & 10 & 7 & 12 & 11 \end{pmatrix} = (1,8)(2,4,5)(3,9,10,7,3)(6)(11,12)$$

Dabei liefern die auftretenden Zyklen die Bahnen von $\langle g \rangle$ auf $\{1, .., n\}$. Bis auf die Reihenfolge der Zyklen und Zyklen der Länge 1, ist diese *Zyklenschreibweise* eindeutig. Wir ordnen die auftretenden Zyklenlängen $k_1, .., k_l$ so dass $k_1 \geq k_2 \geq \cdots \geq k_l$. Dabei ist

$$k_1 + \cdots + k_l = n$$

Das Tupel $(k_1, .., k_l)$ heißt *Typ* von g. Offenbar ist

$$|\langle g \rangle| = \text{kgV}(k_1, .., k_l)$$

8.2.2 Satz: Typ konjugierter Elemente

Sei $n \in \mathbb{N}$. Zwei Elemente in $\text{Sym}(n)$ sind genau dann konjugiert, wenn sie den gleichen Typ haben.

Beweis: Richtung "⇒": Sei $a \in \text{Sym}(n)$ mit Zyklenschreibweise

$$a = (x_1, .., x_k)(y_1, .., y_l) \dots$$

Für $g \in \text{Sym}(n)$ gilt dann

$$gag^{-1} = (g(x_1) \dots g(x_k))\,(g(y_1)..g(y_l)) \dots$$

denn z.B.

$$(gag^{-1})(g(x_i)) = (ga)(x_i) = g(x_{i+1})$$

u.s.w.
Richtung "⇐": Seien $a, a' \in \text{Sym}(n)$ mit Zyklenschreibweise

$$a = (x_1, .., x_k)(y_1, .., y_l) \dots$$
$$a' = (x'_1, .., x'_k)(y'_1, .., y'_l) \dots$$

Dann ist $gag^{-1} = a'$ mit

$$g = \begin{pmatrix} x_1 & \dots & x_k & y_1 & \dots & y_l & \dots \\ x'_1 & \dots & x'_k & y'_1 & \dots & y'_l & \dots \end{pmatrix}$$

8.2.3 Definition: Partition

Sei $n \in \mathbb{N}$. Eine *Partition* von n ist eine endliche Folge $(k_1, .., k_l) \in \mathbb{N}^l$ mit

$$k_1 \geq k_2 \geq \dots \geq k_l \quad , \quad k_1 + \dots + k_l = n$$

Bemerkung: Satz 8.2.2 liefert eine Bijektion zwischen der Menge der Konjugationsklassen von $\text{Sym}(n)$ und der Menge der Partitionen von n.

Beispiel: Die Zahl 5 besitzt genau 7 Partitionen

$$5 = 4+1 = 3+2 = 3+1+1 = 2+2+1 = 2+1+1+1 = 1+1+1+1+1$$

Daher hat Sym(5) Konjugationsklassenzahl 7.

8.2.4 Satz: Länge von Konjugationsklassen

Sei $(k_1, .., k_l)$ eine Partition von $n \in \mathbb{N}$ und sei

$$m_i := |\{j : k_j = i\}|$$

für $i = 1, .., n$. Unter den Zahlen $k_1, .., k_l$ treten also m_1 Einsen auf, m_2 Zweien usw. auf. Dann hat die Konjuationsklasse der Elemente vom Typ $(k_1, .., k_l)$ in $\text{Sym}(n)$ die Länge

$$\frac{n!}{m_1!1^{m_1} \cdot m_2!2^{m_2} \dots m_n!n^{m_n}}$$

8.2.5 Erzeugung von $\mathrm{Sym}(n)$

Offenbar wird $\mathrm{Sym}(n)$ von allen Zyklen erzeugt. Wegen

$$(x_1, .., x_k) = (x_1, x_k)(x_1, x_{k-1}) \dots (x_1, x_2)$$

wird $\mathrm{Sym}(n)$ auch von den 2-Zyklen (*Transpositionen*) erzeugt. Wegen

$$(i, j) = (1, i)(1, j)(1, i)$$

genügen sogar die Transpositionen

$$(1, 2), (1, 3), \dots, (1, n)$$

Wegen

$$(1, i) = (i - 1, i) \dots (2, 3)(1, 2)(2, 3) \dots (i - 1, i)$$

genügen auch die *Basistranspositionen*

$$(1, 2), (2, 3), \dots, (n - 1, n)$$

Wegen

$$(i, i + 1) = (1, 2, .., n)(i - 1, i)(1, 2, .., n)^{-1}$$

gilt auch

$$\mathrm{Sym}(n) = \langle (1, 2),\ (1, 2, .., n) \rangle$$

8.2.6 Definition: Inversion

Sei $n \in \mathbb{N}$ und $g \in \mathrm{Sym}(n)$. Dann heißt ein Paar $(i, j) \in \mathbb{N} \times \mathbb{N}$ mit $1 \leq i < j \leq n$ und $g(i) > g(j)$ *Inversion* von g. Die Anzahl $l(g)$ aller Inversionen von g heißt *Länge* von g.

8.2.7 Satz über die Länge einer Permutation

Sei $n \in \mathbb{N}$. Dann kann man jedes $g \in \mathrm{Sym}(n)$ als Produkt von $l(g)$ Basistranspositionen, aber nicht als Produkt von weniger als $l(g)$ Basistranspositionen schreiben.

Beispiel:

$$g := \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix} \Rightarrow\ l(g) = 2$$

$$(1, 2)g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix} \Rightarrow\ l\left((1, 2)g\right) = 1$$

$$(2, 3)g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} \Rightarrow\ g = (1, 2)(2, 3)$$

Beweis: Allgemein erhöht/erniedrigt die Multiplikation mit einer Basistransposition die Anzahl der Inversionen um Eins. Insbesondere muss man mindestens so oft mit Transpositionen multiplizieren wie in g Inversionen vorhanden sind.
□

8.2.8 Definition: Vorzeichen

Sei $n \in \mathbb{N}$. Für $g \in \mathrm{Sym}(n)$ heißt

$$\mathrm{sgn}(g) := \prod_{1 \leq i < j \leq n} \frac{g(j) - g(i)}{j - i}$$

Vorzeichen von g.

Bemerkung: Offenbar kommen im Zähler und Nenner bis auf das Vorzeichen die gleichen Zahlen vor. Daher ist

$$\operatorname{sgn}(g) = (-1)^{l(g)} \in \{\pm 1\}$$

8.2.9 Satz über das Vorzeichen von Permutationen

Die Abbildung $\operatorname{sgn} : \operatorname{Sym}(n) \to (\{\pm 1\}, \cdot)$ ist ein Homomorphismus.

Beispiele:

(i) Für $g, h \in \operatorname{Sym}(n)$ ist

$$\operatorname{sgn}(ghg^{-1}) = \cancel{\operatorname{sgn}(g)} \cdot \operatorname{sgn}(h) \cdot \cancel{\operatorname{sgn}(g)^{-1}} = \operatorname{sgn}(g)$$

das heißt konjugierte Permutationen haben gleiches Vorzeichen.

(ii) Jeder k-Zyklus hat genau dann Vorzeichen $+1$ wenn k ungerade ist. Insbesondere hat jede Transposition das Vorzeichen -1.

8.2.10 Definition: Alternierende Gruppe

Für $n \in \operatorname{Sym}(n)$ heißt

$$\operatorname{Alt}(n) := \ker\left(\operatorname{sgn} : \operatorname{Sym}(n) \to \{\pm 1\}\right)$$

alternierende Gruppe des Grades n.

Bemerkungen:

(i) Per Konstruktion ist $\operatorname{Alt}(n) \trianglelefteq \operatorname{Sym}(n)$. Nach Homomorphiesatz 4.1.8 ist für $n \geq 2$ außerdem $|\operatorname{Sym}(n) : \operatorname{Alt}(n)| = 2$. Dabei besteht $\operatorname{Alt}(n)$ genau aus den Elementen die Produkte einer geraden Anzahl von Transpositionen sind. Wegen

$$(i,j)(j,k) = (i,j,k) \quad , \quad (i,j)(k,l) = (i,l,k)(i,j,k)$$

für paarweise verschiedene $i, j, k, l \in \{1, .., n\}$, wird $\operatorname{Alt}(n)$ von aller 3-Zyklen erzeugt.

(ii) Nach Lemma 3.3.16 Beispiel (i) ist für Untergruppe $U \leq \operatorname{Sym}(n)$ stets $U \cap \operatorname{Alt}(n) \trianglelefteq U$.

(iii) Da konjugierte Permutationen gleiche Vorzeichen haben, ist jede Konjugationsklasse (von $\operatorname{Sym}(n)$) entweder ganz oder gar nicht in $\operatorname{Alt}(n)$ enthalten.

8.2.11 Satz über die Konjugationsklassen in $\operatorname{Alt}(n)$

Für $x \in \operatorname{Alt}(n)$ ist die Konjugationsklasse von x in $\operatorname{Sym}(n)$ entweder eine Konjugationsklasse in $\operatorname{Alt}(n)$ oder die Vereinigung von zwei gleich großen Konjugationsklassen von $\operatorname{Alt}(n)$. Der letzte Fall liegt genau dann vor, wenn $C_{\operatorname{Sym}(n)}(x) \subseteq \operatorname{Alt}(n)$.

Beweis: Nennen $A := \operatorname{Alt}(n)$ und $S := \operatorname{Sym}(n)$. Sei $x \in A$. Für $y = \underbrace{(1,2)}_{\notin A}$ gilt: $S = A \dot\cup Ay$. Jedes zu x in S konjugierte Element ist also in A zu x oder zu $\underbrace{yxy^{-1}}_{\in A}$ konjugiert. Wegen

$$C_A(yxy^{-1}) = yC_A(x)y^{-1}$$

haben die Konjugationsklassen von x und yxy^{-1} in A die gleiche Länge, und zwar

$$|A : C_A(x)| = |A : A \cap C_S(x)| = |AC_S(x) : C_S(x)| = \begin{cases} |S : C_S(x)| & : C_S(x) \not\subseteq A \\ |S : C_S(x)| \,/ 2 & : \text{sonst} \end{cases}$$

□

Bemerkung: Es kann gezeigt werden, dass für eine Permutation $g \in \mathrm{Alt}(n)$ vom Typ $(k_1, .., k_l)$ genau dann $C_{\mathrm{Sym}(n)}(g) \subseteq \mathrm{Alt}(n)$ ist, wenn die $k_1, .., k_l$ ungerade und paarweise verschieden sind.

Beispiel: Sei $n = 5$. Dann enthält $\mathrm{Alt}(5) =: A$ Elemente der Typen $(1,1,1,1,1)$, $(2,2,1)$, $(3,1,1)$, (5). Wegen $(1,2) \in C_S((1,2)(3,4)) \setminus \mathrm{Alt}(5)$ stimmen die Konjugationsklassen von $(1,2)(3,4)$ in $\mathrm{Sym}(5) =: S$ und $\mathrm{Alt}(5)$ überein, enthalten also

$$\frac{5!}{2!2^2} = 15$$

Elemente. Wegen $(4,5) \in C_S((1,2,3)) \setminus \mathrm{Alt}(5)$ stimmen auch die Konjugationsklassen von $(1,2,3)$ in $\mathrm{Sym}(5)$ und $\mathrm{Alt}(5)$ überein und enthalten

$$\frac{5!}{2!1^2 \cdot 1! \cdot 3^1} = 20$$

Elemente. Die Konjugationsklasse von $(1,2,3,4,5)$ in $\mathrm{Sym}(5)$ enthält

$$\frac{5!}{1!5^1} = 24$$

Elemente. Daher ist

$$|C_S((1,2,3,4,5))| = \frac{|\mathrm{Sym}(n)|}{24} = 5$$

also

$$C_S((1,2,3,4,5)) = \underbrace{\langle (1,2,3,4,5) \rangle}_{\text{Ordnung } 5} \subseteq \mathrm{Alt}(5)$$

das heißt die Konjugationsklasse von $(1,2,3,4,5)$ in $\mathrm{Sym}(5)$ entfällt in zwei Konjugationsklassen der Länge 12 in $\mathrm{Alt}(5)$. Die Erwartung $1 + 15 + 20 + 2 \cdot 12 = 60$ wird auch bestätigt.

Jeder Normalteiler $1 \neq N \trianglelefteq \mathrm{Alt}(5)$ ist Vereinigung von Konjugationsklassen von A (vgl. Beispiel in 8.1.1). Daher $\underbrace{13}_{1+12} \leq |N| \mid 60$, das heißt

$$|N| \in \{15, 20, 30, 60\}$$

Es lässt sich leicht zeigen, dass $|N| = 60$ sein muss. Also ist $\mathrm{Alt}(5)$ eine einfache Gruppe.

8.2.12 Bemerkung zur Operation von $\mathrm{Alt}(n)$

Für $n \geq 3$ operiert $\mathrm{Alt}(n)$ $(n-2)$ - transitiv auf $\{1, .., n\}$, denn für paarweise verschiedene

$$a_1, .., a_n \in \{1, .., n\}$$

gehört entweder

$$\begin{pmatrix} 1 & \dots & n-2 & n-1 & n \\ a_1 & \dots & a_{n-2} & a_{n-1} & a_n \end{pmatrix}$$

oder

$$\begin{pmatrix} 1 & \dots & n-2 & n-1 & n \\ a_1 & \dots & a_{n-2} & a_n & a_{n-1} \end{pmatrix}$$

zu $\mathrm{Alt}(n)$, das heißt je $(a_1, .., a_{n-2})$ können durch geeignete $g \in \mathrm{Alt}(n)$ beliebig auf $(1, .., n-2)$ abgebildet werden und umgekehrt. Offensichtlich operiert $\mathrm{Sym}(n)$ sogar transitiv auf $\{1, .., n\}$.

8.2.13 Satz: Einfachheit von $\mathrm{Alt}(n)$

Für $n \neq 4$ ist $\mathrm{Alt}(n)$ stets einfach, $\mathrm{Alt}(4)$ jedoch nicht.

Erläuterung: Alt(4) ist nicht einfach, denn

$$V_4 := \{1,\ (1,2)(3,4),\ (1,3)(2,4),\ (1,4)(2,3)\} \trianglelefteq \mathrm{Alt}(4) \tag{8.2.13.1}$$

Man nennt V_4 die *Kleinsche Vierergruppe*. Genauer gesagt, hat $A := \mathrm{Alt}(4)$ folgende Konjugationsklassen

$$\mathrm{Orb}_A(1)\ ,\ \mathrm{Orb}_A((1,2)(3,4))\ ,\ \mathrm{Orb}_A((1,2,3))\ ,\ \mathrm{Orb}_A((1,3,2))$$

jeweils der Länge 1, 3, 4 und 4. Dabei sind $1, V_4$ und Alt(4) die einzigen Normalteiler von Alt(4).

8.2.14 Satz über die Kommutatorgruppe von Sym(n)

Für $n \in \mathbb{N}$ gilt stets

$$\mathrm{Sym}(n)' \overset{\mathrm{def}}{=} [\mathrm{Sym}(n), \mathrm{Sym}(n)] = \mathrm{Alt}(n)$$

(vgl. Definition 6.1.8).

Beweis: O.B.d.A sei $n \geq 3,\ S := \mathrm{Sym}(n),\ A := \mathrm{Alt}(n)$. Wegen $|S/A| = 2$ ist S/A abelsch, nach Satz 6.1.9 also $S' \leq A$ und damit $S' \trianglelefteq A$ (da ohnehin schon $S' \trianglelefteq S$). Für $n \neq 4$ ist A einfach, das heißt $S' \in \{\{1\}, A\}$. Da jedoch S nicht abelsch ist, ist der Fall $S' = \{1\}$ ausgeschlossen, die Behauptung stimmt also für $n \neq 4$.

Für $n = 4$ ist wegen

$$S' \geq \overbrace{\mathrm{Sym}(3)}^{\subseteq \mathrm{Sym}(4)}{}' = \underbrace{\mathrm{Alt}(3)}_{\substack{\not\subseteq V_4 \\ (\text{vgl. } (8.2.13.1))}}$$

der Fall $S' = V_4$ ausgeschlossen, natürlich auch der Fall $S' = \{1\}$. Nach der Erläuterung von Satz 8.2.13 bleibt nur noch die Möglichkeit $S' = \mathrm{Alt}(4)$.
□

Folgerung: Insbesondere ist Sym(n) für $n \geq 5$ nicht auflösbar!

8.2.15 Satz über einfache Gruppen der Ordnung 60

Sei G eine einfache Gruppe der Ordnung 60. Dann gilt

$$G \cong \mathrm{Alt}(5)$$

8.3 π-Hallgruppen

8.3.1 Definition: π-Gruppe

Sei $\pi \subseteq \mathbb{P}$ und $\pi' := \mathbb{P} \setminus \pi$. Eine endliche Gruppe G heißt *π-Gruppe* falls jeder Primteiler von $|G|$ in π liegt. Ein Gruppenelement g heißt *π-Element*, falls $\langle g \rangle$ eine π-Gruppe ist.

Eine π-Untergruppe H einer beliebigen endlichen Gruppe G heißt *π-Hallgruppe* von G, falls jeder Primteiler von $|G : H|$ zu π' gehört. Dabei sei $\mathrm{Hall}_\pi(G)$ die Menge aller Hallgruppen von G.

Bemerkungen:

(i) Für $p \in \mathbb{P}$ und $\pi := \{p\}$ sind die π-Gruppen genau die p-Gruppen, die π-Elemente genau die p-Elemente und die π-Hallgruppen genau die p-Sylowgruppen. Statt π' schreibt man auch p'.

(ii) Per Konstruktion gilt für $H \in \mathrm{Hall}_\pi(G)$:

$$\mathrm{ggT}(|H|, |G : H|) = 1$$

(iii) Sei $p_1^{k_1} \dots p_n^{k_n}$ die Primfaktorzerlegung von $|G|$. Eine Untergruppe $H \leq G$ ist genau dann π-Hall, falls

$$|H| = \prod_{p_i \in \pi \cap \{p_1,..,p_n\}} p_i^{k_i}$$

(iv) Ist $V \in \mathrm{Hall}_\pi(G)$ und $V \leq U \leq G$, so ist auch $V \in \mathrm{Hall}_\pi(U)$, denn

$$|U : V| = \frac{|U|}{|V|} \mid \frac{|G|}{|V|}$$

(v) Im allgemeinen ist $\mathrm{Hall}_\pi(G) = \emptyset$, z.B. enthält Alt(5) keine $\{2,5\}$-Hallgruppe. Denn wegen

$$|\mathrm{Alt}(5)| = 60 = 2^2 \cdot 3 \cdot 5$$

wäre $|H| = 20$ und $|G : H| = 3$. Dies würde einen nicht-trivialen Homomorphismus $f : \mathrm{Alt}(5) \to \mathrm{Sym}(3)$ liefern, ein Widerspruch zur Einfachheit von Alt(5).

(vi) Im allgemeinen sind nicht alle π-Hallgruppen einer endlichen Gruppe konjugiert. Z.B. existieren in der Gruppe $\mathrm{GL}(3, \mathbb{F}_2)$ der Ordnung $(2^3-1)(2^3-2)(2^3-2) = 168 = 2^3 \cdot 3 \cdot 7$ nicht-konjugierte Halbgruppen der Ordnung 24.

8.3.2 Satz: π-Hallgruppen und Normalteiler

Seien G eine endliche Gruppe, $\pi \in \mathbb{P}$ und $H \in \mathrm{Hall}_\pi(G)$. Dann gilt:

1. Für $N \trianglelefteq G$ ist
$$H \cap N \in \mathrm{Hall}_\pi(N) \quad \wedge \quad HN/N \in \mathrm{Hall}_\pi(G/N)$$
2. $\mathcal{N}_G(\mathcal{N}_G(H)) = \mathcal{N}_G(H)$.

8.3.3 Satz über normale, abelsche π-Hallgruppen

Seien G eine endliche Gruppe, $\pi \in \mathbb{P}$ und $A \in \mathrm{Hall}_\pi(G)$ normal, abelsch. Dann ist $\mathrm{Hall}_{\pi'}(G) \neq \emptyset$ und

$$H_1 \sim_G H_2 \ \ \forall\ H_1, H_2 \in \mathrm{Hall}_{\pi'}(G)$$

8.3.4 Satz von Schur-Zassenhaus

Seien G eine endliche Gruppe, $\pi \subseteq \mathbb{P}$ und $N \in \mathrm{Hall}_\pi(G)$ normal. Dann ist $\mathrm{Hall}_{\pi'}(G) \neq \emptyset$. Ist N oder G/N auflösbar, so gilt:

$$H_1 \sim_G H_2 \ \ \forall\ H_1, H_2 \in \mathrm{Hall}_{\pi'}(G)$$

Bemerkung: Wegen $\mathrm{ggT}(|N|, |G/N|) = 1$ hat N oder G/N ungerade Ordnung. Nach Satz von Feit-Thomson 6.1.14 (ii) ist also N oder G/N auflösbar, das heißt die Auflösbarkeitsvoraussetzung im Satz ist in Wirklichkeit überflüssig. Ein Beweis dieser Tatsache ohne die Verwendung des Satzes von Feit-Thomson ist bis heute unbekannt.

8.3.5 Satz über π- und auflösbare Gruppen (P. Hall)

Für jede auflösbare, endliche Gruppe G und alle $\pi \subseteq \mathbb{P}$ gilt:

1. G hat eine π-Hallgruppe.
2. Je zwei π-Hallgruppen von G sind in G konjugiert.
3. Jede π-Untergruppe von G ist in einer π-Hallgruppe von G enthalten.

Bemerkung: P. Hall hat auch bewiesen, dass umgekehrt jede endliche Gruppe G mit $\mathrm{Hall}_\pi(G) \neq \emptyset \ \forall\ \pi \subseteq \mathbb{P}$ stets auflösbar sind. Der Beweis benutzt Burnsides $p^a q^b$-Satz (6.1.14 (i)) und verallgemeinert diesen schließlich.

8.3.6 Korollar: Frattini Argument für π-Hallgruppen

Sei G eine endliche, auflösbare Gruppe, $N \trianglelefteq G$ und $H \in \mathrm{Hall}_\pi(N)$. Dann gilt

$$G = N \cdot \mathcal{N}_G(H)$$

(vgl. Frattini für Sylowgruppen 8.1.11).

Beweis: G operiert auf $\mathrm{Hall}_\pi(N)$ durch Konjugation, wobei N auflösbar ist und daher auf $\mathrm{Hall}_\pi(N)$ nach Hall 8.3.5 sogar transitiv operiert. Nach Frattini 7.0.23 ist dann

$$G = N \cdot \mathrm{St}_G(H) = N \cdot \mathcal{N}_G(H)$$

□

8.3.7 Satz von O. Schmidt

Für jede endliche, nicht-nilpotente Gruppe G, in der jede echte Untergruppe nilpotent ist, gilt:

1. G ist auflösbar.
2. $\exists\ p, q \in \mathbb{P}$ derart, dass G eine $\{p,q\}$-Gruppe, mit einer zyklischen p-Sylowgruppe & einer normalen q-Sylowgruppe, ist.

8.3.8 Satz von Wieland

Seien G eine endliche Gruppe, $\pi \subseteq \mathbb{P}$ und $H \in \mathrm{Hall}_\pi(G)$ nilpotent. Dann $\exists$ zu jeder π-Untergruppe $U \leq G$ ein $g \in G$ mit $U \subseteq gHg^{-1}$.

8.3.9 Definition: Komplement

Seien H, K Untergruppen einer Gruppe G mit $H \cap K = \{1\}$ und $HK = G$. Dann heißt K *Komplement* von H in G.

Bemerkung: Gegebenfalls ist $|G| = |H| \cdot |K|$.

8.3.10 Satz von Galois

Jeder minimale Normalteiler M einer endlichen, auflösbaren Gruppe G mit $M = C_G(M)$ hat ein Komplement in G und je zwei Komplemente von M in G sind in G konjugiert.

Bemerkung: Seien G eine endliche Gruppe, $\pi \subseteq \mathbb{P}$. Für π-Normalteiler $M, N \trianglelefteq G$ ist auch $MN \trianglelefteq G$ ein π-Normalteiler. Daher ist das Produkt aller π-Normalteiler von G ein π-Normalteiler, $\mathcal{O}_\pi(G)$, der *π-Kern* von G heißt. Für jeden π-Normalteiler $N \trianglelefteq G$ ist $\mathcal{O}_\pi(G/N) = \mathcal{O}_\pi(G)/N$, insbesondere ist

$$\mathcal{O}_\pi\left(G/\mathcal{O}_\pi(G)\right) = \mathcal{O}_\pi(G)/\mathcal{O}_\pi(G) = 1$$

Für $p \in \mathbb{P}$ und $\pi := \{p\}$ setzt man

$$\mathcal{O}_p(G) := \mathcal{O}_\pi(G)$$

8.3.11 Hal-Higmann-Lemma

Für jede auflösbare, endliche Gruppe G und $\forall\ \pi \subseteq \mathbb{P}$ mit $\mathcal{O}_{\pi'}(G) = 1$ ist

$$C_G(\mathcal{O}_\pi(G)) \subseteq \mathcal{O}_\pi(G)$$

8.4 Lineare Gruppen

8.4.1 Iwasawas Lemma

Sei G eine perfekte Gruppe, Ω eine treue, primitive G-Menge, $\omega \in \Omega$ und A ein auflösbarer Normalteiler von $\mathrm{St}_G(\omega)$ mit $G = \langle gAg^{-1} : g \in G\rangle$. Dann ist G einfach.

Bemerkungen:

(i) Seien $\mathbb{K}$ ein Körper und V ein endlich-dimensionaler $\mathbb{K}$-Vektorraum. Dann gilt:

$$\mathcal{Z} := \{\alpha \cdot \mathrm{Id}_V : \alpha \in \mathbb{K}_+\} \leq Z(\mathrm{GL}(V))$$

denn für $g \in \mathrm{GL}(V),\ \alpha \in \mathbb{K}_+$ und $v \in V$ ist

$$\left[g(\alpha\,\mathrm{Id}_V)g^{-1}\right](v) = g\left(\alpha g^{-1}(v)\right) = \alpha g\left(g^{-1}(v)\right) = (\alpha\,\mathrm{Id}_V)(v)$$

Man nennt $\mathrm{PGL}(V) := \mathrm{GL}(V)/\mathcal{Z}$ *projektive, allgemeine, lineare Gruppe* von V.

(ii) Aus (i) folgt

$$\mathcal{Z} \cap \mathrm{SL}(V) = \left\{\alpha\,\mathrm{Id}_V : \alpha \in \mathbb{K}_+,\ \alpha^{\dim V} = 1\right\} \leq Z(\mathrm{SL}(V))$$

Man nennt $\mathrm{PSL}(V) := \mathrm{SL}(V)/(\mathrm{SL}(V) \cap \mathcal{Z}) \cong \mathrm{SL}(V)\mathcal{Z}/\mathcal{Z} \leq \mathrm{PGL}(V)$ *projektive, spezielle, lineare Gruppe* von V.

(iii) Für $n \in \mathbb{N}$ ist analog

$$\mathcal{Z} := \{\alpha 1_n : \alpha \in \mathbb{K}_+\} \leq Z(\mathrm{GL}(n,\mathbb{K}))$$

und

$$\mathrm{PGL}(n,\mathbb{K}) := \mathrm{GL}(n,\mathbb{K})/\mathcal{Z}$$

heißt *projektive, allgemeine, lineare Gruppe* des Grades n über $\mathbb{K}$.

(iv) Dementsprechend ist

$$\mathcal{Z} \cap \mathrm{SL}(n,\mathbb{K}) = \{\alpha 1_n : \alpha \in \mathbb{K}, \alpha^n = 1\} \leq Z(\mathrm{SL}(n,\mathbb{K}))$$

und

$$\mathrm{PSL}(n,\mathbb{K}) := \mathrm{SL}(n,\mathbb{K})/(\mathrm{SL}(n,\mathbb{K}) \cap \mathcal{Z})$$

heißt *projektive, spezielle, lineare Gruppe* des Grades n über $\mathbb{K}$.

(v) Für jeden $\mathbb{K}$-Vektorraum V der Dimension $n \in \mathbb{N}$ gilt

$$\mathrm{GL}(V) \cong \mathrm{GL}(n,\mathbb{K})\ ,\ \mathrm{SL}(V) \cong \mathrm{SL}(n,\mathbb{K})$$

$$\mathrm{PGL}(V) \cong \mathrm{PGL}(n,\mathbb{K})\ ,\ \mathrm{PSL}(V) \cong \mathrm{PSL}(n,\mathbb{K})$$

8.4.2 Bemerkung: Operation von PGL und PSL

Für jeden Körper $\mathbb{K}$ und $\mathbb{K}$-Vektorraum V mit $\dim V < \infty$ operiert $\mathrm{GL}(V)$ auf der Menge Ω aller 1-dimensionalen Untervektorräume $U \subseteq V$ durch

$${}^gU := g(U)\quad ,\quad g \in \mathrm{GL}(V),\ U \in \Omega$$

Dabei operiert $\mathcal{Z} := \{\alpha\,\mathrm{Id}_V : \alpha \in \mathbb{K}_+\}$ trivial auf Ω. Daher operiert auch $\mathrm{PGL}(V) = \mathrm{GL}(V)/\mathcal{Z}$ und $\mathrm{PSL}(V) = \mathrm{SL}(V)/(\mathrm{SL}(V) \cap \mathcal{Z})$ auf Ω durch

$${}^{g\mathcal{Z}}U := {}^gU := g(U)\quad ,\quad g \in \mathrm{GL}(V),\ U \in \Omega$$

$${}^{g(\mathrm{SL}(V)\cap\mathcal{Z})}U := {}^gU := g(U)\quad ,\quad g \in \mathrm{SL}(V),\ U \in \Omega$$

(vgl. Bemerkung 7.0.33).

8.4.3 Satz über die Operation von PSL

Sei V ein $\mathbb{K}$-Vektorraum mit $1 < \dim V < \infty$. Die Operation von $\mathrm{PSL}(V)$ auf die Menge Ω aller 1-dimensionalen Unterräume von V ist treu und 2-transitiv (vgl. 8.4.2).

Beachte: Der Kern der Operation von $\mathrm{SL}(V)$ auf Ω ist genau $\underbrace{\{\alpha\,\mathrm{Id}_V : \alpha \in \mathbb{K}_+\}}_{\mathcal{Z}} \cap \mathrm{SL}(V)$.

Bemerkung: Seien $\mathbb{K}$ ein Körper und $n \in \mathbb{N}$. Wie bezeichnen die Standardbasis von $\mathbb{K}^{n\times n}$ mit $e_{ij},\ i,j = 1,..,n$, z.B. für $n = 2$:

$$e_{11} := \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\ ,\ e_{12} := \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\ ,\ e_{21} := \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}\ ,\ e_{22} := \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

Für $\alpha \in \mathbb{K}$ und **verschiedene** $i,j \in \{1,..,n\}$ setzen wir

$$u_{ij}(\alpha) := 1_n + \alpha e_{ij} \in \mathrm{SL}(n,\mathbb{K}) \tag{8.4.3.1}$$

8.4.4 Satz: Erzeugung von SL

Für jeden Körper $\mathbb{K}$ und $1 < n \in \mathbb{N}$ gilt:

$$\mathrm{SL}(n,\mathbb{K}) = \langle u_{ij}(\alpha) : i,j = 1,..,n,\ i \neq j,\ \alpha \in \mathbb{K}_+ \rangle$$

8.4.5 Satz: Perfektheit von SL

Seien $\mathbb{K}$ ein Körper und $n \in \mathbb{N}$. Dann ist $\mathrm{SL}(n,\mathbb{K})$ perfekt, außer in den Fällen

$$(n, |\mathbb{K}|) \in \{(2,2),\ (2,3)\}$$

Bemerkungen:

(i) In den obigen Situationen ist auch $\mathrm{PSL}(n,\mathbb{K})$ perfekt.

(ii) Wegen $|\mathrm{GL}(2,\mathbb{F}_2)| = 6$ und $|\mathrm{GL}(2,\mathbb{F}_3)| = 48$ sind $\mathrm{GL}(2,\mathbb{F}_2)$ und $\mathrm{GL}(2,\mathbb{F}_3)$ auflösbar (vgl. Beispiel in Satz 8.1.14). Daher sind auch
$$\mathrm{SL}(2,\mathbb{F}_2)\ ,\ \mathrm{PSL}(2,\mathbb{F}_2)\ ,\ \mathrm{SL}(2,\mathbb{F}_3)\ ,\ \mathrm{PSL}(2,\mathbb{F}_3)$$
auflösbar.

8.4.6 Satz: Einfachheit von PSL

Sei $\mathbb{K}$ ein Körper und $n \in \mathbb{N}$. Dann ist $\mathrm{PSL}(n,\mathbb{K})$ einfach, außer in den Fällen

$$(n, |\mathbb{K}|) \in \{(2,2),\ (2,3)\}$$

Bemerkungen:

(i) In der Algebra lernt man dass $\mathbb{K}_+$ im Fall $|\mathbb{K}| =: q < \infty$ zyklisch ist. Daher hat
$$\mathcal{Z} := \{\alpha 1_n : \alpha \in \mathbb{K},\ \alpha^n = 1\}$$
Ordnung $\mathrm{ggT}(n, q-1)$. Also gilt
$$|\mathrm{PSL}(n,\mathbb{K})| = |\mathrm{SL}(n,\mathbb{K})| \,/\, \mathrm{ggT}(n, q-1)$$
(vgl. Korollar 3.3.11).

(ii) Ähnlich kann man die Einfachheit von anderen *klassischen Gruppen* (orthogonale, symplektische, unitäre u.ä) mit *kleinen Ausnahmen* beweisen.

9 Spezielle Anwendungen

9.1 Die Verlagerung

9.1.1 Vorbetrachtung

Sei G eine endliche Gruppe, $K \trianglelefteq H \leq G$ derart, dass H/K abelsch ist, $\mathscr{R}$ ein Repräsentantensystem für G/H, das heißt

$$G = \biguplus_{r \in \mathscr{R}} rH$$

Für $g \in G,\ r \in \mathscr{R}$ existieren dann eindeutige Elemente

$$\rho_g(r) \in \mathscr{R}\ ,\ \eta_g(r) \in H$$

mit $gr = \rho_g(r)\eta_g(r)$. Dabei ist $\eta_g(r)$ als der *Fehler* von gr bzgl. des Repräsentantensystems zu interpretieren. Wir definieren:

$$V_{H/K}^G(g) := \underbrace{\prod_{r \in \mathscr{R}} \eta_g(r) K}_{\in H/K}$$

Beachte: Da H/K abelsch ist, kommt es bei dem Produkt nicht auf die Reihenfolge an.

9.1.2 Satz über $V_{H/K}^G$

Sei G eine endliche Gruppe, $K \trianglelefteq H \leq G$ so dass H/K abelsch ist und $\mathscr{R}$ irgendein Repräsentantensystem für G/H. Dann ist die in 9.1.1 definierte Abbildung

$$V_{H/K}^G : G \to H/K$$

unabhängig von der Wahl von $\mathscr{R}$ und ein Homomorphismus.

9.1.3 Definition: Verlagerung

Sei G eine endliche Gruppe, $K \trianglelefteq H \leq G$ so dass H/K abelsch ist. Dann heißt der in 9.1.1 definierte Homomorphismus

$$V_{H/K}^G : G \to H/K$$

Verlagerung (engl. *transfer*) von G nach H/K.

Beachte: In der Regel ist $|H : K| < |G|$, daher $V_{H/K}^G$ typischerweise nicht injektiv.

9.1.4 Bemerkung: Berechnung der Verlagerung

Sei G eine endliche Gruppe, $K \trianglelefteq H \leq G$ derart, dass H/K abelsch ist und $g \in G$. Zur Berechnung von $V_{H/K}^G(g)$ ist es zweckmäßig, ein Repräsentantensystem für G/H zu wählen, dass auf g *zugeschnitten* ist.

Auf G/H operiert $\langle g \rangle$ durch Linksmultiplikation. Die Bahnen seien $\Delta_1, .., \Delta_s$, dazu $r_1 H \in \Delta_1, .., r_s H \in \Delta_s$. Für $i \in \{1, .., s\}$ sei $d_i := \underbrace{|\Delta_i|}_{\big|\langle g \rangle}$, dann ist

$$\Delta_i = \left\{ r_1 H,\ g r_i H,\ g^2 r_i H, \ldots,\ g^{d_i - 1} r_i H \right\}$$

und $g^{d_i} r_i H = r_i H$. Folglich ist

$$\mathscr{R} = \left\{ r_1,\ g r_1, ..,\ g^{d_1 - 1} r_1,\ \ldots, r_s,\ g r_s, ..,\ g^{d_s - 1} r_s \right\}$$

ein Repräsentantensystem für G/H und

$$V_{H/K}^G(g) = \prod_{i=1}^{s} r_i^{-1} g^{d_i} r_i K$$

mit

$$r_i^{-1} g^{d_i} r_i \in H \quad , \quad d_1 + \cdots + d_s = |G : H|$$

Oft ist $r_i^{-1} g^{d_i} r_i$ für $i \in \{1, .., s\}$, also

$$V_{H/K}^G(g) = g^{|G:H|} K$$

Beispiele:

(i) Ist $g \in Z(G)$, so gilt stets

$$V_{H/K}^G(g) = g^{|G:H|} K$$

(ii) Die Abbildung

$$G \to Z(G) \quad , \quad g \mapsto g^{|G:Z(G)|}$$

ist ein Homomorphismus, denn

$$V_{Z(G)/\{1\}}^G(g) = g^{|G:Z(G)|}\,\{1\}$$

Beachte dass für $g \in G$ nach Lemma 4.1.6 tatsächlich $g^{|G:Z(G)|} \in Z(G)$ ist.

9.2 Die Fokalgruppe

9.2.1 Definition: Fokalgruppe

Für jede Untergruppe H einer endlichen Gruppe G heißt

$$\mathrm{Foc}_G(H) := \langle [g,h] : g \in G,\ h \in H,\ [g,h] \in H \rangle = \left\langle xy^{-1} : x, y \in H,\ x \sim_G y \right\rangle$$

Fokalgruppe von H in G.

Bemerkungen:

(i) $H' \subseteq \mathrm{Foc}_G(H) \subseteq H \cap G'$. Insbesondere ist $\mathrm{Foc}_G(H) \trianglelefteq G$ und $H/\mathrm{Foc}_G(H)$ abelsch.

(ii) Für $g \in G,\ h \in H$ mit $[g,h] \in H$ ist

$$ghg^{-1}\,\mathrm{Foc}_G(H) = ghg^{-1}h^{-1}\,\mathrm{Foc}_G(H)h = [g,h]\,\mathrm{Foc}_G(H)h = \mathrm{Foc}_G(H)h = h\,\mathrm{Foc}_G(H)$$

Daher

$$V_{H/\mathrm{Foc}_G(H)}^G(h) = h^{|G:H|}\,\mathrm{Foc}_G(H) \quad \forall\ h \in H$$

9.2.2 Satz über die Fokalgruppe

Seien G eine endliche Gruppe, $H \leq G$, $F := \mathrm{Foc}_G(H)$, $N := \ker\left(V_{H/F}^G\right)$ und $\mathrm{ggT}\left(|G:H|, |H:F|\right) = 1$. Dann gilt:

(i) $F = H \cap G' = H \cap N$

(ii) $HN = G$ und $G/N \cong H/F$

(iii) $G/G' = HG'/G' \oplus N/G'$

Beispiel: Die ggT-Bedingung ist z.B. erfüllt, wenn H eine Hallgruppe ist.

9.2.3 Definition: Hyperfokale Untergruppe

Sei H eine Untergruppe einer endlichen Gruppe G. Man setzt $H_{[1]} := H$ und rekursiv $H_{[n+1]} := \mathrm{Foc}_G(H_{[n]})$, $n \in \mathbb{N}$. Ist nun $H_{[m]} = 1$ für irgendein $m \in \mathbb{N}$, so heißt H *hyperfokal* in G.

Bemerkung: Gegebenfalls ist jede Untergruppe $K \leq H$ auch hyperfokal in G, denn

$$\mathrm{Foc}_G(K) \subseteq \mathrm{Foc}_G(H)$$

Ferner ist H auch hyperfokal in jeder Untergruppe $U \leq G$ mit $H \leq U$, denn

$$\mathrm{Foc}_U(H) \subseteq \mathrm{Foc}_G(H)$$

Schließlich ist H wegen $H_{(n)} \subseteq H_{[n]}$ nilpotent.

9.2.4 Satz: Komplemente hyperfokaler Hallgruppen

Jede hyperfokale Hallgruppe H einer endlichen Gruppe G hat ein normales Komplement in G.

9.2.5 Satz über nilpotente Hallgruppen

Sei H eine nilpotente Hallgruppe einer endlichen Gruppe G. Je zwei Elemente in H die in G konjugiert sind, seien auch schon in H konjugiert. Dann hat H ein normales Komplement in G.

9.2.6 Satz über abelsche Hallgruppen

Sei H eine abelsche Hallgruppe einer endlichen Gruppe G. Dann sind je zwei Elemente $x, y \in H$, die in G konjugiert sind, auch in $\mathcal{N}_G(H)$ konjugiert.

9.2.7 Satz von Burnside

Jede Hallgruppe H einer endlichen Gruppe G mit

$$\mathcal{N}_G(H) = C_G(H)$$

hat ein normales Komplement in G.

9.2.8 Satz: Komplemente zyklischer Sylowgruppen

Seien G eine endliche Gruppe, p der kleinste Primteiler von $|G|$ und $P \in \mathrm{Syl}_p(G)$ zyklisch. Dann hat P ein normales Komplement in G.

Bemerkung: Hat G eine zyklische 2-Sylowgruppe P, so hat P ein normales Komplement K in G nach dem Satz. Wegen $2 \nmid |K|$ ist K auflösbar (Feit-Thomson). Daher ist auch G auflösbar.

Spezialfall: Aus dem Satz folgt insbesondere, dass für ungerade n, jede Gruppe der Ordnung $2n$, einen Normalteiler der Ordnung n enthält.

9.2.9 Satz über Sylowgruppen & Auflösbarkeit

Sind alle Sylowgruppen einer endlichen Gruppe G zyklisch, so ist G auflösbar.

Bemerkung: Speziell sind also Gruppen quadratfreier Ordnung[3] n stets auflösbar.

Beispiel: Jede Gruppe der Ordnung $2 \cdot 3 \cdot 5 \cdot 7 = 210$ ist auflösbar.

[3] Das heißt $n = p_1 \cdot .. \cdot p_r$ mit paarweise verschiedenen Primzahlen $p_1, .., p_r \in \mathbb{P}$.

9.2.10 Lemma über einfache, nicht-abelsche Gruppen

Die Ordnung einer nicht-abelschen, endlichen, einfachen Gruppe G ist durch 12, oder die dritte Potenz ihres kleinsten Primteilers p teilbar.

Beispiel: Sei G eine einfache Gruppe der Ordnung $pqrs,\ p,q,r,s \in \mathbb{P}$, o.B.d.A. $p \leq q \leq r \leq s$. Da Gruppen der Ordnung $p^2 s$ auflösbar sind, folgt $12 \mid |G|$, das heißt $p = q = 2,\ r = 3$. Da Gruppen der Ordnung $2^2 \cdot 3$ auflösbar sind, folgt $s \geq 5$. Sei $S \in \mathrm{Syl}_5(G)$, dann $1 \neq |G : \mathcal{N}_G(S)| \,|12$ und $|G : \mathcal{N}_G(S)| = 1 (\mathrm{mod}\ 5)$, insbesondere $|G : \mathcal{N}_G(S)| \geq 6$, also

$$|G : \mathcal{N}_G(S)| \in \{6, 12\}$$

Im Fall $|G : \mathcal{N}_G(S)| = 12$ wäre $s = 11$ und $|\mathcal{N}_G(S)| = 11$, also $S = \mathcal{N}_G(S)$. Insbesondere wäre

$$\underbrace{C_G(S)}_{\supset S} = \mathcal{N}_G(S)$$

(da S abelsch) ein Widerspruch nach Burnside 9.2.7. Also $|G : \mathcal{N}_G(S)| = 6$, das heißt $s = 5$ bzw. $|G| = 60$ und nach Satz 8.2.15 $G \cong \mathrm{Alt}(5)$.

Bemerkung: Jede einfache, nicht-abelsche Gruppe G mit $|G| \leq 1000$ ist isomorph zu $\mathrm{PSL}(2, \mathbb{F}_q)$ für eine geeignete Primzahlpotenz q. Mögliche Ordnungen sind z.B. 60, 168, 360, 504, 660.

9.3 Endliche, p-nilpotente Gruppen

9.3.1 Satz über Komplemente von Sylowgruppen

Sei $p \in \mathbb{P}$. Für jede endliche Gruppe G sind äquivalent:

1. Jede p-Sylowgruppe von G hat ein normales Komplement in G.
2. Eine p-Sylowgruppe von G hat ein normales Komplement in G.
3. $G/\mathcal{O}_{p'}(G)$ ist eine p-Gruppe.
4. G hat einen p'-Normalteiler K derart, dass G/K eine p-Gruppe ist.

9.3.2 Definition: p-Potenz

Sei G eine endliche Gruppe und $p \in \mathbb{P}$. Gilt eine (und somit alle) der Bedingungen in Satz 9.3.1, so heißt G p-nilpotent.

Bemerkung: Gegebenfalls ist $\mathcal{O}_{p'}(G)$ das einzige normale Komplement jeder p-Sylowgruppe von G.

Beispiele:

(i) Jede endliche, nilpotente Gruppe ist nach Satz 8.1.13 auch p-nilpotent. Ist umgekehrt G q-nilpotent $\forall\, q \in \mathbb{P}$ mit $q \mid |G|$, dann ist G nilpotent, denn wegen

$$\bigcap_{\substack{q \in \mathbb{P} \\ q \mid |G|}} \mathcal{O}_{q'}(G) = \{1\}$$

ist die kanonische Abbildung

$$G \to \bigtimes_{\substack{q \in \mathbb{P} \\ q \mid |G|}} G/\mathcal{O}_{q'}(G)$$

ein Monomorphismus in ein direktes Produkt von q-Gruppen.

(ii) Nach Burnside ist eine endliche Gruppe G p-nilpotent, wenn ein $P \in \mathrm{Syl}_p(G)$ existiert mit $\mathcal{N}_G(P) = C_G(P)$.

9.3.3 Lemma über p-nilpotente Gruppen

Sei $p \in \mathbb{P}$ und G eine p-nilpotente Gruppe. Dann ist auch jede Untergruppe und jede Faktorgruppe von G p-nilpotent.

9.3.4 Satz von Frobenius

Sei $p \in \mathbb{P}$. Für jede endliche Gruppe G und $P \in \mathrm{Syl}_p(G)$ sind äquivalent:

1. G ist p-nilpotent.
2. Für jede p-Untergruppe $\{1\} \neq Q \leq G$ ist $\mathcal{N}_G(Q)$ p-nilpotent.
3. Für jede p-Untergruppe $\{1\} \neq Q \leq G$ ist $\mathcal{N}_G(Q)/C_G(Q)$ eine p-Gruppe.
4. Für jede p-Untergruppe $\{1\} \neq Q \leq G$ und alle $R \in \mathrm{Syl}_p(\mathcal{N}_G(Q))$ ist $\mathcal{N}_G(Q) = RC_G(Q)$.
5. Für jede Untergruppe $Q \leq P$ und alle $g \in G$ mit $Q \leq gPg^{-1}$ existieren $z \in C_G(Q),\ \eta \in P$ mit $g = z\eta$.
6. Je zwei Elemente in P, die in G konjugiert sind, sind auch in P konjugiert.

10 Symbol-Referenz

$\mathbb{R}_+$: $= [0, \infty)$.

$\mathbb{C}_+$: $\mathbb{R}_+ + i\mathbb{R}_+$.

$\mathbb{K}$: Beliebiger Körper.

$\mathbb{K}_+$: Für beliebigen Körper $\mathbb{K}_+ := \mathbb{K} \setminus \{0\}$.

$\mathbb{P}$: Primzahlen.

$\mathcal{N}_G(U)$: Normalisator von $U \leq G$ in G, siehe 6.2.9.

$C_G(U)$: Zentralisator von $U \leq G$ in G, siehe (8.1.1.1).

$\mathrm{Core}_G(U)$: Kern von U in G, siehe (7.0.22.1).

$Z(G)$: Zentrum von G, siehe 3.2.7.

ad_g: Durch $g \in G$ induzierter, innerer Automorphismus auf G, siehe 3.2.7.

$\mathrm{St}_G(\omega)$: Stabilisator der Gruppenoperation von G auf Ω, bzgl. $\omega \in \Omega$. Siehe 7.0.20.

$|G : U| := |G/U| = |U \setminus G|$. Index von $U \leq G$ in G, siehe 3.3.5.

$\mathrm{Inn}(G)$: Gruppe aller inneren Automorphismen von G, siehe 3.2.7.

$\mathrm{Aut}(G)$: Gruppe aller Automorphismen von G.

$U \leq G$: U ist Untergruppe von G.

$U \trianglelefteq G$: U ist normal in G, siehe 4.1.2.

e_{ij}: Standardbasis in $\mathbb{K}^{n \times n}$.

$u_{ij}(\alpha)$: Elementare Matrix(operation), die durch Linksmultiplikation das α-fache der j-ten Zeile auf die i-te Zeile addiert. Siehe 8.4.3.1.

$\mathrm{PGL}(V)$: Projektive, allgemeine, lineare Gruppe über dem Vektorraum V. Siehe Bemerkung (i) in 8.4.1.

$\mathrm{PSL}(V)$: Projektive, spezielle, lineare Gruppe über dem Vektorraum V. Siehe Bemerkung (ii) in 8.4.1.

$\mathrm{Syl}_p(G)$: p-Sylowgruppen der Gruppe G. Siehe 8.1.7.

$\mathrm{Hall}_\pi(G)$: π-Hallgruppen der Gruppe G. Siehe 8.3.1.

$\mathcal{O}_\pi(G)$: π-Kern der Gruppe G. Siehe Bemerkung in Satz von Galois 8.3.10.