Gruppentheorie

Prof. Dr. Burkhard Külshammer

Semester: SS 2009

Vorwort

Dieses Dokument wurde als Skript für die auf der Titelseite genannte Vorlesung erstellt und wird jetzt im Rahmen des Projekts „Vorlesungsskripte der Fakultät für Mathematik und Informatik“ weiter betreut. Das Dokument wurde nach bestem Wissen und Gewissen angefertigt. Dennoch garantiert weder der auf der Titelseite genannte Dozent, die Personen, die an dem Dokument mitgewirkt haben, noch die Mitglieder des Projekts für dessen Fehlerfreiheit. Für etwaige Fehler und dessen Folgen wird von keiner der genannten Personen eine Haftung übernommen. Es steht jeder Person frei, dieses Dokument zu lesen, zu verändern oder auf anderen Medien verfügbar zu machen, solange ein Verweis auf die Internetadresse des Projekts `http://uni-skripte.lug-jena.de/` *enthalten ist.*

Diese Ausgabe trägt die Versionsnummer 3482 und ist vom 25. Juli 2011. Eine neue Ausgabe könnte auf der Webseite des Projekts verfügbar sein.

Jeder ist dazu aufgerufen, Verbesserungen, Erweiterungen und Fehlerkorrekturen für das Skript einzureichen bzw. zu melden oder diese selbst einzupflegen – einfach eine E-Mail an die Mailingliste `<uni-skripte@lug-jena.de>` *senden. Weitere Informationen sind unter der oben genannten Internetadresse verfügbar.*

Hiermit möchten wir allen Personen, die an diesem Skript mitgewirkt haben, vielmals danken:

- *Jens Kubieziel* `<jens@kubieziel.de>` *(2009)*
- *Stilianos Louca* `<stilianos.louca@uni-jena.de>` *(2009)*

Inhaltsverzeichnis

Auflistung der Theoreme

Sätze

Definitionen und Festlegungen

1. Einführung

Im folgenden sind einige Beispiele für Gruppen genannt. Die Beispiele erstrecken sich über verschiedene Gebiete der Mathematik. Denn die Gruppenstruktur ist immer wieder anzutreffen.

1.1. Zahlbereiche

(i) $(\mathbb{Z}, +), (\mathbb{Q}, +)$

(ii) $(\mathbb{Q} \setminus \{0\}, \cdot)$

(iii) $\mathbb{Z}/_{n\mathbb{Z}}$ der Restklassenring bzw. die Restklassengruppe modulo n mit der Addition.

(iv) $(\mathbb{Z}/_{n\mathbb{Z}})^\times = \{\, a + n\mathbb{Z} \mid \mathrm{ggT}(a, n) = 1 \,\}$ prime Restklassengruppe modulo n mit der Multiplikation

1.2. Lineare Algebra

Sei $\mathbb{K}$ ein Körper und V ein $\mathbb{K}$-Vektorraum. Dann haben wir:

(i) $\mathrm{GL}(n, \mathbb{K}) = \left\{\, A \in \mathbb{K}^{n\times n} \;\middle|\; |A| \neq 0 \,\right\}$ mit der Matrixmultiplikation. Dies ist die allgemeine lineare Gruppe des Grades n über $\mathbb{K}$.

(ii) $\mathrm{GL}(V) = \{\, f\colon V \to V \mid f \text{ linear und bijektiv} \,\}$.

(iii) $\mathrm{SL}(n, \mathbb{K}) = \left\{\, A \in \mathbb{K}^{n\times n} \;\middle|\; |A| = 1 \,\right\}$ die spezielle lineare Gruppe des Grades n über $\mathbb{K}$.

Sei V ein euklidischer Vektorraum mit dem Skalarprodukt

(i) $\mathrm{O}(V) = \{\, f\colon V \to V \mid f \text{ Isometrie} \,\}$ ist die orthogonale Gruppe von V. Dabei bedeutet Isometrie, dass f linear ist und für alle x, y aus V gilt: $\langle f(x), f(y)\rangle = \langle x, y\rangle$.

(ii) $\mathrm{O}(n) = \mathrm{O}(n, \mathbb{R}) = \left\{\, A \in \mathbb{R}^{n\times n} \;\middle|\; A^\mathsf{T} A = 1_n \,\right\}$ orthogonale Gruppe des Grades n.

Sei V ein unitärer Vektorraum mit dem Skalarprodukt

(i) $\mathrm{U}(V) = \{\, f\colon V \to V \mid f \text{ Isometrie} \,\}$ unitäre Gruppe von V

(ii) $U(n) = U(n, \mathbb{C}) = \left\{ A \in \mathbb{C}^{n \times n} \;\middle|\; \overline{A}^T A = 1_n \right\}$

1.3. Kombinatorik

Sei Ω eine Menge.

(i) $\mathrm{Sym}(\Omega) = \{ f \colon \Omega \to \Omega \mid f \text{ bijektiv} \}$ symmetrische Gruppe auf Ω

(ii) $\mathrm{Alt}(\Omega) = \{ f \in \mathrm{Sym}(\Omega) \mid f \text{ gerade} \}$ alternierende Gruppe auf Ω. Dabei muss Ω endlich sein.

1.4. Geometrie

(i) $\mathrm{AO}(\mathbb{R}^n) = \{ f \colon \mathbb{R}^n \to \mathbb{R}^n \mid \|f(x) - f(y)\| = \|x - y\| \forall x, y \in \mathbb{R}^n \}$ Bewegungsgruppe.

(ii) Die Symmetriegruppe des regelmäßigen n-Ecks P_n wird als **Diedergruppe** mit $G = \left\{ f \in \mathrm{AO}(\mathbb{R}^2) \;\middle|\; f(P_n) = P_n \right\}$ bezeichnet.. Die Gruppe hat $2n$ Elemente.

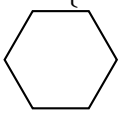
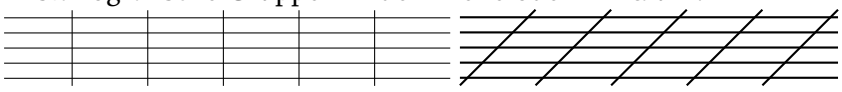


Bild der P_6-Gruppe

(iii) Friesgruppen: Symmetriegruppen von Friesen.

(iv) kristallografische Gruppen in der Ebene oder im Raum:



(v) Symmetriegruppen von Tetraeder, Würfel, Ikosaeder und ähnlichen Objekten.

1.5. Algebra

Sei $L|K$ eine Körpererweiterung. Diese besitzt eine GALOISgruppe

$$\mathbb{F}(L|K) = \{ f \colon L \to L \mid f \text{ Automorphismus von } L, f|K = \mathrm{id}_K \}$$

1.6. Topologie

(i) Fundamentalgruppen, Homologiegruppen, ...,

1.7. Zahlentheorie

Sei K ein algebraischer Zahlkörper und $\mathcal{O}_K$ der Ganzheitsring.

(i) Einheitengruppe: $\mathcal{O}_K^\times = \{\, a \in \mathcal{O}_K \setminus \{0\} \mid 1/a \in \mathcal{O}_K \,\}$

(ii) Klassengruppe

1.8. Beliebige mathematische Theorie

Sei M ein Objekt dieser Theorie. Dann hat man mindestens eine Gruppe, die Automorphismengruppe $\mathrm{Aut}(M)$ von M. Beispiele sind Lie-Algebren, Codierungstheorie, BANACHräume etc.

2. Halbgruppen

Definition 2.1 (Monade, Magma)
Sei M eine Menge. Darauf legen wir eine **Verknüpfung** $M \times M \to M$ mit $(a, b) \mapsto a \times b$ fest.[1] Dann bezeichnet man $(M, \times)$ als **Monade** oder **Magma**.

Beispiel 2.1

(i) Die Addition, Subtraktion und Multiplikation auf den natürlichen, reellen und komplexen Zahlen.

(ii) Der Durchschnitt oder die Vereinigung auf der Potenzmenge $\mathfrak{P}(X)$.

(iii) Der größte gemeinsame Teiler oder das kleinste gemeinsame Vielfache auf $\mathbb{N}$.

(iv) Die Verknüpfung von Abbildungen $\circ$ auf der Menge aller Abbildungen $\mathrm{Abb}(X) = \{ f\colon X \to X \mid f \text{ Abbildung} \}$

Bemerkung 2.1
Wenn M klein ist, kann man eine Verknüpfungstafel aufstellen. Ein Beispiel sind die Wahrheitswerte.

$\wedge$	w	f
w	w	f
f	f	f

Tabelle 2.1.: Wahrheitswerte für die UND-Verknüpfung

Definition 2.2 (rechts-, linksneutral, neutral)
Sei M eine Monade und $e \in M$. Das Element e ist genau dann **rechtsneutral** (oder **linksneutral**), wenn für alle $a \in M$ gilt: $ae = a$ (oder $ea = a$). Man nennt e genau dann **neutral**, wenn es rechts- und linksneutral ist.

Bemerkung 2.2
Sei $e \in M$ linksneutral und $f \in M$ rechtsneutral. Dann folgt, $e = ef = f$. Insbesondere existiert in M höchstens ein neutrales Element.

Beispiel 2.2
Die 0 ist neutral in $(\mathbb{Z}, +)$ und die 1 ist neutral in $(\mathbb{Z}, \cdot)$.

[1] alternativ auch $a + b$, $a \cdot b$ oder ab

Definition 2.3 (Vertauschbarkeit, Kommutativität)
Sei M eine Monade und $a, b \in M$. Die Elemente a und b heißen **vertauschbar**, wenn gilt: $ab = ba$. Die Menge M heißt **kommutativ** oder **abelsch**, wenn alle Elemente vertauschbar sind.

Definition 2.4 (Halbgruppe, Monoid)
Die Menge M heißt genau dann **Halbgruppe**, wenn $(xy)z = x(yz)$ gilt und **Monoid**, wenn M eine Halbgruppe mit neutralem Element ist.

Beispiel 2.3

(i) $(\mathbb{N}, +)$ Halbgruppe, $(\mathbb{N}_0, +)$ Monoid

(ii) Sei X eine Menge. Dann ist $\mathrm{Abb}(X)$ ein Monoid mit der **identischen Abbildung** $\mathrm{id}_X \colon X \to X, x \mapsto x$ als neutrales Element.

(iii) Sei $A \neq \emptyset$ eine Menge (**Alphabet**). Die Elemente von A heißen **Buchstaben**. Ein **Wort** über A ist die endliche Folge $w = (a_1, \ldots, a_m) =: a_1 \cdot \ldots \cdot a_m$. Die **freie Halbgruppe** über A ist definiert als $W := \{ w \mid w \text{ Wort über } A \}$. Das **leere Wort** ist $\varepsilon = () \notin W$. Dann können wir das **freie Monoid** über A mit $W_0 := W \cup \{\varepsilon\}$ definieren. Die zugehörige Abbildung ist definiert als $(a_1, \ldots, a_m) \circ (b_1, \ldots, b_m) := (a_1, \ldots, a_m, b_1, \ldots, b_m)$.

Bemerkung 2.3
Die neutralen Elemente werden oft mit 1 bezeichnet. Falls $+$ die Verknüpfung bezeichnet, verwendet man auch 0 als neutrales Element.

Definition 2.5 (Invertierbarkeit)
Sei M ein Monoid und $a \in M$. Das Element a heißt genau dann **rechtsinvertierbar** (oder **linksinvertierbar**), wenn ein Element $b \in M$ mit $ab = 1$ (oder $ba = 1$) existiert. Man bezeichnet b als das **Rechtsinverse** oder **Linksinverse** zu a.

Bemerkung 2.4
Sei $b \in M$ rechtsinvers und $c \in M$ linksinvers zu $a \in M$. Dann folgt, $b = 1b = (ca)b = c(ab) = c1 = c$. Das Element a heißt dann **invertierbar** und b **Inverses** zu a. Wir schreiben $b =: a^{-1}$ oder bei der Addition $b =: -a$. Es gilt: $a^{-1}a = 1 = aa^{-1}$. Damit ist auch a^{-1} invertierbar und wir haben $(a^{-1})^{-1} = a$. Wenn zwei Elemente $x, y \in M$ invertierbar sind, dann ist xy invertierbar und $(xy)^{-1} = y^{-1}x^{-1}$. Denn $xyy^{-1}x^{-1} = x1x^{-1} = 1$.

Beispiel 2.4
Sei $\mathbb{K}$ ein Körper und n eine natürliche Zahl. Dann folgt für das Monoid bezüglich der Matrixmultiplikation $\mathbb{K}^{n \times n}$ mit der Einheitsmatrix als neutrales Element, dass eine Matrix $A \in \mathbb{K}^{n \times n}$ invertierbar ist, wenn A eine reguläre Matrix ist, d. h. die Determinante von A ist ungleich 0. In der linearen Algebra impliziert die Linksinvertierbarkeit auch die Rechtsinvertierbarkeit.

Definition 2.6 (Potenz)
Sei H eine Halbgruppe und $a \in H, n \in \mathbb{N}$. Die n-te **Potenz** von a ist definiert als $a^n := a \cdot \ldots \cdot a$ mit n Faktoren. Wenn H ein Monoid ist, gilt: $a^0 := 1$. Sollte a invertierbar sein, dann können wir negative Potenzen festlegen: $a^{-n} = (a^{-1})^n$.

Bemerkung 2.5
Rechenregel: $a^n a^m = a^{n+m}, (a^n)^m = a^{nm}$, wenn a, b vertauschbar sind, gilt auch: $(ab)^n = a^n b^n$. Ist $+$ die Verknüpfung, so schreibt man: na statt a^n. Dann sehen die Rechenregeln so aus: $(m+n)a = ma + na, m(na) = (mn)a$, wenn a, b vertauschbar sind, so gilt noch: $n(a+b) = na + nb$.

Definition 2.7 (Homomorphismus)
Seien M, N zwei Monaden und wir betrachten die Abbildung $f\colon M \to N$.

(i) Die Abbildung f heißt genau dann **Homomorphismus**, wenn für alle $a, b \in M$ gilt: $f(ab) = f(a)f(b)$.

(ii) f Monomorphismus $\Leftrightarrow$ f injektiver Homomorphismus

(iii) f Epimorphismus $\Leftrightarrow$ f surjektiver Homomorphismus

(iv) f Isomorphismus $\Leftrightarrow$ f bijektiver Homomorphismus

(v) f Endomorphismus $\Leftrightarrow$ f Homomorphismus und $M = N$

(vi) f Automorphismus $\Leftrightarrow$ f bijektiver Endomorphismus

Wir setzen $\mathrm{Hom}(M, N) := \{ f\colon M \to N \mid f \text{ Homomorphismus} \}, \mathrm{End}(M) := \mathrm{Hom}(M, M)$ und $\mathrm{Aut}(M) := \{ f \in \mathrm{End}(M) \mid f \text{ bijektiv} \}$.

Beispiel 2.5
(i) Sei $\mathbb{K}$ ein Körper und n eine natürliche Zahl. Dann ist $\det\colon (\mathbb{K}^{n\times n}, \cdot) \to (\mathbb{K}, \cdot)$ ein Homomorphismus.

(ii) Die Exponentialfunktion von $(\mathbb{R}, +)$ auf $(\mathbb{R}, \cdot)$.

(iii) Sei W die freie Halbgruppe über einem Alphabet A und $w \in W$ mit $w = a_1, \ldots, a_n$ und $a_1, \ldots, a_n \in A$. Die Funktion $l(w) := n$ ist die Länge des Wortes. Dann ist $l\colon W \to (\mathbb{N}, +)$ ein Homomorphismus.

Bemerkung 2.6
(i) Seien L, M, N Monaden und $f \in \mathrm{Hom}(L, M), g \in \mathrm{Hom}(M, N)$. Dann ist $g \circ f \in \mathrm{Hom}(L, N)$ ein Homomorphismus. Denn $(g \circ f)(ab) = g(f(ab)) = g(f(a) \cdot f(b)) = g(f(a)) \cdot g(f(b)) = (g \circ f)(a) \cdot (g \circ f)(b)$ für $a, b \in L$.

(ii) Sei f ein Isomorphismus. Dann ist f^{-1} ebenfalls ein Isomorphismus. Denn $f^{-1}(xy) = f^{-1}(f(f^{-1}(x)) \cdot f(f^{-1}(y))) = f^{-1}(f(f^{-1}(x) \cdot f^{-1}(y))) = f^{-1}(x)f^{-1}(y)$.

Definition 2.8 (isomorph)
Die Monaden M, N heißen **isomorph** ($M \cong N$), falls ein Isomorphismus $f\colon M \to N$ existiert.

Beispiel 2.6
Es gilt: $(\{w, f\}, \vee) \cong (\{0, 1\}, \cdot)$. Zum Nachweis kann man die Verknüpfungstafel prüfen.

Satz 2.1
Die Isomorphie ist eine Äquivalenzrelation, d. h. es gilt:

(i) $M \cong M$ (Reflexivität)

(ii) $M \cong N \Rightarrow N \cong M$ (Symmetrie)

(iii) $L \cong M \wedge M \cong N \Rightarrow L \cong N$ (Transitivität)

3. Gruppen

Definition 3.1 (Gruppe)
Eine **Gruppe** ist eine Halbgruppe G mit einem linksneutralen Element e, in der zu jedem Element $g \in G$ ein weiteres $h \in G$ mit $hg = e$ existiert.

Satz 3.1
Eine Gruppe ist ein Monoid, in dem jedes Element invertierbar ist.

BEWEIS:
Seien G, e, g, h wie oben. Zu dem Element h existiert ein $k \in G$ mit $kh = e$. Dann ist $ke = khg = eg = g$ und weiter $ge = kee = ke = g$. Folglich ist e neutral. Für den Nachweis der Rechtsinvertierbarkeit sei $g = ke = k$, d. h. $gh = e$. Somit ist g invertierbar. ∎

Beispiel 3.1

(i) $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +)$ sind abelsch. Dagegen ist $(\mathbb{N}, +)$ *keine* Gruppe.

(ii) $(\mathbb{Q} \setminus \{0\}, \cdot), (\mathbb{R} \setminus \{0\}, \cdot), (\mathbb{C} \setminus \{0\}, \cdot)$. Aber $(\mathbb{Z} \setminus \{0\}, \cdot)$ ist *keine* Gruppe.

(iii) Sei M ein Monoid und $U(M) := \{ a \in M \mid a \text{ invertierbar} \}$. Dann heißt $U(M)$ **Einheitengruppe** von M.

(iv) Sei X eine Menge und die Einheiten aller Abbildungen von X in sich: $U(\mathrm{Abb}(X)) = \{ f \colon X \to X \mid f \text{ bijektiv} \}$. Dies wird als **symmetrische Gruppe** $\mathrm{Sym}(X)$ auf X bezeichnet. Die Elemente der Gruppe heißen **Permutation**en auf X. Für $X = \{1, \ldots, n\}$ schreibt man $\mathrm{Sym}(n) := \mathrm{Sym}(X)$. Die Elemente heißen dann Permutationen des Grades n. Schreibweise:

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

Dann ist

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

(v) Sei $\mathbb{K}$ ein Körper und $n \in \mathbb{N}$. Dann ergibt sich die Einheitengruppe von $(\mathbb{K}^{n \times n}, \cdot)$ durch $U(\mathbb{K}^{n \times n}, \cdot) = \left\{ A \in \mathbb{K}^{n \times n} \;\middle|\; \det A \neq 0 \right\} =: \mathrm{GL}(n, \mathbb{K})$.

(vi) Für jede nichtleere Familie $(G_i)_{i \in I}$ von Gruppen G_i. Dann ist auch das **direkte Produkt** $\prod_{i \in I} G_i = \bigtimes_{i \in I} G_i = \{ (g_i)_{i \in I} \mid g_i \in G_i \forall i \in I \}$ eine Gruppe mit $(g_i)(h_i) := (g_i h_i)$. Im Fall $I = \{1, \ldots, n\}$ schreibt man $\prod_{i=1}^{n} G_i = \bigtimes_{i=1}^{n} = G_1 \times \ldots \times G_n$.

Definition 3.2 (Ordnung)
Die **Ordnung** $|G|$ einer Gruppe ist die Anzahl ihrer Elemente.

Satz 3.2

(i) Sei $n \in \mathbb{N}$. Dann ist $|\mathrm{Sym}(n)| = n!$.

(ii) Sei $\mathbb{K}$ ein Körper und $|\mathbb{K}| = q < \infty$. Dann ist $|\mathrm{GL}(n, \mathbb{K})| = (q^n - 1)(q^n - q) \cdot \ldots \cdot (q^n - q^{n-1})$.

BEWEIS:

(i) Sei $f \in \mathrm{Sym}(n) \Rightarrow f(1) \in \{1, \ldots, n\}, f(2) \in \{1, \ldots, n\} \setminus \{f(1)\}, f(3) \in \{1, \ldots, n\} \setminus \{f(1), f(2)\}, \ldots$.

(ii) Sei $A = (a_{ij}) \in \mathrm{GL}(n, \mathbb{K}) \Rightarrow a_1 := (a_{11}, \ldots, a_{1n}) \in \mathbb{K}^n \setminus \{0\}, a_2 := (a_{21}, \ldots, a_{2n}) \in \mathbb{K}^n \setminus \mathrm{span}(a_1), a_3 := (a_{31}, \ldots, a_{3n}) \in \mathbb{K}^n \setminus \mathrm{span}(a_1, a_2), \ldots$. ∎

Satz 3.3
Sei $f\colon G \to H$ ein Gruppenhomomorphismus. Dann ist $f(1_G) = 1_H$ und $f(g^{-1}) = f(g)^{-1}$ für $g \in G$.

BEWEIS:
Es gilt: $f(1_G) = f(1_G)1_H = f(1_G)f(1_G)f(1_G)^{-1} = f(1_G \cdot 1_G)f(1_G)^{-1} = 1_H$ und weiter: $f(g^{-1}) = f(g^{-1})1_H = f(g^{-1})f(g)f(g)^{-1} = f(g^{-1}g)f(g)^{-1} = f(1_G)f(g)^{-1} = 1_H f(g)^{-1} = f(g)^{-1}$. ∎

Beispiel 3.2
Sei $\mathbb{K}$ ein Körper und n eine natürliche Zahl. Dann ist $\det\colon \mathrm{GL}(n, \mathbb{K}) \to \mathbb{K} \setminus \{0\}$ ein Homomorphismus. Somit folgt, $\det(1_n) = 1$ und $\det(a^{-1}) = \det(a)^{-1}$.

Definition 3.3 (Untergruppe)
Eine Teilmenge U einer Gruppe G heißt **Untergruppe** von G, wenn gilt:

(i) $1_G \in U$

(ii) $a, b \in U \Rightarrow ab, a^{-1} \in U$

Bemerkung 3.1
Gegebenenfalls ist U mit der entsprechend eingeschränkten Verknüpfung selbst eine Gruppe. Wir schreiben dann $U \leqslant G$ oder $U < G$, wenn $U \neq G$ ist. Man bezeichnet U dann als **echte Untergruppe**.

Beispiel 3.3

(i) $(\mathbb{Z}, +) < (\mathbb{Q}, +) < (\mathbb{R}, +) < (\mathbb{C}, +)$.

(ii) In jeder beliebigen Gruppe G sind G selbst und die **triviale Untergruppe** $\{1_G\} = 1$ Untergruppen.

(iii) Für jede nichtleere Familie $(G_i)_{i\in I}$ von Gruppen bilden die Elemente $(g_i)_{i\in I}$ aus dem direkten Produkt mit $|\{\, i \in I \mid g_i \neq 1 \,\}| < \infty$ eine Untergruppe von $\prod_{i\in I} G_i$. Diese heißt **direktes eingeschränktes Produkt** von $(G_i)_{i\in I}$. Hierfür nutzen wir die Schreibweise: $\coprod_{i\in I} G_i$. Für $|I| < \infty$ ist $\coprod_{i\in I} G_i = \prod_{i\in I} G_i$.

(iv) Für jede Monade M ist die Automorphismengruppe $\mathrm{Aut}(M)$ eine Untergruppe von $\mathrm{Sym}(M)$.

Satz 3.4
Eine nichtleere Teilmenge U einer Gruppe G ist genau dann eine Untergruppe von G, wenn gilt: $a, b \in U \Rightarrow ab^{-1} \in U$.

BEWEIS:
Wir brauchen nur die Rückrichtung zu zeigen. Die andere Richtung ist klar. Sei dazu U eine nichtleere Teilmenge von G und die obige Bedingung erfüllt. Dann existiert ein $x \in U$. Folglich $1_G = xx^{-1} \in U$. Also $x^{-1} = 1_G x^{-1} \in U$. Andererseits gilt für $y \in U$: $x(y^{-1})^{-1} \in U$. ∎

Definition 3.4
Für Teilmengen X, Y einer Gruppe G setzt man: $XY := \{\, xy \mid x \in X, y \in Y \,\}$ und $X^{-1} := \left\{\, x^{-1} \;\middle|\; x \in X \,\right\}$.

Bemerkung 3.2
Dann ist $(X^{-1})^{-1} = X$, $(XY)^{-1} = Y^{-1}X^{-1}$, $(XY)Z = X(YZ)$ für $X, Y, Z \subseteq G$. Der Satz 3.4 besagt: $X \leqslant G \Leftrightarrow X \neq \emptyset \wedge XX^{-1} \subseteq X$.

Satz 3.5
Für Untergruppen U, V, W einer Gruppe G gilt stets:

(i) $U \cup V \leqslant G \Leftrightarrow U \subseteq V \vee V \subseteq U$

(ii) $UV \leqslant G \Leftrightarrow UV = VU$

(iii) $U \subseteq W \Rightarrow UV \cap W = U(V \cap W)$ (**DEDEKINDsche Identität**)

BEWEIS:

(i) „⇒“: Sei $U \cup V \leqslant G$ und $U \not\subseteq V$. Dann gibt es ein Element $u \in U \setminus V$. Für $v \in V$ ist $uv \in U \cup V$. Im Fall $uv \in V$ wäre $u = uvv^{-1} \in V$. ↯ Also muss $uv \in U$ sein und $v = u^{-1}uv \in U$. Daher ist $V \subseteq U$.
„⇐“ ist trivial.

(ii) Sei $UV \leqslant G$. Dann ist $(UV) = (UV)^{-1} = V^{-1}U^{-1} = VU$ und für $UV = VU$ folgt: $(UV)(UV)^{-1} = UVV^{-1}U^{-1} \subseteq UVU$ nach Bemerkung 3.2 und wegen der Kommutativität gilt: $UVU = UUV = UV$. Somit ist UV eine Untergruppe.

(iii) Sei $U \subseteq W$ und $w \in UV \cap W$. Wir schreiben $w = uv$ mit $u \in U$ und $v \in V$. Dann ist $v = u^{-1}w \in W$, d. h. $w = uv \in U(V \cap W)$. Umgekehrt ist $U(V \cap W) \subseteq UV$ und $U(V \cap W) \subseteq WW \subseteq W$, d. h. $U(V \cap W) \subseteq UV \cap W$. ∎

Definition 3.5 (erzeugte Untergruppe)
Für jede nichtleere Familie $(U_i)_{i\in I}$ von Untergruppen U_i einer Gruppe G gilt stets:

$$\bigcap_{i\in I} U_i \leqslant G$$

Insbesondere ist für $X \subseteq G$ der Durchschnitt D aller Untergruppen $U \leqslant G$ mit $X \subseteq U$ eine Untergruppe von G. Man nennt $D =: \langle X\rangle$ die von X **erzeugte Untergruppe** von G. Für $X = \{a_1, \ldots, a_n\}$ schreibt man $\langle a_1, \ldots, a_n\rangle$.

Satz 3.6
Sei G eine Gruppe und $X \subseteq G$. Dann besteht $\langle X\rangle$ aus den Elementen der Form $x_1^{\varepsilon_1} \cdot \ldots \cdot x_n^{\varepsilon_n}$ mit $n \in \mathbb{N}_0, x_1, \ldots, x_n \in X, \varepsilon_1, \ldots, \varepsilon_n \in \{\pm 1\}$. Im Fall $n = 0$ interpretiert man das Produkt als 1.

BEWEIS:
Die Menge A der angegebenen Elemente ist eine Untergruppe von G, die X enthält. Nach Definition 3.5 ist also $\langle X\rangle \subseteq A$. Ist umgekehrt U eine Untergruppe von G, die X enthält, so enthält U auch A. Nach Definition 3.5 ist $A \subseteq \langle X\rangle$. ∎

Beispiel 3.4
Ist $X = \{x\}$, so heißt $\langle x\rangle = \langle X\rangle = \{\, x^n \mid n \in \mathbb{Z}\,\}$ die von x erzeugte **zyklische Untergruppe** von G. Allgemein heißt jede Menge E mit $\langle E\rangle = G$ ein **Erzeugendensystem** von G. Hat die Gruppe G ein endliches Erzeugendensystem, so heißt G **endlich erzeugte Gruppe**. Natürlich ist jede endliche Gruppe endlich erzeugt.

Satz 3.7
Für jeden Gruppenhomomorphismus $f\colon G \to H$ gilt:

(i) Wenn $U \leqslant G$, dann ist $f(U) = \{\, f(u) \mid u \in U\,\} \leqslant H$. Insbesondere ist $\mathrm{Bld}(f) := f(G) \leqslant H$.

(ii) $V \leqslant H \Rightarrow f^{-1}(V) = \{\, g \in G \mid f(g) \in V\,\} \leqslant G$. Insbesondere ist der Kern von f, definiert durch $\ker(f) := f^{-1}(\{1_H\})$, eine Untergruppe von G.

(iii) $U \leqslant G \Rightarrow f^{-1}(f(U)) = U(\ker f) = (\ker f)U$ oder $V \leqslant H \Rightarrow f(f^{-1}(V)) = V \cap \mathrm{Bld}\, f$.

(iv) Wir haben zueinander inverse Bijektionen $\mathfrak{U} = \{\, U \leqslant G \mid \ker f \leqslant U\,\} \leftrightarrows \mathfrak{V} := \{\, V \leqslant H \mid V \leqslant \mathrm{Bld}\, f\,\}$. Es ist $U \mapsto f(U)$ und $V \mapsto f^{-1}(V)$.

BEWEIS:
(i) Sei $U \leqslant G$. Da $U \neq \emptyset$, ist auch $f(U) \neq \emptyset$. Ferner ist $f(U)f(U)^{-1} = f(U)f(U^{-1}) = f(UU^{-1}) \subseteq f(U)$.

(ii) Sei $V \leqslant H$. Weil $f(1_G) = 1_H \in V$ ist $1_G \in f^{-1}(V)$, d. h. $f^{-1}(V) \neq \emptyset$. Seien $a, b \in f^{-1}(V)$, d. h. $f(a), f(b) \in V$. Dann gilt: $f(ab^{-1}) = f(a)f(b)^{-1} \in V$, d. h. $a, b^{-1} \in V$.

(iii) Zunächst sei $U \leqslant G$. Für $x \in f^{-1}(f(U))$ ist $f(x) \in f(U)$. Also ist $f(x) = f(u)$ für $u \in U$. Dann ist $f(x)f(u)^{-1} = 1 = f(xu^{-1})$, d. h. $xu^{-1} \in \ker f$ und $x = xu^{-1}u \in (\ker f)U$. Daher gilt $f^{-1}(f(U)) \subseteq (\ker f)U$. Andererseits ist für $a \in \ker f, b \in U$: $f(ab) = f(a)f(b) = 1_H f(b) = f(b) \in f(U)$, d. h. $ab \in f^{-1}(f(U))$. Also haben wir $f^{-1}(f(U)) = (\ker f)U$. Nach den obigen beiden Punkten ist $(\ker f)U = f^{-1}(f(U)) \leqslant G$. Mit Satz 3.5 (ii) folgt: $(\ker f)U = U(\ker f)$.

Sei nun $V \leqslant H$ und $x \in f(f^{-1}(V))$. Dann ist $x = f(a)$ für ein $a \in f^{-1}(V)$. Folglich ist $x = f(a) \in V \cap \operatorname{Bld} f$. Daher folgt, $f(f^{-1}(V)) \subseteq V \cap \operatorname{Bld} f$. Sei umgekehrt $v \in V \cap \operatorname{Bld} f$ und $g \in G$ mit $v = f(g)$. Dann ist $g \in f^{-1}(V)$ und $v = f(g) \in f(f^{-1}(V))$. Daher sind beide Mengen gleich.

(iv) Sei $U \in \mathfrak{U}$, d. h. $\ker f \subseteq U$. Dann ist auf jeden Fall $f(U) \subseteq \operatorname{Bld} f$, d. h. $f(U) \in \mathfrak{V}$ und $f^{-1}(f(U)) = U(\ker f) \subseteq UU \subseteq U \subseteq f^{-1}(f(U))$. Also ist $f^{-1}(f(U)) = U$.

Sei jetzt $V \in \mathfrak{V}$, d. h. $V \subseteq \operatorname{Bld} f$. Dann wissen wir: $\ker f = f^{-1}(\{1_H\}) \subseteq f^{-1}(V)$. Dies bedeutet nun: $f^{-1}(V) \in \mathfrak{U}$ und $f(f^{-1}(V)) = V \cap \operatorname{Bld} f = V$. ∎

Bemerkung 3.3 (Bild, Urbild, Kern)
Man bezeichnet $f(U)$ als das **Bild** von U unter f, $f^{-1}(V)$ als das **Urbild** von V unter f, $\operatorname{Bld} f$ als das **Bild** von f und $\ker f$ als den **Kern** von f.

Beispiel 3.5

(i) Sei $\mathbb{K}$ ein Körper und n eine natürliche Zahl. Dann ist die spezielle lineare Gruppe $\mathrm{SL}(n, \mathbb{K}) = \{ A \in \mathrm{GL}(n, \mathbb{K}) \mid \det A = 1 \} = \ker(\det\colon \mathrm{GL}(n, \mathbb{K}) \to \mathbb{K} \setminus \{0\})$.

(ii) Für jedes Element a einer Gruppe G ist $\mathrm{ad}_a\colon G \to G$ mit $x \mapsto axa^{-1}$ ein Homomorphismus. Denn für $x, y \in G$ gilt: $\mathrm{ad}_a(x)\,\mathrm{ad}_a(y) = axa^{-1}aya^{-1} = \mathrm{ad}_a(xy)$. Außerdem ist $(\mathrm{ad}_a \circ \mathrm{ad}_{a^{-1}})(x) = a(a^{-1}x(a^{-1})^{-1})a^{-1} = x$. Daher ist $\mathrm{ad}_a \circ \mathrm{ad}_{a^{-1}}$ die Identität auf G . Analoges gilt auch umgekehrt. Somit ist $\mathrm{ad}_a \in \operatorname{Aut} G$. Man nennt ad_a den von a induzierten **inneren Automorphismus** von G.

Die Abbildung $\mathrm{ad}\colon G \to \operatorname{Aut} G$ mit $a \mapsto \mathrm{ad}_a$ ist ein Homomorphismus. Denn für $a, b, x \in G$ ist $(\mathrm{ad}_a \circ \mathrm{ad}_b)(x) = a(bxb^{-1})a^{-1} = (ab)x(ab)^{-1} = \mathrm{ad}_{ab}\,x$. Nach Satz 3.7 ist $\operatorname{Bld}(\mathrm{ad}) = \{ \mathrm{ad}_a \mid a \in G \} \leqslant \operatorname{Aut} G$. Man nennt $\operatorname{Inn}(G) := \operatorname{Bld}(\mathrm{ad})$ die **innere Automorphismengruppe** von G. Analog ist $\ker(\mathrm{ad}) = \{ a \in G \mid \mathrm{ad} = \mathrm{id}_G \} = \left\{ a \in G \;\middle|\; axa^{-1} = x \,\forall x \in G \right\} = \{ a \in G \mid xa = ax \,\forall x \in G \} =: Z(G) \leqslant G$. Man nennt $Z(G)$ das **Zentrum** von G.

Satz 3.8
Für jeden Gruppenhomomorphismus $f\colon G \to H$ gilt, dass f genau dann injektiv ist, wenn der Kern von f nur aus dem trivialen Element besteht.

BEWEIS:

„⇒“ Sei f injektiv. Wegen $f(1) = 1$ liegt das Einselement im Kern von f. Sei umgekehrt $x \in \ker f$. Dann ist $f(x) = 1 = f(1)$. Also ist $x = 1$, da f injektiv.

„⇐“ Sei jetzt $\ker f = \{1_G\}$. Sind $x, y \in G$ mit $f(x) = f(y)$, so ist $f(x)f(y)^{-1} = 1 = f(xy^{-1})$. Also ist $xy^{-1} \in \ker f = \{1_G\}$. Also $xy^{-1} = 1$, d. h. $x = y$. ∎

4. Nebenklassen

Definition 4.1 (Linkskongruenz)
Sei G eine Gruppe und H eine Untergruppe von G sowie $a, b \in G$ mit $a^{-1}b \in H$. Dann heißt a **linkskongruent** zu b modulo H. Man schreibt $a \equiv_l b \pmod{H}$.

Satz 4.1
Die Linkskongruenz modulo H ist eine Äquivalenzrelation auf G.

BEWEIS:
(i) $a^{-1}a = 1_G \in H$

(ii) $a^{-1}b \in H \Rightarrow (a^{-1}b)^{-1} = b^{-1}(a^{-1})^{-1} = b^{-1}a \in H$

(iii) $a^{-1}b, b^{-1}c \in H \Rightarrow a^{-1}bb^{-1}c = a^{-1}c \in H$ ∎

Bemerkung 4.1 (Linksnebenklasse)
Für Elemente $a, b \in G$ gilt: $a \equiv_l b \pmod{H} \Leftrightarrow a^{-1}b \in H \Leftrightarrow b \in aH := \{ ah \mid h \in H \}$. Daher ist die Äquivalenzklasse von einem Element $a \in G$ bezüglich $\equiv_l \pmod{H}$ die **Linksnebenklasse** von a modulo H. Wir setzen $G/H := \{ aH \mid a \in G \}$. Für $a \in G$ ist $H \to aH$ mit $a \mapsto ah$ bijektiv. Die Surjektivität ist klar und wegen $ah = ah'$ folgt, $h = a^{-1}ah' = a^{-1}ah' = h'$. Insbesondere ist $|aH| = |H|$.

Bemerkung 4.2 (Rechtskongruenz, Rechtsnebenklasse, Index)
Seien G eine Gruppe und H eine Untergruppe von G sowie $a, b \in G$ mit $ab^{-1} \in H$. Dann heißt a **rechtskongruent** zu b modulo H. Man schreibt $a \equiv_r b \pmod{H}$. Es gilt ein zu Satz 4.1 analoges Ergebnis. Die Äquivalenzklasse von a bezüglich $\equiv_r \pmod{H}$ ist die **Rechtsnebenklasse** Ha von a nach H. Wir setzen $H \setminus G := \{ Ha \mid a \in G \}$. Für $a \in G$ ist wieder $|Ha| = |H|$.

Für $R = Ha \in H \setminus G$ ist $R^{-1} = a^{-1}H^{-1} = a^{-1}H \in G/H$. Analog ist $L^{-1} \in H \setminus G$ für $L \in G/H$. So erhält man eine Bijektion $G/H \to H\backslash G$. Man nennt $|G\colon H| := |G/H| = |H\backslash G|$ den **Index** von H in G.

Satz 4.2 (Satz von Lagrange)
Für jede Untergruppe H einer Gruppe G gilt:

$$|G| = |G\colon H| \cdot |H|$$

Insbesondere sind $|H|$ und $|G\colon H|$ in endlichen Gruppen Teiler von $|G|$.

BEWEIS:
Die Gruppe G ist die disjunkte Vereinigung aller Linksnebenklassen nach H. Es gibt $|G\colon H|$ Linksnebenklassen. Jede enthält $|H|$ Elemente. ∎

Beispiel 4.1
Gruppen der Ordnung 24 können keine Untergruppen der Ordnung 7 enthalten.

Bemerkung 4.3
Wir setzen $\mathbb{P} := \{\, p \in \mathbb{N} \mid p \text{ Primzahl} \,\}$ und schreiben $m \mid n$, falls m ein Teiler von n ist.

Satz 4.3
Gruppen von Primzahlordnung sind zyklisch.

BEWEIS:
Sei G eine Gruppe, $|G| = p \in \mathbb{P}$ und $1 \neq g \in G$. Nach dem Satz von LAGRANGE $1 \neq |\langle g\rangle| \mid |G| = p$. Also $|\langle p\rangle| = p$, d. h. $G = \langle p\rangle$ zyklisch. ∎

Definition 4.2
Für jedes Element a in einer Gruppe G heißt die Anzahl der Elemente in der von a erzeugten Gruppe $|\langle a\rangle|$ die **Ordnung** von a.

Bemerkung 4.4
Nach dem Beispiel 3.4 ist $\langle a\rangle = \{\, a^n \mid n \in \mathbb{Z} \,\}$.

1. Fall Alle a^n sind verschieden. Dann ist $|\langle a\rangle| = \infty$.

2. Fall Es existieren ganze Zahlen m und n mit $m < n$ und $a^m = a^n$. Dann ist $n - m \in \mathbb{N}$ mit $a^{n-m} = a^n(a^m)^{-1} = 1$. Sei $k \in \mathbb{N}$ minimal mit $a^k = 1$. Dann sind $a^0 = 1, a^1 = a, a^2, \ldots, a^{k-1}$ paarweise verschieden. Denn wären $a^i = a^j$ mit $0 \leqslant i \leqslant j \leqslant k-1$, so ist $1 = a^{j-i}$ und $j - i = 0$ nach der Wahl von k. Somit ist $i = j$. Für beliebige $i, j \in \{0, \ldots, k-1\}$ ist $a^i a^j = a^{i+j}$. Dabei ist $a^{i+j} = a^{i+j-k}$, falls $i + j \leqslant k$. Daher ist $a^i a^j \in U := \{a^0, \ldots, a^{k-1}\}$. Ferner ist $(a^i)^{-1} = a^{-1} = a^{k-i} \in U$. Daher ist $\langle a\rangle \leqslant U \leqslant \langle a\rangle$. Also ist $\langle a\rangle = U$. Insbesondere ist $|\langle a\rangle| = k$.

In beiden Fällen ist also $|\langle a\rangle| = \inf\left\{\, k \in \mathbb{N} \;\middle|\; a^k = 1 \,\right\}$.

Satz 4.4 (Satz von FERMAT oder EULER)
Für jedes Element a einer endlichen Gruppe G gilt: $a^{|G|} = 1$.

BEWEIS:
Nach Satz 4.2 gilt: $|G| = \underbrace{|G\colon \langle a\rangle|}_{=:\,l} \cdot \underbrace{|\langle a\rangle|}_{=:\,k}$. Nach der vorigen Bemerkung haben wir: $a^k = 1$.
Also $a^{|G|} = a^{kl} = (a^k)^l = 1^l = 1$. ∎

Satz 4.5
Für $U \leqslant \mathbb{Z}$ existiert eine natürliche Zahl n mit $U = \{\, nz \mid z \in \mathbb{Z} \,\} =: n\mathbb{Z}$.

BEWEIS:
Für $n \in \mathbb{N}_0$ ist $n\mathbb{Z}$ das Bild des Homomorphismus $\mathbb{Z} \to \mathbb{Z}$ mit $z \mapsto nz$. Daher ist $n\mathbb{Z} \leqslant \mathbb{Z}$. Sei $U \leqslant \mathbb{Z}$ und Œ[1] ist $U \neq \{0\} = 0\mathbb{Z}$. Für $a \in U \setminus \{0\}$ ist auch $-a \in U$. Daher $U \cap \mathbb{N} \neq \emptyset$. Wie jede nichtleere Teilmenge von $\mathbb{N}$ enthält auch der Durchschnitt ein kleinstes Element n. Dann ist $2n = n + n \in U$, $3n \in U$ usw., d. h. $kn \in U$ für $k \in \mathbb{N}$. Folglich auch $-kn \in U$ und $0 \in U$. Also ist $n\mathbb{Z} \subseteq U$.

Ist $b \in U$ beliebig. Dann liefert die Division mit Rest einen Quotienten $q \in \mathbb{Z}$ und einen Rest mit $r \in \mathbb{Z}$. Dabei gilt: $b = qn + r$. Wegen $n\mathbb{Z} \subseteq U$ ist $r = b - qn \in U$. Nach der Wahl des n muss $r = 0$ gelten. Folglich: $b = qn \in n\mathbb{Z}$. Dann ist gezeigt: $U = n\mathbb{Z}$. ∎

Bemerkung 4.5
Es ist $|\mathbb{Z} : n\mathbb{Z}| = n$ für $n \in \mathbb{N}$. Denn für $z \in \mathbb{Z}$ existieren Quotient und Rest aus $\mathbb{Z}$ mit $z = qn + r$ für $0 \leqslant r < n$. Daher ist $z \in r + n\mathbb{Z}$. Folglich hat man: $\mathbb{Z} = (0 + n\mathbb{Z}) \cup (1 + n\mathbb{Z}) \cup \cdots \cup (n-1+n\mathbb{Z})$. Da $0, 1, \ldots, n-1$ in paarweise verschiedenen Linksnebenklassen nach $n\mathbb{Z}$ liegen, folgt die Behauptung. Daher besitzt $\mathbb{Z}$ für jede natürliche Zahl n genau eine Untergruppe vom Index n.

Satz 4.6
Jede Untergruppe V einer zyklischen Gruppe $G = \langle g \rangle$ ist wieder zyklisch.

BEWEIS:
Sei f ein Homomorphismus (Epimorphismus) von $(\mathbb{Z}, +)$ nach $(G, \cdot)$ mit $n \mapsto g^n$. Nach dem Satz 3.7 (Punkt iv) gilt: $V = f(f^{-1}(V))$ mit $f^{-1}(V) \leqslant \mathbb{Z}$ und nach Satz 4.5 ist $f^{-1}(V) = n\mathbb{Z}$ für ein $n \in \mathbb{N}_0$. Daher $V = f(n\mathbb{Z}) = \langle g^n \rangle$ zyklisch. ∎

Definition 4.3 (Doppelnebenklassen)
Sei G eine Gruppe und H und K zwei Untergruppen. Weiterhin seien a und b zwei Elemente aus G. Wir schreiben $a \equiv b \pmod{H, K}$, falls $h \in H, k \in K$ mit $b = hak$ existieren.

Satz 4.7
Die Kongruenz modulo H und K ist eine Äquivalenzrelation auf G.

BEWEIS:

(i) Für $a \in G$ folgt: $a = 1a1$ mit $1 \in H, 1 \in K$. Also ist $a \equiv a \pmod{H, K}$.

(ii) Sei $a \equiv b \pmod{H, K} \Rightarrow \exists h \in H, k \in K : b = hak \Rightarrow a = h^{-1}bk^{-1}$ mit $h^{-1} \in H, k^{-1} \in K \Rightarrow b \equiv a \pmod{H, K}$.

(iii) $a \equiv b \pmod{H, K}$ und $b \equiv c \pmod{H, K} \Rightarrow \exists h, h' \in H, k, k' \in K : b = hak, c = h'bk' \Rightarrow c = h'hbkk'$. Also ist $a \equiv c \pmod{H, K}$. ∎

Bemerkung 4.6
Für jedes Element $a \in G$ ist die Äquivalenzklasse von a bezüglich der Äquivalenzrelation die **Doppelnebenklasse** $HaK := \{ hak \mid h \in H, k \in K \}$ von a nach H und K. Man setzt: $H \setminus G/K := \{ HaK \mid a \in G \}$. Es gilt, $H \setminus G = H \setminus G/1$ und $G/K = 1 \setminus G/K$. Im Allgemeinen ist die Anzahl der Elemente einer Doppelnebenklasse *kein* Teiler der Gruppenordnung.

[1] Herr Külshammer nutzt dieses als Zeichen für o. B. d. A.

Beispiel 4.2
Sei $G := \mathrm{Sym}(3), H := \langle b \rangle, K := \langle c \rangle, a := 1$ mit $b := \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, c := \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$. Dann besteht H aus $\{1, b\}$ und K aus $\{1, c\}$. Es ist $HaK = \{1, b, c, bc\}$. Also $|HaK| = 4 \nmid 6 = |G|$.

Satz 4.8
Seien G eine Gruppe, $H, K \leqslant G$ und $a \in G$. Dann enthält HaK genau $|H\colon H \cap aKa^{-1}|$ Linksnebenklassen nach K und genau $|K\colon a^{-1}Ha \cap K|$ Rechtsnebenklassen nach H. Insbesondere ist $|HaK| = |H\colon H \cap aKa^{-1}| \cdot |K| = |K\colon a^{-1}Ha \cap K| \cdot |H|$.

BEWEIS:
Es reicht, den Beweis für eine Seite zu führen. Der Rest folgt aus Symmetriegründen. Es ist $HaK = \bigcup_{h \in H} f(h)$ mit $f\colon H \to G/K$ mit $h \mapsto haK$. Dabei gilt für Elemente $h, h' \in H$: $f(h) = f(h') \Leftrightarrow haK = h'aK \Leftrightarrow a^{-1}h^{-1}h'a \in K \Leftrightarrow h^{-1}h' \in aKa^{-1} \cap H \Leftrightarrow h(aKa^{-1} \cap H) = h'(aKa^{-1} \cap H)$. ∎

Bemerkung 4.7
Nach dem Satz 3.7(i) ist $aKa^{-1} = \mathrm{ad}_a(K) \leqslant G$ und analog $a^{-1}Ha \leqslant G$.

Beispiel 4.3
Für $a = 1$ ist $HaK = HK$. Im Allgemeinen ist $HK \not\leqslant K$. Nach dem Satz 4.8 enthält HK genau $|H\colon H \cap K|$ Linksnebenklassen nach K und genau $|K\colon K \cap H|$ Rechtsnebenklassen nach H. Insbesondere gilt:

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

(ii) $|H\colon H \cap K| \leqslant |G\colon K|$

(iii) $|H\colon H \cap K| = |G\colon K| < \infty \Rightarrow G = HK = KH$

Bemerkung 4.8
Den Satz von LAGRANGE (Satz 4.2) kann man folgendermaßen verallgemeinern: Ist G eine Gruppe und $K \leqslant H \leqslant G$, so gilt: $|G\colon K| = |G\colon H| \cdot |H\colon K|$. Denn ist das $G = \dot\bigcup_{i \in I} g_i H$ und $H = \dot\bigcup_{j \in J} h_j K$, so ist $G = \dot\bigcup_{\substack{i \in I \\ j \in J}} g_i h_j K$.

Satz 4.9
Für Untergruppen H und K einer Gruppe G gilt stets:

(i) $|G\colon H \cap K| \leqslant |G\colon H| \cdot |G\colon K|$

(ii) $|G\colon H \cap K| = |G\colon H| \cdot |G\colon K| < \infty \Rightarrow G = HK = KH$

(iii) Seien $|G\colon H|, |G\colon K|$ endlich und teilerfremd. Dann ist $|G\colon H \cap K| = |G\colon H| \cdot |G\colon K|$ und $G = HK = KH$.

BEWEIS:
(i) $|G\colon H \cap K| = |G\colon H| \cdot |H\colon H \cap K| \leqslant |G\colon H| \cdot |G\colon K|$ (letzter Schritt nach Satz 4.8(ii))

(ii) Sei $|G\colon H \cap K| = |G\colon H| \cdot |G\colon K| < \infty$. Dann zeigt der Beweis des ersten Teiles dass $|G\colon K| = |H\colon H \cap K|$. Aus Satz 4.8(iii) folgt dann: $G = HK = KH$.

(iii) Seien $|G\colon H|, |G\colon K|$ endlich und teilerfremd. Die obige Bemerkung zeigt, dass $|G\colon H| \mid |G\colon H\cap K|$ und $|G\colon K| \mid |G\colon H\colon K|$. Daher ist $|G\colon H|\cdot|G\colon K| \mid |G\colon H\cap K|$. Mit dem ersten Punkt folgt, dass $|G\colon H \cap K| = |G\colon H| \cdot |G\colon K|$ und (ii) liefert $G = HK = KH$.∎

5. Normalteiler und Faktorgruppen

Satz 5.1
Für eine Untergruppe N einer Gruppe G sind die folgenden Aussagen äquivalent:

(1) $gNg^{-1} \subseteq N$ für alle $g \in G$

(2) $gNg^{-1} = N$ für alle $g \in G$

(3) $gN = Ng$ für alle $g \in G$

(4) G/N ist eine Gruppe mit $(gN)(hN) := ghN$ für alle $g, h \in G$

(5) Es existiert eine Gruppe H und ein Homomorphismus $f\colon G \to H$ mit $N = \ker f$.

BEWEIS:
(1)⇒(2) Ist die erste Aussage erfüllt, so ist $N = g \underbrace{g^{-1}N(g^{-1})^{-1}}_{\subseteq N} g^{-1} \subseteq gNg^{-1}$.

(2)⇒(3) Multiplizieren mit g von rechts.

(3)⇒(4) Sei die dritte Bedingung erfüllt. Für $g, h, k \in G$ ist dann $(gN)(hN) = gNhN = ghNN = ghN$, d. h. die Multiplikation in G/N ist wohldefiniert. Ferner ist mit $(gN \cdot hN)(kN) = ghN \cdot kN = (gh)kN = g(hk)N = gN(hkN) = gN(hNkN)$ das Assoziativgesetz erfüllt. Daher ist G/N eine Halbgruppe. Außerdem ist $1N \cdot gN = 1gN = gN$ und $(g^{-1}N)(gN) = g^{-1}gN = 1N$.

(4)⇒(5) Sei $H := G/N$ und $f(g) := gN$ für alle $g \in G$. Dann ist $f(g)f(h) = (gN)(hN) = ghN = f(gh)$ für $g, h \in G$, d. h. f ist ein Homomorphismus. Insbesondere $1_{G/N} = f(1_G) = 1N$. Für $x \in G$ gilt ferner: $x \in \ker f \Leftrightarrow f(x) = 1_{G/N}$. Nach der obigen Aussage ist $f(x) = xN$ und $1_{G/N} = 1N$. Somit ist $f(x) = xN = 1N = 1_{G/N} \Leftrightarrow 1^{-1}x = x \in N$. Also $\ker f = N$.

(5)⇒(1) Zuletzt sei (5) erfüllt und weiter $x \in N = \ker f, g \in G$. Dann $f(gxg^{-1}) = f(g)f(x)f(g^{-1}) = f(g)1f(g^{-1}) = f(g)f(g^{-1}) = f(gg^{-1}) = f(1) = 1$, d. h. $gxg^{-1} \in \ker f = N$. ∎

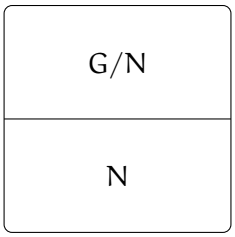
Definition 5.1 (normale Untergruppe, Normalteiler)
Gegebenenfalls heißt das N **normal** oder **Normalteiler** in G. Man schreibt $N \trianglelefteq G$

Definition 5.2 (Faktorgruppe)
Die Gruppe G/N heißt **Faktorgruppe** von G nach N.

Bemerkung 5.1
Für $N \trianglelefteq G$ ist $f\colon G \to G/N$ mit $g \mapsto gn$ ein Epimorphismus. Dieser heißt **kanonischer Epimorphismus** von G auf G/N. Es gilt: $a \equiv_l b \pmod N \Leftrightarrow aN = bN \Leftrightarrow Na = Nb \Leftrightarrow a \equiv_r b \pmod N$. Daher schreibt man kurz $a \equiv b \pmod N$ und sagt, „a ist kongruent zu b modulo N“.

Beispiel 5.1

(i) In jeder Gruppe G sind $\{1\}$ und G normal. Sind dies die einzigen Normalteiler und ist $G \neq 1$, dann heißt die Gruppe **einfach**. Nach dem Satz 4.2 (Satz von LAGRANGE) sind Gruppen von Primzahlordnung stets einfach. Später werden wir weitere einfache Gruppen kennen lernen (Siehe Kapitel 6). Eine nichteinfache Gruppe $G \neq 1$ stellt man sich aus Normalteiler N und Faktorgruppe G/N zusammengesetzt vor:



Auf diese Weise werden einfache Gruppen zu Bausteinen für beliebige Gruppen. Die Bestimmung aller endlichen einfachen Gruppen war eines der größten Projekte der Mathematik überhaupt. Beteiligt daran waren ca. 50 bis 100 Mathematiker. Die entsprechenden Veröffentlichungen haben einen Umfang von etwa 10 000 Seiten. Das Projekt wurde 1980[1] erfolgreich abgeschlossen. Das Buch [11] erzählt einen Teil der Geschichte.

(ii) In jeder Gruppe G ist jede Untergruppe U vom Zentrum von G normal. Denn für $g \in G$ und $u \in U$ ist $gug^{-1} = ugg^{-1} = u \in U$. Insbesondere ist das Zentrum einer Gruppe ein Normalteiler der Gruppe. Ferner gilt, dass G genau dann abelsch ist, wenn $G = Z(G)$. Daher ist in einer abelschen Gruppe jede Untergruppe normal.

(iii) Seien G eine Gruppe und H eine Untergruppe mit $|H\colon G| = 2$. Dann ist $H \trianglelefteq G$. Denn $1H = H = H1$ und $G \setminus H$ sind die einzigen Linksnebenklassen nach H.

(iv) Sei n eine natürliche Zahl und $\mathbb{K}$ ein Körper. Dann ist $SL(n, \mathbb{K}) = \ker(\det) \trianglelefteq GL(n, \mathbb{K})$.

(v) Für jeden Gruppenhomomorphismus $f\colon G \to H$ und $N \trianglelefteq H$ ist $f^{-1}(N) \trianglelefteq G$. Denn für $g \in G$ und $x \in f^{-1}(N)$ ist $f(gxg^{-1}) = f(g)f(x)f(g^{-1}) = f(x)f(g)f(g^{-1}) = f(x)f(gg^{-1}) = f(x) \in N$, d. h. $gxg^{-1} \in f^{-1}(N)$.

(vi) Für jeden Gruppenhomomorphismus $f\colon G \to H$ und jeden Normalteiler $M \trianglelefteq G$ ist $f(M) \trianglelefteq f(G)$. Denn für $g \in G$ und $m \in M$ ist $f(g)f(m)f(g^{-1}) = f(gmg^{-1}) \in f(M)$. Dagegen ist im Allgemeinen $f(M) \not\trianglelefteq H$. (siehe Übung)

(vii) Für jede Familie $(N_i)_{i\in I}$ von Normalteilern N_i einer Gruppe G sind auch $\bigcap_{i\in I} N_i$ und $\langle N_i\colon i \in I\rangle := \langle \bigcup_{i\in I} N_i\rangle$ normal in G.

[1] Manche meinen auch 2000 oder 2005.

(viii) Für jede Gruppe G, jeden Automorphismus $\alpha \in \mathrm{Aut}(G)$ und $a, x \in G$ gilt: $(\alpha \circ \mathrm{ad}_a \circ \alpha^{-1})(x) = \alpha(a\alpha^{-1}(x)a^{-1}) = \alpha(a)\alpha(\alpha^{-1}(x))\alpha(a)^{-1} = \mathrm{ad}_{\alpha(a)}(x)$, d. h.

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

Daher $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$ und es heißt $\mathrm{Out}(G) := \mathrm{Aut}(G)/\mathrm{Inn}(G)$ die **äußere Automorphismengruppe** von G.

(ix) Aus $H \trianglelefteq G$ und $K \trianglelefteq H$ folgt im Allgemeinen *nicht*, dass $K \trianglelefteq G$. Die Relation $\trianglelefteq$ ist *nicht* transitiv. (Beispiel siehe Übungen)

Satz 5.2 (Homomorphiesatz)
Für jeden Gruppenhomomorphismus $f\colon G \to H$ ist $F\colon G/\ker f \to \mathrm{Bld}(f)$ mit $g \ker f \mapsto f(g)$ wohldefiniert und ein Isomorphismus von Gruppen. Insbesondere ist

$$G/\ker f \cong \mathrm{Bld}\, f$$

BEWEIS:
Für $a, b \in G$ gilt: $f(a) = f(b) \Leftrightarrow 1 = f(a)^{-1}f(b) = f(a^{-1}b) \Leftrightarrow a^{-1}b \in \ker f \Leftrightarrow a \ker f = b \ker f$. Daher ist F wohldefiniert und injektiv. Die Surjektivität von F ist klar. Für $g, h \in G$ gilt: $F(g \ker f)F(h \ker f) = f(g)f(h) = f(gh) = F(gh \ker f) = F(g \ker(f)h \ker(f))$. ∎

Beispiel 5.2

(i) Sei $H = \langle h \rangle$ zyklisch. Dann ist $f\colon \mathbb{Z} \to H$ mit $z \mapsto h^z$ ein Epimorphismus. Nach dem Satz 4.5 ist $\ker f = n\mathbb{Z}$ für ein $n \in \mathbb{N}_0$. Daher ist $H \cong \mathbb{Z}/n\mathbb{Z}$. Jede zyklische Gruppe ist also zu $(\mathbb{Z}/n\mathbb{Z}, +)$ für ein $n \in \mathbb{N}_0$ isomorph.

(ii) Für jede Gruppe G ist $\mathrm{ad}\colon G \to \mathrm{Aut}(G)$ mit $a \mapsto \mathrm{ad}_a$ ein Homomorphismus mit dem Kern $Z(G)$ und dem Bild $\mathrm{Inn}(G)$. Also folgt:

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

(iii) Für $n \in \mathbb{N}$ und jeden Körper $\mathbb{K}$ ist $\det\colon \mathrm{GL}(n, \mathbb{K}) \to \mathbb{K} \setminus \{0\}$ ein Epimorphismus mit dem Kern $\mathrm{SL}(n, \mathbb{K})$. Daher ist $\mathrm{GL}(n, \mathbb{K})/\mathrm{SL}(n, \mathbb{K}) \cong \mathbb{K} \setminus \{0\}$. Insbesondere ist die Faktorgruppe $\mathrm{GL}(n, \mathbb{K})/\mathrm{SL}(n, \mathbb{K})$ abelsch.

Satz 5.3 (1. Isomorphiesatz)
Seien G eine Gruppe, H eine Untergruppe und N ein Normalteiler in G. Dann ist $HN \leqslant G$, $N \trianglelefteq HN$, $H \cap N \trianglelefteq H$ und

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

BEWEIS:
Der kanonische Epimorphismus $f\colon G \to G/N$ mit $a \mapsto aN$ hat den Kern N. Nach Satz 3.7 ist also $HN = f^{-1}(f(H))$ eine Untergruppe von G. Wegen $N \trianglelefteq G$ ist sicher $N \trianglelefteq NH$. Die Einschränkung $g\colon H \to H/N$ von f ist ein Homomorphismus mit dem Kern $H \cap \ker f = H \cap N$. Daher ist $H \cap N \trianglelefteq H$. Aus dem Satz 5.2 folgt: $H/(H \cap N) = H/\ker g \cong \operatorname{Bld} g = \{\, aN \mid a \in H \,\} = \{\, anN \mid a \in H, n \in N \,\} = HN/N$. ∎

Bemerkung 5.2
Im Fall $H \trianglelefteq G$ ist auch $HN \trianglelefteq G$. Denn $aHNa^{-1} = aHa^{-1}aNa^{-1} \subseteq HN$ für alle $a \in G$.

Satz 5.4 (2. Isomorphiesatz)
Seien G eine Gruppe, N ein Normalteiler in G und $N \leqslant H \leqslant G$. Dann gilt: $H/N \trianglelefteq G/N \Leftrightarrow H \trianglelefteq G$. Gegebenenfalls ist:

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

BEWEIS:
Sei $f\colon G \to G/N$ mit $a \mapsto aN$ kanonisch. Für $H \trianglelefteq G$ ist $H/N = f(H) \trianglelefteq f(G) = G/N$. Sei umgekehrt $H/N \trianglelefteq G/N$ und $g\colon G/N \to (G/N)(H/N)$ kanonisch. Für $a \in G$ gilt dann: $a \in \ker(g \circ f) \Leftrightarrow g(f(a)) = 1 \Leftrightarrow f(a) \in \ker g = H/N \Leftrightarrow a \in f^{-1}(H/N) = f^{-1}(f(H)) = H$ (letzte Aussage nach dem Satz 3.7).

Daher ist $H = \ker(g \circ f) \trianglelefteq G$. Der Homomorphiesatz liefert: $G/H = G/\ker(g \circ f) \cong \operatorname{Bld}(g \circ f) = (G/N)/(H/N)$. ∎

Satz 5.5 (3. Isomorphiesatz)
Seien G eine Gruppe, $U_0 \trianglelefteq U \leqslant G$ und $V_0 \trianglelefteq V \leqslant G$. 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

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

BEWEIS:
Sei $f\colon U \to U/U_0$ mit $u \mapsto uU_0$ kanonisch. Wegen $V_0 \trianglelefteq V$ ist $(U \cap V) \cap V_0 \trianglelefteq U \cap V$ nach Satz 5.3. Aus dem Beispiel Beispiel 5.1 (vi) folgt: $\underbrace{f(U \cap V_0)}_{(U \cap V_0)U_0/U_0} \trianglelefteq \underbrace{f(U \cap V)}_{(U \cap V)U_0/U_0}$. Daher gilt nach dem Satz 5.4: $(U \cap V_0)U_0 \trianglelefteq (U \cap V)U_0$. Ferner ist $F\colon U \cap V \to (U \cap V)U_0/(U \cap V_0)U_0$ mit $x \mapsto x(U \cap V_0)U_0$ ein Epimorphismus mit dem Kern $(U \cap V) \cap (U \cap V_0)U_0$. Dies kann man durch Anwendung der DEDEKIND-Identität vereinfachen: $(U \cap V) \cap (U \cap V_0)U_0 = (U \cap V_0)(U \cap V \cap U_0) = (U \cap V_0)(V \cap U_0)$. Daher ist $(U \cap V_0)(V \cap U_0) \trianglelefteq U \cap V$. Der Satz 5.2 liefert: $U \cap V/(U \cap V_0)(U_0 \cap V) = U \cap V/\ker F \cong (U \cap V)U_0/(U \cap V_0)U_0$. Die anderen Aussagen folgen aus Symmetriegründen. ∎

Bemerkung 5.3
Der Satz 5.5 wird manchmal auch als Satz von ZASSENHAUS bezeichnet.

Bemerkung 5.4
Für jede Familie $(N_i)_{i\in I}$ von Normalteilern N_i einer Gruppe G ist $G \to \prod_{i\in I} G/N_i$ mit $g \mapsto (gN_i)_{i\in I}$ ein Homomorphismus mit dem Kern $N := \bigcap_{i\in I} N_i$. Nach dem Homomorphiesatz ist also $G/N \to \prod_{i\in I} G/N_i$ mit $gN \mapsto (gN_i)_{i\in I}$ ein Monom.

Satz 5.6
Seien G eine Gruppe und $M, N \trianglelefteq G$ mit $M \cap N = 1$. Dann ist $mn = nm$ für alle $m \in M, n \in N$.

BEWEIS:
$m(nm^{-1}n^{-1}) = (mnm^{-1})n^{-1} \in M \cap N = 1 \Rightarrow mnm^{-1}n^{-1} = 1 \Rightarrow mn = nm$ ∎

Definition 5.3
Eine Untergruppe U einer Gruppe G mit $f(U) \subseteq U$ für alle $f \in \mathrm{Aut}(G)$ bzw. für alle $f \in \mathrm{End}(G)$ heißt **charakteristisch** bzw. **vollinvariant** in G.

Bemerkung 5.5
(i) Für $U \leqslant G$ gilt: $U \trianglelefteq G \Leftrightarrow f(U) \subseteq U$ für alle $f \in \mathrm{Inn}(G)$.

(ii) Daher folgt aus vollinvariant die Eigenschaft charakteristisch und daraus die Eigenschaft normal.

(iii) Für jede charakteristische Untergruppe $U \leqslant G$ und alle $f \in \mathrm{Aut}\, G$ ist $U = f(f^{-1}(U)) \subseteq f(U)$, d. h. $f(U) = U$.

Beispiel 5.3
(i) Für jede Gruppe G ist das Zentrum von G charakteristisch in G. Denn für $z \in Z(G), g \in G$ und $f \in \mathrm{Aut}\, G$ gilt: $f(z)f(g) = f(zg) = f(gz) = f(g)f(z)$, d. h. $f(z) \in Z(G)$ wegen $f(G) = G$. Im Allgemeinen ist $Z(G)$ *nicht* vollinvariant in G (siehe Übung).

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

Satz 5.7
Für jede Gruppe G und $K \leqslant H \leqslant G$ gilt:

(i) Wenn K charakteristisch in H und H charakteristisch in G, dann ist auch K charakteristisch in G.

(ii) Wenn K vollinvariant in H und H vollinvariant in G, dann ist K vollinvariant in G.

(iii) Wenn K charakteristisch in H und H Normalteiler in G, dann ist K Normalteiler in G.

BEWEIS:
(i) Sei die Voraussetzung erfüllt. Für $f \in \mathrm{Aut}\, G$ liegt die Einschränkung g von f auf H nach Bemerkung 5.5(iii) in $\mathrm{Aut}\, H$. Daher ist $f(K) = g(K) \subseteq K$.

(ii) Sei die Voraussetzung erfüllt. Für $f \in \mathrm{End}\, G$ liegt die Einschränkung g von f auf H in $\mathrm{End}\, H$. Daher ist $f(K) = g(K) \subseteq K$.

(iii) Sei die Voraussetzung erfüllt. Für $g \in G$ ist $f\colon H \to H$ mit $x \mapsto gxg^{-1}$ ein Automorphismus von H. Daher ist $gKg^{-1} = f(K) \subseteq K$. ∎

Definition 5.4 (Ω-Gruppe, Operatoren)
Sei Ω eine Menge. Eine **Ω-Gruppe** ist ein Paar, das aus einer Gruppe G und einer Abbildung $\Omega \times G \to G$ mit $(\omega, g) \mapsto {}^{\omega}g$ mit ${}^{\omega}(gh) = ({}^{\omega}g)({}^{\omega}h)$ für alle $\omega \in \Omega, g, h \in G$ besteht. Die Elemente in Ω heißen **Operatoren**.

Bemerkung 5.6
Für $\omega \in \Omega$ gehört die Abbildung $G \to G$ mit $g \mapsto {}^{\omega}g$ zu $\operatorname{End} G$. Dabei können verschiedene Elemente in Ω den gleichen Endomorphismus von G liefern.

Beispiel 5.4
(i) Jeder Vektorraum V über einem Körper Ω lässt sich als Ω-Gruppe auffassen: ${}^{\omega}v := \omega v$ für $\omega \in \Omega, v \in V$.

(ii) Sei G beliebig, $\Omega = \{\operatorname{End} G, \operatorname{Aut} G, \operatorname{Inn} G\}$ und ${}^{\omega}g := \omega(g)$ für $\omega \in \Omega$ und $g \in G$.

(iii) Sei G eine beliebige Gruppe und $\Omega \subseteq G$. Wir definieren ${}^{\omega}g = \omega g \omega^{-1}$

(iv) Für jede Familie $(G_i)_{i\in I}$ von Ω-Gruppen G_i ist auch $\prod_{i\in I} G_i$ eine Ω-Gruppe mit ${}^{\omega}(g_i)_{i\in I} := ({}^{\omega}g_i)_{i\in I}$ für $\omega \in \Omega$.

Definition 5.5 (Ω-Untergruppe)
Seien Ω eine Menge und G eine Ω-Gruppe. Eine Untergruppe $H \leqslant G$ mit ${}^{\omega}h \in H$ für alle $\omega \in \Omega$ und $h \in H$ heißt **Ω-Untergruppe** von G. Ist $H \trianglelefteq G$, so heißt H **Ω-Normalteiler**.

Bemerkung 5.7
(i) Jede Ω-Untergruppe kann man wieder als Ω-Gruppe auffassen.

(ii) Für jeden Ω-Normalteiler $N \trianglelefteq G$ wird die Faktorgruppe G/N zu einer Ω-Gruppe mit ${}^{\omega}(gN) := ({}^{\omega}g)N$ für $g \in G$ und $\omega \in \Omega$. Dies rechnet man leicht nach.

Beispiel 5.5
- Ist G beliebig und $\Omega = \operatorname{End} G$, so sind die Ω-Untergruppen von G genau die vollinvarianten Untergruppen von G.
- Ist G beliebig und $\Omega = \operatorname{Aut} G$, so sind die Ω-Untergruppen von G genau die charakteristischen Untergruppen von G.
- Ist G beliebig und $\Omega = \operatorname{Inn} G$, so sind die Ω-Untergruppen von G genau die normalen Untergruppen von G.

Definition 5.6
Sei Ω eine Menge sowie G, H zwei Ω-Gruppen. Ein Gruppenhomomorphismus $f\colon G \to H$ mit $f({}^{\omega}g) = {}^{\omega}f(g)$ heißt **Ω-Homomorphismus**. Wir üblich hat man auch die anderen Typen von Morphismen und den Begriff Ω-isomorph. Die Notationen sind $\cong_{\Omega}$, $\operatorname{Hom}_{\Omega}(G, H)$, $\operatorname{End}_{\Omega}(H)$ und $\operatorname{Aut}_{\Omega}(G)$.

Beispiel 5.6
Seien G, Ω beliebig. Für jede Ω-Untergruppe $H \leqslant G$ ist die Inklusionsabbildung $H \to G$ mit $h \mapsto h$ ein Ω-Monom. Für jeden Ω-Normalteiler $N \trianglelefteq G$ ist die kanonische Abbildung $G \to G/N$ mit $g \mapsto gN$ ein Ω-Epimorphismus.

Bemerkung 5.8
Viele Aussagen über Gruppen, Untergruppen, Homomorphismen übertragen sich problemlos auf Ω-Gruppen, Ω-Untergruppen und Ω-Homomorphismen. Beispielsweise sind Bild und Kern von Ω-Homomorphismen stets Ω-Untergruppen und jeder Ω-Homomorphismus $f\colon G \to H$ induziert einen Ω-Isomorphismus $G/\ker f \to \operatorname{Bld} f$ mit $g \ker f \mapsto f(g)$. Den „Homomorphiesatz für Ω-Gruppen“ rechnet man schnell nach. Analog übertragen sich auch die anderen Isomorphiesätze auf Ω-Gruppen. Wir werden diese im folgenden ohne Kommentar verwenden.

6. Normalreihen

Definition 6.1 (Subnormalreihe, Länge, Faktor, Normalreihe)
Eine endliche Folge von Untergruppen

$$G = G_0 \trianglerighteq G_1 \trianglerighteq \ldots \trianglerighteq G_l = 1 \tag{6.1}$$

einer Gruppe G heißt **Subnormalreihe** von G der **Länge** l mit **Faktor**en G_0/G_1 bis G_{l-1}/G_l. Ist $G_i \trianglelefteq G$ für alle i, dann heißt Gleichung 6.1 **Normalreihe**. Ist $G_{i-1} \neq G_i$ für alle i, dann heißt Gleichung 6.1 eine **(Sub)normalreihe ohne Wiederholung**. Eine **Verfeinerung** von Gleichung 6.1 ist eine (Sub)Normalreihe

$$G = H_0 \trianglerighteq H_1 \trianglerighteq \ldots \trianglerighteq H_m = 1 \tag{6.2}$$

derart, dass eine Injektion $f\colon \{1,\ldots,l\} \to \{1,\ldots,m\}$ mit $G_i = H_{f(i)}$ für alle i existiert. Im Fall $m > l$ heißt die Verfeinerung **echt**.

Beispiel 6.1
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 $G \trianglerighteq \langle a^2, b\rangle \trianglerighteq \langle b\rangle \trianglerighteq 1$ ist eine Subnormalreihe, aber $\langle b\rangle \not\trianglelefteq G$ keine Normalreihe. Dagegen ist $G \trianglerighteq \langle a^2, b\rangle \trianglerighteq \langle a^2\rangle \trianglerighteq 1$ eine Normalreihe.

Definition 6.2
Subnormalreihen

$$G = G_0 \trianglerighteq G_1 \trianglerighteq \ldots \trianglerighteq G_l = 1 \tag{6.3}$$

und

$$G = H_0 \trianglerighteq H_1 \trianglerighteq \ldots \trianglerighteq H_m = 1 \tag{6.4}$$

einer Gruppe G heißen **isomorph**, wenn $l = m$ ist und ein $f \in \mathrm{Sym}(l)$ mit $G_{i-1}/G_i \cong H_{f(i)-1}/H_{f(i)}$ für alle i existieren. Dies bedeutet, Gleichung 6.3 und Gleichung 6.4 haben die gleiche Länge und ihre Faktoren sind bis auf die Reihenfolge isomorph.

Beispiel 6.2
$\mathbb{Z}/6\mathbb{Z}$ hat isomorphe Normalreihen $\mathbb{Z}/6\mathbb{Z} \trianglerighteq 2\mathbb{Z}/6\mathbb{Z} \trianglerighteq 6\mathbb{Z}/6\mathbb{Z}$ oder $\mathbb{Z}/6\mathbb{Z} \trianglerighteq 3\mathbb{Z}/6\mathbb{Z} \trianglerighteq 6\mathbb{Z}/6\mathbb{Z}$.

Satz 6.1 (Verfeinerungssatz von Schreier)
Je zwei Subnormalreihen einer Gruppe G haben isomorphe Verfeinerungen.

BEWEIS:
Seien Gleichung 6.3 und Gleichung 6.4 zwei Subnormalreihen von G. Setze $G_{ik} := G_i(G_{i-1} \cap H_k)$ und $H_{ik} := H_k(H_{k-1} \cap G_i)$ für $i = 0, \ldots, l$ und $k = 0, \ldots, m$.[1] Dabei sei $G_{-1} := G =: H_{-1}$. Dann ist jeweils $G_{i0} = G_{i-1}$ und $G_{im} = G_i$ sowie $G_{ik} \trianglelefteq G_{i,k-1}$ nach dem 3. Isomorphiesatz (Satz 5.5). Daher ist $G \trianglerighteq G_{00} \trianglerighteq G_{01} \trianglerighteq \ldots \trianglerighteq G_{0m} = G_{10} \trianglerighteq G_{11} \trianglerighteq \ldots \trianglerighteq G_{1m} = G_{20} \trianglerighteq \ldots \trianglerighteq G_{l0} \trianglerighteq \ldots \trianglerighteq G_{lm} = 1$ eine Subnormalreihe, die Gleichung 6.3 verfeinert. Analog ist $H = H_{00} \trianglerighteq H_{10} \trianglerighteq \ldots \trianglerighteq H_{l0} = H_{01} \trianglerighteq H_{11} \trianglerighteq \ldots \trianglerighteq H_{l1} \trianglerighteq \ldots \trianglerighteq H_{0m} \trianglerighteq \ldots \trianglerighteq H_{lm} = 1$ eine Subnormalreihe, die Gleichung 6.4 verfeinert. Dabei gilt jeweils: $G_{i,k-1}/G_{ik} \cong H_{i-1,k}/H_i$ nach dem Satz 5.5. ∎

Definition 6.3 (Kompositionsreihe)
Eine **Kompositionsreihe** einer Gruppe G ist eine Subnormalreihe von G ohne Wiederholungen, die keine echte Verfeinerung ohne Wiederholungen hat.

Beispiel 6.3

(i) Die Subnormalreihen von $\mathbb{Z}/6\mathbb{Z}$ (siehe oben) sind Kompositionsreihen.

(ii) $\mathbb{Z}$ selbst hat keine Kompositionsreihe. Denn jede Subnormalreihe $\mathbb{Z} \triangleright n_1\mathbb{Z} \triangleright \ldots \triangleright n_l\mathbb{Z} \triangleright 0$ kann man zu $\mathbb{Z} \triangleright n_1\mathbb{Z} \triangleright \ldots \triangleright n_l\mathbb{Z} \triangleright 2n_l\mathbb{Z} \triangleright 0$ verfeinern.

(iii) Jede endliche Gruppe hat eine Kompositionsreihe.

Satz 6.2 (Satz von JORDAN-HÖLDER)
Je zwei Kompositionsreihen einer Gruppe G sind isomorph.

BEWEIS:
Nach dem Verfeinerungssatz von SCHREIER (Satz 5.6) haben je zwei Kompositionsreihen von G isomorphe Verfeinerungen. Da man Wiederholungen streichen kann, kann man annehmen, dass die Verfeinerungen keine Wiederholungen haben. Andererseits haben Kompositionsreihen keine echten Verfeinerungen ohne Wiederholungen. Daher sind bereits die ursprünglichen Kompositionsreihen isomorph. ∎

Bemerkung 6.1
Nach dem zweiten Isomorphiesatz (Satz 5.4) ist eine Subnormalreihe genau dann eine Kompositionsreihe, wenn ihre Faktoren einfache Gruppen sind. Diese heißen dann **Kompositionsfaktoren** von G und die Länge einer Kompositionsreihe heißt **Kompositionslänge** von der Gruppe G.

Definition 6.4 ((charakteristisch) einfache Ω-Gruppe)
Sei Ω eine Menge. Eine Ω-Gruppe $G \neq 1$ heißt **einfach**, wenn 1 und G die einzigen Ω-Normalteiler von G sind. Im Fall $\Omega = \operatorname{Aut} G$ heißt G **charakteristisch einfach**.

Bemerkung 6.2
Die Definition von Ω-(Sub-)Normalreihen und Ω-Kompositionsreihen ist klar. Die Sätze von SCHREIER und JORDAN-HÖLDER übertragen sich. Im Fall $\Omega = \operatorname{Inn} G$ heißen Ω-Kompositionsreihen **Hauptreihen**. Die Faktoren heißen **Hauptfaktoren** und ihre Länge **Hauptlänge**. Nach Satz 5.7 (iii) ist jeder Hauptfaktor charakteristisch einfach.

[1] Bemerke: $G_i \subset G_{ik} \subset G_{i-1}$ und $H_k \subset H_{ik} \subset H_{i,k-1}$.

Satz 6.3
Sei Ω eine Menge und G eine Ω-Gruppe mit Ω-Subnormalreihe $G = G_0 \trianglerighteq G_1 \trianglerighteq \ldots \trianglerighteq G_l = 1$.

(i) Für jede Ω-Untergruppe $H \leqslant G$ ist $H = H \cap G_0 \trianglerighteq H \cap G_1 \trianglerighteq \ldots \trianglerighteq H \cap G_l = 1$ eine Ω-Subnormalreihe von H mit $H \cap G_{i-1}/H \cap G_i \cong_\Omega (H \cap G_{i-1})G_i/G_i \leqslant G_{i-1}/G_i$.

(ii) Für jeden Ω-Normalteiler $N \trianglelefteq G$ ist $G/N = G_0N/N \trianglerighteq G_1N/N \trianglerighteq \ldots \trianglerighteq G_lN/N = 1$ 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.

BEWEIS:
(i) Jeweils gilt: $H \cap G_i = (H \cap G_{i-1}) \cap G_i \trianglelefteq H \cap G_{i-1}$ nach dem ersten Isomorphiesatz (Satz 5.3). Der Rest des Satzes lässt sich mit dem gleichen Satz beweisen.

(ii) Wegen $G_i \trianglelefteq G_{i-1}$ ist $G_iN/N \trianglelefteq G_{i-1}N/N$ durch die Anwendung des Homomorphismus nach Beispiel 5.1 (vi). Ferner ist $G_{i-1}N/G_iN = G_{i-1}(G_iN)/G_iN \cong_\Omega G_{i-1}/G_{i-1} \cap G_iN$ nach Satz 5.3. ∎

Definition 6.5 (Normaler Endomorphismus)
Ein Endomorphismus α einer Gruppe G mit $\alpha(xyx^{-1}) = x\alpha(y)x^{-1}$ für alle $x, y \in G$ heißt **normal**.

Bemerkung 6.3
Mit $\Omega := \operatorname{Inn} G$ sind die normalen Endomorphismen von G die Ω-Endomorphismen von G. Ferner ist ein $\alpha \in \operatorname{End} G$ genau dann normal, wenn gilt: $x^{-1}\alpha(x)\alpha(y) = \alpha(y)x^{-1}\alpha(x)$ für alle $x, y \in G$, d. h. wenn $x^{-1}\alpha(x)$ für alle $x \in G$ mit jedem Element in $\alpha(G)$ vertauschbar ist. Insbesondere ist ein $\alpha \in \operatorname{Aut} G$ genau dann normal, wenn $x^{-1}\alpha(x)$ für alle $x \in G$ im Zentrum von G ist.

Beispiel 6.4
Die Identitätsabbildung $\iota_G \colon G \to G$ mit $g \mapsto g$ und die **Nullabbildung** $0_G \colon G \to G$ mit $g \mapsto 1$ sind stets normal.

Satz 6.4 (SCHURS Lemma)
Für jede Menge Ω, jede einfache Ω-Gruppe G und jeden normalen Ω-Endomorphismus $0 \neq \alpha \in \operatorname{End}_\Omega G$ gilt: $\alpha \in \operatorname{Aut}_\Omega G$.

BEWEIS:
Sicher ist das $\alpha(G)$ ein Ω-Normalteiler von G. Wegen $\alpha \neq 0$ ist $\alpha(G) \neq 1$. Also ist $\alpha(G) = G$. Analog ist der Kern von α ein Ω-Normalteiler mit $\ker \alpha \neq G$ (wegen $\alpha \neq 0$). Daher ist der Kern von α gleich 1, d. h. α ist injektiv. ∎

7. Direkte Zerlegungen

Definition 7.1 (Direkte Summe)
Sei $(G_i)_{i\in I}$ eine nichtleere Familie von Normalteilern G_i einer Gruppe G mit den folgenden Eigenschaften:

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

(ii) $i \in I \Rightarrow G_i \cap \langle G_j : i \neq j \in I\rangle = 1$

Dann heißt G die **direkte Summe** von $(G_i)_{i\in I}$. Man schreibt $G = \bigoplus_{i\in I} G_i$. Falls $I = \{1,\dots,n\}$ für ein $n \in \mathbb{N}$ auch $G = G_1 \oplus \dots \oplus G_n$.

Bemerkung 7.1

(i) Für verschiedene Indizes $i, j \in I$ ist dann $G_i \cap G_j = 1$. Nach dem Satz 5.6 ist also jedes $x_i \in G_i$ mit jedem $x_j \in G_j$ vertauschbar. Zu jedem $g \in G$ existieren ferner $i_1,\dots,i_n \in I$, $g_{i_1} \in G_{i_1},\dots,g_{i_n} \in G_{i_n}$ mit $g = g_{i_1}\cdot\ldots\cdot g_{i_n}$ und Œ haben wir $i_1,\dots,i_n$ paarweise verschieden. Auf die Reihenfolge der Faktoren kommt es dabei nicht an. Wir setzen $g_i = 1$ für $i \in I \setminus \{i_1,\dots,i_n\}$ und schreiben auch $g = \prod_{i\in I} g_i$. Hat man eine weitere Familie $(h_i)_{i\in I}$ von Elementen $h_i \in G_i$ mit $|\{\, i \in I \mid h_1 \neq 1\,\}| < \infty$ und $g = \prod_{i\in I} h_i$, so ist $g_i = h_i$ für alle i. Denn im Fall $g_i \neq h_i$ für ein $i \in I$ wäre $1 \neq g_i^{-1}h_i = \prod_{i\neq j\in I} g_j h_j^{-1} \in G_i \cap \langle G_j : i \neq j \in I\rangle = 1$ ↯ Jedes Element in G lässt also in der Form $g = \prod_{i\in I} g_i$ mit eindeutig bestimmten Elementen $g_i \in G_i$ schreiben, von denen nur endlich viele von 1 verschieden sind. Daraus folgt leicht, dass $\coprod_{i\in I} G_i \to G$ mit $(g_i)_{i\in I} \mapsto \prod_{i\in I} g_i$ ein Isomorphismus ist. Man identifiziert daher oft $G = \bigoplus_{i\in I} G_i$ mit $\coprod_{i\in I} G_i$ und schreibt z. B. im Fall $I = \{1,\dots,n\}$ auch $G_1 \times \dots \times G_n$ statt $G_1 \oplus \dots \oplus G_n$.

(ii) Sei umgekehrt $(G_i)_{i\in I}$ eine Familie beliebiger Gruppen. Wir setzen $G := \coprod_{i\in I} G_i$ und $\widehat{G_j} := \left\{\, (g_i)_{i\in I} \in \coprod_{i\in I} G_i \;\middle|\; g_i = 1 \forall j \neq i \in I \,\right\}$. Dann folgt leicht, dass $G = \bigoplus_{i\in I} \widehat{G_j}$ und $\widehat{G_j} \cong G_j$ für alle $j \in I$. Auch hier identifiziert man oft G_j mit $\widehat{G_j}$ und fasst so G_j als Untergruppe von G auf.

Satz 7.1
Seien $G_1,\dots,G_n$ Normalteiler einer Gruppe G mit $G = G_1\cdot\ldots\cdot G_n$ und $G_i \cap G_1\cdot\ldots\cdot G_{i-1} = 1$ für $i = 2,\dots,n$. Dann ist $G = G_1 \oplus \dots \oplus G_n$.

BEWEIS:
Sei $i \in \{1,\dots,n\}$ und $1 \neq g \in G_i \cap \langle G_1,\dots,G_{i-1},G_{i+1},\dots,G_n\rangle = G_i \cap G_1 \cdot \ldots \cdot G_{i-1} \cdot G_{i+1} \cdot \ldots \cdot G_n$. Dann existieren Elemente $g_1 \in G_1,\dots,g_{i-1} \in G_{i-1}, g_{i+1} \in G_{i+1},\dots,g_n \in G_n$ mit $g = g_1 \cdot \ldots \cdot g_{i-1} \cdot g_{i+1} \cdot \ldots \cdot g_n$. Für verschiedene $j, h \in \{1,\dots,n\}$

ist $G_j \cap G_k = 1$, d. h. jedes $x_j \in G_j$ ist mit jedem $x_k \in G_k$ vertauschbar. Daher haben wir $1 = g_1 \cdot \ldots \cdot g_{i-1} \cdot g_i \cdot g_{i+1} \cdot \ldots \cdot g_n$ mit $g_i := g^{-1}$. Sei $j \in \{1, \ldots, n\}$ maximal mit $g_j \neq 1$. Dann $1 \neq g_j^{-1} = g_1 \cdot \ldots \cdot g_{j-1} \in G_j \cap G_1 \cdot \ldots \cdot G_{j-1} = 1$ ↯ ∎

Beispiel 7.1
Sind G_1, G_2 Normalteiler einer Gruppe G mit $G = G_1 \cdot G_2$ und $G_1 \cap G_2 = 1$. Dann ist $G = G_1 \oplus G_2$.

Satz 7.2
Seien $G_1, \ldots, G_n$ Normalteiler einer endlichen Gruppe G mit $|G| = |G_1| \cdot \ldots \cdot |G_n|$ und $ggT(|G_i|, |G_j|) = 1$ für $i \neq j$. Dann ist $G = G_1 \oplus \ldots \oplus G_n$.

BEWEIS:
Der Beweis erfolgt durch Induktion nach i: $G_i \cap G_1 \cdot \ldots \cdot G_{i-1} = 1$ und $|G_1 \cdot \ldots \cdot G_i| = |G_1| \cdot \ldots \cdot |G_{i-1}|$. Für $i = 2$ ist $|G_2 \cap G_1| \mid ggT(|G_2|, |G_1|) = 1$. Also $G_2 \cap G_1 = 1$ und $|G_1 G_2| = |G_1| \cdot |G_2| (\cdot |G_1 \cap G_2|) = |G_1| \cdot |G_2|$. Sei die Aussage für i schon bewiesen. Dann $|G_{i+1} \cap G_1 \cdot \ldots \cdot G_i| \mid ggT(|G_{i+1}|, |G_1 \cdot \ldots \cdot G_i|) = ggT(|G_{i+1}|, |G_1| \cdot \ldots \cdot |G_i|) = 1$. Also $G_{i+1} \cap G_1 \cdot \ldots \cdot G_i = 1$ und $|G_1 \cdot \ldots \cdot G_i \cdot G_{i+1}| = |G_1 \cdot \ldots \cdot G_i| \cdot |G_{i+1}| = |G_1| \cdot \ldots \cdot |G_i| \cdot |G_{i+1}|$. Am Ende hat man $|G| = |G_1| \cdot \ldots \cdot |G_n| = |G_1 \cdot \ldots \cdot G_n|$. Also $G = G_1 \cdot \ldots \cdot G_n$. Aus dem Satz 7.1 folgt die Behauptung. ∎

Definition 7.2 (Minimale, maximale Untergruppe/Normalteiler)
Eine **minimale** bzw. **maximale Untergruppe** einer Gruppe G ist eine Untergruppe $U \neq 1$ bzw. $U \neq G$ von G derart, dass keine Untergruppe $V \leqslant G$ existiert mit $1 < V < U$ bzw. $U < V < G$. Analog definiert man **minimale** bzw. **maximale Normalteiler**

Satz 7.3
(i) Sind $G_1, \ldots, G_n$ nichtabelsche einfache Normalteiler einer Gruppe G mit $G = G_1 \oplus \ldots \oplus G_n$, so sind die Teilsummen $G_{i_1} \oplus \ldots \oplus G_{i_k}$ die einzigen Normalteiler von G_i. Insbesondere existiert zu jedem Normalteiler $N \trianglelefteq G$ ein $M \trianglelefteq G$ mit $G = N \oplus M$.

(ii) Direkte Produkte von endlich vielen isomorphen einfachen Gruppen sind stets charakteristisch einfach.

(iii) Jede endliche charakteristisch einfache Gruppe G ist eine direkte Summe endlich vieler isomorpher einfacher Gruppen.

BEWEIS:
(i) Sei die Voraussetzung erfüllt und $g \in N \trianglelefteq G$. Wir schreiben $g = g_1 \cdot \ldots \cdot g_n$ mit $g_1 \in G_1, \ldots, g_n \in G_n$. Dann genügt zu zeigen:

(7.1) Ist $1 \leqslant i \leqslant n$ mit $g_i \neq 1 \Rightarrow G_i \subseteq N$

Sei $1 \leqslant i \leqslant n$ mit $g_i \neq 1$. Da G_i einfach und nichtabelsch, ist $Z(G_i) = 1$. Also liegt g_i nicht im Zentrum von G. Also gibt es ein Element $h \in G_i$ mit $hg_i \neq g_i h$, d. h. $1 \neq hg_i h^{-1} g_i^{-1} = hgh^{-1} g^{-1} \in G_i \cap N$. Folglich gilt: $G_i \trianglerighteq G_i \cap N \neq 1$ ist ein Normalteiler in G_i. Da aber G_i einfach ist, ist $G_i = G_i \cap N \leqslant N$.

(ii) Sei H eine einfache Gruppe und $G = H \times \ldots \times H$ mit n Faktoren.

1. Fall Sei H nichtabelsch. Dann ist $G = H_1 \oplus \ldots \oplus H_n$ mit $H_i := 1 \times \ldots \times 1 \times H \times 1 \times \ldots \times 1$, d. h. an der i-ten Stelle steht das H. Jede charakteristische Untergruppe $1 \neq N \leqslant G$ enthält nach dem Teil (i) des Satzes ein H_i. Für $f \in \mathrm{Sym}(n)$ ist $\alpha\colon G \to G$ mit $(g_1, \ldots, g_n) \mapsto (g_{f(1)}, \ldots, g_{f(n)})$ ein Automorphismus. Also gilt: $\alpha(H_i) \subseteq N$. So erhält man: $H_j \subseteq N$ für alle $j = 1, \ldots, n$, d. h. $N = G$.

2. Fall Sei H abelsch. Für $1 \neq a \in H$ ist dann $\langle a \rangle = H$. Daher ist die Abbildung $f\colon \mathbb{Z} \to H$ mit $k \mapsto a^k$ ein Epimorphismus. Folglich gilt $H \cong \mathbb{Z}/\ker f$ nach dem Satz 5.2. Nach dem Satz 4.5 ist $\ker f = l\mathbb{Z}$ für ein $l \in \mathbb{N}_0$. Dabei ist $l \neq 0$. Denn andernfalls wäre $\mathbb{Z}/\{0\} \cong \mathbb{Z}$. Aber $\mathbb{Z}$ ist nicht einfach. Ferner ist $l = p$ eine Primzahl. Denn andernfalls gilt für $d \mid l$: $0 \neq d\mathbb{Z}/l\mathbb{Z} \trianglelefteq \mathbb{Z}/l\mathbb{Z}$. Daher sei Œ $G = (\mathbb{Z}/p\mathbb{Z})^n$. Bekanntlich ist $\mathbb{Z}/p\mathbb{Z}$ ein Körper und $(\mathbb{Z}/p\mathbb{Z})^n$ kann man als $\mathbb{Z}/p\mathbb{Z}$-Vektorraum auffassen. Jeder Automorphismus dieses Vektorraums ist auch ein Gruppenhomomorphismus oder besser Gruppenautomorphismus. Wie man in der Vorlesung zur linearen Algebra zeigt, existiert zu je zwei Elementen $x, y \in (\mathbb{Z}/p\mathbb{Z})^n$ ein Vektorraum-Automorphismus α von $(\mathbb{Z}/p\mathbb{Z})^n$ mit $\alpha(x) = y$. Folglich ist G charakteristisch einfach.

(iii) Sei G endlich und charakteristisch einfach. Weiterhin sei N ein minimaler Normalteiler von G. Für $\alpha \in \mathrm{Aut}\, G$ ist dann auch $\alpha(N)$ wieder ein minimaler Normalteiler von G. Wir wählen eine möglichst große Untergruppe $M \leqslant G$, die direkte Summe einiger $\alpha(N)$ ist. Offenbar ist $M \trianglelefteq G$. Wir nehmen nun an, dass es einen Automorphismus $\beta \in \mathrm{Aut}\, G$ mit $\beta(N) \nsubseteq M$ gibt. Dann gilt: $M \cap \beta(N) \trianglelefteq G$ und $M \cap \beta(N) < \beta(N)$. Also ist $M \cap \beta(N) = 1$ wegen der Minimalität von $\beta(N)$. Folglich ist $M\beta(N) = M \oplus \beta(N)$ im Widerspruch zur Wahl des N. Daher ist $M = \langle \beta(N) \colon \beta \in \mathrm{Aut}\, G \rangle$. Insbesondere ist M charakteristisch in G. Also ist $M = G$. Folglich existieren $\alpha_1, \ldots, \alpha_n \in \mathrm{Aut}\, G$ mit $G = \alpha_1(N) \oplus \ldots \oplus \alpha_n(N)$.

Für $i \neq j$ ist jedes $x \in \alpha_i(N)$ mit jedem $y \in \alpha_j(N)$ vertauschbar. Für $i = 1, \ldots, n$ ist jeder Normalteiler K von $\alpha_i(N)$ auch ein Normalteiler von G. Also $K \in \{1, \alpha_i(N)\}$. Daher sind $\alpha_1(N), \ldots, \alpha_n(N)$ isomorphe einfache Gruppen. ∎

Definition 7.3 (Minimal-/Maximalbedingung)
Sei Ω eine Menge. Eine Ω-Gruppe G erfüllt die **Minimalbedingung** bzw. **Maximalbedingung** für Ω-Untergruppen, falls jede nichtleere Menge $\mathfrak{M}$ von Ω-Untergruppen von G ein minimales bzw. maximales Element M enthält. Das heißt, es existiert kein $H \in \mathfrak{M}$ mit $H < M$ bzw. $M < H$.

Satz 7.4 (Satz von FITTING)
Sei Ω eine Menge und G eine Ω-Gruppe mit Minimal- und Maximalbedingung für Ω-Untergruppen. Zu jedem normalen Endomorphismus $\alpha \in \mathrm{End}_\Omega\, G$ existiert dann eine natürliche Zahl k mit:

(i) $G \geqslant \alpha(G) \geqslant \alpha^2(G) \geqslant \cdots \alpha^k(G) = \alpha^{k+1}(G) = \cdots$

(ii) $1 \leqslant \ker(\alpha) \leqslant \ker(\alpha^2) \leqslant \cdots \leqslant \ker(\alpha^k) = \ker(\alpha^{k+1}) = \cdots$

Für jedes k ist

$$G = \ker(\alpha^k) \oplus \alpha^k(G)$$

BEWEIS:
Die Punkte (i) und (ii) folgen aus der Minimal- bzw. Maximalbedingung. Offenbar sind $\ker(\alpha^k)$ und $\alpha^k(G)$ Normalteiler von G. Für $g \in \ker(\alpha^k) \cap \alpha^k(G)$ existiert ein Element $h \in G$ mit $g = \alpha^k(h)$ und $1 = \alpha^k(g) = \alpha^{2k}(h)$. Also ist $h \in \ker(\alpha^{2k}) = \ker(\alpha^k)$. Damit ist $g = \alpha^k(h) = 1$. Wir haben also gezeigt, dass der Durchschnitt der beiden Mengen gleich 1 ist.

Für $g \in G$ ist andererseits $\alpha^k(g) \in \alpha^k(G) = \alpha^{2k}(G)$. Also $\alpha^k(g) = \alpha^{2k}(h)$ für $h \in G$. Daher ist $1 = \alpha^k(g)\alpha^{2k}(h)^{-1} = \alpha^k(g\alpha^{2k}(h)^{-1})$. Also ist $g\alpha^k(h^{-1}) \in \ker(\alpha^k)$ und $g = g\alpha^k(h) \cdot \alpha^k(h^{-1}) \in \ker(\alpha^k) \cdot \alpha^k(G)$. Damit ist $G = \ker \alpha^k \cdot \alpha^k(G)$. Die Behauptung folgt aus Beispiel 7.1. . ■

Bemerkung 7.2
Im Fall $\ker(\alpha^k) = 1$ ist also $G = \alpha^k(G)$, d. h. α^k und α sind bijektiv. Im Fall $\ker(\alpha^k) = G$ ist $\alpha^k = 0$ und α heißt dann **nilpotent**.

Definition 7.4 (Unzerlegbare Ω-Gruppe)
Sei Ω eine Menge. Eine Ω-Gruppe $G \neq 1$ heißt **unzerlegbar**, wenn keine echten Ω-Normalteiler $M, N \trianglelefteq G$ mit $G = M \oplus N$ existieren.

Bemerkung 7.3
Jeder normale Ω-Endomorphismus einer unzerlegbaren Ω-Gruppe mit Minimal- und Maximalbedingung für Ω-Untergruppen ist nach Satz 7.4 nilpotent oder bijektiv.

Satz 7.5
Sei Ω eine Menge und G eine Ω-Gruppe mit Minimalbedingung für Ω-Untergruppen. Dann existieren endlich viele unzerlegbare Ω-Normalteiler $G_1, \ldots, G_n \trianglelefteq G$ mit $G = G_1 \oplus \ldots \oplus G_n$.

BEWEIS:
Andernfalls ist die Menge $\mathfrak{M}$ aller Ω-Untergruppen von G, die sich nicht als direkte Summe von endlich vielen unzerlegbaren Ω-Untergruppen von G schreiben lassen, nichtleer. Daher existiert ein minimales Element $M \in \mathfrak{M}$. Dann ist $M \neq 1$ und M ist selbst keine unzerlegbare Ω-Untergruppe von G. Somit existieren Ω-Untergruppen $M_1, M_2 < M$ mit $M = M_1 \oplus M_2$. Nach der Wahl von M sind M_1 und M_2 direkte Summen von endlich vielen unzerlegbaren Ω-Untergruppen von G, also auch von M. ↯■

Beispiel 7.2

(i) Seien $a = \begin{pmatrix}1&2&3&4&5\\2&3&1&4&5\end{pmatrix}, b = \begin{pmatrix}1&2&3&4&5\\2&1&3&4&5\end{pmatrix}, c = \begin{pmatrix}1&2&3&4&5\\1&2&3&5&4\end{pmatrix} \in \mathrm{Sym}(5)$ und $G := \langle a, b, c\rangle$. Dann: $G = G_1 \oplus G_2$ mit $G_1 := \langle a, b\rangle \cong \mathrm{Sym}(3)$ und $G_2 := \langle c\rangle \cong \mathrm{Sym}(2)$. Aber auch $G = H_1 \oplus H_2$ mit $H_1 := \langle a, bc\rangle \cong \mathrm{Sym}(3)$ und $H_2 := \langle c\rangle$.

(ii) Ein Ω-Vektorraum V über einen Körper Ω ist genau dann unzerlegbar, wenn gilt: $\dim V = 1$.

Definition 7.5 (Addierbare Endomorphismen)

Zwei Endomorphismen α, β einer Gruppe G heißen **addierbar**, falls $\alpha + \beta\colon G \to G$ mit $g \mapsto \alpha(g)\beta(g)$ ein Endomorphismus von G ist.

Satz 7.6

Zwei Endomorphismen α, β einer Gruppe G sind genau dann addierbar, wenn jedes $x \in \alpha(G)$ mit jedem $y \in \alpha(G)$ vertauschbar ist. Gegebenenfalls gilt: $\alpha + \beta = \beta + \alpha$.

BEWEIS:

„$\Rightarrow$“ Sind α, β addierbar, so gilt für alle $g, h \in G$: $\alpha(g)\beta(g)\alpha(h)\beta(h) = (\alpha+\beta)(g)(\alpha+\beta)(h) = (\alpha+\beta)(gh) = \alpha(gh)\beta(gh) = \alpha(g)\alpha(h)\beta(g)\beta(h)$, d. h. $\beta(g)\alpha(h) = \alpha(h)\beta(g)$.

„$\Leftarrow$“ Sind $g, h \in G$ mit $\beta(g)\alpha(h) = \alpha(h)\beta(g)$, so gilt: $(\alpha+\beta)(gh) = \alpha(gh)\beta(gh) = \alpha(g)\alpha(h)\beta(g)\beta(h) = \alpha(g)\beta(g)\alpha(h)\beta(h) = (\alpha+\beta)(g)(\alpha+\beta)(h)$. ∎

Bemerkung 7.4

(i) Sind α, β zwei addierbare Endomorphismen von G, so auch $\alpha\circ\gamma, \beta\circ\gamma$ oder auch $\gamma\circ\alpha, \gamma\circ\beta$ für $\gamma \in \mathrm{End}(G)$ und es gilt: $(\alpha+\beta)\circ\gamma = \alpha\circ\gamma+\beta\circ\gamma$ und $\gamma\circ(\alpha+\beta) = \gamma\circ\alpha+\gamma\circ\beta$. Denn: $((\alpha+\beta)\circ\gamma)(g) = (\alpha+\beta)(\gamma(g)) = \alpha(\gamma(g))\beta(\gamma(g)) = (\alpha\circ\gamma+\beta\circ\gamma)(g)$ und $(\gamma\circ(\alpha+\beta))(g) = \gamma(\alpha(g)\beta(g)) = \gamma(\alpha(g))\gamma(\beta(g)) = (\gamma\circ\alpha+\gamma\circ\beta)(g)$ für $g \in G$.

(ii) Seien 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 $\omega \in \Omega$ und $g \in G$ 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) Es heißen $\alpha_1, \ldots, \alpha_n \in \mathrm{End}\, G$ **paarweise addierbar**, falls die α_i, α_j für alle $i \neq j$ addierbar sind. Gegebenenfalls ist $\alpha_1 + \cdots + \alpha_n\colon G \to G$ mit $g \mapsto \alpha_1(g), \ldots, \alpha_n(g)$ ein Endomorphismus von G und für $i = 1, \ldots, n-q$ gilt: $\alpha_1, \ldots, \alpha_n = (\alpha_1 + \cdots + \alpha_m) + (\alpha_{m+1} + \cdots + \alpha_n)$. Dabei sind die Summen rechts addierbar.

Satz 7.7

Seien Ω eine Menge und $G_1, \ldots, G_n$ alles Ω-Normalteiler einer Gruppe G mit der Eigenschaft $G = G_1 \oplus \ldots \oplus G_n$. Für $i = 1, \ldots, n$ sei die Abbildung $\varepsilon_i\colon G \to G$ definiert durch $\varepsilon_i(g_1\cdot\ldots\cdot g_n) := g_i$ für $g_1 \in G_1, \ldots, g_n \in G_n$. Dann sind die $\varepsilon_1, \ldots, \varepsilon_n \in \mathrm{End}_\Omega(G)$, normal und paarweise addierbar mit $\varepsilon_i^2 = \varepsilon_i$ für alle i, $\varepsilon_i \circ \varepsilon_j = 0$ für $i \neq j$ und $\varepsilon_1 + \cdots + \varepsilon_n = \mathrm{id}_G$.

BEWEIS:
Für $i = 1, \ldots, n$ ist ε_i nach der Definition der direkten Summe wohldefiniert. Es ist auch ein Homomorphismus. Denn für $g_1, h_1 \in G_1, \ldots, g_n, h_n \in G_n$ und $\omega \in \Omega$ gilt: $\varepsilon_i(g_1 \cdot \ldots g_n \cdot h_1 \cdot \ldots \cdot h_n) = \varepsilon_i(g_1 h_1 \cdot \ldots \cdot g_n h_n) = g_i h_i = \varepsilon_i(g_1 \cdot \ldots \cdot g_n)\varepsilon_i(h_1 \cdot \ldots \cdot h_n)$. Weiter ist die Verträglichkeit mit ω zu prüfen: $\varepsilon_i({}^{\omega}(g_1 \cdot \ldots \cdot g_n)) = \varepsilon_i({}^{\omega}g_1 \cdot \ldots \cdot {}^{\omega}g_n) = {}^{\omega}g_i = {}^{\omega}\varepsilon_i(g_1 \cdot \ldots \cdot g_n)$. Weiter haben wir: $\varepsilon_i(g(g_1 \cdot \ldots \cdot g_n)g^{-1}) = \varepsilon_i(gg_1g^{-1} \cdot \ldots \cdot gg_ng^{-1}) = gg_ig^{-1} = g\varepsilon_i(g_1 \cdot \ldots \cdot g_n)g^{-1}$. Für $i \neq j$ sind $\varepsilon_i, \varepsilon_j$ wegen $\varepsilon_i(G) = G_i, \varepsilon_j(G) = G_j$ addierbar. Der Rest des Beweises ist klar. ∎

Satz 7.8
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 sowie addierbar mit $\alpha + \beta \in \mathrm{Aut}_\Omega(G)$. Dann ist $\alpha \in \mathrm{Aut}_\Omega(G)$ oder $\beta \in \mathrm{Aut}_\Omega(G)$.

BEWEIS:
Nach der Bemerkung 7.4 sind $\alpha' := (\alpha + \beta)^{-1} \circ \alpha, \beta' := (\alpha + \beta)^{-1} := \beta \in \mathrm{End}_\Omega(G)$ normal und addierbar mit $\alpha' + \beta' = (\alpha + \beta)^{-1} \circ (\alpha + \beta) = \mathrm{id}_G$.

Für $g \in G$ gilt also:

$$\begin{aligned}\alpha'(\beta'(g)) &= \alpha'(\alpha'(g^{-1})\alpha'(g)\beta'(g)) = \alpha'(\alpha'(g^{-1})(\alpha' + \beta')(g)) \\ &= \alpha'(\alpha'(g^{-1})g) = \alpha'(\alpha'(g^{-1}))\alpha'(g) = \alpha'(\alpha'(g^{-1}))(\alpha' + \beta')(\alpha'(g)) \\ &= \alpha'(\alpha'(g^{-1}))\alpha'(\alpha'(g))\beta'(\alpha'(g)) = \beta'(\alpha'(g))\end{aligned}$$

Falls beide Summanden keine Automorphismen sind, dann wären α', β' nilpotent nach der Bemerkung 7.3. Das heißt $(\alpha')^n = 0 = (\beta')^n$ für ein $n \in \mathbb{N}$. Dann wäre die Identität auf G: $\mathrm{id}_G = (\alpha' + \beta') = (\alpha' + \beta')^n = (\alpha' + \beta')^{2n} = \sum_{j=0}^{2n} \binom{2n}{j} (\alpha')^j \circ (\beta')^{2n-j} = 0$. Dies würde nur gut gehen, wenn $G = 1$. Das ist aber im Widerspruch zur Voraussetzung. Daher ist $\alpha' \in \mathrm{Aut}_\Omega(G)$ oder $\beta' \in \mathrm{Aut}_\Omega(G)$, also auch $\alpha \in \mathrm{Aut}_\Omega(G)$ oder $\beta \in \mathrm{Aut}_\Omega(G)$. ∎

Satz 7.9 (Eindeutigkeitssatz von KRULL-REMAK-SCHMIDT)
Seien Ω eine Menge und G eine Ω-Gruppe mit Minimal- und Maximalbedingung für Ω-Untergruppen. Ferner sei $G = G_1 \oplus \ldots \oplus G_r = H_1 \oplus \ldots \oplus H_s$ mit unzerlegbaren Ω-Normalteilern $G_1, \ldots, G_r, H_1, \ldots, H_s$. Dann ist $r = s$, nach geeigneter Umnummerierung der $H_1, \ldots, H_s$ ist $G = H_1 \oplus \ldots \oplus H_{i-1} \oplus G_i \oplus \ldots \oplus G_r$ für $i = 1, \ldots, r$ und es existiert ein normaler Ω-Automorphismus α von G mit $\alpha(G_i) = H_i$ für $i = 1, \ldots, r$.

BEWEIS:
Wir konstruieren für $i = 1, \ldots, r+1$ einen normalen Ω-Automorphismus α_i von G mit $\alpha_i(G_1) = H_1, \ldots, \alpha_i(G_{i-1}) = H_{i-1}, \alpha_i(G_i) = G_i, \ldots, \alpha_i(G_r) = G_r$ (bei passender Umnummerierung).

Zunächst sei $\alpha_1 := \mathrm{id}_G$. Damit ist der Induktionsanfang klar. Sei nun α_i für ein $i \in \{1, \ldots, r\}$ schon definiert. Dann: $G = \alpha_i(G) = \alpha_i(G_1 \oplus \ldots \oplus G_r) = \alpha_i(G_1) \oplus \ldots \oplus \alpha_i(G_r) = H_1 \oplus \ldots \oplus H_{i-1} \oplus G_i \oplus \ldots \oplus G_r$. Dazu gehören normale Endomorphismen $\varepsilon_1, \ldots, \varepsilon_r \in \mathrm{End}_\Omega(G)$ wie in Satz 7.7 und analog hat man normale $\eta_1, \ldots, \eta_s \in \mathrm{End}_\Omega(G)$ zur Zerlegung $G = H_1 \oplus \ldots \oplus H_s$. Dabei gilt: $\varepsilon_i = \varepsilon_i \circ \mathrm{id}_G = \varepsilon_i \circ \sum_{j=1}^{s} \eta_j = \sum_{j=1}^{s} \varepsilon_i \circ \eta_j$

mit $\eta_j(G) = H_j$ für $j = 1, \ldots, s$. Also ist $\varepsilon_j \circ \eta_j = \eta_j$ für $j \leqslant i-1$ und $\varepsilon_i \circ \eta_j = 0$ für $j = 1, \ldots, i-1$. Daher ist $\varepsilon_i = \sum_{j=i}^{s} \varepsilon_i \circ \eta_j$. Dabei sind die einzelnen Summanden paarweise addierbar mit $\varepsilon_i \circ \eta_i, \ldots, \varepsilon_i \circ \eta_s \in \mathrm{End}_\Omega(G)$. Für $\beta \in \mathrm{End}_\Omega(G)$ mit $\beta(G_i) \subseteq G_i$ sei $\overline{\beta}\colon G_i \to G_i$ die entsprechende Einschränkung. Dann: $\mathrm{id}_{G_i} = \overline{\varepsilon_i} = \sum_{j=i}^{s} \overline{\varepsilon_i \circ \eta_j}$. Da G_i unzerlegbar ist, ist unter $\overline{\varepsilon_i \circ \eta_i}, \ldots, \overline{\varepsilon_i \circ \eta_s}$ ein Automorphismus von G_i nach Satz 7.8. Nach Umnummerierung von $H_i, \ldots, H_s$ kann man $\overline{\varepsilon_i \circ \eta_i} \in \mathrm{Aut}_\Omega(G_i)$ annehmen.

Nun behaupten wir: $H_i = \eta_i(G_i) \oplus (\ker(\varepsilon_i) \cap H_i)$. Da ε_i und η_i Ω-Endomorphismen und normal sind, sind $\eta_i(G_i)$ und $\ker(\varepsilon_i) \cap H_i$ beide Ω-Normalteiler von G. Ist $g \in G_i$ mit der Eigenschaft $1 = \varepsilon_i(\eta_i(g)) = \overline{\varepsilon_i \circ \eta_i}(g) = g$, also auch $\eta_i(g) = 1$. Daher ist $\eta_i(G_i) \cap \ker(\varepsilon_i) \cap H_i = 1$. Für $h \in H_i$ ist $\varepsilon_i(h) \in G_i = \varepsilon_i(\eta_i(G_i))$. Also $\varepsilon_i(h) = \varepsilon_i(\eta_i(k))$ für ein $k \in G_i$. Daher: $1 = \varepsilon_i(\eta_i(k^{-1}))\varepsilon_i(h) = \varepsilon_i(\eta_i(k^{-1})h)$, d. h. $\eta_i(k^{-1}) \in \ker(\varepsilon_i) \cap H_i$ und $h = \eta_i(k)\eta_i(k^{-1})h \in \eta_i(G_i) \cdot \ker(\varepsilon_i) \cap H_i$. Damit ist die Behauptung gezeigt.

Da H_i unzerlegbar und $\eta_i(G_i) \neq 1$ ist, folgt, dass $\ker(\varepsilon_i) \cap H_i = 1$ und $H_i = \eta_i(G_i) = \eta_i(\varepsilon_i(G))$. Für $j = 1, \ldots, i-1$ ist $\varepsilon_j(G) = H_j$ und für $j = i+1, \ldots, r$ ist $\varepsilon_j(G) = G_j$. Ferner ist $\eta_i(g_i) = \eta_i(g_j g_i g_j^{-1}) = g_j \eta_i(g_i) g_j^{-1}$ für $g_i \in G_i = \varepsilon_i(G)$, $g_j \in G_j$ mit $i \neq j$. Daher sind $\varepsilon_1, \ldots, \varepsilon_{i-1}, \eta_i \circ \varepsilon_i, \varepsilon_{i+1}, \ldots, \varepsilon_r$ paarweise addierbar. Folglich ist

$$\delta := \varepsilon_1 + \cdots + \varepsilon_{i-1} + (\eta_i \circ \varepsilon_i) + \varepsilon_{i+1} + \cdots + \varepsilon_r \in \mathrm{End}_\Omega(G)$$

normal mit

$$\begin{aligned} \delta(H_j) &= \varepsilon_j(H_j) = H_j \text{ für } j = 1, \ldots, i-1 \\ \delta(G_i) &= \eta_i(\varepsilon_i(G_i)) = H_i \\ \delta(G_j) &= \varepsilon_j(G_j) = G_j \text{ für } j = i+1, \ldots, r \end{aligned}$$

Daher: $\delta(G) = \delta(H_1 \cdot \ldots \cdot H_{i-1} \cdot G_i \cdot G_{i+1} \cdot \ldots \cdot G_r) = H_1 \cdot \ldots \cdot H_{i-1} \cdot G_i \cdot G_{i+1} \cdot \ldots \cdot G_r$ mit $H_1 \cdot \ldots \cdot H_{i-1} \cdot G_{i+1} \cdot \ldots \cdot G_r = H_1 \oplus \ldots \oplus H_{i-1} \oplus H_i \oplus G_{i+1} \oplus \ldots \oplus G_r$. Hat man $h_1 \in H_1, \ldots, h_{i-1} \in H_{i-1}, g_i \in G_i, \ldots, g_r \in G_r$ mit $1 = \delta(h_1 \cdot \ldots \cdot h_{i-1} g_i \cdot \ldots \cdot g_r) = h_1 \cdot \ldots \cdot h_{i-1}\eta_i(g_i)g_{i+1} \cdot \ldots \cdot g_r$, so folgt, $1 = h_1 = \cdots = h_{i-1} = \eta_i(g_i) = g_{i+1} = \cdots = g_r$. Wegen $\overline{\varepsilon_i \circ \eta_i} \in \mathrm{Aut}_\Omega(G_i)$ ist dann auch $g_i = 1$. Daher ist δ injektiv. Nach der Bemerkung 7.2 ist also $\delta \in \mathrm{Aut}_\Omega(G)$. Insbesondere ist $G = \delta(G) = H_1 \oplus \ldots \oplus H_i \oplus G_{i+1} \oplus \ldots \oplus G_r$. Folglich ist $\alpha_{i+1} := \delta \circ \alpha_i \in \mathrm{Aut}_\Omega(G)$ normal mit den gewünschten Eigenschaften. Am Schluss ist $\alpha_{r+1} \in \mathrm{Aut}_\Omega(G)$ normal mit $\alpha_{r+1}(G_1) = H_1, \ldots, \alpha_{r+1}(G_r) = H_r$. Daher ist $r = s$. ∎

Bemerkung 7.5
Dies ist analog zum Austauschsatz von STEINITZ aus der linearen Algebra.

Beispiel 7.3

(i) Sei Ω eine Menge mit $\Omega = \Omega_1 \dot\cup \ldots \dot\cup \Omega_k$. Dann ist $G := \mathrm{Sym}(\Omega_1) \oplus \ldots \oplus \mathrm{Sym}(\Omega_k) \leqslant \mathrm{Sym}(\Omega)$ die **YOUNG-Untergruppe**.

(ii) Sei $\mathbb{K}$ ein Körper und $n := n_1 + \cdots + n_k$ natürliche Zahlen. Die **LEVI-Untergruppe**

ist dann:

$$G := \begin{pmatrix} \boxed{\mathrm{GL}(n_1, \mathbb{K})} & & 0 \\ & \ddots & \\ 0 & & \boxed{\mathrm{GL}(n_1, \mathbb{K})} \end{pmatrix} \leqslant \mathrm{GL}(n, \mathbb{K})$$

8. Abelsche Gruppen

Bemerkung 8.1
In diesem Kapitel schreiben wir die abelschen Gruppen stets additiv.

Satz 8.1
In jeder abelschen Gruppe A bilden die Elemente endlicher Ordnung eine Untergruppe $T(A)$.

BEWEIS:
Da 0 die Ordnung 1 hat, ist $0 \in T(A)$. Seien nun $x, y \in A$. Dann sind die Ordnungen m von x und n von y endlich. Wegen $nm(x-y) = mnx - mny = 0 - 0 = 0$ hat auch $x-y$ endliche Ordnung, d. h. $x - y \in A$. ∎

Definition 8.1 (Torsionsgruppe, torsionsfrei)
Man bezeichnet $T(A)$ als **Torsionsgruppe** von A. Falls $T(A) = A$ heißt A selbst **Torsionsgruppe** und falls $T(A) = 0$ heißt A **torsionsfrei**.

Beispiel 8.1
$A = \mathbb{C} \setminus \{0\} \Rightarrow T(A) = \left\{ e^{2\pi i k/n} \mid k, n \in \mathbb{N} \right\}$

Satz 8.2
Sei A eine abelsche Gruppe. Dann ist $T(A)$ die Torsionsgruppe und $A/T(A)$ torsionsfrei.

BEWEIS:
Die erste Aussage ist trivial. Zum Beweis der zweiten Aussage habe $a + T(A) \in A/T(A)$ die Ordnung $n < \infty$. Dann ist $0 = n(a + T(A)) = na + T(A)$, d. h. $na \in T(A)$. Folglich ist $m := |\langle na \rangle| < \infty$. Daher $mna = 0$, d. h. $a \in T(A)$ und $a + T(A) = 0$. ∎

Bemerkung 8.2
Das Studium abelscher Gruppen teilt sich also in Torsionsgruppen und torsionsfreie Gruppen auf.

Definition 8.2 (linear (un)abhängig, Basis)
In einer abelschen Gruppe A heißen die Elemente $a_1, \ldots, a_n$ **linear unabhängig**, falls aus $0 = z_1 a_1 + \cdots + z_n a_n$ mit $z_1, \ldots, z_n \in \mathbb{Z}$ stets $z_1 = \cdots = z_n = 0$ folgt. Andernfalls heißen $a_1, \ldots, a_n$ **linear abhängig**. Sind $a_1, \ldots, a_n$ linear unabhängig mit $\langle a_1, \ldots, a_n \rangle = A$, so nennt man $a_1, \ldots, a_n$ eine **Basis** von A. Abelsche Gruppen, die eine Basis haben, heißen **freie abelsche Gruppen**.

Bemerkung 8.3

(i) Sei A eine freie abelsche Gruppe mit der Basis $a_1, \dots, a_n$. Dann ist A torsionsfrei. Denn ist $x = z_1a_1 + \cdots + z_na_n \in A$ mit $k := |\langle x\rangle| < \infty$, so ist $0 = kx = kz_1a_1 + \cdots + kz_na_n$, also $0 = kz_1 = \cdots = kz_n$ und damit ist $z_1 = \cdots = z_n = 0$, d. h. $x = 0$.

(ii) Es ist $(\mathbb{Q}, +)$ torsionsfrei, aber nicht frei. Denn sind $x \in \mathbb{Q}$ und $k \in \mathbb{N}$ mit $kx = 0$, so ist $x = 0$. Ferner ist $(\mathbb{Q}, +)$ nicht zyklisch und für $n \geqslant 2$ sind beliebige $x_1, \dots, x_n \in \mathbb{Q}$ stets linear abhängig. Schreibt man nämlich $x_i = p_i/q_i$ mit $p_i, q_i \in \mathbb{Z}$ und $q_i \neq 0$, so ist $0 = p_2q_1x_1 - p_1q_2x_2 + 0x_3 + \cdots + 0x_n$.

(iii) Für jede freie abelsche Gruppe A mit einer Basis $a_1, \dots, a_n$ ist die Abbildung $f\colon \mathbb{Z}^n \to A$ mit $(z_1, \dots, z_n) \mapsto z_1a_1 + \cdots + z_na_n$ ein Isomorphismus. Umgekehrt ist $\mathbb{Z}^n$ für ein $n \in \mathbb{N}$ frei mit der Basis

$$\begin{aligned} e_1 &= (1, 0, \dots, 0) \\ &\vdots \\ e_n &= (0, \dots, 0, 1) \end{aligned}$$

Satz 8.3

Seien A eine freie abelsche Gruppe, B eine beliebige abelsche Gruppe und $f\colon B \to A$ ein Epimorphismus. Dann ist $B = U \oplus \ker f$ für ein $U \leqslant B$. Insbesondere ist $U \cong B/\ker f \cong A$.

BEWEIS:

Sei $a_1, \dots, a_n$ eine Basis von A und $b_1, \dots, b_n \in B$ mit $f(b_1) = a_1, \dots, f(b_n) = a_n$ sowie $b \in B$. Dann existieren $z_1, \dots, z_n \in \mathbb{Z}$ mit $f(b) = z_1a_1 + \cdots + z_na_n = z_1f(b_1) + \cdots + z_nf(b_n) = f(z_1b_1 + \cdots + z_nb_n) =: f(n)$. Also ist $u \in U := \langle b_1, \dots, b_n\rangle$ mit $f(b - u) = 0$. Folglich: $b - u \in \ker f$ und $b = u + (b - u) \in U + \ker f$. Damit ist gezeigt: $B = U + \ker f$.

Sei andererseits $y \in U \cap \ker f$ und $y = y_1b_1 + \cdots + y_nb_n$. Dann ist $0 = f(y) = y_1f(b_1) + \cdots + y_nf(b_n) = y_1a_1 + \cdots + y_na_n$. Da $a_1, \dots, a_n$ linear unabhängig sind, folgt, $y_1 = \cdots = y_n = 0$ und $y = 0$. Also gilt auch: $U \cap \ker f = \emptyset$. ∎

Satz 8.4

Jede torsionsfreie endlich erzeugte abelsche Gruppe A ist frei.

BEWEIS:

Seien $A = \langle a_1, \dots, a_k\rangle$, $a_1 \neq 0, a_k \neq 0$ und $B = A/\langle a_k\rangle, T(B) = C/\langle a_k\rangle$ mit $\langle a_k\rangle \leqslant C \leqslant A$. Dann: $\langle a_1 + C, \dots, a_{k-1} + C\rangle = A/C \cong B/T(B)$ endlich erzeugt und torsionsfrei. Nun führen wir eine Induktion nach k durch. Der Fall $k = 1$ wurde oben schon erledigt. Also betrachten wir $k > 1$. Nach Induktion ist A/C frei, d. h. A/C ist isomorph zu $\mathbb{Z}^t$ für ein $t \in \mathbb{N}_0$. Nach dem Satz 8.3 ist $A = D \oplus C$ für eine Untergruppe $D \leqslant A$. Insbesondere ist D isomorph $A/C \cong \mathbb{Z}^t$. Daher genügt zu zeigen, dass das C frei ist. Wegen $C \cong A/D = \langle a_1 + D, \dots, a_k + D\rangle$ ist C endlich erzeugt. Sei etwa C erzeugt von $\langle c_1, \dots, c_l\rangle$. Für $c \in C$ ist $c + \langle a_k\rangle \in C/\langle a_k\rangle = T(B)$. Daher existiert ein $r \in \mathbb{N}$ mit der Eigenschaft $0 = r\cdot(c+\langle a_k\rangle) = rc+\langle a_k\rangle$, d. h. $r \in \langle a_k\rangle$, etwa $rc = sa_k$ mit $s \in \mathbb{Z}$. Sind auch $r' \in \mathbb{N}$ und $s \in \mathbb{Z}$ mit $r'c = s'a_k$, so ist $(r's-rs')a_k = r'sa_k-rs'a_k = r'rc-rr'c = 0$. Da

A torsionsfrei ist, folgt, dass $r's = rs'$, d. h. $s/r = s'/r'$ in $\mathbb{Q}$. Durch $f(c) := s/r$ erhalten wir eine wohldefinierte Abbildung $f\colon C \to \mathbb{Q}$. Seien $\tilde{c} \in C, \tilde{r} \in \mathbb{N}, \tilde{s} \in \mathbb{Z}$ mit $\tilde{r}\tilde{c} = \tilde{s}a_k$. Dann haben wir: $(r\tilde{s} + \tilde{r}s)a_k = r\tilde{s}a_k + \tilde{r}sa_k = r\tilde{r}\tilde{c} + \tilde{r}rc = r\tilde{r}(c + \tilde{c})$ d. h. $f(c + \tilde{c}) = \frac{r\tilde{s}+\tilde{r}s}{r\tilde{r}} = s/r + \tilde{s}/\tilde{r} = f(c) + f(\tilde{c})$. Somit ist f ein Homomorphismus. Ist $f(c) = 0$, so ist $s/r = 0$, also $s = 0$ oder $rc = sa_k = 0$. Somit muss $c = 0$ sein. Denn A ist torsionsfrei. Folglich ist das f ein Monomorphismus, da der Kern 0 ist. Wegen $C = \subseteq c_1, \dots, c_l\rangle$ ist $f(C) = \langle f(c_1), \dots, f(c_l)\rangle \leqslant (\mathbb{Q}, +)$. Es ist $f(C)$ zyklisch (siehe Übungsaufgabe Abschnitt A.3.2), d. h. $f(C) = 0$ oder $f(C) \cong \mathbb{Z}$. Insbesondere ist $f(C)$ frei und damit auch C frei. Insgesamt ist $A = D \oplus C$ frei. ∎

Übungen korrekt referenzieren

Bemerkung 8.4
Der Beweis zeigt genauer, dass man im Fall $A = \langle a_1, \dots, a_k\rangle$ eine Basis $b_1, \dots, b_t$ von A mit $t \leqslant k$ wählen kann. Dies funktioniert wie bei Vektorräumen in der linearen Algebra. Hingegen kann man im Allgemeinen $b_1, \dots, b_t$ nicht aus $\{a_1, \dots, a_k\}$ wählen. Denn $\mathbb{Z} = \langle 2, 3\rangle$, aber nicht nur von 2 oder 3 erzeugt.

Satz 8.5
Sei A eine freie abelsche Gruppe mit Basen $a_1, \dots, a_k$ und $b_1, \dots, b_l$. Dann ist k gleich l.

BEWEIS:
Offenbar ist $2A := \{\, 2a \mid a \in A \,\} \leqslant A$ und $A/2A$ wird zu einem Vektorraum über dem Körper $\mathbb{K} := \mathbb{Z}/2\mathbb{Z}$ mit $(z+2\mathbb{Z})(a+2a) := za+2A$ mit $z \in \mathbb{Z}$ und $a \in A$. Diese Definition ist wohldefiniert, wie man schnell nachrechnet. Wir behaupten, dass $a_1+2A, \dots, a_k+2A$ eine $\mathbb{K}$-Basis von $A/2A$ bilden. Sicher wird $A/2A$ von $a_1 + 2A, \dots, a_k + 2A$ aufgespannt. Seien $z_1, \dots, z_k \in \mathbb{Z}$ mit $0 = (z_1 + 2\mathbb{Z})(a_1 + 2A) + \cdots + (z_k + 2\mathbb{Z})(a_k + 2A) = z_1a_1 + \cdots + z_ka_k + 2A$. Dann ist $x := z_1a_1 + \cdots + z_ka_k \in 2A$, d. h. $x = 2y$ für ein $y \in A$. Schreibe $y = y_1a_1 + \cdots + y_ka_k$ mit $y_1, \dots, y_k \in \mathbb{Z}$. Dann ist $0 = x - 2y = (x_1 - 2y_1)a_1 + \cdots + (z_k - 2y_k)a_k$, also $z_i = 2y_i$. Somit ist $z_i + 2\mathbb{Z} = 0$ für $i = 1, \dots, n$. Damit ist gezeigt, dass $a_1 + 2A, \dots, a_k + 2A$ eine $\mathbb{K}$-Basis von $A/2A$ bilden. Analog bilden auch $b_1+2A, \dots, b_l+2A$ eine $\mathbb{K}$-Basis von $A/2A$. Nach den Aussagen aus der linearen Algebra ist dann $k = l$. ∎

Definition 8.3 (Rang)
Es heißt $k = \mathrm{rg}(A)$ der **Rang** von A.

Satz 8.6
Sei A eine endlich erzeugte abelsche Gruppe. Dann ist $T(A)$ endlich und $A = T(A) \oplus F$ mit einer freien abelschen Untergruppe $F \leqslant A$.

BEWEIS:
Da $A/T(A)$ endlich erzeugt und torsionsfrei ist, ist $A/T(A)$ nach Satz 8.4 eine freie abelsche Gruppe. Nach dem Satz 8.3 ist $A = T(A) \oplus F$ für ein $F \leqslant A$. Insbesondere ist $F \cong A/T(A)$ freie abelsche Gruppe. Außerdem ist $T(A) \cong A/F$ endlich erzeugt, etwa $T(A) = \langle t_1, \dots, t_l\rangle$. Mit $k_i := |\langle t_i\rangle| < \infty$ ist also $T(A) = \{\, z_1t_1 + \cdots + z_lt_l \mid 0 \leqslant z_i < k_i \,\}$ endlich. ∎

Bemerkung 8.5
Wegen $F \cong A/T(A)$ ist F durch A bis auf Isomorphie eindeutig bestimmt. Insbesondere ist der Rang von F durch A eindeutig bestimmt. Dagegen ist F selbst i. A. *nicht* eindeutig bestimmt.

Satz 8.7
Sei A eine abelsche Gruppe der Ordnung $n < \infty$ und $n = p_1^{k_1} \cdot \ldots \cdot p_r^{k_r}$ die Primfaktorzerlegung von n. Dann ist $A = A_1 \oplus \ldots \oplus A_r$ mit $A_i := \left\{ a \in A \;\middle|\; p_i^{k_i} a = 0 \right\} \leqslant A$ für $i = 1, \ldots, r$.

BEWEIS:
Für $a \in A$ gilt: $m := |\langle a \rangle| \mid n$. Daher existiert eine Primfaktorzerlegung $m = p_1^{l_1} \cdot \ldots \cdot p_r^{l_r}$ mit $l_1 \leqslant k_1, \ldots, l_r \leqslant k_r$. Für $i = 1, \ldots, r$ sei $m_i := m/p_i^{l_i}$. Dann ist $|\langle m_i a \rangle| = p_i^{l_i}$. Nach LAGRANGE ist die Ordnung der Untergruppe $\langle m_1 a, \ldots, m_r a \rangle$ von $\langle a \rangle$ teilbar durch $p_1^{l_1}, \ldots, p_r^{l_r}$, also auch durch m. Folglich ist $a \in \langle a \langle = \langle m_1 a, \ldots, m_r a \rangle \in A_1 + \cdots + A_r$. Damit ist gezeigt, dass $A = A_1 + \cdots + A_r$.

Sei $x_1 \in A_1 \cap (A_1 + \cdots + A_r)$. Wir schreiben $x_1 = x_2 + \cdots + x_r$ mit $x_2 \in A_2, \ldots, x_r \in A_r$. Für $i = 1, \ldots, r$ ist $p_i^{k_i} x_i = 0$ und es folgt mit $n_1 := p_2^{k_2} \cdot \ldots \cdot p_r^{k_r}$: $n_1 x_1 = n_1 x_2 + \cdots + n_1 x_r = 0 = p_1 k_1 x_1$. Daher ist die Ordnung von $\langle x_1 \rangle$ ein Teiler des größten gemeinsamen Teilers von n_1 und $p_1^{k_1}$. Dieser ist aber 1, d. h. $x_1 = 0$. Also $A_1 \cap (A_2 + \cdots + A_r) = 0$. Aus Symmetriegründen folgt somit $A = A_1 \oplus \ldots \oplus A_r$. ∎

Satz 8.8
Seien $p \in \mathbb{P}$, $k \in \mathbb{N}$ und A eine endliche abelsche Gruppe mit $p^k a = 0$ für alle $a \in A$. Dann existieren endlich viele natürliche Zahlen $t_1, \ldots, t_s$ mit $A \cong (\mathbb{Z}/p^{t_1}\mathbb{Z}) \times \ldots \times (\mathbb{Z}/p^{t_s}\mathbb{Z})$.

BEWEIS:
Aus der Voraussetzung folgt leicht, dass für alle $a \in A$ gilt: $|\langle a \rangle| \mid p^k$. Sei $a_1 \in A$ derart, dass $p^{t_1} = |\langle a_1 \rangle|$ maximal ist. Dann erfüllt $B := A/\langle a_1 \rangle$ die gleichen Voraussetzungen wie A. Aber $|B| < |A|$. Wir verwenden jetzt eine Induktion nach der Gruppenordnung. Daher können wir annehmen, dass $B \cong (\mathbb{Z}/p^{t_2}\mathbb{Z}) \times \ldots \times (\mathbb{Z}/p^{t_s}\mathbb{Z})$ mit $t_2, \ldots, t_s \in \mathbb{N}$. Also existieren Elemente $\overline{b_2} = b_2/\langle a_1 \rangle, \ldots, \overline{b_s} = b_s/\langle a_1 \rangle \in B = A/\langle a_1 \rangle$ der Ordnungen $p^{t_2}, \ldots, p^{t_s}$ mit $B = \langle \overline{b_2} \rangle \oplus \ldots \oplus \langle \overline{b_s} \rangle$. Für $i = 2, \ldots, s$ ist $0 = p^{t_i}\overline{b_i} = p^{t_i} b_i + \langle a_1 \rangle$, d. h. $p^{t_i} b_i$ mit in der Gruppe $\langle a_1 \rangle$ liegen. Wir schreiben $p^{t_i} b_i = z_i a_1$ mit $z_i \in \mathbb{Z}$. Wegen $p^{t_1}\overline{b_i} = p^{t_1} b_i + \langle a_1 \rangle = 0$ ist $t_i \leqslant t_1$ und $0 = p^{t_1} b_i = p^{t_1 - t_i} p^{t_i} b_i = p^{t_1 - t_i} z_i a_1$. Daher ist z_i durch p^{t_i} teilbar, etwa $z_i = p^{t_i} y_i$. Also: $0 = p^{t_i} b_i - p^{t_i} y_i a_1 = p^{t_i} (\underbrace{b_i - y_i a_1}_{=: a_i})$ und $a_i + \langle a_1 \rangle = b_i + \langle a_1 \rangle$. Ferner gilt: $|\langle a_i \rangle| = p^{t_i}$.

Wegen $A/\langle a_1 \rangle = \langle \overline{b_2}, \ldots, \overline{b_s} \rangle = \langle a_2 + \langle a_1 \rangle, \ldots, a_s + \langle a_1 \rangle \rangle$ ist $A = \langle a_1, a_2, \ldots, a_s \rangle$. Die Abbildung $f\colon \mathbb{Z}/p^{t_1}\mathbb{Z} \times \ldots \mathbb{Z}/p^{t_s}\mathbb{Z} \to A$ mit $(x_1 + p^{t_1}\mathbb{Z}, \ldots, x_s + p^{t_s}\mathbb{Z}) \mapsto x_1 a_1 + \cdots + x_s a_s$ ist wohldefiniert und ein surjektiver Homomorphismus (Epimorphismus). Dabei gilt: $|A| = |A/\langle a_1 \rangle| \cdot |\langle a_1 \rangle| = p^{t_2} \cdot \ldots \cdot p^{t_s} p^{t_1} = |\mathbb{Z}/p^{t_1}\mathbb{Z} \times \ldots \times \mathbb{Z}/p^{t_s}\mathbb{Z}|$. Also ist f bijektiv, d. h. ein Isomorphismus. ∎

Bemerkung 8.6
Für $t \in \mathbb{N}$ sind $\mathbb{Z}/p^t\mathbb{Z}, p\mathbb{Z}/p^t\mathbb{Z}, p^2\mathbb{Z}/p^t\mathbb{Z}, \ldots, p^t\mathbb{Z}/p^t\mathbb{Z} = 0$ die einzigen Untergruppen von $\mathbb{Z}/p^t\mathbb{Z}$. Es existieren also keine echten Untergruppen H_1, H_2 mit $\mathbb{Z}/p^t\mathbb{Z} = H_1 \oplus H_2$, d. h. $\mathbb{Z}/p^t\mathbb{Z}$ ist unzerlegbar. Nach dem Satz von KRULL-REMAK-SCHMIDT sind also $\mathbb{Z}/p^{t_1}\mathbb{Z}, \ldots, \mathbb{Z}/p^{t_s}\mathbb{Z}$ in Satz 8.8 bis auf Isomorphie eindeutig. Daher sind $t_1, \ldots, t_s$ durch A eindeutig bestimmt.

Beispiel 8.2
Bis auf Isomorphie existiert genau eine abelsche Gruppe der Ordnung 2, nämlich $\mathbb{Z}/2\mathbb{Z}$, genau zwei abelsche Gruppen der Ordnung 4, nämlich $\mathbb{Z}/4\mathbb{Z}$ und $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$, genau drei abelsche Gruppen der Ordnung 8, nämlich $\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ und $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ sowie genau fünf Gruppen der Ordnung 16 usw.

Satz 8.9 (Hauptsatz über endlich erzeugte Gruppen)
Jede endlich erzeugte Gruppe ist zu einem direkten Produkt endlich vieler zyklischer Gruppen isomorph, die entweder endlich sind oder Primzahlpotenzordnung haben. Die dabei auftretenden Faktoren sind bis auf Isomorphie und Reihenfolge eindeutig bestimmt.

BEWEIS:
Es folgt aus den vorigen Aussagen in Satz 8.6, Satz 8.7 und Satz 8.8. ∎

9. Auflösbare Gruppen

Definition 9.1 (Kommutator)
Für Elemente x und y einer Gruppe G heißt $[x,y] := xyx^{-1}y^{-1}$ **Kommutator** von x und y.

Bemerkung 9.1

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

(ii) Wegen $[x,y] = 1 \Leftrightarrow xy = yx$ misst der Kommutator in gewisser Weise die Abweichung von der Vertauschbarkeit. Ferner gilt: $xy = [x,y]yx$ und $[x,y]^{-1} = [y,x]$.

(iii) Für jeden Gruppenhomomorphismus $f\colon G \to H$ gilt: $f([x,y]) = [f(x), f(y)]$ für alle $x, y \in G$.

(iv) Für $x, y, z \in G$ gilt ein schwacher Ersatz für die Bilinearität aus der linearen Algebra: $[xy,z] = xyzy^{-1}x^{-1}z^{-1} = x[y,z]zx^{-1}z^{-1} = x[y,z]x^{-1}[x,z]$ und $[x,yz] = xyzx^{-1}z^{-1}y^{-1} = xyx^{-1}[x,z]y^{-1} = [x,y]y[x,z]y^{-1}$.

Definition 9.2 (rechtsnormierter höherer Kommutator)
Für Elemente $x_1, \ldots, x_n$ einer Gruppe G definiert man induktiv den **(rechtsnormierten) höheren Kommutator** $[x_1, \ldots, x_n] := [x_1, [x_2, \ldots, x_n]]$.

Bemerkung 9.2

(i) Manche Bücher bevorzugen linksnormierte Kommutatoren.

(ii) Für $x, y, z \in G$ gilt dann: $[xy,z] = [x,y,z][y,z][x,z]$ und $[x,yz] = [x,y][y,x,z][x,z]$.

(iii) Die folgende Aussage hat Ähnlichkeit mit der JACOBI-Identität für Lie-Algebren.

Satz 9.1
Für Elemente $x, y, z \in G$ gilt stets die WITT-Identität:

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

BEWEIS:
Wegen

$$\begin{aligned} y[x,y^{-1},z]y^{-1} &= yx[y^{-1},z]x^{-1}[z,y^{-1}]y^{-1} = yxy^{-1}zyz^{-1}x^{-1}zy^{-1}z^{-1}yy^{-1} \\ z[y,z^{-1},x]z^{-1} &= zy[z^{-1},x]y^{-1}[x,z^{-1}]z^{-1} = zyz^{-1}xzx^{-1}y^{-1}xz^{-1}x^{-1}zz^{-1} \\ x[z,x^{-1},y]x^{-1} &= xz[x^{-1},y]z^{-1}[y,x^{-1}]x^{-1} = xzx^{-1}yxy^{-1}z^{-1}yx^{-1}y^{-1}xx^{-1} \end{aligned}$$

gilt, dass sich die linke Seite der Gleichung durch folgendes zusammensetzt:

$$(yxy^{-1}zyz^{-1}x^{-1}zy^{-1}z^{-1}) \cdot (zyz^{-1}xzx^{-1}y^{-1}xz^{-1}x^{-1}) \cdot (xzx^{-1}yxy^{-1}z^{-1}yx^{-1}y^{-1})$$

Wie man leicht nachprüft, entspricht das Produkt dem gewünschten Ergebnis. ∎

Definition 9.3 (Kommutator zweier Teilmengen)
Für jede Gruppe G und Teilmengen $A, B \subseteq G$ sei $[A, B] := \langle [a, b] : a \in A, b \in B \rangle$ der **Kommutator zweier Teilmengen**.

Bemerkung 9.3

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

(ii) Für jeden Gruppenhomomorphismus $f : G \to H$ ist $f([A, B]) = [f(A), f(B)]$. Sind A und B normale oder charakteristische Untergruppen von G, so ist der Kommutator eine normale oder charakteristische Untergruppe von G.

(iii) $[A, B] = 1 \Leftrightarrow \forall a \in A \, \forall b \in B : ab = ba$

Satz 9.2
Für Untergruppen A und B einer Gruppe G gilt stets:

(i) $[A, B] \trianglelefteq \langle A, B \rangle$.

(ii) $[A, B] \leqslant A \Leftrightarrow \forall b \in B : bAb^{-1} \subseteq A$. Man sagt hierzu, dass das A von B normalisiert wird.

BEWEIS:

(i) Für beliebige $a, a' \in A, b \in B$ gilt nach Bemerkung 9.1 (iv):

$$\begin{aligned} a[a', b]a^{-1} &= aa'b(a')^{-1}b^{-1}a^{-1} = aa'b(a')^{-1}a^{-1}b^{-1}bab^{-1}a^{-1} \\ &= [aa', b][a, b]^{-1} \in [A, B] \end{aligned}$$

Also gilt auch: $a[A, B]a^{-1} \subseteq [A, B]$. Analog ist $b[A, B]b^{-1} \subseteq [A, B]$.

(ii) $[A, B] \leqslant A \Rightarrow \forall a \in A \, \forall b \in B : aba^{-1}b^{-1} \in A \Leftrightarrow \forall a \in A \, \forall b \in B : ba^{-1}b^{-1} \in A \Leftrightarrow \forall b \in B : bAb^{-1} \subseteq A$. ∎

Definition 9.4
Für jede Gruppe G und beliebige Teilmengen $X_1, \ldots, X_n \subseteq G$ definiert man induktiv:

$$[X_1, \ldots, X_n] := [X_1, [X_2, \ldots, X_n]]$$

Bemerkung 9.4

(i) $[X_1, \ldots, X_n]$ enthält alle Elemente der Form $[x_1, \ldots, x_n]$ mit $x_1 \in X_1, \ldots, x_n \in X_n$. Aber es wird nicht unbedingt von diesen erzeugt.

(ii) Für jeden Gruppenhomomorphismus $f : G \to H$ haben wir die Gleichheit von $f([X_1, \ldots, X_n])$ und $[f(X_1), \ldots, f(X_n)]$.

Satz 9.3
Für Untergruppen A, B, C einer Gruppe G gilt stets:

(i) $[A, B] \leqslant A \wedge [C, B] \leqslant C \Rightarrow [A, BC] = [A, B][B, C]$.

(ii) $[A, B, C] = 1 = [B, C, A] \Rightarrow [C, A, B] = 1$. Dies wird auch als **3-Untergruppen-Lemma** bezeichnet.

BEWEIS:

(i) Aus der Voraussetzung folgt, dass $BC = CB$ nach dem Satz 9.2 (ii), d. h. $BC \leqslant G$. Ferner ist $[A, C] \trianglelefteq \langle A, C\rangle$. Insbesondere bedeutet das: $x[A, C]x^{-1} = [A, C]$ für $x \in [A, B] \leqslant A$. Daher $[A, B][A, C] = [A, C][A, B] \leqslant G$. Ferner: $[a, bc] = [a, b]b[a, c]b^{-1} = [a, b][\underbrace{bab^{-1}}_{\in A}, \underbrace{bcb^{-1}}_{\in C}] \in [A, B][A, C]$ für $a \in A$, $b \in B$ und $c \in C$.
Folglich gilt: $[A, BC] \subseteq [A, B][A, C]$.

Umgekehrt: $[A, B] \subseteq [A, BC]$ und $[A, C] \subseteq [A, BC]$, also auch $[A, B][A, C] \subseteq [A, BC]$.

(ii) Aus der Voraussetzung folgt wegen der WITT-Identität: $[c, [a, b]] = 1$ für $a \in A$, $b \in B$, $c \in C$. Folglich ist jedes $c \in C$ mit jedem $x \in [A, B]$ vertauschbar. Daher gilt: $[C, [A, B]] = 1$. ∎

Definition 9.5 (Kommutatorgruppe)
Für jede Gruppe G heißt $G' := [G, G] = \langle [g, h] : g, h \in G\rangle$ die **Kommutatorgruppe** von G. Ist $G' = G$, dann heißt die Gruppe **perfekt**.

Bemerkung 9.5
Für jeden Gruppenhomomorphismus $f : G \to H$ ist $f(G') = f(G)' \leqslant H'$. Insbesondere ist $G' \subseteq G$ vollinvariant und damit auch charakteristisch und normal.

Satz 9.4
Für jede Untergruppe H von G sind äquivalent: (1) $G' \subseteq H$ sowie (2) $H \trianglelefteq G$ und G/H abelsch.

BEWEIS:
Wir betrachten zunächst die Richtung von (1) nach (2): Sei $G' \subseteq H$. Dann folgt: $ghg^{-1} = \underbrace{[g, h]}_{\in G'} h \in H$. Folglich: $H \trianglelefteq G$. Für $x, y \in G$ ist ferner $1 = [x, y]H = [xH, yH]$, d. h. $(xH)(yH) = (yH)(xH)$.

Sei nun die Bedingung (2) erfüllt: Für $x, y \in G$ ist dann: $[x, y]H = [xH, yH] = 1$, d. h. $[x, y] \in H$. Folglich ist $G' \subseteq H$. ∎

Beispiel 9.1
Wir werden später zeigen, dass „meist“ $GL(n, \mathbb{K})' = SL(n, \mathbb{K})$ gilt.

Definition 9.6
Die **höheren Kommutatorgruppen** einer Gruppe G definiert man induktiv:

$$G^{(0)} := G, G^{(1)} := G', G^{(2)} := (G')' = G'' = [G', G'], \ldots, G^{(i+1)} := [G^{(i)}, G^{(i)}]$$

Bemerkung 9.6

(i) Für jeden Gruppenhomomorphismus $f\colon G \to H$ und jede natürliche Zahl i ist $f(G^{(i)}) = f(G)^{(i)} \leqslant H^{(i)}$. Insbesondere ist $G^{(i)} \leqslant G$ vollinvariant.

(ii) Für $U \leqslant G$ und $i \in \mathbb{N}_0$ folgt, $U^{(i)} \leqslant G^{(i)}$.

(iii) Offenbar ist $G = G^{(0)} \geqslant G^{(1)} \geqslant G^{(2)} \geqslant \cdots$. Wir setzen $G^{(\infty)} := \bigcap_{i\in\mathbb{N}} G^{(i)}$.

Definition 9.7 (Auflösbare Gruppe)

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

Bemerkung 9.7

(i) Folgende Äquivalenzen gelten:

$$s = 0 \Leftrightarrow G = 1$$
$$s \leqslant 1 \Leftrightarrow G' = 1 \Leftrightarrow G \text{ abelsch}$$
$$s \leqslant 2 \Leftrightarrow G'' = 2 \Leftrightarrow G \text{ metaabelsch}$$

(ii) Untergruppen und Faktorgruppen von auflösbaren Gruppen sind auflösbar.

(iii) Für auflösbare Gruppen G, H ist auch $G \times H$ auflösbar. Denn $(G \times H)^{(i)} = G^{(i)} \times H^{(i)}$ für $i \in \mathbb{N}_0$.

(iv) Sind $M, N \trianglelefteq G$ und $G/M, G/N$ auflösbar, so ist auch $G/M \cap N$ auflösbar. Denn nach der Bemerkung 5.4 ist $G/M \cap N$ zu einer Untergruppe von $G/M \times G/N$ isomorph.

(v) Ist G auflösbar der Stufe s, so ist $G = G^{(0)} \trianglerighteq G^{(1)} \trianglerighteq \ldots \trianglerighteq G^{(s)} = 1$ eine Normalreihe mit abelschen Faktoren.

Satz 9.5

Für jede Gruppe G sind äquivalent:

(i) G auflösbar.

(ii) G hat eine Normalreihe mit abelschen Faktoren.

(iii) G hat eine Subnormalreihe $G = G_0 \trianglerighteq G_1 \trianglerighteq \ldots \trianglerighteq G_t = 1$ mit abelschen Faktoren.

BEWEIS:

Die Richtung von Aussage 1 zu Aussage 2 folgt nach der obigen Bemerkung. Die von 2 nach 3 ist trivial. So bleibt nur noch die Richtung von 3 zu 1 zu zeigen: Wir nehmen an, dass die Voraussetzung erfüllt ist. Dann zeigen wir induktiv: $G^{(i)} \leqslant G_i$ für $i \in \mathbb{N}_0$. Die Aussage ist für $i = 0$ klar. Sei also $i > 0$ und $G^{(i-1)} \leqslant G_{i-1}$. Da $G_i \trianglelefteq G_{i-1}$ und G_{i-1}/G_i abelsch ist, folgt aus Satz 9.4: $G^{(i)} = (G^{(i-1)})' \leqslant G'_{i-1} \leqslant G_i$. Am Schluss ist also $G^{(t)} \leqslant G_t = 1$. ∎

Beispiel 9.2
Für $n \in \mathbb{N}$ und jeden Körper $\mathbb{K}$ ist die Gruppe $B(n, \mathbb{K})$ aller oberen Dreiecksmatrizen in $GL(n, \mathbb{K})$ auflösbar.

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

Satz 9.6
Für jede Gruppe G und $N \trianglelefteq G$ gilt: G ist genau dann auflösbar, wenn N und G/N auflösbar sind.

BEWEIS:
Wir müssen nur die Rückrichtung zeigen. Denn die andere Richtung wurde bereits in Bemerkung 9.7 (ii) gezeigt. Seien N und G/N auflösbar. Dann existieren $s, t \in \mathbb{N}_0$ mit $N^{(i)} = 1$ und $1 = (G/N)^{(t)} = G^{(t)}N/N$. Folglich: $G^{(t)} \leqslant N$ und $G^{(t+s)} \leqslant N^{(s)} = 1$. ∎

Bemerkung 9.8
Für auflösbare Normalteiler M, N einer Gruppe G ist auch MN ein auflösbarer Normalteiler von G. Dies folgt aus dem Satz wegen $MN/N \cong M/M \cap N$. Ist G endlich, so ist also das Produkt aller auflösbaren Normalteiler ein auflösbarer Normalteiler von G. Dieser heißt **auflösbares Radikal** von G.

Satz 9.7
Für jede endliche Gruppe G sind äquivalent:

(i) G ist auflösbar.

(ii) Jeder Kompositionsfaktor von G ist zu $\mathbb{Z}/p\mathbb{Z}$ für ein $p \in \mathbb{P}$ isomorph.

(iii) Jeder Hauptfaktor von G ist zu $(\mathbb{Z}/p\mathbb{Z})^n$ für geeignete $p \in \mathbb{P}$ und natürliche n isomorph.

BEWEIS:
Die Richtungen (ii)⇒(i) und (iii)⇒(i) folgen nach Satz 9.5. Also zeigen wir zuerst (i)⇒(ii): Sei G auflösbar mit der Kompositionsreihe $G = G_0 \trianglerighteq G_1 \trianglerighteq \dots \trianglerighteq G_l = 1$. Für $i = 1, \dots, l$ ist dann $S_i := G_{i-1}/G_i$ auflösbar und einfach. Daher $S_i' \lhd S_i$[1], also $S_i' = 1$, d. h. S_i abelsch. Sei $1 \neq x \in S_i$. Dann ist $1 \neq \langle x \rangle \trianglelefteq S_i$, also $S_i = \langle x \rangle$ zyklisch. Da S_i einfach ist, folgt, $p_i := |S_i| \in \mathbb{P}$. Folglich: $S_i \cong \mathbb{Z}/p_i\mathbb{Z}$.

Nun bleibt noch die Richtung (i)⇒(iii): Sei dazu G auflösbar mit Hauptreihe $G = G_0 \trianglerighteq G_1 \trianglerighteq \dots \trianglerighteq G_l = 1$. Für $i = 1, \dots, l$ ist dann $T_i := G_{i-1}/G_i$ auflösbar und charakteristisch einfach. Nach Satz 7.3 ist $T_i \cong S_i^{n_i}$ für eine auflösbar einfache Gruppe S_i und ein natürliches n_i. Wie oben ist $S_i \cong \mathbb{Z}/p_i\mathbb{Z}$ für eine Primzahl p_i. ∎

Bemerkung 9.9
Man hat die folgenden Auflösbarkeitskriterien:

[1] Sonst wäre $S_i'' = S_i' = S_i$ usw.

(i) BURNSIDES $p^a q^b$-Satz von 1904: Für $p, q \in \mathbb{P}$ und $a, b \in \mathbb{N}_0$ ist jede Gruppe der Ordnung $p^a q^b$ auflösbar.

(ii) Satz von FEIT-THOMPSON von 1963: Gruppen ungerader Ordnung sind stets auflösbar. Der Beweis des Satzes umfasst etwa 250 Seiten.

10. Nilpotente Gruppen

Definition 10.1
Für $n \in \mathbb{N}$ und jede Gruppe G definiert man induktiv:

$$G^1 := G \qquad G^2 := [G, G] \qquad G^{n+1} := [G, G^n]$$

Bemerkung 10.1

(i) $n \in \mathbb{N} \Rightarrow G^n = [G, \ldots, G]$

(ii) $n \in \mathbb{N} \wedge U \leqslant G \Rightarrow U^n \leqslant G^n$

(iii) $n \in \mathbb{N} \wedge f\colon G \to H$ Gruppenhomomorphismus $\Rightarrow f(G^n) = f(G)^n \leqslant H^n$. Insbesondere ist G^n vollinvariant in G.

(iv) Nach dem obigen Punkt ist jeweils $G^n \trianglelefteq G$, also $G^{n+1} \leqslant G^n$ nach dem Satz 9.2. Wir erhalten so eine Folge vollinvarianter Untergruppen $G = G^1 \geqslant G^2 \geqslant G^3 \geqslant \cdots$. Diese wird als **absteigende Zentralfolge** von G bezeichnet. Wir setzen $G^\infty := \bigcap_{i \in \mathbb{N}} G^i$.

(v) $n \in \mathbb{N} \Rightarrow [G/G^{n+1}, G^n/G^{n+1}] = [G, G^n]G^{n+1}/G^{n+1} = G^{n+1}/G^{n+1} = 1 \Rightarrow G^n/G^{n+1} \leqslant Z(G/G^{n+1})$. Dies erklärt den Begriff „**Zentralfolge**“.

Satz 10.1
Für $1 \neq n \in \mathbb{N}$ und jede Gruppe G gilt:

$$G^n = \langle [g_1, \ldots, g_n] \colon g_1, \ldots, g_n \in G \rangle$$

BEWEIS:
Wir führen Induktion nach n durch. Für die Fälle $n = 1$ und $n = 2$ ist alles klar und nichts zu tun. Daher sei Œ $n \geqslant 3$. Offenbar ist $N := \langle [g_1, \ldots, g_n] \colon g_1, \ldots, g_n \in G \rangle \trianglelefteq G$ und $N \leqslant G^n$. Nach Induktion dürfen wir $G^{n-1} = \langle [g_2, \ldots, g_n] \colon g_2, \ldots, g_n \in G \rangle$ voraussetzen. Dann ist $G^{n-1}/N = \langle [g_2, \ldots, g_n]N \colon g_2, \ldots, g_n \in G \rangle$ und für $g_1, \ldots, g_n \in G$ gilt: $[g_1N, [g_2, \ldots, g_n]N] = [g_1, [g_2, \ldots, g_n]N] = [g_1, g_2, \ldots, g_nN] = 1$. Folglich: $G^{n-1}/N \leqslant Z(G/N)$ und $G^n/N = [G, G^{n-1}]/N = [G/N, G^{n-1}/N] = 1$, d. h. $G^n = N$. ∎

Satz 10.2
Für $m, n \in \mathbb{N}$ und jede Gruppe G gilt:

(i) $[G^m, G^n] \subseteq G^{m+n}$

(ii) $G^{(n)} \subseteq G^{2^n}$

BEWEIS:

(i) Wir führen Induktion nach n durch: Für $n = 1$ ist $[G^m, G] = [G, G^m] = G^{m+1}$. Sei also $n \geqslant 2$ und die Aussage für $n-1$ bereits bewiesen. Mit $H := G/G^{m+n}$ gilt dann:

$$\begin{aligned}[G^m, G^n]G^{m+n}/G^{m+n} &= [G^m/G^{m+n}, G^n/G^{m+n}] = [H^m, H^n] \\ &= [H^m, [H, H^{n-1}]] = 1\end{aligned}$$

wegen

$$\begin{aligned}[H, [H^{n-1}, H^m]] &= [H, [H^m, H^{n-1}]] \subseteq [H, H^{m+n-1}] = H^{m+n} \\ &= G^{m+n}/G^{m+n} = 1\end{aligned}$$

und

$$\begin{aligned}[H^{n-1}, [H^m, H]] &= [[H^m, H], H^{n-1}] = [[H, H^m], H^{n-1}] \\ &= [H^{m+1}, H^{n-1}] \subseteq H^{m+n} = 1\end{aligned}$$

nach dem 3-Untergruppen-Lemma. Also ist $[G^m, G^n] \subseteq G^{m+n}$.

(ii) Auch hier wird der Beweis per Induktion nach n geführt. Offenbar ist $G^{(0)} = G = G^1 = G^{2^0}$. Sei also n eine natürliche Zahl und bereits gezeigt, dass $G^{(n-1)} \subseteq G^{2^{n-1}}$ gilt. Dann folgt aus der obigen Aussage, dass $G^{(n)} = [G^{(n-1}, G^{(n-1)}] \subseteq [G^{2^{n-1}}, G^{2^{n-1}}] \subseteq G^{2^n}$. ∎

Definition 10.2 (Aufsteigende Zentralfolge)
Für jede Gruppe G definiert man die **aufsteigende Zentralfolge** induktiv durch:

$$Z_0(G) := 1 \qquad Z_1(G) := Z_2(G) \qquad Z_i/Z_{i-1}(G) := Z(G/Z_{i-1}(G))$$

Bemerkung 10.2

(i) Für $i \in \mathbb{N}_0$ ist $Z_i(G) \subseteq G$ charakteristisch. Dies ist für $i = 0$ und $i = 1$ klar. Ist $Z_{i-1}(G) \subseteq G$ charakteristisch für ein $i \in \mathbb{N}_0$, so induziert jedes $\alpha \in \mathrm{Aut}(G)$ ein $\overline{\alpha} \in \mathrm{Aut}(G/Z_{i-1}(G))$ mit $\overline{\alpha}(gZ_{i-1}(G)) := \alpha(g)Z_{i-1}(G)$ für $g \in G$. Da $Z(G/Z_{i-1}(G)) \subseteq G/Z_{i-1}(G)$ charakteristisch ist, folgt: $\overline{\alpha}(Z_i(G)/Z_{i-1}(G)) = Z_i(G)/Z_{i-1}(G)$. Folglich: $\alpha(g) \in Z_i(G)$ für $g \in Z_i(g)$.

(ii) $1 = Z_0(G) \leqslant Z_1(G) \leqslant Z_2(G) \leqslant \cdots$ und $Z_\infty := \bigcup_{i\in\mathbb{N}} Z_i(G)$ heißt **Hyperzentrum** von G. Dann ist $Z_\infty(G) \leqslant G$ eine charakteristische Untergruppe.

Definition 10.3 (Nilpotente Gruppe)
Eine Gruppe G mit $Z_c(G) = G$ für ein $c \in \mathbb{N}_0$ heißt **nilpotent**. Gegebenenfalls heißt das kleinste $c \in \mathbb{N}_0$ mit $Z_c(G) = G$ die **Nilpotenzklasse** von G.

Bemerkung 10.3
$c = 0 \Leftrightarrow G = 1$ und $c \leqslant 1 \Leftrightarrow G$ abelsch.

Definition 10.4 (Zentralreihe)
Eine Normalreihe $G = G_0 \trianglerighteq G_1 \trianglerighteq \ldots \trianglerighteq G_r = 1$ einer Gruppe G mit $G_{i-1}/G_i \subseteq Z(G/G_i)$ für alle i heißt **Zentralreihe**.

Beispiel 10.1
Ist G nilpotent der Klasse c, so ist $G = Z_c(G) \trianglerighteq Z_{c-1}(G) \trianglerighteq \ldots \trianglerighteq Z_1(G) \trianglerighteq Z_0(G) = 1$ eine Zentralreihe, die **obere** oder **aufsteigende Zentralreihe** von G.

Satz 10.3
Für Untergruppen $G_0, \ldots, G_r$ einer Gruppe G mit $G = G_0 \supseteq G_1 \supseteq \ldots \supseteq G_r = 1$ sind folgenden Aussagen äquivalent:

(1) $G = G_0 \trianglerighteq G_1 \trianglerighteq \ldots \trianglerighteq G_r = 1$ ist eine Zentralreihe.

(2) $[G, G_{i-1}] \subseteq G_i$ für $i = 1, \ldots, r$.

BEWEIS:
(1)⇒(2) Ist die erste Aussage erfüllt, so gilt für alle i:

$$[G, G_{i-1}]G_i/G_i = [G/G_i, G_{i-1}/G_i] = 1, \text{ d. h. } [G, G_{i-1}] \subseteq G_i$$

(2)⇒(1) Für $i = 1, \ldots, r$ sei $[G, G_{i-1}] \subseteq G_i \subseteq G_{i-1}$. Nach dem Satz 9.2 (ii) ist dann $G_{i-1} \trianglelefteq G$, d. h. wir haben eine Normalreihe. Ferner ist $[G/G_i, G_{i-1}/G_i] = [G, G_{i-1}]G_i/G_i = 1$, d. h. $G_{i-1}/G_i \subseteq Z(G/G_i)$. ∎

Bemerkung 10.4
Wegen der obigen zweiten Aussage ist jede Verfeinerung einer Zentralreihe wieder eine Zentralreihe.

Satz 10.4
Sei $G = G_0 \trianglerighteq G_1 \trianglerighteq \ldots \trianglerighteq G_r = 1$ eine Zentralreihe einer Gruppe G. Für $i = 0, \ldots, r$ ist dann $G_{r-i} \subseteq Z_i(G)$ und $G^{i+1} \subseteq G_i$. Insbesondere ist $Z_r(G) = G$ und $G^{r+1} = 1$, d. h. G ist nilpotent und die Klasse von G ist höchstens r.

BEWEIS:
Der Beweis wird per Induktion nach i geführt. Offenbar ist $G_r = 1 = Z_0(G)$ und $G^1 = G = G_0$. Sei also $i > 0$ und bereits $G_{r-i+1} \subseteq Z_{i-1}(G)$ sowie $G^i \subseteq G_{i-1}$ bewiesen. Dann haben wir:

$$\begin{aligned}[G/Z_{i-1}(G), G_{r-i}Z_{i-1}(G)/Z_{i-1}(G)] &= [G, G_{r-i}]Z_{i-1}(G)/Z_{i-1}(G) \\ &\subseteq G_{r-i+1}Z_{i-1}(G)/Z_{i-1}(G) = 1\end{aligned}$$

Also ist

$$G_{r-i}Z_{i-1}(G)/Z_{i-1}(G) \subseteq Z(G/Z_{i-1}(G)) = Z_i(G)/Z_i(G)$$

Folglich

$$G_{r-i} \subseteq Z_i(G)$$
$$G^{i+1} = [G, G^i] \subseteq [G, G_{i-1}] \subseteq G_i \qquad \blacksquare$$

Bemerkung 10.5

(i) Nach Satz 10.3 und Satz 10.4 ist eine Gruppe G genau dann nilpotent, wenn sie eine Zentralreihe hat. Gegebenenfalls ist die Klasse von G durch die Länge einer Zentralreihe beschränkt.

(ii) Für jede nilpotente Gruppe G der Klasse c $G^{c+1} = 1$. Daher ist $G = G^1 \trianglerighteq G^2 \trianglerighteq \ldots \trianglerighteq G^{c+1} = 1$ eine Zentralreihe. Sie wird als **untere** oder **absteigende Zentralreihe** von G. Nach der ersten Bemerkung ist ferner $G^c \neq 1$.

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

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

(v) Jede nilpotente Gruppe ist auflösbar.

(vi) Die Hauptfaktoren einer endlichen nilpotenten Gruppe G haben Primzahlordnung. Durch Verfeinerung der oberen Zentralreihe erhält man nämlich eine Kompositionsreihe, die gleichzeitig Zentralreihe ist. Diese ist also insbesondere eine Normalreihe und damit eine Hauptreihe von G. Da G auflösbar ist, haben ihre Faktoren Primzahlordnung.

Beispiel 10.2

(i) $\mathrm{Sym}(3)$ ist auflösbar, aber wegen $Z(\mathrm{Sym}(3)) = 1$ nicht nilpotent.

(ii) Eine typische nilpotente Gruppe ist die Untergruppe von $GL(n, \mathbb{K})$, die aus allen Matrizen der Form:

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

besteht.

Bemerkung 10.6

Für jede Teilmenge X einer Gruppe G ist der **Normalisator**

$$N_G(X) := \left\{ g \in G \;\middle|\; gXg^{-1} = X \right\}$$

eine Untergruppe von G. Dies rechnet man leicht nach. Ist $X \leqslant G$, so ist $X \trianglelefteq N_G(X)$.

Satz 10.5

Für jede echte Untergruppe U einer nilpotenten Gruppe G ist $U < N_G(U)$.

BEWEIS:
Da G nilpotent ist, existiert eine natürliche Zahl n mit $G^n = 1 \subseteq U$. Sei $m \in \mathbb{N}$ minimal mit $G^m \subseteq U$. Wegen $G^1 = G \nsubseteq U$ ist $m \geqslant 2$. Wegen $[U, G^{m-1}] \subseteq [G, G^{m-1}] = G^m \subseteq U$ ist $G^{m-1} \subseteq N_G(U)$ nach dem Satz 9.2 (ii), aber $G^{m-1} \nsubseteq U$. ∎

Satz 10.6
Für jeden Normalteiler $N \neq 1$ einer nilpotenten Gruppe G ist $[G, N] < N$ und $Z(G) \cap N \neq 1$. Insbesondere liegt jeder minimale Normalteiler einer nilpotenten Gruppe im Zentrum.

BEWEIS:
Wir definieren $N_1 := N$ und $N_{i+1} := [G, N_i]$ für $i \in \mathbb{N}$. Dann ist $N_i \trianglelefteq G, N_i \leqslant N$ und $N_i \subseteq G^i$. Da G nilpotent ist, existiert ein $m \in \mathbb{N}$ mit $1 = G^m = N_m$. Dann: $N_2 = [G, N] < N$. Denn im Fall $N_2 = N$ wäre auch $N_3 = [G, N_2] = [G, N] = N_2 = N$ etc. ↯ Sei n eine natürliche Zahl mit $N_n = 1 \neq N_{n-1}$. Dann ist $[G, N_{n-1}] = N_n = 1$, also $N_{n-1} \subseteq Z(G) \cap N$. ∎

Satz 10.7
Für nilpotente Normalteiler A und B 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 $a + b$.

BEWEIS:
Nach Satz 9.3 (i) gelten für $L, M, N \trianglelefteq G$ die Aussagen $[L, MN] = [L, M][L, N]$ und $[LM, N] = [L, N][M, N]$. Daraus folgt, dass $(AB)^{a+b+1}$ ein Produkt von Gruppen der Form $[H_0, \ldots, H_{a+b}]$ mit $H_0, \ldots, H_{a+b} \in \{A, B\}$ ist. Wegen der Bemerkung 10.5 (i) genügt es zu zeigen, dass jede dieser Gruppen trivial ist. Sei also $m := |\{ i \mid H_i = A \}|$ und $n := |\{ i \mid H_i = B \}|$. Dann ist $a + b + 1 = m + n$, also $m > a$ oder $n > b$. Sei Œ $m > a$. Dann ist $[H_0, \ldots, H_{a+b}] \subseteq A^m \subseteq A^{a+1} = 1$. ∎

Bemerkung 10.7
Im Allgemeinen ist eine Gruppe G, die einen nilpotenten Normalteiler N mit einer nilpotenten Faktorgruppe G/N hat, selbst nicht nilpotent.

Beispiel 10.3
$G = \mathrm{Sym}(3), N = \langle \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \rangle$

11. Gruppenoperationen

Definition 11.1 (Operation)
Eine **Linksoperation** einer Gruppe G auf einer Menge Ω ist eine Abbildung $G \times \Omega \to \Omega$ mit $(g, \omega) \mapsto {}^{g}\omega$ mit folgenden Eigenschaften:

- ${}^{1}\omega = \omega$
- ${}^{a}({}^{b}\omega) = {}^{ab}\omega$ für alle $a, b \in G, \omega \in \Omega$. Man sagt auch, G operiert auf Ω oder Ω ist eine G-Menge.

Bemerkung 11.1

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

(ii) Man beachte die Analogie zur Multiplikation von Vektoren eines Vektorraums mit Skalaren eines Körpers.

Beispiel 11.1

(i) Für jede Menge Ω operiert $\mathrm{Sym}(\Omega)$ auf Ω durch ${}^{g}\omega := g(\omega)$. Dabei ist $g \in \mathrm{Sym}(\Omega)$ und $\omega \in \Omega$.

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

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

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

(iii) Für eine natürliche Zahl n und jeden Körper $\mathbb{K}$ operiert $\mathrm{GL}(n, \mathbb{K})$ auf $\mathbb{K}^{n \times n}$ durch ${}^{A}B := ABA^{-1}$.

(iv) Für $m, n \in \mathbb{N}$ und jeden Körper $\mathbb{K}$ operiert $\mathrm{GL}(m, \mathbb{K}) \times \mathrm{GL}(n, \mathbb{K})$ auf $\mathbb{K}^{m \times n}$ durch ${}^{(A,B)}C := ACB^{-1}$ für $A \in \mathrm{GL}(n, \mathbb{K})$, $B \in \mathrm{GL}(n, \mathbb{K})$ und $C \in \mathbb{K}^{m \times n}$.

(v) Für eine natürliche Zahl n operiert die **orthogonale Gruppe**

$$\mathrm{O}(n, \mathbb{R}) = \left\{ A \in \mathbb{R}^{n \times n} \;\middle|\; AA^{T} = 1_n \right\}$$

des Grades n über $\mathbb{R}$ auf der Menge S aller reellen symmetrischen $n \times n$-Matrizen durch ${}^{A}B := ABA^{T}$.

(vi) Analog operiert die **unitäre Gruppe**

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

des Grades n über $\mathbb{C}$ auf der Menge H aller hermiteschen $n \times n$-Matrizen $B = \overline{B}^{T}$ durch ${}^{A}B := AB\overline{A}^{T}$.

Satz 11.1
Für jede Gruppe G, jede G-Menge Ω und $g \in G$ ist $\tau_g \colon \Omega \to \Omega$ mit $\omega \mapsto {}^{g}\omega$ bijektiv, d. h. $\tau_g \in \mathrm{Sym}(\Omega)$. Außerdem ist $\tau \colon G \to \mathrm{Sym}(G)$ mit $g \mapsto \tau_g$ ein Homomorphismus.

BEWEIS:
Für $a, b \in G, \omega \in \Omega$ ist $(\tau_a \circ \tau_b)(\omega) = {}^{a}({}^{b}\omega) = {}^{ab}\omega = \tau_{ab}(\omega)$ und $\tau_1(\omega) = {}^{1}\omega = \omega$. Daher gilt: $\tau_a \circ \tau_b = \tau_{ab}$ und $\tau_1 = \mathrm{id}_\Omega$. Insbesondere $\tau_a \circ \tau_{a^{-1}} = \tau_{aa^{-1}} = \tau_1 = \mathrm{id}_\Omega$ und analog $\tau_{a^{-1}} \circ \tau_a = \mathrm{id}_\Omega$. Folglich ist τ_a bijektiv. Ferner ist τ ein Homomorphismus. ∎

Bemerkung 11.2
Nach Satz 11.1 induziert jede Operation einer Gruppe G einen Homomorphismus $G \to \mathrm{Sym}(G)$. Wir zeigen jetzt umgekehrt, dass jeder Homomorphismus $G \to \mathrm{Sym}(G)$ eine Operation von G auf Ω induziert. Man sieht sofort, dass beide Prozesse zueinander invers sind.

Satz 11.2
Seien G eine Gruppe, Ω eine Menge und und $\tau \colon G \to \mathrm{Sym}(G)$ ein Homomorphismus. dann erhält man durch ${}^{g}\omega := (\tau(g))(\omega)$ eine Operation von G auf Ω. Dabei sind $g \in G$ und $\omega \in \Omega$.

BEWEIS:
Da τ ein Homomorphismus ist, ist $\tau(1) = 1_{\mathrm{Sym}(\Omega)} = \mathrm{id}_\Omega$. Daher ist ${}^{1}\omega = (\tau(1))(\omega) = \mathrm{id}_\Omega(\omega) = \omega$ und ${}^{a}({}^{b}\omega) = (\tau(a))((\tau(b))(\omega)) = (\tau(a) \circ \tau(b))(\omega) = (\tau(ab))(\omega) = {}^{ab}\omega$ für $\omega \in \Omega$ und $a, b \in G$. ∎

Definition 11.2
Seien G eine Gruppe, Ω eine G-Menge und $\tau \colon G \to \mathrm{Sym}(G)$ der entsprechende Homomorphismus. Dann heißt

$$\ker(\tau) := \{\, g \in G \mid \tau_g = \mathrm{id}_\Omega \,\} = \{\, g \in G \mid {}^{g}\omega = \omega \text{ für } \omega \in \Omega \,\}$$

der **Kern** der Operation. Ist $\ker\tau = G$, d. h. ${}^{g}\omega = \omega$ für alle $g \in G, \omega \in \Omega$, so heißt die Operation **trivial**. Ist $\ker\tau = 1$, d. h. τ ist injektiv, so heißt die Operation **treu**. Gegebenenfalls gilt: $G \cong \tau(G) \leqslant \mathrm{Sym}(\Omega)$.

Satz 11.3 (Satz von CAYLEY)
Jede Gruppe G ist zu einer Untergruppe einer symmetrischen Gruppe isomorph.

BEWEIS:
Durch ${}^{g}\omega := g\omega$ wird G zu einer G-Menge für $g, \omega \in G$. Diese ist treu. Denn aus ${}^{g}\omega = \omega$ für alle $g \in G$ folgt $g = 1$. Mit den obigen Bezeichnungen ist: $G \cong \tau(G) \leqslant \mathrm{Sym}(\Omega)$. ∎

Satz 11.4
Seien G eine Gruppe und Ω eine G-Menge. Für $\alpha, \beta \in \Omega$ schreiben wir $\alpha \sim \beta$, falls ein $g \in G$ mit ${}^g\alpha = \beta$ existiert. Dann ist $\sim$ eine Äquivalenzrelation auf Ω.

BEWEIS:
Die Reflexivität $\alpha \sim \alpha$ erhalten wir durch ${}^1\alpha = \alpha$. Für die Symmetrie sei $g \in G$. Dann ist auch $g^{-1} \in G$ mit ${}^{g^{-1}}\beta = {}^{g^{-1}}({}^g\alpha) = {}^{g^{-1}g}\alpha = \alpha$. Schließlich seien $g, h \in G$ mit ${}^g\alpha = \beta$ und ${}^h\beta = \gamma$. Dann ist $hg \in G$ mit ${}^{hg}\alpha = {}^h({}^g\alpha) = {}^h\beta = \gamma$. Somit haben wir auch die Transitivität. ∎

Bemerkung 11.3
Für $\alpha \in \Omega$ ist die **Bahn** $\mathrm{Orb}_G(\alpha) := \{ {}^g\alpha \mid g \in G \}$ die Äquivalenzklasse von α bezüglich $\sim$. Man bezeichnet mit $|\mathrm{Orb}_G(\alpha)|$ die **Länge** der Bahn von α. Aus allgemeinen Tatsachen über Äquivalenzrelationen folgt, dass Ω die disjunkte Vereinigung der verschiedenen Bahnen von G auf Ω ist. Für jedes Repräsentantensystem R dieser Bahnen gilt also die **Bahnengleichung**:

$$\Omega = \dot{\cup}_{\alpha \in R} \mathrm{Orb}_G(\alpha) \qquad |\Omega| = \sum_{\alpha \in R} |\mathrm{Orb}_G(\alpha)|$$

Beispiel 11.2

(i) Für eine natürliche Zahl n und jeden Körper $\mathbb{K}$ liegen zwei Matrizen aus $\mathbb{K}^{n\times n}$ genau dann in der gleichen Bahn unter der Operation von $\mathrm{GL}(n,\mathbb{K})$ auf $\mathbb{K}^{n\times n}$ durch ${}^A B := ABA^{-1}$ mit $A \in \mathrm{GL}(n,\mathbb{K})$, $B \in \mathbb{K}^{n\times n}$, wenn sie **ähnlich** im Sinne der linearen Algebra sind.

(ii) Für $m, n \in \mathbb{N}$ und jeden Körper $\mathbb{K}$ liegen zwei Matrizen aus $\mathbb{K}^{m\times n}$ genau dann in der gleichen Bahn unter der Operation von $\mathrm{GL}(m,\mathbb{K}) \times \mathrm{GL}(n,\mathbb{K})$ auf $\mathbb{K}^{m\times n}$ durch ${}^{(A,B)}C = ACB^{-1}$ mit $A \in \mathrm{GL}(m,\mathbb{K})$, $B \in \mathrm{GL}(n,\mathbb{K})$ und $C \in \mathbb{K}^{m\times n}$, wenn sie **äquivalent** im Sinne der linearen Algebra sind.

Definition 11.3 (Stabilisator)
Für jede Gruppe G, jede G-Menge Ω und $\omega \in \Omega$ ist der **Stabilisator** von ω in G gegeben durch $\mathrm{Stb}_G(\omega) := G_\omega := \{ g \in G \mid {}^g\omega = \omega \}$.

Satz 11.5
In dieser Situation gilt:

(i) $\mathrm{Stb}_G(\omega) \leqslant G$

(ii) $x \in G \Rightarrow \mathrm{Stb}_G({}^x\omega) = x\,\mathrm{Stb}_G(\omega)x^{-1}$

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

BEWEIS:

(i) Wegen ${}^1\omega = \omega$ ist $1 \in \mathrm{Stb}_G(\omega)$ und für $a, b \in \mathrm{Stb}_G(\omega)$ ist $ab^{-1} \in \mathrm{Stb}_G(\omega)$. Schließlich gilt: ${}^{ab^{-1}}\omega = {}^{ab^{-1}}({}^b\omega) = {}^a\omega = \omega$.

(ii) $g \in \mathrm{Stb}_G(\omega)({}^x\omega) \Leftrightarrow {}^{gx}\omega = {}^x\omega \Leftrightarrow {}^{x^{-1}gx}\omega = \omega \Leftrightarrow x^{-1}gx \in \mathrm{Stb}_G(\omega) \Leftrightarrow g \in x\,\mathrm{Stb}_G(\omega)x^{-1}$.

(iii) Für $g, h \in G$ gilt: ${}^g\omega = {}^h\omega \Leftrightarrow {}^{g^{-1}h}\omega = \omega \Leftrightarrow g^{-1}h \in \mathrm{Stb}_G(\omega) \Leftrightarrow g\,\mathrm{Stb}_G(\omega) = h\,\mathrm{Stb}_G(\omega)$. ∎

Definition 11.4 (Transitive Operation)
Seien G eine Gruppe und $\Omega \neq \emptyset$ eine G-Menge mit einer einzigen Bahn. Dann heißt die Operation **transitiv**.

Beispiel 11.3
Für jede Gruppe G und $h \leqslant G$ operiert G transitiv auf G/H durch ${}^x(gH) := xgH$ mit $x, g \in G$. Dabei gilt:

$$xgH = gH \Leftrightarrow g^{-1}xgH = H \Leftrightarrow g^{-1}xg \in H \Leftrightarrow x \in gHg^{-1}$$

Daher: $\mathrm{Stb}_G(gH) = gHg^{-1}$. Insbesondere ist $\mathrm{Stb}_G(H) = H$ und der Kern der Operation von G auf G/H ist $\bigcap_{g\in G} \mathrm{Stb}_G(gH) = \bigcap_{g\in G} gHg^{-1}$. Man bezeichnet das auch als den **Kern** von H in G. Offenbar ist dies der größte Normalteiler $N \trianglelefteq G$ mit $N \subseteq H$. Weiter ist G faktorisiert nach dem Kern von H zu einer Untergruppe von $\mathrm{Sym}(G/H)$ isomorph. So kann man oft nichttriviale Normalteiler von G konstruieren.

Bemerkung 11.4
Eine G-Menge $\Omega \neq \emptyset$ ist genau dann transitiv, wenn zu je zwei $\alpha, \beta \in \Omega$ ein $g \in G$ mit ${}^g\alpha = \beta$ existiert. Gegebenenfalls ist $|\Omega| = |G\colon \mathrm{Stb}_G(\omega)|$ für $\omega \in \Omega$. Existieren zu je zwei $\alpha, \beta \in \Omega$ genau ein $g \in G$ mit ${}^g\alpha = \beta$, so heißt die Operation **regulär**: Gegebenenfalls ist $|\Omega| = |G|$.

Satz 11.6 (FRATTINI-Argument)
Seien G eine Gruppe, $H \leqslant G$ und $\Omega \neq \emptyset$ eine G-Menge. Operiert H transitiv auf Ω, so ist $G = \mathrm{Stb}_G(\omega)H$ für $\omega \in \Omega$.

BEWEIS:
Seien $\omega \in \Omega$ und $g \in G$. Da H transitiv operiert, existiert ein $h \in H$ mit ${}^h({}^g\omega) = \omega$. Folglich ist $hg \in \mathrm{Stb}_G(\omega)$ und $g = h^{-1}hg \in H\,\mathrm{Stb}_G(\omega)$. Daher $G = H\,\mathrm{Stb}_G(\omega) = \mathrm{Stb}_G(\omega)H$. ∎

Definition 11.5 (Fixpunkt)
Seien G eine Gruppe, Ω eine G-Menge, $x \in G$ und $Y \subseteq G$. Dann heißen die Elemente in

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

Fixpunkte von x bzw. Y.

Satz 11.7 (Lemma von BURNSIDE)
Seien G eine endliche Gruppe und Ω eine endliche G-Menge.

(i) Für die Anzahl n der Bahnen von G auf Ω gilt dann:

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

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

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

BEWEIS:

(i) Offenbar ist $\sum_{g\in G}|\mathrm{Fix}_\Omega(g)| = |\{\,(g,\omega) \in G \times \omega \mid {}^g\omega = \omega\,\}| = \sum_{\omega\in\Omega}|\mathrm{Stb}_G(\omega)|$. Auf jeder Bahn ist $|\mathrm{Stb}_G(\omega)|$ konstant nach Satz 11.5 (ii) und die Bahn von $\omega \in \Omega$ enthält genau $|G\colon \mathrm{Stb}_G(\omega)|$ Elemente. Mit dem Satz von LAGRANGE ergibt sich: $\sum_{\omega\in\Omega}|\mathrm{Stb}_G(\omega)| = n \cdot |G|$.

(ii) Offenbar gilt:

$$\begin{aligned}\sum_{g\in G} |\mathrm{Fix}_\Omega(g)|^2 &= |\{\,(g,\alpha,\beta) \in G \times \Omega \times \Omega \mid {}^g\alpha = \alpha, {}^g\beta = \beta\,\}| \\ &= \sum_{\beta\in\Omega} |\{\,(g,\alpha) \in \mathrm{Stb}_G(\beta) \times \Omega \mid {}^g\alpha = \alpha\,\}|\end{aligned}$$

Für $\beta, \beta' \in \Omega$ existiert wegen der Transposition ein $x \in G$ mit $\beta' = {}^x\beta$. Man rechnet leicht nach, dass dann die Abbildung:

$$\begin{aligned}\{\,(g,\alpha) \in \mathrm{Stb}_G(\beta) \times \Omega \mid {}^g\alpha = \alpha\,\} &\to \left\{\,(g,\alpha) \in \mathrm{Stb}_G(\beta') \times \Omega \;\middle|\; {}^g\alpha = \alpha\,\right\} \\ (g,\alpha) &\mapsto (xgx^{-1}, {}^x\alpha)\end{aligned}$$

bijektiv ist. Daher gilt wie in (i):

$$\begin{aligned}\sum_{g\in G} |\mathrm{Fix}_\Omega(g)|^2 &= |\Omega| \cdot |\{\,(g,\alpha) \in \mathrm{Stb}_G(\omega) \times \Omega \mid {}^g\alpha = \alpha\,\}| \\ &= |\Omega| \cdot m|\mathrm{Stb}_G(\omega)| = |G|m\end{aligned}$$

∎

Definition 11.6
Seien G eine Gruppe, Ω eine G-Menge und $|\Omega| \geqslant n \in \mathbb{N}$. Die Operation heißt **$n$-transitiv**, wenn zu je zwei n-Tupeln $(\alpha_1, \ldots, \alpha_n), (\beta_1, \ldots, \beta_n)$ paarweise verschiedener Elemente in Ω ein $g \in G$ existiert mit ${}^g\alpha_1 = \beta_1, \ldots, {}^g\alpha_n = \beta_n$.

Satz 11.8
In dieser Situation gilt:

(i) Ist das $n \geqslant 2$, G ist n-transitiv auf Ω und $\omega \in \Omega$, so operiert $\mathrm{Stb}_G(\omega)$ $(n-1)$-transitiv auf $\Omega \setminus \{\omega\}$.

(ii) Ist das $n \geqslant 2$, $\omega \in \Omega$ und G transitiv auf Ω sowie $\mathrm{Stb}_G(\omega)$ noch $(n-1)$-transitiv auf $\Omega \setminus \{\omega\}$, so operiert G insgesamt n-transitiv auf Ω.

(iii) Ist G transitiv auf Ω, $\omega \in \Omega$ und $H := \mathrm{Stb}_G(\omega)$, dann gilt: G operiert genau dann 2-transitiv auf Ω, wenn $|H \setminus G/H| = 2$.

(iv) Sind Ω und G endlich und operiert G transitiv auf Ω, dann gilt, G operiert genau dann 2-transitiv auf Ω, wenn $\frac{1}{|G|}\sum_{g\in G}|\mathrm{Fix}_\Omega(g)|^2 = 2$.

BEWEIS:

(i) Seien $(\alpha_1,\dots,\alpha_{n-1}), (\beta_1,\dots,\beta_{n-1})$ zwei $(n-1)$-Tupel paarweise verschiedener Elemente in $\Omega\setminus\{\omega\}$. Dann sind $(\alpha_1,\dots,\alpha_{n-1},\omega), (\beta_1,\dots,\beta_{n-1}),\omega)$ zwei n-Tupel paarweise verschiedener Elemente in Ω. Daher existiert ein $g \in G$ mit ${}^g\alpha_1 = \beta_1,\dots,{}^g\alpha_{n-1} = \beta_{n-1}, {}^g\omega = \omega$. Insbesondere ist $g \in \mathrm{Stb}_G(\omega)$.

(ii) Seien $(\alpha_1,\dots,\alpha_n), (\beta_1,\dots,\beta_n)$ zwei n-Tupel paarweise verschiedener Elemente in Ω. Da G transitiv auf Ω ist, existieren zwei Elemente $x, y \in G$ mit ${}^x\alpha_n = \omega = {}^y\alpha_n$. Dann sind $({}^x\alpha_1,\dots,{}^x\alpha_{n-1}), ({}^y\alpha_1,\dots,{}^y\alpha_{n-1})$ zwei $(n-1)$-Tupel paarweise verschiedener Elemente in $\Omega\setminus\{\omega\}$. Nach der Voraussetzung existiert ein Element $g \in \mathrm{Stb}_G(\omega)$ mit ${}^{gx}\alpha_1 = {}^y\beta_1,\dots,{}^{gx}\alpha_{n-1} = {}^y\beta_{n-1}$. Dann ist $y^{-1}gx \in G$ und ${}^{y^{-1}gx}\alpha_{n-1} = \beta_{n-1}, {}^{y^{-1}gx}\alpha_n = {}^{y^{-1}g}\omega = {}^{y^{-1}}\omega = \beta_n$.

(iii) Wir zeigen zunächst die Richtung „⇒“: Dazu sei G zweitransitiv auf Ω und $x, y \in G\setminus H$. Dann ist ${}^x\omega \neq \omega \neq {}^y\omega$. Da H nach (i) transitiv auf $\Omega\setminus\{\omega\}$ operiert, existiert ein $h \in H$ mit ${}^{hx}\omega = {}^y\omega$. Folglich haben wir ${}^{y^{-1}hx}\omega = \omega$, d. h. $y^{-1}hx$ liegt im Stabilisator von ω und $x \in h^{-1}yH \subseteq HyH$. Damit ist gezeigt, $G = H\cup HyH$.

Für die Richtung „⇐“ sei $|H\setminus G/H| = 2$ und $\alpha, \beta \in \Omega\setminus\{\omega\}$. Wegen der Transitivität von G existieren zwei Elemente $x, y \in G$ mit ${}^x\omega = \alpha, {}^y\omega = \beta$. Dabei hat man $x, y \notin H$. Andernfalls wäre ${}^x\omega = \omega$. Daher existieren $h, h' \in H$ mit $y = hxh'$. Folglich: $\beta = {}^{hxh'}\omega = {}^{hx}\omega = {}^h\alpha$. Dies zeigt, H ist transitiv auf $\Omega\setminus\{\omega\}$. Also operiert G zweitransitiv auf Ω.

(iv) Aus den bisherigen Resultaten folgt: G operiert genau dann zweitransitiv auf Ω, wenn $\mathrm{Stb}_G(\omega)$ transitiv auf $\Omega\setminus\{\omega\}$ operiert. Dies ist genau dann, wenn der Stabilisator von ω genau 2 Bahnen auf Ω hat. Schließlich ist das genau dann der Fall, wenn $\frac{1}{|G|}\sum_{g\in G}|\mathrm{Fix}_\Omega(g)|^2 = 2$. ∎

Satz 11.9

Für jede Gruppe G und jede transitive G-Menge Ω mit mindestens zwei Elementen sind äquivalent:

(1) Es existiert eine echte Teilmenge $\Delta \subsetneq \Omega$ derart, dass $|\Delta| > 1$ und für $g \in G$ entweder $({}^g\Delta)\cap\Delta = \emptyset$ oder ${}^g\Delta = \Delta$ gilt.

(2) Es existiert eine Zerlegung $\Omega = \dot\bigcup_{\Lambda\in\mathcal{L}}\Lambda$, wobei $\Lambda \subsetneq \Omega, |\Lambda| > 1$ und ${}^g\Lambda \in \mathcal{L}$ für $g \in G, \Lambda \in \mathcal{L}$ ist.

Das dotcup ist groß

BEWEIS:
(1)⇒(2) Sei die erste Aussage erfüllt und $\mathcal{L} := \{ {}^{g}\Delta \mid g \in G \}$ und $\delta \in \Delta$. Für ein $\omega \in \Omega$ existiert dann ein $g \in G$ mit $\omega = {}^{g}\delta \in {}^{g}\Delta$. Also ist $\Omega = \bigcup_{\Lambda \in \mathcal{L}} \Lambda$. Sind $g, h \in G$ mit ${}^{g}\Delta \bigcap {}^{g}\Delta \neq \emptyset$, so ist $\emptyset \neq {}^{h^{-1}}({}^{g}\Delta \bigcap {}^{h}\Delta) = {}^{h^{-1}g}\Delta \cap \Delta$. Nach der Voraussetzung ist der Durchschnitt gleich der gesamten Menge Δ und die Zerlegung ist somit disjunkt. Für $g \in G$ ist ${}^{g}\Delta \subsetneq \Omega$, $|{}^{g}\Delta| > 1$ und ${}^{h}({}^{g}\Delta) = {}^{hg}\Delta \in \mathcal{L}$ für $h \in G$.

(2)⇒(1) Wähle $\Delta \in \mathcal{L}$ beliebig. ∎

Bemerkung 11.5
In der obigen Situation operiert G auch transitiv auf der Menge $\mathcal{L}$. Sind nämlich $\Lambda, \Delta \in \mathcal{L}$, dann wähle man zwei Elemente $\alpha \in \Lambda$, $\beta \in \Delta$ und $g \in G$ mit ${}^{g}\alpha = \beta$. Dann ist ${}^{g}\Lambda \cap \Delta \neq \emptyset$, also ist ${}^{g}\Lambda = \Delta$. Für $\Lambda \in \mathcal{L}$ ist $|\mathcal{L}| = |G\colon \operatorname{Stb}_G(\Lambda)|$ und $|\Omega| = |\Lambda| \cdot |\mathcal{L}| = |\Lambda| \cdot |G\colon \operatorname{Stb}_G(\Lambda)|$. Für $\lambda \in \Lambda$ ist ferner $\operatorname{Stb}_G(\lambda) \subseteq \operatorname{Stb}_G(\Lambda)$. Denn ${}^{x}\lambda = \lambda \Rightarrow {}^{x}\Lambda \cap \Lambda \neq \emptyset \Rightarrow {}^{x}\Lambda = \Lambda$.

Definition 11.7
Sind (1) und (2) erfüllt, dann heißt die Operation **imprimitiv**, sonst **primitiv**.

Beispiel 11.4
Ist $|\Omega| \in \mathbb{P}$, dann ist jede transitive Operation auf Ω primitiv. Denn die Bedingungen oben widersprechen sich.

Satz 11.10
Für jede Gruppe G und jede transitive G-Menge Ω mit mehr als zwei Elementen sind äquivalent:

(1) Ω ist primitiv.

(2) $\operatorname{Stb}_G(\omega)$ ist für jedes $\omega \in \Omega$ eine maximale Untergruppe von G.

(3) $\operatorname{Stb}_G(\omega)$ ist für ein $\omega \in \Omega$ eine maximale Untergruppe von G.

(1)⇒(2) Sei (1) erfüllt und $\omega \in \Omega$ beliebig. Nach dem Satz 11.5 ist $G/\operatorname{Stb}_G(\omega) \to \Omega$ mit $g \operatorname{Stb}_G(\omega) \mapsto {}^{g}\omega$ bijektiv. Insbesondere haben wir: $|G\colon \operatorname{Stb}_G(\omega)| = |\Omega| \geqslant 2$, d. h. ist $G \neq \operatorname{Stb}_G(\omega)$. Wir nehmen an, dass ein H mit $\operatorname{Stb}_G(\omega) < H < G$ existiert. Dann ist analog $H/\operatorname{Stb}_G(\omega) \to \Delta := \operatorname{Orb}_H(\omega), h \operatorname{Stb}_G(\omega) \mapsto {}^{h}\omega$ bijektiv. Insbesondere ist $|\Delta| = |H\colon \operatorname{Stb}_G(\omega)| \neq 1$. Wegen $H \neq G$ ist auch $\Delta \subsetneq \Omega$. Sei $g \in G$ mit ${}^{g}\Delta \cap \Delta \neq \emptyset$. Dann existieren zwei Elemente $h, h' \in H$ mit ${}^{h}\omega = {}^{gh'}\omega$, also $h^{-1}gh' \in \operatorname{Stb}_G(\omega) \subseteq H$ und damit $g \in H$. Folglich ist ${}^{g}\Delta = \Delta$. Insgesamt zeigt dies, dass G imprimitiv auf der Menge Ω ist. ↯zur Annahme.

(2)⇒(3) ist trivial.

(3)⇒(1) Sei (3) erfüllt. Wir nehmen an: Ω imprimitiv. Dann existiert eine Zerlegung $\Omega = \cup_{\Lambda \in \mathcal{L}} \Lambda$ wie in obigen Satz. Sei $\Lambda \in \mathcal{L}$ mit $\omega \in \Lambda$. Dann $\operatorname{Stb}_G(\omega) \leqslant \operatorname{Stb}_G(\Lambda) \leqslant G$. Ferner sind die Abbildungen $G/\operatorname{Stb}_G(\omega) \to \Omega, g \operatorname{Stb}_G(\omega) \mapsto {}^{g}\omega$; $G/\operatorname{Stb}_G(\Lambda) \to \Lambda, g \operatorname{Stb}_G(\Lambda) \mapsto {}^{g}\Lambda$ bijektiv. Insbesondere $|G \operatorname{Stb}_G(\Lambda)| = |\mathcal{L}| \neq 1$, d. h. $G \neq \operatorname{Stb}_G(\Lambda)$. Wegen (3) folgt, $\operatorname{Stb}_G(\Lambda) = \operatorname{Stb}_G(\omega)$. Sei $\lambda \in \Lambda \setminus \{\omega\}$. Dann existiert ein $g \in G$ mit ${}^{g}\omega = \lambda$, d. h. $g \notin \operatorname{Stb}_G(\omega) = \operatorname{Stb}_G(\Lambda)$. Also $\lambda = {}^{g}\omega \in {}^{g}\Lambda \neq \Lambda$. ↯

Satz 11.11
Seien G eine Gruppe, $N \trianglelefteq G$ und Ω eine primitive G-Menge. Dann operiert N transitiv oder trivial auf Ω.

BEWEIS:
Sei N intransitiv auf Ω und Δ eine Bahn von N auf Ω, also $\Delta \subsetneq \Omega$. Für $g \in G$ ist dann ${}^g\Delta$ eine Bahn von $gN^{-1}g{=}N$, also ${}^g\Delta = \Delta$ oder ${}^g\Delta \cap \Delta = \emptyset$. Aus der Primitivität folgt also $|\Delta| = 1$. Daher operiert N trivial auf Ω. ∎

Satz 11.12
Jede zweitransitive Operation einer Gruppe G auf eine Menge Ω ist primitiv.

BEWEIS:
Wir nehmen an, dass eine Teilmenge $\Delta \subsetneq \Omega$ existiert derart, dass $|\Delta| > 1$ und für $g \in G$ entweder ${}^g\Delta = \Delta$ oder ${}^g\Delta \cap \Delta = \emptyset$ gilt. Wähle paarweise verschiedene Elemente $\alpha, \beta \in \Delta, \gamma \in \Omega \setminus \Delta$. Nach Voraussetzung existiert eine $g \in G$ mit ${}^g\alpha = \alpha$, ${}^g\beta = \gamma$. Dann ist ${}^g\Delta \cap \Delta \neq \emptyset$ und ${}^g\Delta \neq \Delta$. ↯ ∎

12. Sylowgruppen

Bemerkung 12.1
Jede Gruppe G operiert auf sich selbst durch **Konjugation**: ${}^g x = gxg^{-1}$ für alle $g, x \in G$. Dabei heißt $\mathrm{Orb}_G(x) = \{ gxg^{-1} \mid g \in G \}$ **Konjugationsklasse** von x in G. Liegen zwei Elemente $x, y \in G$ in der gleichen Konjugationsklasse, d. h. existiert ein $g \in G$ mit $y = gxg^{-1}$, dann heißen x und y **konjugiert** in G. Wir schreiben hierfür $x \sim_g y$ oder $x \sim y$. Für $x \in G$ heißt der Stabilisator $\mathrm{Stb}_G(x) = \{ g \in G \mid gxg^{-1} = x \} = \{ g \in G \mid gx = xg \} =: C_G(x)$ der **Zentralisator** von x in G. Nach dem Satz 11.5 enthält die Konjugationsklasse von x in G genau $|G\colon C_G(x)|$ Elemente. Ist R ein Repräsentantensystem für die Konjugationsklassen, so erhält die Bahnengleichung die Form:

$$|G| = \sum_{x \in R} |G\colon C_G(x)| \tag{12.1}$$

Die wird auch als **Klassengleichung** bezeichnet.

Die Anzahl aller Klassen $|R|$ heißt manchmal **Klassenzahl** von G. Dies muss kein Teiler der Gruppenordnung sein. Die Konjugationsklasse von einem Element x in G ist genau dann einelementig, wenn $|G\colon C_G(x)| = 1$ gilt, d. h. $G = C_G(x)$. Dies ist äquivalent zu $x \in Z(G)$.

Satz 12.1 (Satz von LANDAU)
Für jede endliche Gruppe G mit Klassenzahl k gilt: $|G| \leqslant k^{2^{k-1}}$.

BEWEIS:
Seien $x_1, x_2, \ldots, x_k = 1$ Repräsentanten für die Konjugationsklassen, $n_i := |C_{(G)}(x_i)|$ für $i = 1, \ldots, k$. Œ gilt $n_1 \leqslant n_2 \leqslant \cdots \leqslant n_k = |G|$. Wegen Gleichung 12.1 ist: $\frac{k}{n_1} \geqslant \frac{1}{n_1} + \frac{1}{n_2} + \cdots + \frac{1}{n_k} = 1$, d. h. $n_1 \leqslant k$. Daher: $\frac{k}{n_2} \leqslant \frac{1}{n_2} + \cdots + \frac{1}{n_k} = 1 - \frac{1}{n_1} \geqslant \frac{1}{n_1} \geqslant \frac{1}{k}$, d. h. $n_2 \leqslant k^2$. Daher: $\frac{k}{n_3} \geqslant \frac{1}{n_3} + \cdots + \frac{1}{n_k} = 1 - \frac{1}{n_1} - \frac{1}{n_2} \geqslant \frac{1}{n_1 n_2} \geqslant \frac{1}{k^3}$, d. h. $n_3 \leqslant k^4$. Weiter folgt, dass $n_4 \leqslant k^8$. Induktiv erhält man $n_i \leqslant k^{2^{i-1}}$, insbesondere gilt $|G| = n_k \leqslant k^{2^{k-1}}$. ∎

Beispiel 12.1
Sei $k = 1$. Dann ist $|G| = 1$. Für $k = 2$ ist $\frac{1}{n_1} + \frac{1}{n_2} = 1$ und es gibt nur die Lösung $n_1 = n_2 = 2$. Also ist $|G| = 2$. Schließlich betrachten wir $k = 3$. Aus $\frac{1}{n_1} + \frac{1}{n_2} + \frac{1}{n_3} = 1$ folgt $n_1 \in \{2, 3\}$.

1. Fall Sei $n_1 = 2$. Dann ist $\frac{1}{n_2} + \frac{1}{n_3} = \frac{1}{2}$ und n_2 ist entweder 3 oder 4. Für $n_2 = 3$ folgt $n_3 = 6$, d. h. $|G| = 6$ und für $n_2 = 4$ ist $n_3 = 4$. Hierzu passt keine Gruppe. Denn Gruppen der Ordnung 4 sind kommutativ.

2. Fall Sei $n_1 = 3$. Dann ist $\frac{1}{n_2} + \frac{1}{n_3} = \frac{2}{3}$ und $n_2 = 3 = n_3$. Also $|G| = 3$.

Definition 12.1
Sei $p \in \mathbb{P}$. Eine endliche Gruppe, deren Ordnung eine p-Potenz ist, heißt **Primgruppe** oder **p-Gruppe**. Ein Gruppenelement, dessen Ordnung eine p-Potenz ist, heißt **p-Element**.

Satz 12.2
Für $p \in \mathbb{P}$ ist jede endliche p-Gruppe nilpotent.

BEWEIS:
Sei $|G| = p^n$ und Œ $|G| \neq 1$. In der Klassengleichung (Gleichung 12.1) $p^n = |G| = |G\colon C_G(x_1)| + \cdots + |G\colon C_G(x_k)|$ ist jeder Summand eine p-Potenz. Wegen $G = C_G(1)$ ist mindestens ein Summand gleich 1. Daher existiert mindestens ein $x_i \neq 1$ mit der Eigenschaft $|G\colon C_G(x_i)| = 1$, d. h. $1 \neq x_i \in Z(G)$. Also $Z(G) \neq 1$.

Im Fall $Z(G) = G$ ist G abelsch und damit nilpotent. Sei nun $Z(G) \neq G$. Dann ist $G/Z(G) \neq 1$ eine p-Gruppe. Daher ist analog $1 \neq Z(G/Z(G)) = Z_2(G)/Z(G)$. Im Fall $Z_2(G) = G$ ist G nilpotent. Andernfalls ist $G/Z_3(G) \neq 1$ eine p-Gruppe. So fährt man fort und erhält $1 < Z(G) < Z_2(G) < Z_3(G) < \cdots$. Wegen $|G| < \infty$ bricht das Verfahren ab. ∎

Satz 12.3
Für jede Primzahl p und jede endliche p-Gruppe gilt:

(i) $|G\colon Z(G)| \neq p$

(ii) Aus $|G| = p^2$ folgt, dass G abelsch ist.

BEWEIS:
(i) Annahme: $|G\colon Z(G)| = p$. Dann ist $G/Z(G)$ zyklisch. Nach einer der Übungsaufgaben ist G abelsch, d. h. $G/Z(G) = 1$.

(ii) Sei $|G| = p^2$. Nach Satz 12.2 ist $Z(G) \neq 1$. Nach dem ersten Teil des Satzes ist $|Z(G)| \neq 1$. Daher $|Z(G)| =^2$, d. h. G abelsch. ∎

Bemerkung 12.2 (Konjugation(sklasse), Normalisator)
Jede Gruppe G operiert auf $\mathfrak{P}(G)$ (Potenzmenge von G) durch **Konjugation**: ${}^gX := gXg^{-1} = \{\, gxg^{-1} \mid x \in X \,\}$. Dabei heißt die Bahn $\mathrm{Orb}_G(X) = \{\, gXg^{-1} \mid g \in G \,\}$ **Konjugationsklasse** von X in G. Liegen zwei Teilmengen $X, Y \in \mathfrak{P}(G)$ in der gleichen Konjugationsklasse, d. h. existiert ein $g \in G$ mit $Y = gXg^{-1}$, so heißen die X, Y in G **konjugiert**. Dies wird ebenso als $X \sim_g Y$ oder $X \sim Y$ geschrieben. Für ein $X \in \mathfrak{P}(G)$ ist $\mathrm{Stb}_G(X) = \{\, g \in G \mid gXg^{-1} = X \,\} = \{\, g \in G \mid gX = Xg \,\} = N_G(X)$ der **Normalisator**. Die Konjugationsklasse von X enthält genau $|G\colon N_G(X)|$ Elemente.

Definition 12.2 (p-Sylowgruppe)
Seien G eine endliche Gruppe, p eine Primzahl und $|G| = p^a m$ mit $p \nmid m \in \mathbb{N}$. Dann heißen die Untergruppen der Ordnung p^a von G die **p-Sylowgruppen** von G. Die Menge aller p-Sylowgruppen von G sei $\mathrm{Syl}_p(G)$.

Satz 12.4 (Satz von SYLOW)
Seien G eine endliche Gruppe, p eine Primzahl und $|G| = n = p^a m$ mit $p \nmid m \in \mathbb{N}$. Dann gilt:

(i) Für $n \in \mathbb{N}_0$ mit $b \leqslant a$ enthält G garantiert eine Untergruppe der Ordnung p^b. Genauer gilt für die Anzahl $Z_G(p^b)$ dieser Untergruppen:

$$Z_G(p^b) \equiv 1 \pmod{p}$$

Das heißt, $p \mid Z_G(p^b) - 1$.

(ii) Jede Untergruppe U der Ordnung p^b von G ist in einer p-Sylowgruppe von G enthalten.

(iii) Je zwei p-Sylowgruppen von G sind in G konjugiert. Insbesondere gilt für $P \in \mathrm{Syl}_p(G)$:

$$|G\colon N_G(P)| = |\mathrm{Syl}_p(G)| = Z_G(p^a) \equiv 1 \pmod{p}$$

Ist das $\mathcal{P}$ richtig?

BEWEIS:
(i) Die Gruppe G operiert auf $\Omega := \{ M \in \mathcal{P}(G) \mid |M| = p^b \}$ durch $gM = gM$ für $g \in G, M \in \Omega$. Sei $\mathfrak{R}$ ein Repräsentantensystem für die Bahnen. Dann hat man die Bahnengleichung:

$$\binom{n}{p^b} = |\Omega| = \sum_{M \in \mathfrak{R}} |G\colon \mathrm{Stb}_G(M)|$$

Dabei ist jeweils $\mathrm{Stb}_G(M) = \{ g \in G \mid gM = M \}$, also $\mathrm{Stb}_G(M)M = M$. Für jedes $x \in M$ ist also $\mathrm{Stb}_G(M)x \in M$, d. h. M ist die Vereinigung von Rechtsnebenklassen nach $\mathrm{Stb}_G(M)$. Insbesondere ist $|\mathrm{Stb}_G(M)| \mid |M| = p^b$. Im Fall $|\mathrm{Stb}_G(M)| = p^b$ ist M eine einzige Rechtsnebenklasse $\mathrm{Stb}_G(M)x$ und $\mathrm{Orb}_G(M)$ enthält auch $x^{-1}M = x^{-1}\,\mathrm{Stb}_G(M)x \leqslant G$. Umgekehrt hat eine Bahn, die eine Untergruppe U enthält, die Form $\{ gU \mid g \in G \} = G/U$. Insbesondere ist U die einzige Untergruppe in dieser Bahn und $|\mathrm{Orb}_G(U)| = |G\colon U| = p^{a-b}m$.

Als Fazit lässt sich feststellen, dass Bahnen, die keine Untergruppen enthalten, haben eine durch $p^{a-b+1}m$ teilbare Länge. Bahnen, die eine Untergruppe enthalten, haben die Länge $p^{a-b}m$ und enthalten genau eine Untergruppe. Also:

$$\begin{aligned} \binom{n}{p^b} &= |\Omega| \pmod{p^{a-n+1}m} \\ &\equiv Z_G(p^b) \cdot p^{a-b}m \end{aligned} \tag{12.2}$$

Sei H eine zyklische Gruppe der Ordnung n. Dann gilt analog:

$$\binom{n}{p^b} = Z_H(p^b)p^{a-b} \pmod{p^{a-b+1}} \tag{12.3}$$

fügen

Bekanntlich enthält H genau eine Untergruppe der Ordnung p^b (siehe Übungsaufgabe), d. h. $Z_H(p^b) = 1$. Aus den obigen Gleichungen (Gleichung 12.2, Gleichung 12.3) folgt, $Z_G(p^b)p^{a-b}m = p^{a-b}m \pmod{p^{a-b+1}m}$, d. h. $Z_G(p^b) \equiv 1 \pmod{p}$. Insbesondere ist $Z_G(p^b) \neq 0$.

(ii) Sei $P \in \mathrm{Syl}_p(G)$ und $\mathfrak{R}$ ein Repräsentantensystem für $U\backslash G/P$. Dann ist $G = \dot{\cup}_{x\in\mathfrak{R}} UxP$, d. h. $|G| = \sum_{x\in\mathfrak{R}} |UxP|$. Wegen $p^{a+1} \nmid |G|$ existiert ein $x \in G$ mit $p^{a+1} \nmid |UxP| = |U\colon U \cap xPx^{-1}| \cdot |P|$. Der erste Ausdruck ist eine Potenz von P und $|P| = p^a$. Also $|U\colon U \cap xPx^{-1}| = 1$, d. h. $U = U \cap xPx^{-1} \subseteq xPx^{-1} \in \mathrm{Syl}_p(G)$.

Großes dotcup

(iii) Ist $U \in \mathrm{Syl}_p(G)$, so folgt weiter $U = xPx^{-1}$. Außerdem operiert G durch Konjugation auf $\mathrm{Syl}_p(G)$ mit ${}^gP = gPg^{-1}$ für $g \in G, P \in \mathrm{Syl}_p(G)$. Nach der ersten Aussage ist die Operation transitiv. Also $|\mathrm{Syl}_p(G)| = |G\colon \mathrm{Stb}_G(P)| = |G\colon N_G(P)|$. ∎

Beispiel 12.2

Sei p eine Primzahl, q eine Potenz von p, $\mathbb{K}$ ein Körper mit $|\mathbb{K}| = q, n \in \mathbb{N}$ und $G := \mathrm{GL}(n, \mathbb{K})$. Dann gilt, $|G| = (q^n - 1)(q^n - q) \cdot \ldots \cdot (q^n - q^{n-1}) = q^{1+2+\cdots+(n-1)}(q^n - 1)(q^{n-1} - 1) \cdot \ldots \cdot (q - 1) = q^{\binom{n}{2}}(q^n - 1)(q^{n-1} - 1) \cdot \ldots \cdot (q - 1)$. Daher hat jede p-Sylowgruppe von G die Ordnung $q^{\binom{n}{2}}$. Andererseits ist die Menge aller Matrizen der Form

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

eine Untergruppe $P \leqslant G$ mit $|P| = qq^2 \cdot \ldots \cdot q^{n-1} = q^{\binom{n}{2}}$, d. h. $P \in \mathrm{Syl}_p(G)$. Mann kann sich überlegen, dass $N_G(P)$ aus allen Matrizen der folgenden Form besteht:

$$\begin{pmatrix} x & & * \\ & \ddots & \\ 0 & & x \end{pmatrix}$$

Insbesondere ist $|N_G(P)| = q^{\binom{n}{2}}(q - 1)^n$. Daher gilt, $|\mathrm{Syl}_p(G)| = |G\colon N_G(P)| = (q^{n-1} + \cdots + q + 1)(q^{n-2} + \cdots + q + 1) \cdot \ldots \cdot (q + 1) \equiv 1 \pmod{q}$.

Offenbar ist auch die Menge Q aller Matrizen der folgenden Form eine p-Sylowgruppe von G:

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

Bekanntlich gilt:

$$Q = \begin{pmatrix} 0 & & & 1 \\ & \ddots & \iddots & \\ & \iddots & \ddots & \\ 1 & & & 0 \end{pmatrix} P \begin{pmatrix} 0 & & & 1 \\ & \ddots & \iddots & \\ & \iddots & \ddots & \\ 1 & & & 0 \end{pmatrix}^{-1}$$

Satz 12.5 (Satz von CAUCHY)
Seien G eine endliche Gruppe und $p \in \mathbb{P}$ mit $p \mid |G|$. Dann enthält G ein Element der Ordnung p.

BEWEIS:
Nach Satz 12.4 enthält G eine Untergruppe U der Ordnung p und U enthält $p-1$ Elemente der Ordnung p. ∎

Satz 12.6 (Argument von FRATTINI)
Seien $p \in \mathbb{P}$, G eine endliche Gruppe, $K \trianglelefteq G$ und $Q \in \mathrm{Syl}_p(K)$. Dann ist $G = K \cdot N_G(Q)$.

BEWEIS:
Die Gruppe G operiert auf $\mathrm{Syl}_p(K)$ durch Konjugation. Nach dem Satz von SYLOW (Satz 12.4) operiert K transitiv auf $\mathrm{Syl}_p(K)$. Aus dem Satz 11.6 folgt also, $G = K \cdot \mathrm{Stb}_G(Q) = K \cdot N_G(Q)$. ∎

Satz 12.7
Für $p \in \mathbb{P}$, jede endliche Gruppe G und $P \in \mathrm{Syl}_p(G)$ gilt:

(i) $N \trianglelefteq G \Rightarrow P \cap N \in \mathrm{Syl}_p(N)$ und $PN/N \in \mathrm{Syl}_p(G/N)$

(ii) $N_G(P) \leqslant H \leqslant G \Rightarrow N_G(H) = H$. Insbesondere ist $N_G(N_G(P)) = N_G(P)$.

(i) Wegen $|P \cap N| \mid |P|$ ist $|P \cap N|$ eine p-Potenz und wegen $|N\colon P \cap N| = |NP\colon P| \mid |G\colon P|$ ist $p \nmid |N\colon P \cap N|$. Somit haben wir $P \cap N \in \mathrm{Syl}_p(N)$. Wegen $|PN/N| = |P/P \cap N| \mid |P|$ ist $|PN/N|$ ebenfalls eine p-Potenz. Wegen $|G/N\colon PN/N| = |G\colon PN| \mid |G\colon P|$ ist $p \nmid |G/N\colon PN/N|$ und daher $PN/N \in \mathrm{Syl}_p(G/N)$.

(ii) Wegen $P \leqslant N_G(P) \leqslant H \trianglelefteq N_G(H) \leqslant G$ und $P \in \mathrm{Syl}_p(N_G(H))$ folgt aus dem Satz 12.6:

$$N_G(H) = H \cdot N_{N_G}(P) \leqslant HN_G(P) \subseteq H \subseteq N_G(H)$$

Satz 12.8
Sei G eine endliche Gruppe. Die Primfaktorzerlegung von $n := |G|$ sei $n := p_1^{a_1} \cdot \ldots \cdot p_n^{a_n}$. Für $i = 1, \ldots, r$ sei $P_i \in \mathrm{Syl}_{p_i}(G)$. Dann sind äquivalent:

(1) Die Gruppe G ist nilpotent.

(2) $P_i \trianglelefteq G$ für $i = 1, \ldots, r$.

(3) $G = P_1 \oplus \ldots \oplus P_r$.

BEWEIS:

(1)⇒(2) Sei G nilpotent und $i \in \{1, \dots, r\}$. Nach dem Satz 12.7 ist $N_G(N_G(P_i)) = N_G(P_i)$. Aus Satz 10.5 folgt, $N_G(P_i) = G$, d. h. $P_i \trianglelefteq G$.

(2)⇒(3) Wegen Satz 7.2

(3)⇒(1) Nach dem Satz 12.2 ist jedes P_i nilpotent, also auch G nach dem Satz 10.7. ∎

Satz 12.9

Für $p, q, r \in \mathbb{P}$ und jede endliche Gruppe G gilt:

(i) Sei $|G| = p^a q$ für ein $a \in \mathbb{N}_0$. Dann ist G auflösbar.

(ii) Sei $|G| = p^2 q^2$. Dann ist G auflösbar.

(iii) Sei $|G| = pqr$. Dann ist G auflösbar.

BEWEIS:

(i) Sei G ein Gegenbeispiel minimaler Ordnung. Es existiert ein Normalteiler $1 \neq N \neq G$, so erfüllen N und G/N die Voraussetzungen von (i) oder von Satz 12.2. Also sind sie nach der Wahl von G auflösbar. Dann ist aber auch G auflösbar.↯

Daher ist G einfach und $p \neq q$ nach dem Satz 12.2. Für $P \in \mathrm{Syl}_p(G)$ ist $|G\colon N_G(P)| \mid q$.

Im Fall $|G\colon N_G(P)| = 1$ wäre $P \trianglelefteq G$. Dies stellt einen Widerspruch zur Einfachheit von G dar. Also ist $q = |G\colon N_G(P)| = |\mathrm{Syl}_p(G)|$. Ist $P_1 \cap P_2 = 1$ für je zwei verschiedene $P_1, P_2 \in \mathrm{Syl}_p(G)$, so enthalten die p-Sylowgruppen von G insgesamt $q(p^a - 1) = |G| - q$ Elemente ungleich 1. Daher ist nur noch Platz für eine einzige p-Sylowgruppen Q. Also ist $Q \trianglelefteq G$ ↯ zur Einfachheit.

Also existieren verschiedene $P_1, P_2 \in \mathrm{Syl}_p(G)$ mit $D := P_1 \cap P_2 \neq 1$. Wir wählen P_1 und P_2 so, dass D möglichst groß wird. Für $i = 1, 2$ ist P_i nach dem Satz 12.2 nilpotent, also $D < N_{P_i}(D) =: Q_i \leqslant P_i$ nach dem Satz 10.5. Daher ist $D \trianglelefteq \langle Q_1, Q_2 \rangle =: H$. Ist $|H|$ eine p-Potenz, so existiert ein $P_3 \in \mathrm{Syl}_p(G)$ mit $H \subseteq P_3$. Damit $P_i \cap P_3 \geqslant Q_i > D = P_1 \cap P_2$. Nach der Wahl von P_1 und P_3 ist dann $P_i = P_3$. Somit hat man den Widerspruch $P_1 = P_2$. Also ist $|H|$ keine p-Potenz, d. h. $|H| = p^b q$ für ein $b \in \mathbb{N}_0$.

⩽ oder ⊆

Folglich ist $p^a = |P_1| \mid |P_1 H|$ und $q \mid |H| \mid |P_1 H|$, d. h. $G = P_1 H$. Zu jedem $g \in G$ existiert also ein $h \in H, x \in P_1$ mit $g = xh$. Dann ist $gDg^{-1} = xhDh^{-1}x^{-1} = xDx^{-1} \leqslant P_1$, denn die letzte Gleichheit ergibt sich aus $H \leqslant N_G(D)$. Also ist $1 \neq K := \langle gDg^{-1} \colon g \in G \rangle \trianglelefteq G$ und $K \leqslant P_1$ im Widerspruch zur Einfachheit von G.

(ii) Œ sei $p > q$. Existiert ein Normalteiler $1 \neq N \neq G$, dann sind $N, G/N$ nach dem ersten Teil auflösbar. Also ist auch G auflösbar. Daher sei G einfach. Für $P \in \mathrm{Syl}_p(G)$ ist $|\mathrm{Syl}_p(G)| = |G\colon N_G(P)| \equiv 1 \pmod p$ und $|G\colon N_G(P)| \mid q^2$. Die Fälle $|G\colon N_G(P)| \in \{1, q\}$ sind unmöglich. Daher ist $|G\colon N_G(P)| = q^2$. Ist $P_1 \cap P_2 = 1$ für je zwei verschiedene $P_1, P_2 \in \mathrm{Syl}_p(G)$, so folgt aus der Übungsaufgabe 42:

$q^2 = |\mathrm{Syl}_p(G)| \equiv 1 \pmod{p^2}$. ↯ Somit existieren $P_1, P_2 \in \mathrm{Syl}_p(G)$ mit $1 < D := P_1 \cap P_2 < P_1$. Für $i = 1, 2$ ist $|P_i| = p^2$, d. h. P_i ist nach Satz 12.3 abelsch. Insbesondere ist $D \trianglelefteq P_i$ und $P_i < N_G(D) < G$. Somit muss $|N_G(D)| = p^2 q$ gelten. Nach der Aufgabe 38 ist $N_G(D) \trianglelefteq G$. ↯ da G einfach.

(iii) Œ sei $p > q > r$, sonst kommen die obigen Fälle ins Spiel und weiter sei G einfach. Für $P \in \mathrm{Syl}_p(G)$ ist dann $|\mathrm{Syl}_p(G)| = |G : N_G(P)| \equiv 1 \pmod{p}$ und $|G : N_G(P)| \mid qr$, also $|\mathrm{Syl}_p(G)| = qr$. Analog haben wir $|\mathrm{Syl}_q(G)| \geqslant p$, $|\mathrm{Syl}_r(G)| \geqslant q$. Da sich je zwei Sylowgruppen trivial schneiden, enthält G genau $(p-1)qr$ Elemente der Ordnung p, mindestens $p(q-1)$ Elemente der Ordnung q und mindestens $q(r-1)$ Elemente der Ordnung r. Also $pqr = |G| \geqslant 1 + qr(p-1) + p(q-1) + q(r-1) = pqr + (p-1)(q-1)$ ↯ ■

Beispiel 12.3
Es folgt aus den Überlegungen leicht, dass Gruppen der Ordnungen 1 bis 59 auflösbar. Es ist 60 die kleinste Ordnung einer nichtauflösbaren Gruppe.

13. Symmetrische Gruppen

Bemerkung 13.1
Sei $n \in \mathbb{N}$. Elemente in der symmetrischen Gruppe des Grades n schreibt man in der Form $g = \begin{pmatrix} 1 & 2 & \dots & n \\ g(1) & g(2) & \dots & g(n) \end{pmatrix}$. Existieren paarweise verschiedene $x_1, \dots, x_k \in \{1, \dots, n\}$ mit $g(x_1) = x_2, g(x_2) = x_3, \dots, g(x_{k-1}) = x_k, g(x_k) = 1$ und $g(y) = y$, so heißt g ein **k-Zyklus** oder **Zyklus** der **Länge** k. Man schreibt $g = (x_1, \dots, x_k) = (x_2, \dots, x_k, x_1) = (x_k, x_1, \dots, x_{k-1})$.

Zyklen $(x_1, \dots, x_k), (y_1, \dots, y_l)$ mit $\{x_1, \dots, x_k\} \cap \{y_1, \dots, y_l\} = \emptyset$ heißen **disjunkt**. Gegebenenfalls sind sie vertauschbar. Offenbar kann man jede Permutation $a \in \mathrm{Sym}(n)$ als Produkt disjunkter Zyklen schreiben:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 8 & 4 & 9 & 5 & 2 & 6 & 3 & 1 & 10 & 7 & 12 & 11 \end{pmatrix}$$
$$= (1,8)(2,4,5)(3,9,10,7)(6)(11,12)$$

Dabei liefern die auftretenden Zyklen die Bahnen von der zyklischen Gruppe, die von a erzeugt wird ($\langle a \rangle$) auf $\{1, \dots, n\}$. Bis auf die Reihenfolge der Zyklen und Zyklen der Länge 1 ist die **Zyklenschreibweise** eindeutig. Wir ordnen in der Regel die auftretenden Zyklenlängen $k_1, \dots, k_l$ der Größe nach. Dann gilt: $k_1 + \dots + k_l = n$ und $(k_1, \dots, k_l)$ heißt **Typ** von a. Offenbar ist $|\langle a \rangle| = \mathrm{kgV}(k_1, \dots, k_l)$.

Satz 13.1
Zwei Elemente in $\mathrm{Sym}(n)$ sind genau dann konjugiert, wenn sie den gleichen Typ haben.

BEWEIS:
Zunächst betrachten wir die Richtung von links nach rechts („⇒“). Dazu sei $a \in \mathrm{Sym}(n)$ mit der Zyklenschreibweise $a = (x_1, \dots, x_k)(y_1, \dots, y_l) \dots$ und für $g \in \mathrm{Sym}(n)$ ist dann $gag^{-1} = (g(x_1), g(x_2), \dots, g(x_k)) \cdot (g(y_1), \dots, g(y_l))$. Denn beispielsweise ist $(gag^{-1})(g(x_1)) = (ga)(x_1) = g(x_2)$.

Die Rückrichtung erhalten wir durch $a, a' \in \mathrm{Sym}(n)$ mit Zyklenschreibweise: $a = (x_1, \dots, x_k)(y_1, \dots, y_l) \dots$ und $a' = (x'_1, \dots, x'_k)(y'_1, \dots, y'_l) \dots$. Dann ist $gag^{-1} = a'$ mit $\begin{pmatrix} x_1 & \dots & x_k & y_1 & \dots & y_l & \dots \\ x'_1 & \dots & x'_k & y'_1 & \dots & y'_l & \dots \end{pmatrix}$. ∎

Definition 13.1 (Partition)
Sei n eine natürliche Zahl. Eine **Partition** von n ist eine endliche Folge $(k_1, \dots, k_l) \in \mathbb{N}^l$ mit $k_1 \geqslant k_2 \geqslant \dots \geqslant k_l$ und $k_1 + \dots + k_l = n$.

Bemerkung 13.2
Der Satz 13.1 liefert eine Bijektion zwischen der Menge der Konjugationsklassen von $\mathrm{Sym}(n)$ und der Menge der Partitionen von n.

Beispiel 13.1
$5 = 4+1 = 3+2 = 3+1+1 = 2+2+1 = 2+1+1+1 = 1+1+1+1+1$. Daher hat $\mathrm{Sym}(5)$ die Klassenzahl 7.

Satz 13.2
Sei $k_1, \ldots, k_l$ eine Partition von n und $m_i := |\{\, j \mid kj = i \,\}|$ für $i = 1, \ldots, n$. Unter den Zahlen $k_1, \ldots, k_l$ treten also m_1 Einsen, m_2 Zweien usw. auf. Dann hat die Konjugationsklasse der Elemente vom Typ $(k_1, \ldots, k_l)$ in $\mathrm{Sym}(n)$ die Länge:

$$\frac{n!}{m_1!1^{m_1}m_2!2^{m_2} \cdot \ldots \cdot m_n!n^{m_n}}$$

BEWEIS:
Jedes Element vom Typ $k_1, \ldots, k_l$ hat die Form: m_1 Einszyklen, m_2 Zweizyklen usw. Es gibt $n!$ Möglichkeiten, die Zahlen $1, \ldots, n$ auf die Positionen zu verteilen. Dabei liefern jeweils $m_1!1^{m_1}m_2!2^{m_2}\ldots$ Verteilungen die gleiche Permutation. ∎

Bemerkung 13.3
Offenbar wird $\mathrm{Sym}(n)$ von allen Zyklen erzeugt. Die Gruppe $\mathrm{Sym}(n)$ wird wegen der Beziehung $(x_1, \ldots, x_k) = (x_1, x_k)(x_1, x_{k-1})\ldots(x_1, x_2)$ von den 2-Zyklen (oder **Transposition**en) erzeugt. Wegen $(i, j) = (1, i)(1, j)(1, i)$ genügen sogar die Transpositionen $(1, 2), (1, 3), \ldots, (1, n)$. Wegen $(1, i) = (i-1, i)\ldots(2, 3)(1, 2)(2, 3)\ldots(i-1, i)$ genügen analog auch die so genannten **Basistransposition**en $(1, 2), (2, 3), \ldots, (n-1, n)$. Wegen $(i, i+1) = (1, 2, \ldots, n)(i-1, i)(1, 2, \ldots, n)^{-1}$ gilt auch $\mathrm{Sym}(n) = \langle (1, 2), (1, 2, \ldots, n)\rangle$.

Definition 13.2 (Inversion)
Sei $g \in \mathrm{Sym}(n)$. Dann heißt ein Paar $(i, j) \in \mathbb{N} \times \mathbb{N}$ mit $1 \leqslant i < j \leqslant n$ und $g(i) > g(j)$ **Inversion** oder **Fehlstand** von g. Die Anzahl $l(g)$ aller Inversionen von g heißt **Länge** von g.

Satz 13.3
Jedes $g \in \mathrm{Sym}(n)$ kann man als Produkt von $l(g)$ Basistranspositionen, aber nicht als Produkt von weniger als $l(g)$ Basistranspositionen schreiben.

BEWEIS:
Wir geben hier nur ein Beispiel an: Sei $g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix} \Rightarrow l(g) = 2$. Es ist $(1, 2)g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix} \Rightarrow l((1, 2)g) = 1$. Für $(2, 3)(1, 2)g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = 1 \Rightarrow g = (1, 2)(2, 3)$.

Allgemein erhöht/erniedrigt sich die Multiplikation mit einer Basistransposition die Anzahl der Inversionen um 1. ∎

Definition 13.3 (Vorzeichen)
Für $g \in \mathrm{Sym}(n)$ heißt $\operatorname{sgn} g := \prod_{1 \leqslant i < j \leqslant n} \frac{g(j)-g(i)}{j-i}$ das **Vorzeichen** von g.

Bemerkung 13.4
Offenbar kommen in Zähler und Nenner bis auf das Vorzeichen die gleichen Zahlen vor. Daher ist $\operatorname{sgn} g = (-1)^{l(g)} \in \{-1, 1\}$

Satz 13.4
$\operatorname{sgn}\colon \mathrm{Sym}(n) \to \{1, -1\}$ ist ein Homomorphismus.

BEWEIS:
Für $g \in \mathrm{Sym}(n)$ und $i = 1, \ldots, n-1$ ist $l((i, i+1)g) = l(g) \pm 1$. Also ist $\operatorname{sgn}((i, i+1)g) = (-1)^{l(g)\pm 1} = -(-1)^{l(g)} = \operatorname{sgn}(i, i+1)\operatorname{sgn}(g)$. Für beliebige Basistranspositionen $b_1, \ldots, b_k$ und $f := b_1 \cdot \ldots \cdot b_k$ gilt also $\operatorname{sgn}(fg) = \operatorname{sgn}(b_1 \cdot \ldots \cdot b_k g) = \operatorname{sgn}(b_1 \cdot \ldots \cdot b_k)\operatorname{sgn}(g) = \cdots = \operatorname{sgn}(b_1) \ldots \operatorname{sgn}(b_k)\operatorname{sgn}(g) = \operatorname{sgn}(f)\operatorname{sgn}(g)$. ∎

Beispiel 13.2
Für $g, h \in \mathrm{Sym}(n)$ ist $\operatorname{sgn}(ghg^{-1}) = \operatorname{sgn}(g)\operatorname{sgn}(h)\operatorname{sgn}(g^{-1}) = \operatorname{sgn}(h)$. Daher haben konjugierte Permutationen das gleiche Vorzeichen. Insbesondere hat jede Transposition das Vorzeichen -1.

Bemerkung 13.5
Für $n \in \mathbb{N}$ heißt $\mathrm{Alt}(n) := \ker(\operatorname{sgn}\colon \mathrm{Sym}(n) \to \{-1, 1\})$ **alternierende Gruppe** des Grade n. Dann ist $\mathrm{Alt}(n) \trianglelefteq \mathrm{Sym}(n)$, $|\mathrm{Sym}(n)\colon \mathrm{Alt}(n)| = 2$ für $n \geqslant 2$ nach dem Homomorphiesatz. Jedes Element in $\mathrm{Alt}(n)$ ist Produkt einer geraden Anzahl von Transpositionen. Dabei ist $(i, j)(j, k) = (i, j, k)$ und $(i, j)(k, l) = (i, l, k)(i, j, k)$ für paarweise verschiedene $i, j, k, l \in \{1, \ldots, n\}$. Daher wird $\mathrm{Alt}(j)$ von allen Dreizyklen erzeugt.

Satz 13.5
Für $x \in \mathrm{Alt}(n) \Rightarrow A$ ist die Konjugationsklasse von x in $S := \mathrm{Sym}(n)$ entweder eine Konjugationsklasse in A oder die Vereinigung von zwei gleich großen Konjugationsklassen von A. Der letzte Fall liegt dann vor, wenn $C_S(x) \subseteq A$.

BEWEIS:
Für $y = (1, 2)$ gilt: $S = A \cup Ay$. Jedes zu x in S konjugierte Element ist also in A zu x oder zu yxy^{-1} 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 $|A\colon C_A(x)| = |A\colon A \cap C_S(x)| = |AC_S(x)\colon C_S(x)|$. Es ergibt sich für $C_S(x) \nsubseteq A$ der Index $|S\colon C_S(x)|$ oder $|S\colon C_S(x)|/2$ in allen sonstigen Fällen. ∎

Beispiel 13.3
Sei $n = 5$. Dann enthält A Elemente der Typen $(1, 1, 1, 1, 1)$, $(2, 2, 1)$, $(3, 1, 1)$, (5). Wegen $(1, 2) \in C_S((12)(34)) \setminus A$ stimmen die Konjugationsklassen von $(1, 2)(3, 4)$ in S und A überein. Sie enthalten also $\frac{5!}{2!2^2} = \frac{120}{8} = 15$ Elemente.

Wegen $(4, 5) \in C_S((123)) \setminus A$ stimmen die Konjugationsklassen von $(1, 2, 3)$ in S und A überein und enthalten $\frac{5!}{2!1^2 1!3^1} = 20$ Elemente.

Die Konjugationsklasse von $(1,2,3,4,5)$ in S enthält $\frac{5!}{1!5^1} = 24$ Elemente. Daher ist $|C_S((1,2,3,4,5))| = 5$ und $C_S((1,2,3,4,5)) = \langle(1,2,3,4,5)\rangle \subseteq A$. Also zerfällt die Konjugationsklasse von $(1,2,3,4,5)$ in S in zwei Konjugationsklassen der Länge 12 in A. Zur Probe: $1+15+20+12+12 = 60$ Elemente.

Jeder Normalteiler $1 \neq N \trianglelefteq A$ ist die Vereinigung von Konjugationsklassen von A. Daher ist $13 \leqslant N \mid 60$, d. h. $|N| \in \{15, 20, 30, 60\}$. Keine der Elemente außer der 60 kann als Summe der Zahlen $1, 12, 15, 20$ dargestellt werden. Damit ist $|N| = 60$. Also ist $\mathrm{Alt}(5)$ eine einfache Gruppe.

Bemerkung 13.6
Für $n \geqslant 3$ operiert $\mathrm{Alt}(n)$ mehrfach oder genauer $(n-2)$-transitiv auf $\{1,\dots,n\}$, denn für paarweise verschiedene Elemente $a_1,\dots,a_n \in \{1,\dots,n\}$ gehört entweder $\begin{pmatrix} 1 & 2 & \dots & n-2 & n-1 & n \\ a_1 & a_2 & \dots & a_{n-2} & a_{n-1} & a_n \end{pmatrix}$ oder $\begin{pmatrix} 1 & 2 & \dots & n-2 & n-1 & n \\ a_1 & a_2 & \dots & a_{n-2} & a_n & a_{n1} \end{pmatrix}$ zu $\mathrm{Alt}(n)$. Natürlich operiert $\mathrm{Sym}(n)$ sogar n-transitiv auf $\{1,\dots,n\}$.

Satz 13.6
Für $n \geqslant 5$ ist $\mathrm{Alt}(n)$ immer einfach.

BEWEIS:
Der Beweis wird durch Induktion über n geführt. Für $n = 5$ wurde die Behauptung im obigen Beispiel nachgerechnet. Daher nehmen wir $n \geqslant 6$ an. Da $A := \mathrm{Alt}(n)$ mindestens 4-transitiv operiert und damit nach Satz 11.12 primitiv auf $\Omega := \{1,\dots,n\}$ operiert, operiert auch jeder Normalteiler $1 \neq N \trianglelefteq A$ nach Satz 11.11 transitiv auf Ω. Daher $A = N \cdot \mathrm{Stb}_A(n)$ wegen des FRATTINI-Argument (Satz 11.6). Außerdem $N \cap \mathrm{Stb}_A(n) \trianglelefteq \mathrm{Stb}_A(n)$. Da $\mathrm{Stb}_A(n) \cong \mathrm{Alt}(n-1)$ einfach ist, folgt: $N \cap \mathrm{Stb}_A(n) \in \{1, \mathrm{Stb}_A(n)\}$.

Im Fall $\mathrm{Stb}_A(n) = \mathrm{Stb}_A(n) \cap N \subseteq N$ ist $A = N \cdot \mathrm{Stb}_A(n) = N$, d. h. wir sind fertig.

Andernfalls sei $N \cap \mathrm{Stb}_A(n) = 1$. Dann operiert der Normalteiler N regulär auf Ω. Insbesondere ist $|N| = n$. Für $i = 1,\dots,n$ existiert genau ein Element $x_i \in N$ mit $x_i(n) = i$ und die Abbildung $\Omega \to N$ mit $i \mapsto x_i$ ist bijektiv. Für $g \in \mathrm{Stb}_A(n)$ ist $gx_ig^{-1} \in N$ mit $(gx_ig^{-1})(n) = (gx_i)(n) = g(i)$, also $gx_ig^{-1} = x_{g(i)}$. Daher operiert $\mathrm{Stb}_A(n)$ auf N durch Konjugation genauso wie auf Ω und auf $\Omega \setminus \{n\}$ genauso wie auf $N \setminus \{1\}$, nämlich $(n-3)$-transitiv. Wegen $n \geqslant 6$ folgt aus der Aufgabe 41, dass $n-3 \leqslant 3$, d. h. $n = 6$. Dann ist einerseits $n-3 = 3$ und andererseits $n = |N| = 4$. ↯ ∎

Link einfügen

Beispiel 13.4
Wegen $|\mathrm{Alt}(3)| = 3$ ist auch $\mathrm{Alt}(3)$ einfach. Dagegen ist $\mathrm{Alt}(4)$ *nicht* einfach. Denn $V_4 = \{(1), (12)(34), (13)(24), (14)(23)\} \trianglelefteq \mathrm{Alt}(4)$. Genauer hat $\mathrm{Alt}(4)$ die folgenden Konjugationsklassen (1) mit Länge 1, $(12)(34)$ mit Länge 3, (123) mit Länge 4 und (132) mit Länge 4. Daher sind $1, V_4$ und $\mathrm{Alt}(4)$ die einzigen Normalteiler von $\mathrm{Alt}(4)$.

Satz 13.7
Es ist $\mathrm{Sym}(n)' = \mathrm{Alt}(n)$ für $n \in \mathbb{N}$.

BEWEIS:
Œ sei $n \geqslant 3$ und $S := \mathrm{Sym}(n)$, $A := \mathrm{Alt}(n)$. Wegen $|S/A| = 2$ ist S/A abelsch, insbesondere ist $S' \subseteq A$ und damit $S' \trianglelefteq A$. Für $n \neq 4$ ist A einfach. Daher ist $S' \in \{1, A\}$.

Falls $S' = 1$ wäre S abelsch.↯ Daher ist $S' = A$ für $n \neq 4$.

Sei $n = 4$. Dann müssen wir nur noch die Möglichkeit, dass $S' = V_4$ ausschließen. Dies folgt aber wegen $S' \geqslant \mathrm{Sym}(3)' = \mathrm{Alt}(3)$ und $\mathrm{Alt}(3) \nsubseteq V_4$. ∎

Satz 13.8
Sei G einfach, $|G| = 60 \Rightarrow G \cong \mathrm{Alt}(5)$.

BEWEIS:
Wir nehmen vorerst an, dass es eine Untergruppe $H < G$ mit $|G\colon H| =: n \leqslant 4$. Dann induziert die G-Menge G/H einen Homomorphismus $f\colon G \to \mathrm{Sym}(n)$ mit der Kern $K := \bigcap_{g \in G} gHg^{-1} \leqslant H < G$. Da G einfach, folgt $K = 1$, also ist f injektiv. Dies steht im Widerspruch wegen $|G| > |\mathrm{Sym}(n)|$.

Nun nehmen wir an $|G\colon H| \geqslant 6$ für alle $H < G$. Sei $P \in \mathrm{Syl}_2(G)$, also $|P| = 4$ und $P \leqslant N_G(P) < G$. Wegen $|G\colon N_P(G)| \geqslant 6$ folgt $N_G(P) = P$. Folglich ist die Anzahl der 2-Sylowgruppe von G: $|\mathrm{Syl}_2(G)| = |G\colon N_G(P)| = 15 \not\equiv 1 \pmod 4$. Nach der Aufgabe 42existieren $P, P^* \in \mathrm{Syl}_2(G)$ mit $1 < D := P \cap P^* < P$. Also $P < \langle P, P^* \rangle \subseteq N_G(D) < G$. Widerspruch wegen $|G\colon N_G(D)| \geqslant 6$.

link einfügen

Also enthält G eine Untergruppe H vom Index 5. Die G-Menge G/H liefert einen Homomorphismus $f\colon G \to \mathrm{Sym}(5)$ mit $\ker f =: K = \bigcap_{g \in G} gHg^{-1} \leqslant H < G$. Somit folgt, dass $K = 1$. Nach dem Homomorphiesatz ist $B := \mathrm{Bld}(f) \leqslant \mathrm{Sym}(5)$ und $|B| = 60$. Weil $|\mathrm{Sym}(5)\colon B| = 2$ ist $B \trianglelefteq \mathrm{Sym}(5)$ und $\mathrm{Sym}(5)/B$ ist abelsch. Daher enthält $B \supseteq \mathrm{Sym}(5)' = \mathrm{Alt}(5)$, d. h. $\mathrm{Alt}(5) = B \cong G$. ∎

14. Hallgruppen

Es geht um Verallgemeinerungen des Satzes von SYLOW.

Definition 14.1
Sei $\pi \subseteq \mathbb{P}$ und $\pi' := \mathbb{P} \setminus \pi$. Eine endliche Gruppe G heißt **π-Gruppe**, falls jeder Primteiler der Gruppenordnung 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-HALL-Gruppe** von G, falls jeder Primteiler vom Index $|G\colon H|$ zu π' gehört. Sei $\mathrm{Hall}_\pi(G)$ die Menge aller π-Hallgruppen von G.

Bemerkung 14.1

(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 dann auch p'.

(ii) Im Allgemeinen ist $\mathrm{Hall}_\pi(g) = \emptyset$. Beispielsweise enthält die alternierende Gruppe vom Grad 5 $\mathrm{Alt}(5)$ keine $\{2,5\}$-Hallgruppe H. Denn wegen $|\mathrm{Alt}(5)| = 60 = 2^2 \cdot 3 \cdot 5$ wäre die Ordnung von $H = 20$ und der Index 3. Dies würde einen nichttrivialen Homomorphismus $f\colon \mathrm{Alt}(5) \to \mathrm{Sym}(3)$ liefern und das steht im Widerspruch zur Einfachheit von $\mathrm{Alt}(5)$.

(iii) Im Allgemeinen sind nicht alle π-Hallgruppen einer endlichen Gruppe konjugiert, z. B. existiert in der Gruppe $\mathrm{GL}(3, \mathbb{F}_2)$ der Ordnung $(2^3-1)(2^3-2)(2^3-2^2) = 168 = 2^3 \cdot 3 \cdot 7$ nichtkonjugierte Hallgruppen der Ordnung 24 (siehe Übung).

Satz 14.1
Seien G eine endliche Gruppe, $\pi \subseteq \mathbb{P}$ und $H \in \mathrm{Hall}_\pi(G)$. Dann gilt:

(i) $N \trianglelefteq G \Rightarrow H \cap N \in \mathrm{Hall}_\pi(N)$ und $HN/N \in \mathrm{Hall}_\pi(G/N)$

(ii) $N_G(N_G(H)) = N_G(H)$

BEWEIS:

(i) Einerseits ist $H \cap N$ eine π-Gruppe wegen $|H \cap N| \mid |H|$ und wegen $|N\colon H \cap N| = |NH\colon H| \mid |G\colon H|$ gehört jeder Primteiler vom Index $|N\colon H \cap N|$ zu π'. Also ist $H \cap N \in \mathrm{Hall}_\pi(N)$.

Wegen $|HN/N| = |H/H \cap N| \mid |H|$ ist HN/N eine π-Gruppe. Wegen $|G/N\colon HN/N| = |G\colon HN| \mid |G\colon H|$ gehört jeder Primteiler von $|G/N\colon HN/N|$ zu π'. Daher ist HN/N eine π-Hallgruppe von G/N.

(ii) Sicher ist $H \trianglelefteq N_G(H)$ $H \in \mathrm{Hall}_\pi(N_G(H))$. Für $x \in N_G(N_G(H))$ ist $xHx^{-1} \trianglelefteq xN_G(H)x^{-1} = N_G(H)$. Wegen $|H(xHx^{-1}) : H| = |xHx^{-1} : xHx^{-1} \cap H| \mid |xHx^{-1}| = |H|$ und $|H(xHx^{-1}) : H| \mid |G : H|$ gehört jeder Primteiler von $|H(xHx^{-1}) : H|$ zu $\pi \cap \pi' = \emptyset$. Daher muss der Index gleich 1 sein. Das heißt, $H = H(xHx^{-1}) \geqslant xHx^{-1}$. Wegen $|H| = |xHx^{-1}|$ folgt, $H = xHx^{-1}$, d. h. $x \in N_G(H)$. Damit ist gezeigt, $N_G(N_G(H)) \subseteq N_G(H) \subseteq N_G(N_G(H))$. ∎

Satz 14.2
Seien G eine endliche Gruppe, $\pi \subseteq \mathbb{P}$ und $A \in \mathrm{Hall}_\pi(G)$ normal und abelsch. Dann ist $\mathrm{Hall}_{\pi'}(G) \neq \emptyset$ und es gilt $H_1 \sim_G H_2$ für alle $H_1, H_2 \in \mathrm{Hall}_{\pi'}(G)$.

BEWEIS:
Der Beweis geht auf WIELANDT zurück. Die Nebenklassen nach dem Normalteiler A seien von 1 bis $n = |G : A|$ nummeriert. Für jedes Repräsentantensystem R für die Nebenklassen G/A und $i = 1, \ldots, n$ sei $r_i \in R$ das Element in der i-ten Nebenklasse. Außerdem sei $\mathfrak{R}$ die Menge aller Repräsentantensysteme. Für $R, S \in \mathfrak{R}$ setzt man $R \sim S :\Leftrightarrow \prod_{i=1}^n r_i s_i^{-1} = 1$. Es ist immer $r_i s_i^{-1} \in A$. Da A abelsch ist, ist die Relation ein Äquivalenzrelation. Die Menge der Äquivalenzklassen $[R]$ sei $\mathfrak{R}/_\sim$. Es operiert G auf $\mathfrak{R}$ durch Linksmultiplikation. Für $g \in G$ und $R, S \in \mathfrak{R}$ mit $R \sim S$ gilt $gR \sim gS$. Daher operiert G auf $\mathfrak{R}/_\sim$ durch $g[R] := [gR]$. Insbesondere operiert A auf $\mathfrak{R}/_\sim$. Wir behaupten, dass A regulär auf $\mathfrak{R}/_\sim$ operiert.

Zum Beweis der Regularität seien $R, S \in \mathfrak{R}$. Dann: $\prod_{i=1}^n r_i s_i^{-1} =: a \in A$. Wegen der Eigenschaft, dass $\mathrm{ggT}(n, |A|) = 1$ ist die Abbildung $A \to A$ mit $b \mapsto b^n$ injektiv, also auch bijektiv. Folglich existiert ein $x \in A$ mit $x^n = a^{-1}$. Daher ist $\prod_{i=1}^n xr_i s_i^{-1} = x^n a = 1$, d. h. $xR \sim S$. Also ist $x[R] = [xR] = [S]$. Dies zeigt, A ist transitiv auf $\mathfrak{R}/_\sim$.

Seien $R \in \mathfrak{R}$ und $x \in A$ mit $[R] = x[R] = [xR]$, d. h. $xR \sim R$. Dann haben wir $1 = \prod_{i=1}^n xr_i r_i^{-1} = x^n$. Also $x = 1$. Somit operiert A regulär auf $\mathfrak{R}/_\sim$.

Insbesondere ist $|\mathfrak{R}/_\sim| = |A|$ und G operiert transitiv auf $\mathfrak{R}/_\sim$. Für $H := \mathrm{Stb}_G([R])$ gilt also: $|A| = |\mathfrak{R}/_\sim| = |G : H|$ und $|H| = |G : A|$. Daher ist $H \in \mathrm{Hall}_{\pi'}(G)$.

Sei $K \in \mathrm{Hall}_{\pi'}(G)$ beliebig. Dann ist $|K| = |G : A| = n$ und $K \cap A = 1$, denn eines ist eine π-Gruppe und das andere ein π'-Gruppe. Dies bedeutet, $|KA| = |K| \cdot |A| = |G : A| \cdot |A| = |G|$. Insbesondere ist $K \in \mathfrak{R}$. Da G transitiv auf der Menge $\mathfrak{R}/_\sim$ operiert, ist $|G : \mathrm{Stb}_G([K])| = |\mathfrak{R}/_\sim| = |A| = |G : K|$. Wegen $K \subseteq \mathrm{Stb}_G([K])$ folgt, $K = \mathrm{Stb}_G([K])$. Da G transitiv auf $\mathfrak{R}/_\sim$ operiert, sind $H = \mathrm{Stb}_G([R])$ und $K\,\mathrm{Stb}_G([K])$ in G konjugiert. ∎

Satz 14.3 (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, $H_1 \sim H_2$ für $H_1, H_2 \in \mathrm{Hall}_{\pi'}(G)$.

BEWEIS:
Zur Existenz: Man macht eine Induktion nach der Gruppenordnung. Œ sei $N \neq 1$. Denn andernfalls ist G eine π'-Hallgruppe. Weiter sei $\pi \in \mathbb{P}$ mit $p \mid |N|$ und $P \in \mathrm{Syl}_p(N)$. Nach dem FRATTINI-Argument gilt dann $G = N \cdot N_G(P)$, also $|N_G(P) : N_G(P) \cap$

$N| = |N_G(P)N/N| = |G\colon N|$. Daher ist $N_G(P) \cap N \in \mathrm{Hall}_\pi(N_G(P))$ normal und jede π-Hallgruppe von $N_G(P)$ ist auch eine von G. Daher sei Œ $G = N_G(P)$, d. h. $P \trianglelefteq G$. Wegen $p \neq 1$ ist $1 \neq Z(P) \trianglelefteq G$ und $N/Z(P) \in \mathrm{Hall}_\pi(G/Z(P))$ normal. Nach Induktion existiert eine Untergruppe $U/Z(P) \in \mathrm{Hall}_{\pi'}(G/Z(P))$. Dann ist das Zentrum von P eine normale und abelsche π-Hallgruppe von U. Nach Satz 14.2 existiert ein $H \in \mathrm{Hall}_{\pi'}(U)$. Wegen $|H| = |U\colon Z(P)| = |G/Z(P)\colon N/Z(P)| = |G\colon N|$ ist $H \in \mathrm{Hall}_{\pi'}(G)$.

Nun müssen wir uns Gedanken zur Eindeutigkeit machen. Hierzu führen wir eine Induktion über die Gruppenordnung durch. Seien $H, H^* \in \mathrm{Hall}_{\pi'}(G)$. Insbesondere ist $|G| = |G\colon N| = |H^*|$. Nun sei Œ $N \neq 1$. Zunächst nehmen wir an, dass N auflösbar ist und $n \in \mathbb{N}_0$ mit $N^{(n)} \neq 1 = N^{(n+1)}$ ist. Dann ist $N^{(n)} \trianglelefteq G$ und $N/N^{(n)} \in \mathrm{Hall}_\pi(G/N^{(n)})$ normal. Ferner: $HN^{(n)}/N^{(n)}, H^*N^{(n)}/N^{(n)} \in \mathrm{Hall}_{\pi'}(G/N^{(n)})$. Nach Induktion existiert ein $gN^{(n)} \in G/N^{(n)}$ mit

$$H^*N^{(n)}/N^{(n)} = (gN^{(n)})(HN^{(n)}/N^{(n)})(gN^{(n)})^{-1} = (gHg^{-1})N^{(n)}/N^{(n)}$$

Das heißt, $H^*N^{(n)} = (gHg^{-1})N^{(n)}$. Daher ist $H^*, gHg^{-1} \in \mathrm{Hall}_{\pi'}(H^*N^{(n)})$. Nach dem Satz 14.2 sind H^*, gHg^{-1} in $H^*N^{(n)}$ konjugiert und wir sind in diesem Fall fertig.

Sei nun also G/N auflösbar und Œ $G/N \neq 1$. Sei M/N ein minimaler Normalteiler von G/N. Dann ist M/N charakteristisch einfach, also abelsche p-Gruppe für ein $p \in \pi'$. Ferner: $H \cap M \in \mathrm{Hall}_{\pi'}(M)$ und $(H \cap M)N/N \in \mathrm{Hall}_{\pi'}(M/N)$. Da M/N eine π'-Gruppe ist, folgt, $(H \cap M)N/N = M/N$ und $(H \cap M)N = M$. Insbesondere $H \cap M \cong H \cap M/H \cap M \cap N \cong (H \cap M)N/N = M/N$, d. h. $H \cap M \in \mathrm{Syl}_p(M)$ abelsch. Analog: $H^* \cap M \in \mathrm{Syl}_p(M)$. Nach dem Satz von Sylow (Satz 12.4) existiert ein $m \in M$ mit $H \cap M = m(H^* \cap M)m^{-1} = mH^*m^{-1} \cap M$. Daher ist $H, H^{**} := mH^*m^{-1} \in \mathrm{Hall}_{\pi'}(U)$ für $U := N_G(H \cap M)$. Außerdem haben wir $|U\colon U \cap N| = |UN/N| \mid |G\colon N|$, d. h. $U \cap N \in \mathrm{Hall}_\pi(U)$ normal. Im Fall $U < G$ gilt nach Induktion: $H \sim_U H^{**}$ und wir sind fertig.

Sei daher $U = G$, d. h. $P := H \cap M \trianglelefteq G$. Dann $NP/P \in \mathrm{Hall}_\pi(G/P)$ normal und $H/P, H^{**}/P \in \mathrm{Hall}_{\pi'}(G/P)$. Nach Induktion ist $H/P \sim_{G/P} H^{**}/P$, also auch $H \sim_G H^{**}$. Damit gilt auch $H \sim_G H^*$. ∎

Bemerkung 14.2
Wegen $\mathrm{ggT}(|N|, |G/N|) = 1$ hat N oder G/N ungerade Ordnung. Nach dem Satz von Feit-Thompson ist N oder G/N auflösbar. Das heißt, die Auflösbarkeitsvoraussetzung ist also in Wirklichkeit überflüssig. Der Beweis der Tatsache *ohne* Verwendung des Satzes von Feit-Thompson ist bis heute unbekannt.

Satz 14.4 (Satz von Hall)
Für jede auflösbare endliche Gruppe G und alle $\pi \subseteq \mathbb{P}$ gilt:

(i) G hat ein π-Hallgruppe.

(ii) Je zwei π-Hallgruppen von G sind konjugiert.

(iii) Jede π-Untergruppe von G ist in einer π-Hallgruppe von G enthalten.

BEWEIS:
Der Beweis wird wie schon in den obigen Aussagen per Induktion nach der Gruppenordnung durchgeführt. Œ sei $G \neq 1$ und N ein minimaler Normalteiler von G. Dann ist N eine abelsche p-Gruppe für ein $p \in \mathbb{P}$.

(i) Da G/N auflösbar ist, existiert nach Induktion ein $H/N \in \mathrm{Hall}_\pi(G/N)$. Im Fall $p \in \pi$ ist $H \in \mathrm{Hall}_\pi(G)$. Sei also $p \notin \pi$. Dann: $N \in \mathrm{Syl}_p(H)$ normal. Nach dem Satz von SCHUR-ZASSENHAUS (Satz 14.3) existiert ein $K \in \mathrm{Hall}_{\pi'}(N)$. Dann: $K \in \mathrm{Hall}_\pi(H)$ und $K \in \mathrm{Hall}_\pi(G)$.

(ii) Hier ist gleich der Beweis der dritten Aussage mit eingeschlossen. Seien U eine π-Untergruppe von G und $H \in \mathrm{Hall}_\pi(G)$. Wir zeigen, dass ein $g \in G$ mit $U \subseteq gHg^{-1}$ existiert. Offenbar ist $UN/N \cong U/U \cap N$ eine π-Untergruppe von G/N und $HN/N \in \mathrm{Hall}_\pi(G/N)$. Nach Induktion existiert ein $xN \in G/N$ mit $UN/N \subseteq (xN)(HN/N)(xN)^{-1} = (xHx^{-1})N/N$, d. h. $U \subseteq UN \subseteq (xHx^{-1})N$. Offenbar ist U eine π-Untergruppe von $(xHx^{-1})N$ und $xHx^{-1} \in \mathrm{Hall}_\pi((xHx^{-1})N)$. Im Fall $(xHx^{-1})N < G$ existiert also nach Induktion ein $y \in (xHx^{-1})N$ mit $U \subseteq yxHx^{-1}y^{-1}$ und wir sind fertig.

Sei also $G = (xHx^{-1})N = xHNx^{-1}$, also auch $G = HN$. Im Fall $p \in \pi$ ist G eine π-Gruppe, also $G = H$ und die Behauptung ist trivial. Daher sei $p \in \pi'$. Dann: $N \in \mathrm{Syl}_p(NU)$ normal und $U \in \mathrm{Hall}_{\pi'}(NU)$. Andererseits ist $|NU \cap H| = \frac{|NU||H|}{|NUH|} = \frac{|N||U||H|}{|G|} = |U|$, d. h. $NU \cap H \in \mathrm{Hall}_{\pi'}(NU)$. Nach dem Satz von SCHUR-ZASSENHAUS existiert ein $g \in NU$ mit $U = g(NU \cap H)g^{-1} \subseteq gHg^{-1}$.

(iii) Siehe Beweis zum oben stehenden Punkt. ∎

Bemerkung 14.3
P. HALL hat auch bewiesen, dass umgekehrt jede endliche Gruppe G mit $\mathrm{Hall}_\pi(G) \neq \emptyset$ für alle $\pi \subseteq \mathbb{P}$ auflösbar ist. Der Beweis verwendet den $p^a q^b$-Satz von BURNSIDE.

Satz 14.5 (Satz von O. SCHMIDT)
Für jede endliche nichtnilpotente Gruppe G, in der jede echte Untergruppe nilpotent ist, gilt:

(i) G ist auflösbar.

(ii) Es existieren $p, q \in \mathbb{P}$ derart, dass G eine $\{p, q\}$-Gruppe mit einer zyklischen p-Sylowgruppe und einer normalen q-Sylowgruppe ist.

BEWEIS:
(i) Seien G ein Gegenbeispiel minimaler Ordnung und N ein minimaler Normalteiler von G. Dann ist jede echte Untergruppe von G/N nilpotent. Da G/N kein Gegenbeispiel ist, ist G/N auflösbar. Im Fall $N < G$ ist N nilpotent, also ist G auflösbar.

Sei also $N = G$. Dann ist G einfach. Seien M_1, M_2 verschiedene maximale Untergruppen von G derart, dass $D := M_1 \cap M_2$ möglichst groß ist.

Ist $D \neq 1$, so folgt für $i = 1, 2$ aus der Nilpotenz von M_i und der Einfachheit von G: $D < N_{M_i}(D) \leqslant N_G(D) < G$. Daher existiert eine maximale Untergruppe $M_3 \leqslant G$ mit $N_G(D) \subseteq M_3$. Dann ist $D < N_{M_i}(D) \leqslant M_i \cap M_3$, also $M_i = M_3$ nach der Wahl von M_1 und M_2. Daher sind M_1 und M_2 gleich. Das ist aber ein Widerspruch zur Voraussetzung.

Folglich ist $M \cap M^* = 1$ für je zwei verschiedene maximale Untergruppen $M, M^* \leqslant G$. Da G einfach ist, ist $N_G(M) = M$. Insbesondere hat M genau $|G\colon M|$ Konjugationen in G. Seien $M_1, \ldots, M_s$ Repräsentanten für die Konjugationsklassen maximaler Untergruppen von G. Dann:

$$\begin{aligned} |G| &= 10 \sum_{i=1}^{s} (|M_i| - 1)|G\colon M_i| = 1 + s|G| - \sum_{i=1}^{s} \underbrace{|G\colon M_i|}_{\leqslant |G|/2} \\ &\geqslant 1 + s|G| - s\frac{|G|}{2} = 1 + s\frac{|G|}{2} \end{aligned}$$

(ii) Sei $|G| = p_1^{a_1} \cdot \ldots \cdot p_r^{a_r}$ die Primfaktorzerlegung von $|G|$ und H ein maximaler Normalteiler von G. Nach dem obigen Punkt ist $|G\colon H| \in \mathbb{P}$. Œ setzen wir $|G\colon H| = p_1$. Nach der Voraussetzung ist H nilpotent, hat also für $i = 2, \ldots, r$ genau eine p_i-Sylow-Gruppe P_i. Dann ist P_i charakteristisch in H, also $P_i \trianglelefteq G$ und $P_i \in \mathrm{Syl}_{p_i}(G)$. Ferner sei $P_1 \in \mathrm{Syl}_p(G)$.

Wir nehmen an, dass $r \geqslant 3$ ist. Für $i = 2, \ldots, r$ ist dann $P_1P_i < G$, d. h. P_1P_i ist nilpotent. Insbesondere ist $P_i \subseteq N_G(P_1)$. Wegen $P_1 \subseteq N_G(P_1)$ ist also $|G| = p_1^{a_1} \cdot \ldots \cdot p_r^{a_r} \mid |N_G(P_1)|$. Folglich ist $P_1 \trianglelefteq G$. Nach dem Satz 12.8 ist G nilpotent. ↯ Also ist $r = 2$.

Nun nehmen wir weiter an, dass P_1 nicht zyklisch ist. Für $x \in P_1$ ist dann $\langle x \rangle P_2 < G$, also $\langle x \rangle P_2$ nilpotent. Insbesondere $P_2 \subseteq C_G(P_1) \subseteq N_G(P_1)$, also wieder $P_1 \trianglelefteq G$ ↯■

Satz 14.6 (Satz von WIELANDT)
Seien G eine endliche Gruppe, $\pi \subseteq \mathbb{P}$ und $H \in \mathrm{Hall}_\pi(G)$ nilpotent. Dann existiert zu jeder π-Untergruppe $U \leqslant G$ ein $g \in G$ mit $U \leqslant gHg^{-1}$.

BEWEIS:
Der Beweis wird per Induktion nach $|U|$ durchgeführt. Sei Œ $U \neq 1$. Nach Induktion existiert zu jeder Untergruppe $V < U$ ein $g \in G$ mit $V \subseteq gHg^{-1}$. Dann sind $gHg^{-1} \cong H$ und V nilpotent.

Ist U nicht nilpotent, so existiert nach Satz 14.5 ein $q \in \mathbb{P}$ und $Q \in \mathrm{Syl}_q(U)$ mit $1 \neq Q \trianglelefteq U$ und U/Q ist eine endliche p-Gruppe für ein $p \in \mathbb{P} \setminus \{q\}$.

Ist U nilpotent und $p \in \mathbb{P}$ mit $p \mid |U|$ sowie $P \in \mathrm{Syl}_p(U)$, so existiert ein $Q \trianglelefteq U$ mit $U = P \oplus Q$.

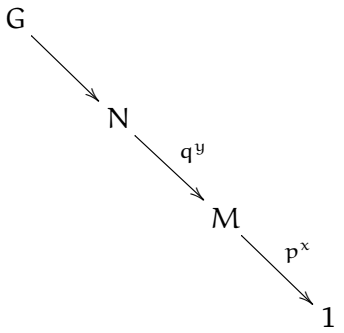
In beiden Fällen ist $Q \trianglelefteq U$. Mit $\rho := \pi \setminus \{p\}$ ist Q eine ρ-Untergruppe von G. Da H nilpotent ist, existiert eine Zerlegung $H = H_1 \oplus H_2$ mit $H_1 \in \mathrm{Syl}_p(H)$. Dann ist $H_2 \in \mathrm{Hall}_\rho(H) \subseteq \mathrm{Hall}_\rho(G)$. Nach Induktion existiert ein $x \in G$ mit $Q \subseteq xH_2x^{-1}$. Insbesondere $N_G(Q) \geqslant \langle xH_1x^{-1}, U\rangle$. Offenbar: $xH_1x^{-1} \in \mathrm{Syl}_p(G)$ und $xH_1x^{-1} \in \mathrm{Syl}_p(N_G(Q))$. Zu der p-Untergruppe $P \leqslant N_G(Q)$ existiert also ein $y \in N_G(Q)$ mit $P \subseteq y(xH_1x^{-1})y^{-1}$. Wegen $Q = yQy^{-1} \subseteq yxH_2x^{-1}y^{-1}$ ist $U = P \oplus Q \subseteq yxH_1x^{-1}y^{-1} \cdot yxH_2x^{-1}y^{-1} \subseteq yxH_1H_2x^{-1}y^{-1} = yxHx^{-1}y^{-1}$. ∎

Definition 14.2 (Komplement)
Seien H und K Untergruppen einer Gruppe G mit $H \cap K = 1$ und $HK = G$. Dann heißt K **Komplement** von H in G.

Bemerkung 14.4
Gegebenenfalls ist $|G| = |H| \cdot |K|$.

Satz 14.7 (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.

BEWEIS:
Sei Œ $M \neq G$. Da M charakteristisch einfach ist, ist M eine abelsche p-Gruppe für ein $p \in \mathbb{P}$. Sei N/M ein minimaler Normalteiler von G/M.



Dann ist N/M eine abelsche q-Gruppe für ein $q \in \mathbb{P}$. Im Fall $p = q$ wäre N eine p-Gruppe, also nilpotent. Folglich wäre $1 \neq Z(N) \cap M \trianglelefteq G$, also $M = Z(N) \cap M \subseteq Z(N)$ nach der Wahl von M. Dann ist $N \subseteq C_G(M)$ und steht somit im Widerspruch zu $C_G(M) = M$.

Somit ist $p \neq q$. Für $Q \in \mathrm{Syl}_q(N)$ ist $N = QM$ und $G = N_G(Q)N = N_G(Q)QM = N_G(Q)M$ nach dem Argument von FRATTINI. Offenbar ist $N_G(Q) \cap M \trianglelefteq N_G(Q)$ und $N_G(Q) \cap M \trianglelefteq M$, da M abelsch ist. Somit gilt:

$$N_G(Q) \cap M \trianglelefteq N_G(Q)M = G \tag{14.1}$$

Wegen der Minimalität von M ist $N_G(Q) \cap M \in \{1, M\}$. Im Fall $M = N_G(Q) \cap M \subseteq N_G(Q)$ wäre $G = N_G(Q)$ wegen Gleichung 14.1, d. h. $Q \trianglelefteq G$. Wegen $M \cap Q = 1$ wäre also $Q \subseteq C_G(M) = M$. Also haben wir $N_G(Q) \cap M = 1$, d. h. $N_G(Q)$ ist Komplement von M in G.

Sei H ein beliebiges Komplement von M in G. Dann ist $R := H \cap N \trianglelefteq H$ und $N = G \cap N = MH \cap N = M(H \cap N) = MR$. Die vorletzte Gleichheit resultiert aus der DEDEKINDschen Identität. Weiterhin haben wir auch $M \cap R \subseteq M \cap H = 1$. Folglich: $|R| = |N\colon M| = |Q|$, d. h. $R \in \mathrm{Syl}_q(N)$. Daher existiert ein $g \in N$ mit $R = gQg^{-1}$ (nach SYLOW). Daher: $H \subseteq N_G(R) = N_G(gQg^{-1}) = gN_G(Q)g^{-1}$. Andererseits ist $|H| = |G\colon M| = |N_G(Q)| = |gN_G(Q)g^{-1}|$, d. h. $H = gN_G(Q)g^{-1}$. ∎

Bemerkung 14.5
Seien G eine endliche Gruppe und $\pi \subseteq \mathbb{P}$. Für die 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, $O_\pi(G)$, der **π-Kern** von G heißt. Für jeden π-Normalteiler $N \trianglelefteq G$ ist $O_\pi(G/N) = O_\pi(G)/N$, insbesondere ist $O_\pi(G/O_\pi(G)) = O_\pi(G)/O_\pi(G) = 1$. Für $p \in \mathbb{P}$ und $\pi := \{p\}$ setzt man $O_p(G) := O_\pi(G)$.

Satz 14.8 (HALL-HIGMANN-Lemma)
Für jede auflösbare endliche Gruppe G und für alle $\pi \subseteq \mathbb{P}$ mit $O_{\pi'}(G) = 1$ ist $C_G(O_\pi(G)) \subseteq O_\pi(G)$.

BEWEIS:
Wegen $O_\pi(G) \trianglelefteq G$ ist $C := C_G(O_\pi(G)) \trianglelefteq G$, d. h. der Zentralisator eines Normalteilers ist wieder ein Normalteiler. Weiterhin ist $O_\pi(G) \trianglelefteq G$, d. h. $O_\pi(C) \subseteq O_\pi(G)$ Im Fall $C = O_\pi(C)$ sind wir fertig.

Sei also $O_\pi(C) < C$ und $N \trianglelefteq G$ möglichst klein mit $O_\pi(C) < N \leqslant C$. Dann ist $N/O_\pi(C)$ charakteristisch einfach, also eine abelsche p-Gruppe für ein $p \in \mathbb{P}$. Wegen $O_\pi(C/O_\pi(C)) = 1$ ist $p \notin \pi$. Für $P \in \mathrm{Syl}_p(N)$ ist

$$N = O_\pi(C)P \tag{14.2}$$

und $O_\pi(C) \cap P = 1$. Außerdem: $P \subseteq N \subseteq G = C_G(O_\pi(G)) \subseteq C_G(O_\pi(C))$, d. h. mit Gleichung 14.2 ist $P \trianglelefteq N$. Also: $\mathrm{Syl}_p(N) = \{P\}$. Insbesondere ist P charakteristisch in N. Also: $P \trianglelefteq G$ und $1 \neq P \subseteq O_{\pi'}(G) = 1$. ∎

15. Lineare Gruppen

Satz 15.1 (Lemma von IWASAWA)
Sei G eine perfekte Gruppe, Ω eine treue, primitive G-Menge, $\alpha \in \Omega$ und A ein auflösbarer Normalteiler von $H := \mathrm{Stb}_G(\alpha)$ mit $G = \langle gAg^{-1} \colon g \in G \rangle$. Dann ist G einfach.

BEWEIS:
Sei $1 \lhd N \trianglelefteq G$. Da G treu und primitiv auf Ω operiert, ist N transitiv auf Ω. Nach dem Argument von FRATTINI ist also $G = NH$. Wegen $A \trianglelefteq H$ ist $H \subseteq N_G(NA)$. Wegen $NA \subseteq N_G(NA)$ ist $G = NH \subseteq N_G(NA) \subseteq G$, d. h. $NA \trianglelefteq G$. Daher:

$$G = \langle gAg^{-1} \colon g \in G \rangle = \langle gNAg^{-1} \colon g \in G \rangle = NA$$

Folglich: $G/N = AN/N \cong A/(A \cap N)$ auflösbar. Andererseits ist $(G/N)' = G'N/N = G/N$. Insgesamt haben wir $G/N = 1$, d. h. $N = G$. ∎

Bemerkung 15.1

(i) Seien $\mathbb{K}$ ein Körper und V ein endlich-dimensionaler $\mathbb{K}$-Vektorraum. Dann gilt:

$$Z := \{ \alpha \,\mathrm{id}_V \mid \alpha \in \mathbb{K}^* \} \leqslant Z(\mathrm{GL}(V))$$

Denn für $g \in \mathrm{GL}(V), \alpha \in \mathbb{K}^*, v \in V$ gilt: $(g(\alpha \,\mathrm{id}_V)g^{-1})(v) = g(\alpha g^{-1}(v)) = \alpha g(g^{-1}(v)) = (\alpha \,\mathrm{id}_V)(v)$. Man nennt $\mathrm{PGL}(V) := \mathrm{GL}(V)/Z$ **projektive allgemeine lineare Gruppe** von V.

(ii) Aus (i) folgt: $Z \cap \mathrm{SL}(V) = \left\{ \alpha \,\mathrm{id}_V \;\middle|\; \alpha \in \mathbb{K}, \alpha^{\dim V} = 1 \right\} \leqslant Z(\mathrm{SL}(V))$. Man nennt $\mathrm{PSL}(V) := \mathrm{SL}(V)/(\mathrm{SL}(V) \cap Z) \cong \mathrm{SL}(V)Z/Z \leqslant \mathrm{PGL}(V)$ die **projektive spezielle lineare Gruppe** von V.

(iii) Für eine natürliche Zahl n ist also $Z := \{ \alpha 1_n \mid \alpha \in \mathbb{K}^* \} \leqslant Z(\mathrm{GL}(n, \mathbb{K}))$ und $\mathrm{GL}(n, \mathbb{K})/Z =: \mathrm{PGL}(n, \mathbb{K})$ heißt **projektive allgemeine lineare Gruppe** des Grades n über $\mathbb{K}$.

(iv) Daher ist $Z \cap \mathrm{SL}(n, \mathbb{K}) = \{ \alpha 1_n \mid \alpha \in \mathbb{K}, \alpha^n = 1 \} \leqslant Z(\mathrm{SL}(n, \mathbb{K}))$ und $\mathrm{PSL}(n, \mathbb{K}) := \mathrm{SL}(n, \mathbb{K})/\mathrm{SL}(n, \mathbb{K}) \cap Z$ heißt **projektive spezielle lineare Gruppe** de Grades n über $\mathbb{K}$.

(v) Für jeden $\mathbb{K}$-Vektorraum V der Dimension $n < \infty$ gilt:

$$\mathrm{GL}(V) \cong \mathrm{GL}(n, \mathbb{K}) \qquad \mathrm{SL}(V) \cong \mathrm{SL}(n, \mathbb{K})$$
$$\mathrm{PGL}(V) \cong \mathrm{PGL}(n, \mathbb{K}) \qquad \mathrm{PSL}(V) \cong \mathrm{PSL}(n, \mathbb{K})$$

Bemerkung 15.2
Für jeden Körper $\mathbb{K}$ und jeden $\mathbb{K}$-Vektorraum V mit $1 < \dim V < \infty$ operiert $\mathrm{GL}(V)$ auf der Menge Ω aller eindimensionalen Untervektorräume $U \subseteq V$:

$$^{g}U := g(U) \qquad g \in \mathrm{GL}(U), U \in \Omega$$

Dabei operiert $Z = \{ \alpha \,\mathrm{id}_V \mid \alpha \in \mathbb{K}^* \}$ trivial auf Ω. Daher operiert auch $\mathrm{PGL}(V) = \mathrm{GL}(V)/Z$ und $\mathrm{PSL}(V) = \mathrm{SL}(V)/\mathrm{SL}(V) \cap Z$ auf Ω:

$$^{\overline{g}}U := {}^{g}U := g(U) \qquad g \in \mathrm{GL}(V), \overline{g} := gZ, U \in \Omega$$
$$^{\overline{g}}U := {}^{g}U := g(U) \qquad g \in \mathrm{SL}(V), \overline{g} := g(\mathrm{SL}(V) \cap Z), U \in \Omega$$

Satz 15.2
Die Operation von $\mathrm{PSL}(V)$ ist treu und 2-transitiv.

BEWEIS:
Seien $U_1 := \mathbb{K}u_1, U_2 := \mathbb{K}u_2 \in \Omega$ verschieden. Dann sind u_1 und u_2 linear unabhängig und lassen sich zu einer Basis $u_1, \ldots, u_n$ ergänzen. Sind auch $W_1 = \mathbb{K}w_1, W_2 = \mathbb{K}w_2 \in \Omega$ verschieden, so erhält man analog eine Basis $w_1, \ldots, w_n$ von V.

Dann existiert genau ein $g \in \mathrm{GL}(V)$ mit $g(U_i) = W_i$. Sei $\delta_i = \det(g)$ für $i = 1, \ldots, n$. Dann existiert genau ein $h \in \mathrm{GL}(V)$ mit $h(U_i) = \delta^{-1}w$ und $h(U_i) = w_i$ für $i = 2, \ldots, n$. Dabei ist $\det(h) = 1$, d. h. $h \in \mathrm{SL}(V)$. Dann ${}^{h}U_1 = W_1$, ${}^{h}U_2 = W_2$.

Da Z sowieso trivial auf Ω operiert, operiert $\mathrm{PSL}(V)$ zweitransitiv auf V. Sei $g \in \mathrm{SL}(V)$ im Kern der Operation. Für $1 = 1, \ldots, n$ existiert dann ein $\alpha_i \in \mathbb{K}$ mit $g(U_i) = \alpha_i u_i$. Für verschiedene $i, j \in \{1, \ldots, n\}$ existiert auch ein $b_{ij} \in \mathbb{K}$ mit $g(u_i + u_j) = b_{ij}(u_i + u_j)$. Dann: $b_{ij}u_i + b_{ij}u_j = g(u_i + u_j) = g(u_i) + g(u_j) = \alpha_i u_i + \alpha_j u_j$. Wegen der Basiseigenschaft folgt damit $\alpha_i = b_{ij} = \alpha_j$. Also ist $g = \alpha_1 \,\mathrm{id}_V \in Z$ und daher ist $Z \cap \mathrm{SL}(V)$ der Kern der Operation von $\mathrm{SL}(V)$ auf Ω und $\mathrm{PSL}(V)$ operiert treu auf Ω. ∎

Bemerkung 15.3
Seien $\mathbb{K}$ ein Körper und n eine natürliche Zahl. Wir bezeichnen die Standardbasis von $\mathbb{K}^{n\times n}$ mit e_{ij} für $i, j = \{1, \ldots, n\}$. Beispielsweise für $n = 2$:

$$e_{11} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \qquad e_{12} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$
$$e_{21} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \qquad e_{22} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

Für $\alpha \in \mathbb{K}$ und *verschiedene* $i, j \in \{1, \ldots, n\}$ setzen wir

$$u_{ij}(\alpha) := 1_n + \alpha e_{ij} \in \mathrm{SL}(n, \mathbb{K})$$

Satz 15.3
Für jeden Körper $\mathbb{K}$ und $1 < n \in \mathbb{N}$ gilt:

$$\mathrm{SL}(n, \mathbb{K}) = \langle u_{ij}(\alpha) \colon i, j = 1, \ldots, n, i \neq j, \alpha \in \mathbb{K}^* \rangle$$

BEWEIS:
Für alle i, j, α und beliebige $a \in \mathrm{SL}(n, \mathbb{K})$ ist $u_{ij}(\alpha)a$ die Matrix, die aus a durch Addition des α-fachen der j-ten Zeile zur i-ten entsteht. Die erste Spalte von a ist nicht 0. Falls nötig, multiplizieren wir a mit einem geeigneten $u_{ij}(\alpha)$ so, dass der Eintrag an der Position $(1,1)$ gleich 1 ist. Analog kann man erreichen, dass die weiteren Einträge in der ersten Spalte von a verschwinden.

In Spalte 2 von a können nicht alle Einträge an den Positionen $(2,2), \ldots, (n,2)$ verschwinden. Durch Multiplikation mit einem geeigneten $u_{ij}(\alpha)$ kann man erreichen, dass der Eintrag an der Position $(2,2)$ gleich 1 ist. Weiter kann man erreichen, dass alle anderen Einträge in der ersten Spalte verschwinden. So fährt man fort. Am Ende hat man eine Matrix der Form

$$g = \begin{pmatrix} 1 & 0 & 0 & \ldots & 0 \\ 0 & 1 & 0 & \ldots & 0 \\ \vdots & 0 & \ddots & 0 & \vdots \\ 0 & 0 & \ldots & 1 & 0 \\ 0 & 0 & \ldots & 0 & \gamma \end{pmatrix}$$

Da die Determinante der Matrix 1 ist, muss $\gamma = 1$ gelten, also ist g die Einheitsmatrix. Wir haben also $b_1, \ldots, b_r \in \mathrm{SL}(n, \mathbb{K})$ mit $b_1 \cdot \ldots \cdot b_r a = 1_n$, wobei jedes b_k ein geeignetes $u_{ij}(\alpha)$ ist. Wegen $a = b_r^{-1} \cdot \ldots b_1^{-1}$ folgt die Behauptung. ∎

Satz 15.4
Seien $\mathbb{K}$ ein Körper und $1 < n \in \mathbb{N}$. Dann ist $\mathrm{SL}(n, \mathbb{K})$ perfekt, außer im Fall $(n, |\mathbb{K}|) \in \{(2,2), (2,3)\}$.

BEWEIS:
Nach Satz 15.3 genügt es zu zeigen, dass jedes $u_{ij}(\alpha)$ ein Kommutator ist. Für $i \neq j$ ist $e_{ij}^2 = 0$, also $(1 + \alpha e_{ij})(1 - \alpha e_{ij}) = 1$. Folglich: $u_{ij}(\alpha)^{-1} = u_{ij}(-u)$.

Sei zunächst $n \geqslant 3$. Für paarweise verschiedene $i, j, k \in \{1, \ldots, n\}$ gilt dann $[1 + e_{ij}, 1 + \alpha e_{jk}] = 1 + \alpha e_{ik}$.

Nun sei $n = 2$. Für $\beta, \gamma \in \mathbb{K}_+$ und $b := \begin{pmatrix} \beta & 0 \\ 0 & \beta^{-1} \end{pmatrix}, c := \begin{pmatrix} 1 & \gamma \\ 0 & 1 \end{pmatrix}$ gilt dann

$$[b, c] = \cdots = \begin{pmatrix} 1 & (\beta^2 - 1)\gamma \\ 0 & 1 \end{pmatrix}$$

Im Fall $|\mathbb{K}| \geqslant 3$ existiert ein $\beta \in \mathbb{K}_+$ mit $0 \neq \beta^2 - 1 = (\beta - 1)(\beta + 1)$. Daher existiert also ein γ mit $(\beta^2 - 1)\gamma = \alpha$, d. h. $[b, c] = u_{12}(\alpha)$. Durch Transposition erhält man, dass auch $u_{21}(\alpha)$ ein Kommutator ist. Der Rest folgt aus Satz 15.3. ∎

Bemerkung 15.4
(i) In der obigen Situation ist auch $\mathrm{PSL}(n, \mathbb{K}) = \mathrm{SL}(n, \mathbb{K})/Z$ perfekt.

(ii) Wegen $|\mathrm{GL}(2,\mathbb{F}_2)| = (2^2-1)(2^2-2) = 6$ und $|\mathrm{GL}(2,\mathbb{F}_3)| = (3^2-1)(3^2-3) = 48$ sind $\mathrm{GL}(2,\mathbb{F}_2)$ und $\mathrm{GL}(2,\mathbb{F}_3)$ auflösbar. Daher sind auch $\mathrm{SL}(2,\mathbb{F}_2)$, $\mathrm{SL}(2,\mathbb{F}_3)$, $\mathrm{PSL}(2,\mathbb{F}_2)$ und $\mathrm{PSL}(2,\mathbb{F}_3)$ auflösbar.

Satz 15.5
Sei $\mathbb{K}$ ein Körper und $n > 1$ eine natürliche Zahl. Dann: $\mathrm{PSL}(n,\mathbb{K})$ einfach außer im Fall $(n,\mathbb{K}) \in \{(2,2),(2,3)\}$.

BEWEIS:
Sei $V := \mathbb{K}^n$. Dann operiert $G := \mathrm{SL}(n,\mathbb{K}) \cong \mathrm{SL}(V)$ zweitransitiv, also auch primitiv auf der Menge Ω aller eindimensionalen Untervektorräume $U \subseteq V$. Seien $e_1,\dots,e_n$ die Standardbasis von V, $j \in \{1,\dots,n\}$, $U_j := \mathbb{K}e_j \in \Omega$, $H_j := \mathrm{Stb}_G(U_j)$. Beispielsweise ist

$$H_1 = \left\{ \left(\begin{array}{c|cc} * & * & \\ \hline 0 & & \\ \vdots & & * \\ 0 & & \end{array} \right) \right\}$$

Für $h \in H_j$ ist $\tilde{h}\colon V/U_j \to V/U_j$ mit $v + U_j \mapsto h(v) + U_j$. Ferner ist $f_j\colon H_j \to \mathrm{GL}(V/U_j)$ mit $h \mapsto \tilde{h}$ ein Gruppenhomomorphismus. Sei $A_j := \ker(f_j)$. So ist beispielsweise

$$A_1 = \left\{ \left(\begin{array}{c|ccc} 1 & & * & \\ \hline 0 & 1 & & 0 \\ \vdots & & \ddots & \\ 0 & 0 & & 1 \end{array} \right) \right\}$$

Daher operiert jedes $a \in A_j$ trivial auf U_j und auf V/U_j. Wegen

$$\left(\begin{array}{c|c} * & x \\ \hline 0 & \\ \vdots & 1_{n-1} \\ 0 & \end{array} \right) \left(\begin{array}{c|c} * & y \\ \hline 0 & \\ \vdots & 1_{n-1} \\ 0 & \end{array} \right) = \left(\begin{array}{c|c} * & x+y \\ \hline 0 & \\ \vdots & 1_{n-1} \\ 0 & \end{array} \right) \qquad x,y \in \mathbb{K}^{n-1}$$

ist A_1 abelsch und $A_1 \trianglelefteq H_1$. Für $i \neq j$ und $\alpha \in \mathbb{K}_+$ ist $U_{ij}(\alpha) \in A_i$. Da G transitiv auf Ω operiert, existiert für $j = 1,\dots,n$ ein $g_j \in G$ mit $U_j = {}^{g_j}U_1$. Dann ist $H_j = g_j H_1 g_j^{-1}$ und $A_j = g_j A_1 g_j^{-1}$. Folglich ist $G = \langle U_{ij}(\alpha)\colon i \neq j, \alpha \in \mathbb{K}_+\rangle = \langle A_1,\dots,A_n\rangle \subseteq \langle gA_1g^{-1}\colon g \in G\rangle$.

Sei $Z := \{\, \alpha 1_n \mid \alpha \in \mathbb{K}, \alpha^n = 1 \,\}$, also $Z \trianglelefteq G$. Dann operiert $\overline{G} := G/Z = \mathrm{PSL}(n,\mathbb{K})$ treu und primitiv auf Ω sowie

$$\begin{aligned} \overline{H_i} &:= \mathrm{Stb}_{\overline{G}}(U_1) = \mathrm{Stb}_G(U_1)/Z = H_1/Z \\ \overline{A_1} &:= A_1Z/Z \trianglelefteq \overline{H_1} \text{ abelsch mit} \\ \overline{G} &= \langle \overline{g}\,\overline{A_1}\,\overline{g}^{-1}\colon \overline{g} \in \overline{G}\rangle \end{aligned}$$

Nach dem Lemma von IWASAWA (Satz 15.1) ist $\overline{G}$ einfach. ∎

Bemerkung 15.5

(i) In der Algebra lernt man, dass $\mathbb{K}_+$ im Fall $|\mathbb{K}| = q < \infty$ zyklisch ist. Daher hat $Z := \{ \alpha 1_n \mid \alpha \in \mathbb{K}, \alpha^n = 1 \}$ die Ordnung $\operatorname{ggT}(n, q-1)$, da $\alpha^{q-1} = 1$ für alle $\alpha \in \mathbb{K}_+$. Also gilt, $|\mathrm{PSL}(n, \mathbb{K})| = |\mathrm{SL}(n, \mathbb{K})| / \operatorname{ggT}(n, q-1)$.

(ii) Ähnlich (mit „kleinen“ Ausnahmen) kann man die Einfachheit von anderen klassischen Gruppen beweisen (orthogonal, symplektisch, unitär).

16. Die Verlagerung

Bemerkung 16.1
Sei G eine endliche Gruppe und $K \trianglelefteq H \leqslant G$ derart, dass H/K abelsch ist. Schließlich sei R ein Repräsentantensystem für G/H, d. h. $G = \dot{\cup}_{r\in R} rH$. Dann existieren für $g \in G$ und $r \in R$ eindeutig bestimmte Elemente $\rho_g(r) \in R, \eta_g(r) \in H$ mit $gr = \rho_g(r)\eta_g(r)$. Wir setzen als **Verlagerung**:

$$V^G_{H/K}(g) := \prod_{r\in R} \eta_g(r)K \in H/K$$

Da H/K abelsch ist, kommt es bei dem Produkt nicht auf die Reihenfolge an.

Satz 16.1
Die so definierte Abbildung $V^G_{H/K}\colon G \to H/K$ ist unabhängig von R und ein Homomorphismus.

BEWEIS:
Jedes weitere Repräsentantensystem für G/H hat die Form

$$R' = \{\, rh_r \mid r \in R \,\}$$

Für $g \in G, r \in R$ ist $grh_r = \rho_g(r)\eta_g(r)h_r = \underbrace{\rho_g(r)h_{\rho_g(r)}}_{=:\,\rho'_g(r)\in R'} \underbrace{h_{\rho_g^{-1}(r)}\eta_g(r)}_{=:\,\eta'_g(r)\in H}$. Da H/K abelsch ist und $R \to R, r \mapsto \rho_g(r)$ für $g \in G$ eine bijektive Abbildung ist, gilt:

$$\prod_{r\in R} \eta'_g(rh_r)K = \prod_{r\in R} h^{-1}_{\eta_g(r)}h_rK = \prod_{r\in R} \eta_g(r)K$$

Für $f, g \in G, r \in R$ gilt ferner: $\underbrace{\rho_{fg}(r)}_{\in R}\underbrace{\eta_{fg}(r)}_{\in H} = fgr = f\rho_g(r)\eta_g(r) = \underbrace{\rho_f(\rho_g(r))}_{\in R}\underbrace{\eta_f(\eta_g(r))}_{\in H}$, d. h. $\eta_{fg}(r) = \eta_f(\rho_g(r))\eta_g(r)$. Daher gilt:

$$\begin{aligned} V^G_{H/K}(fg) &= \prod_{r\in R} \eta_{fg}(r)K = \prod_{r\in R} \eta_f(\rho_g(r))K \prod_{r\in R} \eta_g(r) \\ &= V^G_{H/K}(f) = V^G_{H/K}(g) \end{aligned}$$

∎

Definition 16.1 (Verlagerung)
Die Abbildung $V^G_{H/K}$ heißt **Verlagerung**[1] von G nach H/K.

[1] vom englischen Wort „transfer“

Beachte: In der Regel ist $|H/K| < G$. Daher ist die Verlagerung typischerweise *nicht* injektiv. Aber G/G' ist stets abelsch.

Bemerkung 16.2
Sei G eine endliche Gruppe und $K \trianglelefteq H \leqslant G$ derart, dass H/K abelsch ist. Weiterhin sei $g \in G$. Zur Berechnung von $V^G_{H/K}(g)$ wählen wir ein Repräsentantensystem für G/H, das von g abhängt.

Auf G/H operiert $\langle g\rangle$ durch Linksmultiplikation. Die Bahnen seien $\Delta_1, \dots, \Delta_s$. Wähle $r_1H \in \Delta_1, \dots, r_sH \in \Delta_s$. Ist $i \in \{1, \dots, s\}$ und $d_i := |\Delta_i|$, so ist d_i ein Teiler von $|\langle g\rangle|$ und

$$\Delta_i = \{r_iH, gr_iH, g^2r_iH, \dots, g^{d_i-1}r_iH\} \qquad g^{d_i}r_iH = r_iH$$

Folglich ist $R := \{r_1, gr_1, g^2r_1, \dots, g^{d_1-1}r_1, \dots, r_s, gr_s, g^2r_s, \dots, g^{d_s-1}r_s\}$ ein Repräsentantensystem für G/H und $V^G_{H/K}(g) = \prod_{i=1}^s r_i^{-1}g^{d_i}r_iK$ mit $d_i + \dots + d_s = |G\colon H|$ und $r_i^{-1}g^{d_i}r_i \in H$. In der Gleichung tauchen die einzigen Fehler bei $g^{d_i-1}r_i$ auf. „Oft“ ist $r_i^{-1}g_i^{d_i}r_i = g^{d_i}$ für $i = 1, \dots, s$, also

$$V^G_{H/K}(g) = g^{|G\colon H|}K$$

Beispiel 16.1

(i) Sei $g \in Z(G)$. Dann ist $V^G_{H/K}(g) = g^{|G\colon H|}K$.

(ii) Die Abbildung $G \to Z(G)$ mit $g \mapsto g^{|G\colon Z(G)|}$ ist ein Homomorphismus, denn $G^G_{Z(G)/\{1\}}(g) = g^{|G\colon Z(G)|}\{1\}$. Tatsächlich ist auch $g^{|G\colon Z(G)|} \in Z(G)$ nach dem Satz von LAGRANGE (Satz 4.2).

Definition 16.2 (Fokalgruppe)
Für jede Untergruppe H einer endlichen Gruppe G heißt

$$\mathrm{Foc}_G(H) := \langle \underbrace{[g,h]}_{ghg^{-1}h^{-1}} : g \in G, h \in H, [g,h] \in H\rangle = \langle xy^{-1} \colon x, y \in H, x \sim_G y\rangle$$

Fokalgruppe von H in G.

Bemerkung 16.3
Dann: $H' \subseteq F := \mathrm{Foc}_G(H) \subseteq H \cap G'$. Das bedeutet insbesondere $F \trianglelefteq H$ und H/F abelsch.Für alle $g \in G, h \in H$ mit $[g,h] \in H$ ist ferner $ghg^{-1}F = ghg^{-1}h^{-1}Fh = [g,h]Fh = Fh = hF$. Folglich $V^G_{H/F}(h) = h^{|G\colon H|}F$ für alle $h \in H$.

Satz 16.2
Seien G eine endliche Gruppe, H eine Untergruppe von G, F die Fokalgruppe, $N := \ker(V^G_H)$ und $\mathrm{ggT}(|G\colon H|, |H\colon F|) = 1$. Dann gilt:

(i) $F = H \cap G' = H \cap N$

(ii) $HN = G$ und $G/N \cong H/F$

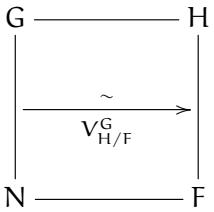
(iii) $G/G' = HG'/G' \oplus N/G'$

BEWEIS:

(i) Wegen $G/N \cong \mathrm{Bld}(V^G_{H/F}) \leqslant H/F$ ist G/N abelsch, d. h. $G' \subseteq N$ und $F \subseteq H \cap G' \subseteq H \cap N$. Für $h \in H \cap N$ ist umgekehrt $1 = V^G_{H/F}(h) = h^{|G:H|}F$. Ferner haben wir $h^{|H:F|} = 1$ nach FERMAT. Nach Voraussetzung ist also $hF = 1$, d. h. $h \in F$.

(ii) Aus Teil (i) folgt: $|G/N| \geqslant |HN/N| = |H/H \cap N| = |H/F| \geqslant |G/N|$. Daher folgt: $HN = G$ und Verlagerung ist surjektiv. Folglich ist $G/N \cong H/F$.

(iii) Nach Teil (ii) ist $G/G' = (HG'/G')(N/G')$. Nach Teil (i) ist $N \cap HG' = (N \cap H)G'$ wegen der Dedekindschen Identität. Insgesamt ergibt sich weiter $(N \cap H)G' = G'$, d. h. $(N/G') \cap (HG'/G') = 1$. ∎



Beispiel 16.2
Die oben geforderte Teilerfremdheit ist dann erfüllt, wenn H eine Hallgruppe von G ist.

Definition 16.3 (Hyperfokale Gruppe)
Sei H eine Untergruppe einer endlichen Gruppe G. Setze $H_1 := H, H_{n+1} := \mathrm{Foc}_G(H_n)$ für alle natürlichen Zahlen n. Ist $H_m = 1$ für ein $m \in \mathbb{N}$, so heißt die Fokalgruppe **hyperfokal**.

Bemerkung 16.4
Gegebenenfalls ist jede Untergruppe $K \leqslant H$ wieder hyperfokal in G wegen $\mathrm{Foc}_G(K) \subseteq \mathrm{Foc}_G(H)$. Ferner ist H auch hyperfokal in jeder Untergruppe $U \leqslant G$ mit $H \leqslant U$ wegen $\mathrm{Foc}_U(H) \subseteq \mathrm{Foc}_G(H)$. Schließlich ist H nilpotent wegen $H^n \subseteq H_n$ für alle natürlichen n.

Satz 16.3
Jede hyperfokale Hallgruppe H einer endlichen Gruppe G hat ein normales Komplement in G.

BEWEIS:
Der Beweis wird per Induktion über die Gruppenordnung durchgeführt. Œ sei $H \neq 1$. Dann $F := \mathrm{Foc}_G(H) < H$. Nach Satz 16.2 ist $N := \ker(V^G_{H/F}) \trianglelefteq G$ und $G/N \cong H/F \neq 1$. Die Hallgruppe $H \cap N$ von N ist nach obiger Bemerkung hyperfokal in G und auch in N. Wegen der Induktion hat $H \cap N$ ein normales Komplement K in N. Als Hallgruppe von N ist K charakteristisch in N. Daher ist $K \trianglelefteq G$. Ferner $HK = H(H \cap N)K = HN = G$ und $H \cap K = H \cap N \cap K = 1$. ∎

Satz 16.4
Sei H eine nilpotente Hallgruppe einer endlichen Gruppe G. Je zwei Elemente in H, die in G konjugiert sind, seien auch in H konjugiert. Dann hat H ein normales Komplement in G.

BEWEIS:
Setze $H_1 := H, H_{n+1} := \mathrm{Foc}_G(H_n)$ für $n \in \mathbb{N}$. Nach Satz 16.3 genügt es zu zeigen, dass $H_n \subseteq H^n$ für natürliche Zahlen n. Für $n = 1$ ist das klar. Sei also $H_n \subseteq H^n$ für $n \in \mathbb{N}$. Für $g \in G$ und $h \in H_n$ mit $ghg^{-1}h^{-1} \in H_n$ ist $ghg^{-1} \in H_n$. Nach Voraussetzung existiert eine Element $k \in H$ mit $ghg^{-1} = khk^{-1}$. Folglich: $[g,h] = ghg^{-1}h^{-1} = khk^{-1}h^{-1} = [k,h] \in [H,H_n] \subseteq [H,H^n] = H^{n+1}$. Dies zeigt, dass das $H_{n+1} = \langle [g,h] \colon g \in G, h \in H_n, [g,h] \in H_n \rangle \subseteq H^{n+1}$. ∎

Satz 16.5
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 $N_G(H)$ konjugiert.

BEWEIS:
Sei $g \in G$ mit $y = gxg^{-1} \in H \cap gHg^{-1}$. Dann sind H und gHg^{-1} Hallgruppen von $C_G(y)$. Nach Satz 14.6 (Satz von WIELANDT) existiert ein $c \in C_G(y)$ mit $H = cgHg^{-1}c^{-1}$ und $y = cyc^{-1} = cgxg^{-1}c^{-1}$ mit $cg \in N_G(H)$. ∎

Satz 16.6 (Satz von BURNSIDE)
Jede Hallgruppe H einer endlichen Gruppe G mit $N_G(H) = C_G(H)$ hat ein normales Komplement in G.

BEWEIS:
Seien $x, y \in H$ mit $x \sim_G y$. Nach Satz 16.5 ist $x \sim_{N_G(H)} y$ und wegen der Voraussetzung $x \sim_{C_G(H)} y \Rightarrow x = y$, d. h. $x \sim_H y$. Nun wenden wir Satz 16.4 an. ∎

Bemerkung 16.5
Nach der Voraussetzung des obigen Satzes ist H auf jeden Fall abelsch.

Satz 16.7
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.

BEWEIS:
Sei $|P| = p^n$. Dann: $|\mathrm{Aut}(P)| = p^n - p^{n-1} = p^{n-1}(p-1)$. Da $N_G(P)/C_G(P)$ zu einer Untergruppe von $\mathrm{Aut}(P)$ isomorph ist, folgt, $|N_G(P)/C_G(P)| \mid p-1$. Nach der Wahl von p ist $N_G(P)/C_G(P) = 1$, d. h. $N_G(P) = C_G(P)$. Nun wenden wir Satz 16.6 an. ∎

Bemerkung 16.6
Hat G eine zyklische 2-Sylow-Gruppe P, so hat P ein normales Komplement K in G nach dem Satz. Wegen $2 \nmid |K|$ ist K auflösbar (wegen FEIT-THOMPSON). Somit ist auch G auflösbar.

Beispiel 16.3
Aus dem Satz folgt insbesondere, dass für ungerade $n \in \mathbb{N}$ jede Gruppe der Ordnung $2n$ einen Normalteiler der Ordnung n enthält (vgl. Übung).

Satz 16.8
Sind alle Sylow-Gruppen einer endlichen Gruppe G zyklisch, so ist G auflösbar.

BEWEIS:

Bemerkung 16.7
Speziell sind also Gruppen quadratfreier Ordnung n, d. h. $n = p_1 \cdot \ldots \cdot p_r$ mit paarweise verschiedenen Primzahlen $p_1, \ldots, p_r$, stets auflösbar.

Beispiel 16.4
Jede Gruppe der Ordnung $210 = 2 \cdot 3 \cdot 5 \cdot 7$ ist auflösbar.

A. Übungsaufgaben

A.1. Übungsblatt 1

A.1.1. Aufgabe 1

(i) Sind $(\mathbb{N}, \text{ggT})$ und $(\mathbb{N}, \text{kgV})$ Halbgruppen (Monoide)?

(ii) Für $n \in \mathbb{N}$ sei $f(n)$ die Anzahl der Primfaktoren von n. Ist $f\colon (\mathbb{N}, \text{kgV}) \to (\mathbb{Z}, +)$ ein Homomorphismus?

A.1.2. Aufgabe 2

(i) Konstruieren Sie eine Halbgruppe mit unendlich vielen linksneutralen Elementen. Hinweis: Versuchen Sie es mit einer geeigneten Menge von 2×2-Matrizen.

(ii) Geben Sie ein Monoid M und ein Element $a \in M$ an, das unendlich viele Linksinverse hat.

A.1.3. Aufgabe 3

(i) Zeigen Sie, dass für jede Menge X die Abbildung $f\colon (\mathcal{P}(X), \cup) \to (\mathcal{P}(X), \cap)$ mit $A \mapsto X \setminus A$ ein Isomorphismus ist.

(ii) Gegeben seien Mengen X, Y und eine Bijektion $f\colon X \to Y$. Konstruieren Sie einen Isomorphismus $F\colon (\text{Abb}(X), \circ) \to (\text{Abb}(Y), \circ)$.

A.1.4. Aufgabe 4

Beantworten Sie die folgenden Fragen mit GAP:

(i) Wie viele Untergruppen von $\text{Sym}(9)$ haben die Ordnung 4?

```
G:=SymmetricGroup(9);
sum:=Size(Filtered(G,x->Order(x)=4))/2; #zyklische Untergruppen
F:=Filtered(G,x->Order(x)=2);
C:=0; #initialisieren, nicht unbedingt noetig
H:=0; #initialisieren
for x in F do
C:=Intersection(Centralizer(G,x),F);
H:=Filtered(C,y->x*y in C);
sum:=sum+Size(H)/2; #noch nicht gezaehlte Kleinsche Vierergruppe
F:=Difference(F,[x]);
od;
Print(sum,"\n"); #Loesung: 56007
```

(ii) Wie viele Untergruppen hat $\mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z}$?

```
% skript-check aus
    LoadPackage("sonata"); #fuer den Befehl "Subgroups"
% skript-check an
    G:=DirectProduct(CyclicGroup(12),CyclicGroup(15));
    Print(Size(Subgroups(G)),"\n"); #Loesung: 36
```

(iii) Gegeben seien die folgenden Permutationen von $\Omega := \{0, 1, \ldots, 9, 10\} \cup \{\infty\}$:

$$\alpha\colon x \mapsto x+1 \qquad \beta\colon x \mapsto 2x \qquad \gamma\colon x \mapsto x^{-1}$$

Dabei rechnet man jeweils modulo 11 und das Rechnen mit ∞ wird geeignet definiert. Welche Ordnung hat die von α, β, γ erzeugte Untergruppe von $\mathrm{Sym}(\Omega)$?

```
alpha:=(11,1,2,3,4,5,6,7,8,9,10); #ersetze 0 durch 11 und unendli
beta:=(1,2,4,8,5,10,9,7,3,6);
gamma:=(1,10)(2,5)(3,7)(4,8)(6,9)(11,12);
Print(Size(Group([alpha,beta,gamma])),"\n"); #Loesung: 1320
```

A.2. Übungsblatt 2

A.2.1. Aufgabe 5

(i) Wie viele Automorphismen hat $\mathrm{Sym}(3)$?
Bekanntlich ist $\mathrm{Sym}(3) = \langle (12), (123) \rangle$. Also ist jeder Automorphismus durch die Bilder von (12) und (123) eindeutig bestimmt. Weiter wissen wir, dass jeder Automorphismus die Ordnung der Elemente erhält. Daher ist $\varphi((12)) \in \{(12), (13), (23)\}$ und $\varphi((123)) \in \{(123), (132)\}$ für $\varphi \in \mathrm{Aut}(\mathrm{Sym}(3))$. Dies zeigt, $|\mathrm{Aut}(\mathrm{Sym}(3))| \leqslant 6$. Umgekehrt haben wir die Relation $6 = |\mathrm{Sym}(3)| = |\mathrm{Sym}(3)/Z(\mathrm{Sym}(3))| =$

$|\mathrm{Inn}(\mathrm{Sym}(3))| \leqslant |\mathrm{Aut}(\mathrm{Sym}(3))|$. Die erste Gleichheit folgt nach dem zweiten Teil der Aufgabe.

Es ist $Z(\mathrm{Sym}(n)) = \begin{cases} 1 & n \neq 2 \\ \mathrm{Sym}(2) & n = 2 \end{cases}$. Denn sei o. B. d. A. $n \geqslant 3$ und $1 \neq \sigma \in \mathrm{Sym}(n)$. Dann gibt es ein Element $k \neq \sigma(k) =: l$ mit $k, l \in \{1, \ldots, n\}$. Für $m \in \{1, \ldots, n\} \setminus \{k, l\}$ ist dann $((m, l) \circ \sigma)(k) = m$ und $(\sigma \circ (m, l))(k) = l$. Aber es gilt: $k \neq l$ und $\sigma \notin Z(\mathrm{Sym}(n))$.

(ii) Bestimmen Sie $Z(\mathrm{Sym}(n))$ und $Z(\mathrm{GL}(n, \mathbb{K}))$ für $n \in \mathbb{N}$ und jeden Körper $\mathbb{K}$.

(iii) Zeigen Sie: $\mathrm{GL}(2, \mathbb{F}_2) \cong \mathrm{Sym}(3)$.

A.2.2. Aufgabe 6

Für alle Elemente a in dem Monoid M sei $a^2 = 1$. Zeigen Sie, dass M eine abelsche Gruppe ist.
Wegen $a^2 = 1$ ist a invers zu a für alle $a \in M$. Also ist M eine Gruppe. Aus $ab = a^{-1}b^{-1} = (ba)^{-1} = ba$ folgt, dass M abelsch ist.

A.2.3. Aufgabe 7

Zeigen Sie, dass eine nichtleere endliche Teilmenge H einer Gruppe G genau dann eine Untergruppe von G ist, wenn $ab \in H$ für alle $a, b \in H$ gilt.

„⇒“ klar

„⇐“ Sei $x \in H$ mit $H \neq \emptyset$. Dann ist $x^n \in H$ für alle $n \in \mathbb{N}$. Wegen $|H| < \infty$ existieren $n, m \in \mathbb{N}$ mit $n < m$ und $x^n = x^m$. Also ist $1 = x^{m-n} \in H$ und $x^{-1} = x^{m-n-1} \in H$. Da x beliebig war, hat jedes Element in H ein Inverses in H und $H \leqslant G$ folgt.

A.2.4. Aufgabe 8

Zeigen Sie, dass für Untergruppen H, K einer Gruppe G mit $G = HK$ folgende Aussagen gelten:

(i) Für $x, y \in G$ ist $G = (xHx^{-1})(yKy^{-1})$.

(ii) Sind H, K abelsch, so ist $Z(G) = (Z(G) \cap H)(Z(G) \cap K)$.

A.2.5. Aufgabe 9

Sei $G := \langle a, b \rangle$ mit $a := \begin{pmatrix} i & 0 \\ 0 & -1 \end{pmatrix}, b := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in GL(2, \mathbb{C})$.

(i) Zeigen Sie: $|G| = 8$ und $|Z(G)| = 2$.

```
i:=E(4); #(erste) primitive 4-te Einheitswurzel
a:=[[i,0],[0,-i]];
b:=[[0,1],[1,0]];
G:=Group([a,b]);
Print(Size(G),"\n"); #Formel: |G|=|<a,b>|=|<a><b>|=|<a>||<b>|/|<
Print(Size(Center(G)),"\n");
```

(ii) Bestimmen sie alle Elemente in G und deren Ordnungen.

```
Print(Elements(G),"\n");
Print(List(G,Order),"\n");
```

(iii) Bestimmen Sie die Untergruppen und Normalteiler von G und deren Ordnungen.

```
% skript-check aus
    LoadPackage("sonata");
% skript-check an
    Print(Subgroups(G),"\n");
    Print(List(Subgroups(G),Size),"\n");
    Print(NormalSubgroups(G),"\n");
    Print(List(NormalSubgroups(G),Size),"\n");
```

(iv) Finden Sie die Untergruppen A, B von G mit $A \trianglelefteq B \trianglelefteq G$, aber $A \not\trianglelefteq G$.

```
A:=Subgroup(G,[b]);
B:=Subgroup(G,[b,a^2]);
Print(IsNormal(B,A),"\n"); #normal, da Index=2
Print(IsNormal(G,B),"\n"); #normal, da Index=2
Print(IsNormal(G,A),"\n"); #nicht normal, da nicht in NormalSubgr
```

Bei dieser Aufgabe können Sie GAP verwenden.

A.3. Übungsblatt 3

A.3.1. Aufgabe 10

Seien $\mathbb{K}$ ein Körper und n eine natürliche Zahl.

(i) Zeigen Sie, dass die Abbildung $f\colon \mathrm{Sym}(n) \to \mathrm{GL}(n,\mathbb{K}), \sigma \mapsto (\delta_{i\sigma(j)})_{i,j=1}^{n}$ ein Monomorphismus ist. Die Elemente in $S := \mathrm{Bld}(f)$ heißen **Permutationsmatrizen**.

(ii) Zeigen Sie, dass die regulären oberen Dreiecksmatrizen eine Untergruppe B von $\mathrm{GL}(n,\mathbb{K})$ bilden.

(iii) Bestimmen Sie $|B|$ im Fall $q := |\mathbb{K}| < \infty$.

(iv) Zeigen Sie: $\mathrm{GL}(n,\mathbb{K}) = \langle B, S\rangle$.

A.3.2. Aufgabe 11

Zeigen Sie, dass jede endlich erzeugte Untergruppe von $(\mathbb{Q},+)$ zyklisch ist.
Sei $H := \langle x_1/y_1, \dots, x_n/y_n\rangle$ eine Untergruppe von $(\mathbb{Q},+)$ mit $x_1,\dots,x_n,y_1,\dots,y_n \in \mathbb{Z}$ und $k := \mathrm{kgV}(y_1,\dots,y_n)$. Für jedes $i \in \{1,\dots,n\}$ lässt sich dann der Bruch x_i/y_i zu z_i/k mit $z_i \in \mathbb{Z}$ erweitern. Also ist $x_i/y_i = z_i/k \in \langle 1/k\rangle$ für alle $i \in \{1,\dots,n\}$ und es folgt, $H \leqslant \langle 1/k\rangle$. Als Untergruppe einer zyklischen Gruppe ist dann auch H zyklisch.

A.3.3. Aufgabe 12

Beweisen Sie, dass $G \neq \bigcup_{g\in G} gHg^{-1}$ für jede echte Untergruppe H einer endlichen Gruppe gilt.
Im Fall $H \trianglelefteq G$ ist $\bigcup_{g\in H} gGg^{-1} = H < G$ nach Voraussetzung. Sei also $H \ntrianglelefteq G$. Für $x,y \in G$ gilt:

$$xH = yH \Rightarrow Hx^{-1} = (xH)^{-1} = (yH)^{-1} = Hy^{-1} \Rightarrow xHx^{-1} = yHx^{-1} = yHy^{-1}$$

wobei $(xH)^{-1} := \left\{ a^{-1} \;\middle|\; a \in xH \right\}$ die Menge der Inversen von xH sei (nicht etwa das Inverse von xH in der nicht vorhandenen Faktorgruppe G/H). Diese Rechnung zeigt:

$$\left|\left\{ gHg^{-1} \;\middle|\; g \in G \right\}\right| \leqslant |G\colon H|$$

Sei nun $g \in G$ mit $H \neq gHg^{-1}$ (Erinnerung: $H \ntrianglelefteq G$). Dann ist $1 \in H \cap gHg^{-1}$. Insbesondere sind H und gHg^{-1} nicht disjunkt. Da gHg^{-1} das Bild von H unter einem inneren Automorphismus ist, gilt $|H| = |gHg^{-1}|$ für alle $g \in G$. Also ist

$$\left|\bigcup_{g\in G} gHg^{-1}\right| < |G\colon H||H| = |G|$$

nach LAGRANGE (Satz 4.2).

A.3.4. Aufgabe 13

(i) Geben Sie einen Homomorphismus von Gruppen $f\colon G \to H$ und einen Normalteiler $M \trianglelefteq G$ mit $f(M) \not\trianglelefteq H$ an.
Setze $G := M := \langle (12) \rangle$ und $H := \mathrm{Sym}(3)$. Dann ist $f\colon G \to H, x \mapsto x$ ein Homomorphismus mit $f(M) = M$. Wegen $(123)(12)(123)^{-1} = (23) \notin M$ ist $M \not\trianglelefteq H$.

(ii) Zeigen Sie, dass in $\mathrm{Sym}(4)$ die Normalteiler-Relation nicht transitiv ist.

```
G:=SymmetricGroup(4);
A:=Subgroup(G,[(1,2)(3,4)]);
B:=Subgroup(G,[(1,2)(3,4),(1,3)(2,4)]);
Print(IsNormal(B,A),"`\n"');
Print(IsNormal(G,B),"`\n"');
Print(IsNormal(G,A),"`\n"');
```

(iii) Finden Sie eine Gruppe, in der das Zentrum nicht vollinvariant ist.

```
LoadPackage("`sonata"');
for i in [1..12] do
Print(Filtered(AllSmallGroups(i),G->not
IsFullinvariant(G,Center(G))),"`\n"');
od;
```

(iv) Zeigen Sie, dass $G := \mathrm{Sym}(6)$ von zwei Elementen erzeugt wird, aber eine Untergruppe H hat, die sich nicht durch zwei Elemente erzeugen lässt.

```
G:=SymmetricGroup(6);
Print(Filtered(Subgroups(G),H->Size(GeneratorsOfGroup(H))>2 and
IsSolvable(H) and Size(MinimalGeneratingSet(H))>2),"`\n"');
#MinimalGeneratingSet ist bisher nur fuer aufloesbare Gruppen im
```

Bei dieser Aufgabe können Sie wieder GAP verwenden.

A.4. Übungsblatt 4

A.4.1. Aufgabe 14

Gegeben seien Gruppen K, H und ein Homomorphismus $\varphi\colon H \to \mathrm{Aut}(K), h \mapsto \varphi_h$. Auf $G := H \times K$ wird eine Multiplikation durch $(k,h)(k',h') := (k\varphi_h(k'), hh')$ für $h, h' \in H$ und $k, k' \in K$ definiert. Zeigen Sie, dass G eine Gruppe ist, die eine zu H isomorphe Untergruppe $\tilde{H}$ und einen zu K isomorphen Normalteiler $\tilde{K}$ mit $G = \tilde{K}\tilde{H}$ und $\tilde{K} \cap \tilde{H} = 1$ besitzt. (Man nennt G das **semidirekte Produkt** von K und H bezüglich φ und schreibt $G = K \rtimes H$ oder genauer $G = K \rtimes_\varphi H$).

A.4.2. Aufgabe 15

(i) Zeigen Sie, dass es bis auf Isomorphie genau zwei Gruppen der Ordnung 4 gibt.

(ii) Beweisen Sie, dass für jede Gruppe G mit $Z(G) = 1$ gilt: $Z(\mathrm{Aut}(G)) = 1$.

A.4.3. Aufgabe 16

Seien $\mathbb{K}$ ein Körper, n eine natürliche Zahl und G die Untergruppe von $\mathrm{GL}(n, \mathbb{K})$, die aus allen Matrizen der folgenden Form besteht:

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

Bestimmen Sie $Z(G)$.

A.4.4. Aufgabe 17

Sei $n \in \mathbb{N} \setminus \{4\}$. Zeigen Sie, dass zu jedem $\sigma \in \mathrm{Sym}(n) \setminus \{1\}$ ein $\tau \in \mathrm{Sym}(n)$ mit $\mathrm{Sym}(n) = \langle \sigma, \tau \rangle$ existiert. Zeigen Sie weiter, dass diese Aussage für $n = 4$ falsch ist.
Sei $n \in \mathbb{N}\setminus\{4\}$ und $\sigma \in \mathrm{Sym}(n)\setminus\{1\}$. Da man σ durch eine beliebige Potenz ersetzen kann, können wir annehmen, dass σ Primzahlordnung p hat (Erinnerung: Wegen $\langle \sigma^k, \tau \rangle \subseteq \langle \sigma, \tau \rangle$ für alle $k \in \mathbb{N}$ genügt es $\langle \sigma^k, \tau \rangle = \mathrm{Sym}(n)$ für ein $k \in \mathbb{N}$ zu zeigen.) Dann ist σ ein Produkt von disjunkten Zyklen (Erinnerung: Die Ordnung eines Elements ist das kgV der Zyklenlängen.). Œ können wir annehmen, dass σ die Form $\sigma = (12 \dots p) \dots$ hat. Ist $\sigma = (12)$ oder $\sigma = (12 \dots n)$, so können wir bekanntlich $\tau = (12 \dots n)$ bzw. $\tau = (12)$ wählen. Andernfalls werden wir τ als ein disjunktes Produkt einer Transposition (x, y) und eines r-Zyklus' wählen, wobei $r = n-2$ (bzw. $r = n-3$) für ungerades (bzw. gerades) n gilt. Insbesondere ist r stets ungerade. Folglich ist $\tau^r = (x, y)$ und der r-Zyklus eine Potenz von τ^2. Wir werden dann zeigen, dass $(i, k) \in \langle \sigma, \tau \rangle$ für ein festes $k \in \{1, \dots, n\}$ und alle $i \in \{1, \dots, n\}$ gilt. Somit folgt die Behauptung.

1. Fall Sei $\sigma = (12 \dots p)$ für $2 < p < n$. Wähle

$$\tau = \begin{cases} (1, n)(23 \dots n-1) & n \text{ ungerade} \\ (1, n)(34 \dots n-1) & n \text{ gerade} \end{cases}$$

Konjugiert man nun $(1, n)$ mit den Potenzen von σ und τ^2, so erhält man $(i, n) \in \langle \sigma, \tau \rangle$ für alle $i \in \{1, \ldots, n\}$ (Zur Erinnerung: Für $k \in \mathbb{N}$ ist $\sigma(a_1, a_2, \ldots, a_k)\sigma^{-1} = (\sigma(a_1), \sigma(a_2), \ldots, \sigma(a_k))$).

2. Fall Sei $\sigma = (12 \ldots p)(p+1 \ldots 2p) \ldots$ das Produkt von mindestens zwei p-Zyklen und p ungerade. Wähle

$$\tau = \begin{cases} (12)(34 \ldots n) & n \text{ ungerade} \\ (12)(34 \ldots p, p+2 \ldots n) & n \text{ gerade} \end{cases}$$

Konjugiert man nun (12) mit σ, so erhält man $(23) \in \langle \sigma, \tau \rangle$. Konjugiert man (23) weiter mit den Potenzen von τ^2, so erhält man $(2, i) \in \langle \sigma, \tau \rangle$ für alle $i \in \{1, \ldots, p, p+2, \ldots, n\}$. Konjugiert man $(2, p+2)$ mit σ^{-1}, so erhält man $(1, p+1) \in \langle \sigma, \tau \rangle$. Konjugiert man weiter mit (12), so erhält man schließlich auch $(2, p+1) \in \langle \sigma, \tau \rangle$.

3. Fall Sei $\sigma = (12)(34) \ldots$ das Produkt von mindestens zwei Transpositionen. Insbesondere ist in diesem Fall $n > 4$ (wegen $n \neq 4$). Wähle

$$\tau = \begin{cases} (13)(245 \ldots n) & n \text{ ungerade} \\ (13)(45 \ldots n) & n \text{ gerade} \end{cases}$$

Konjugiert man (13) mit σ, so erhält man $(24) \in \langle \sigma, \tau \rangle$. Konjugiert man (24) mit den Potenzen von τ^2, so erhält man $\mathrm{Sym}(2, 4, 5, \ldots, n) \subseteq \langle \sigma, \tau \rangle$. Insbesondere ist $(n, i) \in \langle \sigma, \tau \rangle$ für $i \in \{2, 4, 5, \ldots, n\}$. Konjugiert man nun $(n, 2)$ und $(n, 4)$ mit σ, so erhält man entweder $(n, 1), (n, 3) \in \langle \sigma, \tau \rangle$ oder $(n+1, 1), (n+1, 3) \in \langle \sigma, \tau \rangle$. Im zweiten Fall konjugiert man zusätzlich mit $(n, n-1)$.

Sei nun $n = 4$ und $\sigma = (12)(34)$. Wir nehmen indirekt $\mathrm{Sym}(4) = \langle \sigma, \tau \rangle$ für ein $\tau \in \mathrm{Sym}(4)$ an. Dann ist

$$\begin{aligned} \mathrm{Sym}(4)/\langle (12)(34), (13)(24) \rangle &= \langle \tau \rangle \langle (12)(34), (13)(24) \rangle / \langle (12)(34), (13)(24) \rangle \\ &\cong \langle \tau \rangle / \langle \tau \rangle \cap \langle (12)(34), (13)(24) \rangle \end{aligned}$$

zyklisch. Da $\mathrm{Sym}(4)$ aber kein Element der Ordnung größer gleich 6 besitzt, erhalten wir einen Widerspruch.

A.5. Blatt 5

A.5.1. Aufgabe 18

Seien g, h Elemente einer Gruppe G der endlichen Ordnungen m, n. Zeigen Sie die untenstehenden Aussagen:

(i) Ist $k \in \mathbb{Z}$ mit $g^k = 1$, so gilt $m \mid k$.

(ii) Für $k \in \mathbb{Z}$ hat g^k die Ordnung $\frac{m}{ggT(m,k)}$.

(iii) Gilt $gh = hg$ und $ggT(m,n) = 1$, so hat gh die Ordnung mn.

A.5.2. Aufgabe 19

Seien G eine Gruppe, $n \in \mathbb{N}$ und $H \leqslant \mathrm{Sym}(n)$. Zeigen Sie, dass

$$G \wr H := \{(g_1, \ldots, g_n; h) \colon g_1, \ldots, g_n \in G, h \in H\}$$

mit der folgenden Multiplikation zu einer Gruppe wird:

$$(g_1, \ldots, g_n; h)(g'_1, \ldots, g'_n; h) := (g_1 g'_{h^{-1}(1)}, \ldots, g_n g'_{h^{-1}(n)}; hh')$$

Man nennt $G \wr H$ das **Kranzprodukt** von G und H. Beweisen Sie, dass $G \wr H$ einen Normalteiler N mit $N \cong G \times \ldots \times G$ (n Faktoren) und eine Untergruppe U mit $U \cong H$, $G \wr H = NU$ und $N \cap U = 1$ hat.

A.5.3. Aufgabe 20

Zeigen Sie, dass für jede einfache nichtabelsche Gruppe G gilt:

(i) $\mathrm{Inn}(G)$ ist eine charakteristische Untergruppe von $\mathrm{Aut}(G)$.

(ii) $\mathrm{Aut}(\mathrm{Aut}(G)) = \mathrm{Inn}(\mathrm{Aut}(G))$.

A.5.4. Aufgabe 21

(i) Geben Sie eine Kompositionsreihe und eine Hauptreihe von $\mathrm{SL}(2, \mathbb{Z}/3\mathbb{Z})$ an.

(ii) Zeigen Sie, dass es bis auf Isomorphie genau zwei Gruppen der Ordnung 6 gibt.

A.6. Blatt 6

A.6.1. Aufgabe 22

Zeigen Sie, dass jede endliche Gruppe G, die eine einfache $\mathrm{End}(G)$-Gruppe ist, charakteristisch einfach ist. (Hinweis: Zeigen Sie, dass für jeden echten Normalteiler N in G möglichst großer Ordnung der Durchschnitt aller Normalteiler M von G mit $G/M \cong G/N$ eine vollinvariante Untergruppe von G ist.)

A.6.2. Aufgabe 23

Geben Sie Beispiele für Gruppen an, die die folgenden Bedingungen für Untergruppen erfüllen (bzw. nicht erfüllen):

(i) Minimal-/Maximalbedingung

(ii) Minimal- und nicht Maximalbedingung

(iii) Maximal- und nicht Minimalbedingung

(iv) weder Minimal- noch Maximalbedingung

A.6.3. Aufgabe 24

Zeigen Sie, dass für jede Gruppe G gilt:

(i) Die Abbildung $G \to G, x \mapsto x^{-1}$ ist genau dann ein Automorphismus, wenn G abelsch ist.

(ii) Die Abbildung $G \to G, x \mapsto x^2$ ist genau dann ein Endomorphismus, wenn G abelsch ist.

(iii) Im Fall $|G| < \infty$ ist die Abbildung $G \to G, x \mapsto x^2$ genau dann ein Automorphismus, wenn G abelsch von ungerader Ordnung ist.

A.6.4. Aufgabe 25

(i) Zeigen Sie, dass die komplexen Matrizen

$$a = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \qquad b = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

eine nichtabelsche Gruppe G der Ordnung 8 erzeugen.

(ii) Zeigen Sie, dass jede Untergruppe von G normal in G ist.

(iii) Ist G zu der Gruppe aus Aufgabe 9 (Abschnitt A.2.5) isomorph?

A.7. Blatt 7

A.7.1. Aufgabe 26

(i) Zeigen Sie: $\mathbb{Z}/120\mathbb{Z} \cong \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$.

(ii) Bestimmen Sie die Anzahl der Isomorphieklassen abelscher Gruppen der Ordnung 36.

(iii) Sei $A := \mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})$. Bestimmen Sie $T(A)$ und geben Sie zwei verschiedene Untergruppen F_1, F_2 von A mit $A = T(A) \oplus F_1 = T(A) \oplus F_2$ an.

A.7.2. Aufgabe 27

Sei N ein Normalteiler einer Gruppe G mit $N \cong \mathrm{Sym}(3) \cong G/N$. Zeigen Sie, dass G zu $\mathrm{Sym}(3) \times \mathrm{Sym}(3)$ isomorph ist.

A.7.3. Aufgabe 28

Seien G_1, G_2 Gruppen. Konstruieren Sie eine Bijektion zwischen der Menge aller Untergruppen von $G_1 \times G_2$ und der Menge aller 5-Tupel $(H_1, K_1, H_2, K_2, \varphi)$ mit den folgenden Eigenschaften:

(i) $K_1 \trianglelefteq H_1 \leqslant G_1$ und $K_2 \trianglelefteq H_2 \leqslant G_2$.

(ii) $\varphi\colon H_1/K_1 \to H_2/K_2$ Isomorphismus.

A.7.4. Aufgabe 29

Finden Sie mit GAP eine endliche Gruppe G, in der nicht jedes Element aus G' ein Kommutator ist.

A.8. Blatt 8

A.8.1. Aufgabe 30

Zeigen Sie, dass für Elemente a, b einer Gruppe G stets gilt:

(i) Ist $[a, b]$ mit a vertauschbar, so ist $[a^n, b] = [a, b^n]$ für $n \in \mathbb{Z}$.

(ii) Ist $[a, b]$ mit a und b vertauschbar, so ist $(ab)^n = a^n b^n [b, a]^{\binom{n}{2}}$ für $n \in \mathbb{N}$.

A.8.2. Aufgabe 31

Seien $\mathbb{K}$ ein Körper und $n \in \mathbb{N}$.

(i) Zeigen Sie, dass die Untergruppe U von $\mathrm{GL}(n, \mathbb{K})$, die aus allen Matrizen der Form

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

besteht, nilpotent ist und bestimmen Sie die Nilpotenzklasse von U.

(ii) Zeigen sie, dass die Untergruppe B von $\mathrm{GL}(n, \mathbb{K})$, die aus allen Matrizen der Form

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

besteht, auflösbar ist.

A.8.3. Aufgabe 32

(i) Zeigen Sie, dass es bis auf Isomorphie genau fünf Gruppen der Ordnung 8 gibt.

(ii) Zeigen Sie, dass es bis auf Isomorphie genau zwei Gruppen der Ordnung 10 gibt.

A.8.4. Aufgabe 33

Beweisen Sie, dass eine zyklische Gruppe der Ordnung $n < \infty$ zu jedem Teiler d von n genau eine Untergruppe der Ordnung d enthält.

A.9. Blatt 9

A.9.1. Aufgabe 34

Seien G eine endliche Gruppe und $\alpha \in \mathrm{Aut}(G)$ mit $\{ x \in G \mid \alpha(x) = x \} = \{1\}$. (Automorphismen mit dieser Eigenschaft heißen **fixpunktfrei**.) Zeigen Sie:

(i) $G = \left\{ \alpha(x)x^{-1} \;\middle|\; x \in G \right\}$

(ii) Ist $\alpha^2 = \mathrm{id}_G$, so ist G abelsch von ungerader Ordnung.

A.9.2. Aufgabe 35

Sei $\mathbb{K}$ ein Körper mit $|\mathbb{K}| = 3$. Zeigen Sie, dass $\mathrm{GL}(2, \mathbb{K})/Z(\mathrm{GL}(2, \mathbb{K}))$ zu $\mathrm{Sym}(4)$ isomorph ist.

A.9.3. Aufgabe 36

Beweisen Sie folgende Aussage: Sei G eine Gruppe. Wenn $G/Z(G)$ zyklisch ist, so ist die Gruppe G abelsch.

A.9.4. Aufgabe 37

Zeigen Sie, dass eine endlich erzeugte Gruppe für $n \in \mathbb{N}$ nur endlich viele Untergruppen vom Index n enthält.

A.9.5. Aufgabe 38

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

A.10. Blatt 10

A.10.1. Aufgabe 39

Wie viele verschiedene Armbänder aus insgesamt 10 Perlen lassen sich herstellen, wenn Perlen in den Farben rot, gelb und blau zur Verfügung stehen?

A.10.2. Aufgabe 40

(i) Zeigen Sie, dass es bis auf Isomorphie genau zwei Gruppen der Ordnung 9 gibt.

(ii) Bestimmen Sie bis auf Isomorphie alle endlichen Gruppen der Klassenzahl 4.

A.10.3. Aufgabe 41

Seien $G \neq 1$ eine endliche Gruppe und $A \leqslant \mathrm{Aut}(G)$. Wir betrachten die natürliche Operation von A auf $G \setminus \{1\}$. Zeigen Sie:

(i) Ist die Operation transitiv, so ist G abelsch und es existiert ein $p \in \mathbb{P}$ mit $x^p = 1$ für alle $x \in G$.

(ii) Ist sie 2-transitiv, so ist $p = 2$ oder $|G| = 3$.

(iii) Ist sie 3-transitiv, so ist $|G| = 4$.

(iv) Sie ist nie 4-transitiv.

A.10.4. Aufgabe 42

Seien G eine endliche Gruppe, $p \in \mathbb{P}$ und S, T verschiedene p-Sylowgruppen von G derart, dass $|S \cap T|$ möglichst groß. Zeigen Sie:

$$|\mathrm{Syl}_p(G)| \equiv 1 \pmod{|S \colon S \cap T|}$$

A.11. Blatt 11

A.11.1. Aufgabe 43

Sei G eine Gruppe der Ordnung $2n$, wobei $n \in \mathbb{N}$ ungerade ist. Zeigen Sie, dass G einen Normalteiler H vom Index 2 enthält.

A.11.2. Aufgabe 44

Seien $\mathbb{K}$ ein Körper, $n \in \mathbb{N}$ und U die Untergruppe von $G \coloneqq \mathrm{GL}(n, \mathbb{K})$, die aus allen oberen Dreiecksmatrizen mit lauter Einsen auf der Hauptdiagonale besteht. Berechnen Sie $N_G(U)$.

A.11.3. Aufgabe 45

Sei $g \in \mathrm{Alt}(n)$ für ein $n \in \mathbb{N}$. Wie kann man am Typ $(k_1, \ldots, k_l)$ von g erkennen, ob $C_{\mathrm{Sym}(n)}(g) \subseteq \mathrm{Alt}(n)$ ist?

A.11.4. Aufgabe 46

(i) Zeigen Sie, dass für $p \in \mathbb{P}$ und $n \in \mathbb{N}$ Gruppen der Ordnungen $4p^n$ und $8p^n$ stets auflösbar sind.

(ii) Beweisen Sie, dass Gruppen der Ordnungen $61, \ldots, 119$ auflösbar sind.

(iii) Zeigen Sie, dass eine Gruppe der Ordnung 120 nicht einfach sein kann.

(iv) Sind $\mathrm{Sym}(5)$ und $\mathrm{SL}(2, \mathbb{F}_5)$ isomorph?

A.12. Blatt 12

A.12.1. Aufgabe 47

(i) Zeigen Sie, dass $\mathrm{Alt}(4)$ keine Untergruppe der Ordnung 6 enthält.

(ii) Ist $\mathrm{Sym}(4)$ zu $\mathrm{SL}(2, \mathbb{F}_3)$ isomorph?

(iii) Konstruieren Sie zwei nichtkonjugierte Untergruppen der Ordnung 24 in $\mathrm{GL}(3, \mathbb{F}_2)$.

A.12.2. Aufgabe 48

(i) Beweisen Sie, dass es bis auf Isomorphie genau fünf Gruppen der Ordnung 12 gibt.

(ii) Zeigen Sie, dass jede Gruppe der Ordnung 15 zyklisch ist.

A.12.3. Aufgabe 49

wie viele verschiedene Färbungen der sechs Seiten eines Würfels mit höchstens 3 Farben gibt es?

A.12.4. Aufgabe 50

Seien G eine endliche auflösbare Gruppe, $\pi \subseteq \mathbb{P}$, $H \in \mathrm{Hall}_\pi(G)$ und $N_G(H) \leqslant U \leqslant G$. Zeigen Sie: $N_G(U) = U$.

A.13. Blatt 13

A.13.1. Aufgabe 51

(i) Sei $n \in \mathbb{N}$ mit $n \geqslant 3$. Zeigen Sie, dass die Permutationen

$$a = (1, 2, \ldots, n) \qquad b = (1, n)(2, n-1)(3, n-2)\ldots$$

eine Untergruppe der Ordnung $2n$ von $\mathrm{Sym}(n)$ erzeugen. Man nennt $D_{2n} := \langle a, b\rangle$ **Diedergruppe** der Ordnung $2n$.

(ii) Beweisen Sie, dass D_{2n} zur Symmetriegruppe eines regelmäßigen n-Ecks isomorph ist.
Bemerkung: Manchmal betrachtet man die KLEINsche Vierergruppe

$$V_4 = \{(1), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\} \leqslant \mathrm{Sym}(4)$$

als Diedergruppe der Ordnung 4.

A.13.2. Aufgabe 52

Sei G eine endliche Gruppe und seien $x, y \in G$ zwei verschiedene Involutionen (d. h. Elemente der Ordnung 2). Zeigen Sie, dass $\langle x, y\rangle$ zu einer Diedergruppe isomorph ist.

A.13.3. Aufgabe 53

(i) Beweisen Sie, dass es für $p \in \mathbb{P}$ bis auf Isomorphie genau zwei Gruppen der Ordnung $2p$ gibt.

(ii) Zeigen Sie, dass es bis auf Isomorphie genau zwei Gruppen der Ordnung 21 gibt.

A.13.4. Aufgabe 54

Seien G eine endliche Gruppe, $p \in \mathbb{P}, Q \leqslant G$ eine p-Untergruppe und $N \trianglelefteq G$ ein p'-Normalteiler. Zeigen Sie:

$$N_{G/N}(QN/N) = N_G(Q)N/H \qquad C_{G/N}(QN/N) = C_G(Q)N/N$$

B. Artikel zum begleitendem Lesen

Herr Külshammer teilte zu Beginn der Vorlesung einen Ausschnitt aus einer Zeitschrift aus. Das Dokument kann auf der Seite http://www.math.auckland.ac.nz/~obrien/research/gnu.pdf nachgelesen werden.

Literaturverzeichnis

[1] ALPERIN-BELL. Groups and representations.

[2] ASCHBACHER. Finite group theory.

[3] ISAACS. Finite group theory.

[4] KURZWEIL-STELLMACHER. Theorie der endlichen Gruppen.

[5] ROBINSON. course in the theory of groups.

[6] ROTMAN. An introduction to the theory of groups.

[7] HUPPERT. Endliche Gruppen I.

[8] HUPPERT-BLACKBURN. Finite groups II–III.

[9] SUZUKI. Group theory I–II.

[10] GORENSTEIN. Finite Groups.

[11] RONAN. Symmetry and the monster.

Index

Z