Gruppentheorie

Vorlesung im Wintersemester 1992/93

B. Külshammer

Ausarbeitung:
Markus Deiml

Inhaltsverzeichnis

KAPITEL 1

Halbgruppen

1.1. Definition. Eine (innere) *Verknüpfung* auf einer Menge M ist eine Abbildung $M \times M \to M$. Das Bild von $(a, b) \in M \times M$ schreibt man häufig in der Form $a * b,\ a \cdot b,\ a + b,\ ab$.

Beispiel.

(i) Addition, Multiplikation, Subtraktion in $\mathbb{Z},\ \mathbb{R},\ \mathbb{C}$.
(ii) Durchschnitt und Vereinigung auf der *Potenzmenge* $\mathcal{P}(X)$, der Menge aller Teilmengen der Menge X.
(iii) ggT und kgV in $\mathbb{N}$.
(iv) Komposition von Abbildungen auf der Menge $\mathrm{Abb}(X)$ aller Abbildungen $X \to X$.

Bemerkung. Verknüpfungen auf kleinen Mengen kann man oft durch ihre Verknüpfungstafel angeben:

	$\cdots$	b	$\cdots$
$\vdots$		$\vdots$	
a	$\cdots$	ab	$\cdots$
$\vdots$		$\vdots$	

z.B.

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

1.2. Definition. Gegeben sei eine Verknüpfung auf einer Menge M. Ein Element $e \in M$ mit $ae = a$ (bzw. $ea = a$) für alle $a \in M$ heißt *rechtsneutral* (bzw. *linksneutral*). Ist e rechtsneutral und linksneutral, so nennt man e *neutral*.

Bemerkung. Ist $e \in M$ linksneutral und $f \in M$ rechtsneutral, so ist $e = ef = f$; insbesondere enthält M höchstens ein neutrales Element.

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

1.3. Definition. Gegeben sei eine Verknüpfung auf einer Menge M. Zwei Elemente $a, b \in M$ mit $ab = ba$ nennt man *vertauschbar*. Sind je zwei Elemente in M vertauschbar, so nennt man M *kommutativ* oder *abelsch*. Man nennt M eine *Halbgruppe*, falls alle $a, b, c \in M$ das *Assoziativgesetz* erfüllen: $(ab)c = a(bc)$. Eine Halbgruppe mit neutralem Element nennt man *Monoid*.

Beispiel.

(i) $(\mathbb{N}, +)$ ist abelsche Halbgruppe, $(\mathbb{N}_0, +)$ ist abelsches Monoid.
(ii) Für jede Menge X ist $\mathrm{Abb}(X)$ ein Monoid mit neutralem Element id_X; dabei ist $\mathrm{id}_X : X \to X,\ x \mapsto x$ die *identische Abbildung* auf X.
(iii) A sei eine nichtleere Menge und W die Menge aller endlichen Folgen $(a_1, \ldots, a_m)$ von Elementen $a_1, \ldots, a_m \in A$ $(m \in \mathbb{N})$. Für $(a_1, \ldots, a_m), (b_1, \ldots, b_n) \in W$ definiert man

$$(a_1, \ldots, a_m)(b_1, \ldots, b_n) := (a_1, \ldots, a_m, b_1, \ldots, b_n).$$

Auf diese Weise wird W zu einer Halbgruppe. Man nennt W die *freie Halbgruppe* über dem *Alphabet* A. Die Elemente in W nennt man auch *Wörter* in A, die in A *Buchstaben*. Statt $(a_1, \ldots, a_m)$ schreibt man kurz $a_1 \ldots a_m$. Nimmt man zu W das *leere* Wort $\varepsilon = ()$ hinzu, so erhält man das *freie Monoid* W_0 über A.

Bemerkung. Das neutrale Element bezeichnen wir oft mit 1 (oder 0, falls wir + als Bezeichnung für die Verknüpfung wählen).

1.4. Definition. Gegeben sei ein Monoid M und ein Element $a \in M$. Ein Element $b \in M$ mit $ab = 1$ (bzw. $ba = 1$) heißt *rechtsinvers* (bzw. *linksinvers*) zu a. Ist b rechtsinvers und linksinvers zu a, so nennt man b *invers* zu a. Man nennt a dann auch *rechtsinvertierbar* bzw. *linksinvertierbar* bzw. *invertierbar*.

Bemerkung. Ist $b \in M$ rechtsinvers zu a und $c \in M$ linksinvers zu a, so ist $b = 1b = (ca)b = c(ab) = c1 = c$; insbesondere besitzt a höchstens ein inverses Element. Dieses bezeichnet man mit a^{-1} (bzw. mit $-a$, falls man $+$ für die Verknüpfung schreibt). Mit a ist auch a^{-1} invertierbar, und $(a^{-1})^{-1} = a$. Sind $a, b \in M$ invertierbar, so auch ab, und $(ab)^{-1} = b^{-1}a^{-1}$.

1.5. Definition. In einer Halbgruppe H definiert man für $a \in H$ und $n \in \mathbb{N}$ die n-te *Potenz* von a durch $a^n := a \dots a$ (n Faktoren). Ist H Monoid, so definiert man außerdem $a^0 := 1$. Ist a invertierbar, so setzt man $a^{-n} := (a^{-1})^n$ für $n \in \mathbb{N}$.

Bemerkung. Wie üblich ist dann jeweils $a^m a^n = a^{m+n}$ und $(a^m)^n = a^{mn}$. Sind $a, b \in H$ vertauschbar, so ist auch $(ab)^n = a^n b^n$.

KAPITEL 2

Gruppen

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

Bemerkung. Daraus folgt leicht, daß e neutrales Element und jedes Element in G invertierbar ist. Die Anzahl der Elemente in G bezeichnet man als *Ordnung* $|G|$ von G.

Beispiel.

(i) $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ sind abelsche Gruppen, jedoch nicht $(\mathbb{N}, +)$.

(ii) $(\mathbb{Q} \setminus \{0\}, \cdot)$, $(\mathbb{R} \setminus \{0\}, \cdot)$, $(\mathbb{C} \setminus \{0\}, \cdot)$, $(]0, \infty[, \cdot)$ sind abelsche Gruppen, nicht jedoch $(\mathbb{Z} \setminus \{0\}, \cdot)$ oder $(\mathbb{Q}, \cdot)$.

(iii) $\{1\}$ ist Gruppe bzgl. $\cdot$, $\{0\}$ Gruppe bzgl. $+$.

(iv) Für jede Menge X bilden die Bijektionen $X \to X$ eine Gruppe $\mathrm{Sym}(X)$ bzgl. der Komposition von Abbildungen. Man nennt $\mathrm{Sym}(X)$ die *symmetrische Gruppe* auf X und ihre Elemente *Permutationen*. Ist $|X| = n < \infty$, so ist $|\mathrm{Sym}(X)| = n!$. Wir schreiben $\mathrm{Sym}(n) = \mathrm{Sym}(\{1, \ldots, n\})$ und sprechen von der symmetrischen Gruppe des Grades n. Die Elemente in $\mathrm{Sym}(n)$ schreiben wir in der Form $f = \left(\begin{smallmatrix} 1 & 2 & \cdots & n \\ f(1) & f(2) & \cdots & f(n) \end{smallmatrix}\right)$, z.B. $\left(\begin{smallmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{smallmatrix}\right)$. Dann ist $f^{-1} = \left(\begin{smallmatrix} f(1) & f(2) & \cdots & f(n) \\ 1 & 2 & \cdots & n \end{smallmatrix}\right)$.

(v) Für $n \in \mathbb{N}$ und jeden Körper K (stets kommutativ) bilden die invertierbaren $n \times n$-Matrizen mit Koeffizienten in K eine Gruppe bzgl. $\cdot$, die *allgemeine lineare Gruppe* $\mathrm{GL}(n, K)$ des Grades n über K.

(vi) Für jede nichtleere Familie von Gruppen $(G_i)_{i \in I}$ ist ihr *direktes Produkt*

$$\prod_{i \in I} G_i := \bigtimes_{i \in I} G_i = \{(g_i)_{i \in I} : g_i \in G_i \text{ für } i \in I\}$$

eine Gruppe, wenn man definiert: $(g_i)_{i \in I}(h_i)_{i \in I} := (g_i h_i)_{i \in I}$ für $(g_i)_{i \in I}, (h_i)_{i \in I} \in \prod_{i \in I} G_i$. Im Fall $I = \{1, \ldots, n\}$ für ein $n \in \mathbb{N}$ schreibt man auch $\bigtimes_{i=1}^{n} G_i = \prod_{i=1}^{n} G_i = G_1 \times \ldots \times G_n$ statt $\bigtimes_{i \in I} G_i$ und $(g_1, \ldots, g_n)$ statt $(g_i)_{i \in I}$.

2.2. Definition. Eine Abbildung f einer Gruppe G in eine Gruppe H nennt man

(i) *Homomorphismus*, falls $f(ab) = f(a)f(b)$ für $a, b \in G$ ist.

(ii) *Monomorphismus*, falls f ein injektiver Homomorphismus ist.

(iii) *Epimorphismus*, falls f ein surjektiver Homomorphismus ist.

(iv) *Isomorphismus*, falls f ein bijektiver Homomorphismus ist.

(v) *Endomorphismus*, falls f ein Homomorphismus und $G = H$ ist.

(vi) *Automorphismus*, falls f ein bijektiver Endomorphismus ist.

Bemerkung. Für jeden Homomorphismus $f : G \to H$ ist $f(1_G) = 1_H$ und $f(g^{-1}) = f(g)^{-1}$ $(g \in G)$. Für Gruppen G, H, K und Homomorphismen $f : G \to H$, $g : H \to K$ ist auch $g \circ f : G \to K$ ein Homomorphismus. Ist f ein Isomorphismus, so auch $f^{-1} : H \to G$. Wir setzen

$$\begin{array}{lcl} \mathrm{Hom}(G, H) & := & \{f : G \to H : f \text{ Homomorphismus}\} \\ \mathrm{End}(G) & := & \mathrm{Hom}(G, G) \\ \mathrm{Aut}(G) & := & \{f \in \mathrm{End}(G) : f \text{ bijektiv}\} \end{array}$$

Beispiel.

(i) Für $n \in \mathbb{Z}$ ist die Abbildung $(\mathbb{Z}, +) \to (\mathbb{Z}, +),\ z \mapsto nz$ ein Homomorphismus.

(ii) Für $n \in \mathbb{N}$ ist der *alternierende Charakter*

$$\operatorname{sgn} : \operatorname{Sym}(n) \to (\{1, -1\}, \cdot),\ g \mapsto \prod_{\substack{i,j \in \mathbb{N} \\ 1 \le i < j \le n}} \frac{g(i) - g(j)}{i - j}$$

ein Homomorphismus. Für $g \in \operatorname{Sym}(n)$ nennt man $\operatorname{sgn}(g)$ das *Vorzeichen* oder *Signum* von g. Ist $\operatorname{sgn}(g) = 1$, so nennt man g *gerade*, sonst *ungerade*.

(iii) Für $n \in \mathbb{N}$ und jeden Körper K ist die Determinante $\det : \operatorname{GL}(n, K) \to (K \setminus \{0\}, \cdot)$ ein Homomorphismus.

(iv) Für jede Gruppe G und jedes Element $a \in G$ ist die Abbildung $f_a : G \to G,\ g \mapsto aga^{-1}$ ein Automorphismus von G. Man nennt f_a den von a induzierten *inneren Automorphismus* von G.

2.3. Definition. Man nennt zwei Gruppen G, H *isomorph* und schreibt $G \cong H$, falls es einen Isomorphismus $f : G \to H$ gibt.

Bemerkung. Die Isomorphie von Gruppen ist eine Äquivalenzrelation, d.h. es gilt:

(i) $G \cong G$ (Reflexivität).

(ii) $G \cong H \ \Rightarrow\ H \cong G$ (Symmetrie).

(iii) $G \cong H \ \wedge\ H \cong K \ \Rightarrow\ G \cong K$ (Transitivität).

Beispiel. Für jeden Körper K und jeden K-Vektorraum V bilden die linearen Bijektionen $f : V \to V$ bzgl. der Komposition von Abbildungen eine Gruppe $\operatorname{GL}(V)$, die *allgemeine lineare Gruppe* von V. Im Fall $\dim V = n < \infty$ ist bekanntlich $\operatorname{GL}(V) \cong \operatorname{GL}(n, K)$.

2.4. Definition. Eine nichtleere Teilmenge H einer Gruppe G mit $ab^{-1} \in H$ für $a, b \in H$ nennt man eine *Untergruppe* von G.

Bemerkung. In diesem Fall ist $1_G \in H$, und H wird mit der entsprechend eingeschränkten Verknüpfung selbst zu einer Gruppe. Wir schreiben $H \le G$ (bzw. $H < G$ im Fall $H \ne G$).

Beispiel.

(i) In jeder Gruppe G sind $\{1\}$ und G Untergruppen. Wir schreiben 1 statt $\{1\}$ und nennen 1 die *triviale* Untergruppe von G. Untergruppen H von G mit $H \ne G$ nennen wir *echte* Untergruppen von G. Eine echte Untergruppe M von G nennt man *maximale* Untergruppe von G, falls keine Untergruppe H von G mit $M < H < G$ existiert. Eine nichttriviale Untergruppe N von G nennt man *minimale* Untergruppe von G, falls keine Untergruppe H von G mit $1 < H < N$ existiert. Es gibt Gruppen, die weder minimale noch maximale Untergruppen enthalten.

(ii) Für jede nichtleere Familie $(H_i)_{i \in I}$ von Untergruppen einer Gruppe G ist $\bigcap_{i \in I} H_i \le G$. Insbesondere ist für jede Teilmenge X von G der Durchschnitt aller Untergruppen H von G mit $X \subseteq H$ eine Untergruppe $\langle X \rangle$ von G. Man nennt $\langle X \rangle$ die von X *erzeugte* Untergruppe von G. Sie besteht aus allen Elementen der Form

$$x_1^{\varepsilon_1} \dots x_n^{\varepsilon_n} \qquad \text{mit } n \in \mathbb{N}_0,\ x_1, \dots, x_n \in X,\ \varepsilon_1, \dots, \varepsilon_n \in \{\pm 1\}.$$

(Im Fall $n = 0$ muß man das Produkt als 1 interpretieren). Im Fall $X = \{a_1, \dots, a_n\}$ schreibt man auch $\langle a_1, \dots, a_n \rangle$ statt $\langle X \rangle$. Ist $G = \langle X \rangle$, so nennt man X ein *Erzeugendensystem* von G. Besitzt G ein endliches Erzeugendensystem, so nennt man G *endlich erzeugt*. Ist $G = \langle a \rangle$ für ein $a \in G$, so nennt man G *zyklisch*.

(iii) Für jede nichtleere Familie $(G_i)_{i \in I}$ von Gruppen bilden die Elemente $(g_i)_{i \in I} \in \prod_{i \in I} G_i$ mit $|\{i \in I : g_i \ne 1\}| < \infty$ eine Untergruppe $\coprod_{i \in I} G_i$ von $\prod_{i \in I} G_i$, die man das *eingeschränkte direkte Produkt* von $(G_i)_{i \in I}$ nennt.

(iv) Für jede Gruppe G ist $\operatorname{Aut}(G) \le \operatorname{Sym}(G)$. Man nennt $\operatorname{Aut}(G)$ die *Automorphismengruppe* von G.

(v) $(\mathbb{Z}, +) \le (\mathbb{Q}, +) \le (\mathbb{R}, +) \le (\mathbb{C}, +)$, $(\mathbb{Q} \setminus \{0\}, \cdot) \le (\mathbb{R} \setminus \{0\}, \cdot) \le (\mathbb{C} \setminus \{0\}, \cdot)$.

(vi) Für jeden Homomorphismus von Gruppen $f : G \to H$ und beliebige Untergruppen $U \leq G,\ V \leq H$ ist $f(U) \leq H$ und $f^{-1}(V) \leq G$; insbesondere ist $\mathrm{Bild}(f) := f(G) \leq H$ und $\mathrm{Ker}(f) := f^{-1}(\{1_H\}) = \{g \in G : f(g) = 1\} \leq G$. Man nennt $\mathrm{Bild}(f)$ das *Bild* und $\mathrm{Ker}(f)$ den *Kern* von f. Genau dann ist f injektiv, wenn $\mathrm{Ker}(f) = \{1_G\}$ ist.

(vii) Für $n \in \mathbb{N}$ nennt man den Kern $\mathrm{Alt}(n)$ von $\mathrm{sgn} : \mathrm{Sym}(n) \to \{\pm 1\}$ die *alternierende Gruppe* des Grades n, und für jeden Körper K nennt man den Kern $\mathrm{SL}(n, K)$ von $\det : \mathrm{GL}(n, K) \to K \setminus \{0\}$ die *spezielle lineare Gruppe* des Grades n über K.
Für $n \in \mathbb{N}_0$ ist das Bild $n\mathbb{Z}$ von $\mathbb{Z} \to \mathbb{Z},\ z \mapsto nz$ eine Untergruppe von $\mathbb{Z}$. Man zeigt leicht, daß man auf diese Weise alle Untergruppen von $\mathbb{Z}$ erhält.

(viii) Ist G eine Gruppe und f_a der von $a \in G$ induzierte innere Automorphismus von G, so ist die Abbildung $F : G \to \mathrm{Aut}(G), a \mapsto f_a$ ein Homomorphismus. Sein Bild $\mathrm{Inn}(G)$ ist eine Untergruppe von $\mathrm{Aut}(G)$, sein Kern $Z(G)$ eine Untergruppe von G. Offensichtlich ist $Z(G) = \{a \in G : aga^{-1} = g \text{ für } g \in G\} = \{a \in G : ag = ga \text{ für } g \in G\}$. Man nennt $\mathrm{Inn}(G)$ die *innere Automorphismengruppe* und $Z(G)$ das *Zentrum* von G.

2.5. Definition. Für Teilmengen X, Y einer Gruppe G setzt man $XY := \{xy : x \in X,\ y \in Y\}$ und $X^{-1} := \{x^{-1} : x \in X\}$.

Bemerkung. Dann ist $(X^{-1})^{-1} = X,\ (XY)^{-1} = Y^{-1}X^{-1}$ und $X(YZ) = (XY)Z$ für $X, Y, Z \leq G$, und es gilt: $X \leq G \ \Leftrightarrow\ X \neq \emptyset$ und $XX^{-1} \subseteq X$.

Satz. *Für Untergruppen U, V, W einer Gruppe G gilt:*

(i) $U \cup V \leq G \ \Leftrightarrow\ U \subseteq V$ *oder* $V \subseteq U$.

(ii) $UV \leq G \ \Leftrightarrow\ UV = VU$.

(iii) $U \subseteq W \ \Rightarrow\ UV \cap W = U(V \cap W)$ *(Dedekind-Identität).*

Beweis. Algebra. □

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

(i) ${}^1\omega = \omega$.

(ii) ${}^a({}^b\omega) = {}^{ab}\omega$ für $a, b \in G,\ \omega \in \Omega$.

Man sagt auch: „G operiert auf Ω“ oder „Ω ist eine G-Menge“.

Bemerkung.

(i) In diesem Fall erhält man eine Äquivalenzrelation $\sim$ auf Ω, wenn man für $\alpha, \beta \in \Omega$ definiert:

$$\alpha \sim \beta \ :\Leftrightarrow\ {}^g\alpha = \beta \quad \text{für ein } g \in G.$$

Die Äquivalenzklassen bzgl. $\sim$ nennt man die *Bahnen* (orbits) von Ω unter G. Für $\omega \in \Omega$ bezeichne $\mathrm{Orb}_G(\omega) := \{{}^g\omega : g \in G\}$ die Bahn von ω unter G. Man bezeichnet $|\mathrm{Orb}_G(\omega)|$ auch als *Länge* der Bahn von ω. Gibt es nur eine einzige Bahn, so nennt man die Operation *transitiv*.

(ii) Für jede Operation einer Gruppe G auf einer nichtleeren Menge Ω und jedes Element $g \in G$ ist die Abbildung $\tau_g : \Omega \to \Omega,\ \omega \mapsto {}^g\omega$ bijektiv. Ferner ist die Abbildung $\tau : G \to \mathrm{Sym}(\Omega),\ g \mapsto \tau_g$ ein Homomorphismus. Man bezeichnet $\mathrm{Ker}(\tau)$ auch als *Kern* der Operation. Im Fall $\mathrm{Ker}(\tau) = 1$ (bzw. $\mathrm{Ker}(\tau) = G$) nennt man die Operation *treu* (bzw. *trivial*).

(iii) Umgekehrt liefert jeder Homomorphismus ρ einer Gruppe G in eine symmetrische Gruppe $\mathrm{Sym}(\Omega)$ eine Operation von G auf Ω, indem man für $g \in G$ und $\omega \in \Omega$ definiert: ${}^g\omega := (\rho(g))(\omega)$.

(iv) Für jede Operation einer Gruppe G auf einer nichtleeren Menge Ω und jedes Element $\omega \in \Omega$ ist der *Stabilisator* $\mathrm{Stb}_G(\omega) := \{g \in G : {}^g\omega = \omega\}$ von ω in G eine Untergruppe von G. Auf diese Weise verschafft man sich häufig Untergruppen einer vorgegebenen Gruppe. Für $g \in G$ und $\omega \in \Omega$ gilt: $\mathrm{Stb}_G({}^g\omega) = g\,\mathrm{Stb}_G(\omega)g^{-1}$. Sind $(\Delta_i)_{i \in I}$ die Bahnen von Ω unter G, so hat man die triviale, aber nützliche *Bahnengleichung*:

$$|\Omega| = \sum_{i \in I} |\Delta_i|.$$

Beispiel.

(i) Jede Untergruppe H einer Gruppe G operiert auf G durch Linksmultiplikation: ${}^h g := hg$ ($h \in H,\ g \in G$). In diesem Fall ist $\mathrm{Orb}_H(g) = \{hg : h \in H\} =: Hg$. Man bezeichnet Hg als Rechtsnebenklasse von g nach H und setzt $H\backslash G := \{Hg : g \in G\}$. Ferner bezeichnet man $|G : H| := |H\backslash G|$ als *Index* von H nach G. Für $g \in G$ ist die Abbildung $H \to Hg,\ h \mapsto hg$ bijektiv; insbesondere ist $|Hg| = |H|$. Die Bahnengleichung liefert also:

$$|G| = |G : H| \cdot |H| \qquad \text{(Satz von Lagrange).}$$

Im Fall $|G| < \infty$ sind insbesondere $|H|$ und $|G : H|$ Teiler von $|G|$.

(ii) Analog operiert jede Untergruppe H einer Gruppe G auf G durch Rechtsmultiplikation: ${}^h g := gh^{-1}$ ($h \in H,\ g \in G$). In diesem Fall erhält man als Bahnen die *Linksnebenklassen* $gH := \{gh : h \in H\}$ und setzt $G/H := \{gH : g \in G\}$. Die Abbildung $G/H \to H\backslash G,\ gH \to Hg^{-1} = (gH)^{-1}$ ist bijektiv; insbesondere ist $|G/H| = |G : H|$.

(iii) Jede Gruppe G operiert auf $\mathcal{P}(G)$ durch *Konjugation*: ${}^g X := gXg^{-1} = \{gxg^{-1} : x \in X\}$ ($g \in G,\ X \subseteq G$). Man nennt $\mathrm{Orb}_G(X) = \{gXg^{-1} : g \in G\}$ die *Konjugationsklasse* von X in G. Teilmengen in der gleichen Bahn nennt man *konjugiert* (unter G). Für $X \subseteq G$ nennt man $\mathrm{Stb}_G(X) = \{g \in G : gXg^{-1} = X\} =: N_G(X)$ den *Normalisator* von X in G. Im Fall $X \leq G$ ist $X \leq N_G(X)$ wegen $xXx^{-1} \subseteq X = x\underbrace{x^{-1}Xx}_{\subseteq X}x^{-1} \subseteq xXx^{-1}$ für $x \in X$.

(iv) Jede Gruppe G operiert auf sich selbst durch *Konjugation*: ${}^g x = gxg^{-1}$ ($g, x \in G$). Man nennt $\mathrm{Orb}_G(x) = \{gxg^{-1} : g \in G\}$ die *Konjugationsklasse* von $x \in G$ in G. Elemente in der gleichen Konjugationsklasse nennt man auch *konjugiert* (in G). Die Anzahl der Konjugationsklassen von G bezeichnet man als *Klassenzahl* von G. Für $x \in G$ nennt man $\mathrm{Stb}_G(x) = \{g \in G : gxg^{-1} = x\} = \{g \in G : gx = xg\} =: C_G(x)$ den *Zentralisator* von x in G. Für $X \subseteq G$ nennt man $C_G(X) := \bigcap_{x \in X} C_G(x) = \{g \in G : gx = xg \text{ für } x \in X\}$ den *Zentralisator* von X in G. Offenbar ist $C_G(X) \leq N_G(X)$ und $C_G(G) = Z(G)$.

(v) Jede Gruppe G operiert auf G/H für jede Untergruppe H von G durch Linksmultiplikation: ${}^g(xH) = gxH$ ($g, x \in G$). Diese Operation ist transitiv mit Kern

$$\begin{aligned}
\{g \in G : gxH = xH \text{ für } x \in G\} &= \{g \in G : x^{-1}gxH = H \text{ für } x \in G\} \\
&= \{g \in G : x^{-1}gx \in H \text{ für } x \in G\} \\
&= \{g \in G : g \in xHx^{-1} \text{ für } x \in G\} \\
&= \bigcap_{x \in G} xHx^{-1} =: \mathrm{Core}_G(H).
\end{aligned}$$

Man bezeichnet $\mathrm{Core}_G(H)$ als *Kern* von H in G.

(vi) Für Untergruppen H, K einer Gruppe G operiert $H \times K$ auf G: ${}^{(h,k)}g := hgk^{-1}$ ($g \in G,\ h \in H,\ k \in K$). Die Bahn eines Elements $g \in G$ ist dann die *Doppelnebenklasse* $HgK = \{hgk : h \in H,\ k \in K\}$. Wir setzen $H\backslash G/K = \{HgK : g \in G\}$. Im allgemeinen sind weder $|HgK|$ noch $|H\backslash G/K|$ Teiler von $|G|$ (im Fall $|G| < \infty$). Für $h \in H$ und $g \in G$ ist $hgK \subseteq HgK$. Für $h, h' \in H$ und $g \in G$ gilt ferner:

$$\begin{aligned}
hgK = h'gK &\Leftrightarrow g^{-1}h^{-1}h'gK = K \Leftrightarrow g^{-1}h^{-1}h'g \in K \\
&\Leftrightarrow h^{-1}h' \in gKg^{-1} \Leftrightarrow h^{-1}h' \in H \cap gKg^{-1} \\
&\Leftrightarrow h^{-1}h'(H \cap gKg^{-1}) = H \cap gKg^{-1} \\
&\Leftrightarrow h'(H \cap gKg^{-1}) = h(H \cap gKg^{-1}).
\end{aligned}$$

Daher ist jede Doppelklasse HgK disjunkte Vereinigung von $|H : H \cap gKg^{-1}|$ Linksnebenklassen nach K und analog disjunkte Vereinigung von $|K : K \cap g^{-1}Hg|$ Rechtsnebenklassen nach H; insbesondere ist $|HgK| = |H : H \cap gKg^{-1}| \cdot |K| = |K : K \cap g^{-1}Hg| \cdot |H|$.

2.7. Satz. *Für Untergruppen H, K einer Gruppe G gilt:*

(i) $K \leq H \Rightarrow |G:K| = |G:H| \cdot |H:K|$ *(Lagrange). Insbesondere sind* $|G:H|$ *und* $|H:K|$ *im Fall* $|G:K| < \infty$ *Teiler von* $|G:K|$.
(ii) HK *ist disjunkte Vereinigung von* $|H : H \cap K|$ *Linksnebenklassen nach* K *und disjunkte Vereinigung von* $|K : H \cap K|$ *Rechtsnebenklassen nach* H.
(iii) $|HK| = |H : H \cap K| \cdot |K| = |K : H \cap K| \cdot |H|$.
(iv) $|H : H \cap K| \leq |G : K|$.
(v) $|H : H \cap K| = |G : K| < \infty \Rightarrow G = HK = KH$.
(vi) $|G : H \cap K| \leq |G : H| \cdot |G : K|$.
(vii) $|G : H \cap K| = |G : H| \cdot |G : K| < \infty \Rightarrow G = HK = KH$.
(viii) $|G : H|, |G : K|$ *endlich und teilerfremd* $\Rightarrow |G : H \cap K| = |G : H| \cdot |G : K|$.

Beweis.

(i) Wir schreiben $G = \dot{\bigcup}_{r \in R} rH$ und $H = \dot{\bigcup}_{s \in S} sK$. Dann ist $G = \dot{\bigcup}_{r \in R,\ s \in S} rsK$, also $|G : K| = |R| \cdot |S| = |G : H| \cdot |H : K|$.
(ii),(iii) Setze $g := 1$ in Beispiel 2.6(vi).
(iv) folgt aus (ii) wegen $HK \subseteq G$.
(v) Im Fall $|H : H \cap K| = |G : K| < \infty$ folgt aus (ii): $G = HK$. Mit Satz 2.5(ii) ergibt sich $G = KH$.
(vi) Nach (i) und (iv) ist $|G : H \cap K| = |G : H| \cdot |H : H \cap K| \leq |G : H| \cdot |G : K|$.
(vii) Im Fall $|G : H \cap K| = |G : H| \cdot |G : K| < \infty$ zeigt die Argumentation in (vi): $|H : H \cap K| = |G : K|$. Mit (v) folgt $G = HK = KH$.
(viii) Nach (i) und (iv) ist $|G : H| \cdot |H : H \cap K| = |G : H \cap K| = |G : K| \cdot |K : H \cap K| \leq |G : K| \cdot |G : H| < \infty$. Sind $|G : H|$ und $|G : K|$ teilerfremd, so ist $|G : K|$ Teiler von $|H : H \cap K|$. Aus (iv) folgt daher $|G : K| = |H : H \cap K|$, und man hat $|G : H \cap K| = |G : H| \cdot |G : K|$.

□

2.8. Satz. *Für jede Operation einer Gruppe* G *auf einer nichtleeren Menge* Ω *und jedes* $\omega \in \Omega$ *ist die Abbildung* $G/\operatorname{Stb}_G(\omega) \to \operatorname{Orb}_G(\omega),\ g \operatorname{Stb}_G(\omega) \mapsto {}^g\omega$ *wohldefiniert und bijektiv; insbesondere ist* $|\operatorname{Orb}_G(\omega)| = |G : \operatorname{Stb}_G(\omega)|$, *und dies teilt* $|G|$ *im Fall* $|G| < \infty$.

Beweis. Algebra. □

Bemerkung. Sind Δ_i $(i \in I)$ die Bahnen von Ω unter G und wählt man aus jedem Δ_i ein Element ω_i, so kann man also die Bahnengleichung auch in der Form

$$|\Omega| = \sum_{i \in I} |G : \operatorname{Stb}_G(\omega_i)|$$

schreiben.

Beispiel. Jede Teilmenge X einer Gruppe G besitzt genau $|G : N_G(X)|$ Konjugierte in G. Analog enthält die Konjugationsklasse eines Elementes $x \in G$ genau $|G : C_G(x)|$ Elemente. Die Bahnengleichung wird in diesem Fall zur *Klassengleichung*:

$$|G| = \sum_{i \in I} |G : C_G(x_i)|.$$

Dabei ist $(x_i)_{i \in I}$ ein Repräsentantensystem für die Konjugationsklassen von G.

2.9. Definition. Für jedes Element g einer Gruppe G bezeichnet man $|\langle g \rangle|$ als *Ordnung* von g. Elemente der Ordnung 2 nennt man *Involutionen*. Ist $|\langle g \rangle| < \infty$ und π eine Menge von Primzahlen, die alle Primteiler von $|\langle g \rangle|$ enthält, so nennt man g ein π*-Element*. Ist jedes Element in G ein π-Element, so nennt man G eine π*-Gruppe*. Besteht π aus genau einer Primzahl p, so spricht man kürzer von p*-Elementen* und p*-Gruppen*.

Bemerkung.

(i) In der Algebra wurde gezeigt, daß für ein Element g unendlicher Ordnung die Potenzen g^n ($n \in \mathbb{Z}$) paarweise verschieden sind. Für ein Element g der endlichen Ordnung k und für $m, n \in \mathbb{Z}$ gilt dagegen: $g^m = g^n \Leftrightarrow m \equiv n \pmod{k}$ ($:\Leftrightarrow$ k teilt $m-n$). Insbesondere gilt:

$$g^m = 1 \Leftrightarrow m = 0 \pmod{k} \Leftrightarrow k \text{ teilt } m \Leftrightarrow: k \mid m.$$

Daher gilt stets: $|\langle g\rangle| = \inf\{n \in \mathbb{N} : g^n = 1\}$, und im Fall $|G| < \infty$ folgt der *Satz von Fermat*:

$$g^{|G|} = 1.$$

Ferner folgt leicht, daß g^l für $l \in \mathbb{Z}$ die Ordnung $\frac{k}{\mathrm{ggT}(k,l)}$ hat.

(ii) Haben alle Element in G außer 1 unendliche Ordnung, so nennt man G *torsionsfrei*. Haben alle Elemente in G endliche Ordnung, so nennt man G eine *Torsionsgruppe*. Sind zusätzlich die Ordnungen der Elemente in G beschränkt, so nennt man G *periodisch*. In diesem Fall bezeichnet man die kleinste natürliche Zahl e mit $g^e = 1$ für alle $g \in G$ als *Exponenten* von G und schreibt $e = \exp(G)$.

(iii) In einer Gruppe G seien vertauschbare Elemente g, h der endlichen Ordnungen k bzw. l gegeben. Dann ist $(gh)^{kl} = g^{kl}h^{kl} = 1^l 1^k = 1$, also ist $|\langle gh\rangle| \mid kl$. Sei jetzt zusätzlich $\mathrm{ggT}(k,l) = 1$. Ist $n \in \mathbb{Z}$ mit $1 = (gh)^n = g^n h^n$, so ist $g^n = h^{-n} \in \langle g\rangle \cap \langle h\rangle$. Wegen $|\langle g\rangle \cap \langle h\rangle| \mid |\langle g\rangle|$ und $|\langle g\rangle \cap \langle h\rangle| \mid |\langle h\rangle|$ ist aber $|\langle g\rangle \cap \langle h\rangle| \mid \mathrm{ggT}(k,l) = 1$, also $g^n = 1 = h^{-n}$ und damit $k \mid n$, $l \mid n$. Insgesamt ist dann $kl \mid n$, d.h. $|\langle gh\rangle| = |\langle g\rangle| \cdot |\langle h\rangle|$. Dieses Ergebnis läßt sich durch Induktion auf Produkte von endlich vielen paarweise vertauschbaren Elementen endlicher paarweise teilerfremder Ordnungen ausdehnen.

(iv) Gegeben sei ein Element g der endlichen Ordnung k in einer Gruppe G. Die eindeutige Primfaktorzerlegung von k sei $k = p_1^{a_1} \dots p_r^{a_r}$. Dann sind $q_1 := k/p_1^{a_1}, \dots, q_r := k/p_r^{a_r}$ teilerfremd. Daher existieren $b_1, \dots, b_r \in \mathbb{Z}$ mit $b_1 q_1 + \dots + b_r q_r = 1$. Folglich ist $g = g^1 = g^{b_1 q_1 + \dots + b_r q_r} = g^{b_1 q_1} \dots g^{b_r q_r}$. Für $i = 1, \dots, r$ ist $(g^{b_i q_i})^{p_i^{a_i}} = g^{k b_i} = 1^{b_i} = 1$, also $|\langle g^{b_i q_i}\rangle| \mid p_i^{a_i}$. Wegen $|\langle g\rangle| = k = p_1^{a_1} \dots p_r^{a_r}$ folgt aus (iii) sogar: $|\langle g^{b_i q_i}\rangle| = p_i^{a_i}$. Daher läßt sich g als Produkt von Elementen $g_1, \dots, g_r$ schreiben, die die Ordnungen $p_1^{a_1}, \dots, p_r^{a_r}$ haben und Potenzen von g sind; insbesondere sind $g_1, \dots, g_r$ paarweise vertauschbar. Diese Schreibweise ist in folgendem Sinne eindeutig: Ist auch $g = h_1 \dots h_r$ mit paarweise vertauschbaren Elementen $h_1, \dots, h_r \in G$ der Ordnungen $p_1^{a_1}, \dots, p_r^{a_r}$, so ist $g_i = h_i$ für $i = 1, \dots, r$. Die Elemente $h_1, \dots, h_r$ sind nämlich mit g und daher mit g_i für $i = 1, \dots, r$ vertauschbar. Aus $g_1 \dots g_r = h_1 \dots h_r$ folgt also: $g_1^{-1} h_1 = g_2 \dots g_r h_r^{-1} \dots h_2^{-1} = g_2 h_2^{-1} \dots g_r h_r^{-1}$, wobei $|\langle g_1^{-1} h_1\rangle| \mid p_1^{2a_1}$ und $|\langle g_2 h_2^{-1} \dots g_r h_r^{-1}\rangle| \mid p_2^{2a_2} \dots p_r^{2a_r}$ nach (iii). Wegen $\mathrm{ggT}(p_1^{2a_1}, p_2^{2a_2} \dots p_r^{2a_r}) = 1$ folgt also: $g_1^{-1} h_1 = 1$, d.h. $h_1 = g_1$. Analog ist $g_i = h_i$ für $i = 2, \dots, r$. Man nennt die Zerlegung $g = g_1 \dots g_r$ auch die *Primfaktorzerlegung* von g, und für $i = 1, \dots, r$ nennt man g_i auch den *p_i-Faktor* von g. Häufige Schreibweise: g_{p_i} statt g_i. Allgemeiner definiert man für jede Primzahlenmenge π den *π-Faktor* g_π von g durch $g_\pi := \prod_{p \mid k,\ p \in \pi} g_p$.

2.10. Satz (Frattini-Argument)**.** *Gegeben sei eine transitive Operation einer Gruppe G auf einer nichtleeren Menge Ω. Operiert eine Untergruppe H von G auch transitiv auf Ω, so ist $G = \mathrm{Stb}_G(\omega) H$ für $\omega \in \Omega$.*

Beweis. Sei H transitiv auf Ω und $\omega \in \Omega$. Für $g \in G$ existiert dann 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 ist $G = H\,\mathrm{Stb}_G(\omega) = \mathrm{Stb}_G(\omega) H$. □

2.11. Satz (Burnsides Lemma)**.** *Gegeben sei eine Operation einer Gruppe G auf einer nichtleeren Menge Ω. Die Anzahl der Bahnen von G auf Ω sei n, und für $g \in G$ sei $f(g)$ die Anzahl der* Fixpunkte *von g auf Ω, d.h. $f(g) = |\{\omega \in \Omega : {}^g\omega = \omega\}|$. Dann gilt: $|G| n = \sum_{g \in G} f(g)$.*

Beweis. Offenbar ist $\sum_{g \in G} f(g) = |\{(g, \omega) \in G \times \Omega : {}^g\omega = \omega\}| = \sum_{\omega \in \Omega} |\,\mathrm{Stb}_G(\omega)|$. Auf jeder Bahn ist $|\,\mathrm{Stb}_G(\omega)|$ konstant nach Bemerkung 2.6(iv), und die Bahn eines $\omega \in \Omega$ enthält genau $|G : \mathrm{Stb}_G(\omega)|$ Elemente. Mit Lagrange ergibt sich: $\sum_{\omega \in \Omega} |\,\mathrm{Stb}_G(\omega)| = n|G|$. □

KAPITEL 3

Normalteiler und Faktorgruppen

3.1. Satz. *Für eine Untergruppe N einer Gruppe G sind äquivalent:*

(1) $gNg^{-1} \subseteq N$ *für* $g \in G$.
(2) $gNg^{-1} = N$ *für* $g \in G$.
(3) $gN = Ng$ *für* $g \in G$.
(4) G/N *ist Gruppe, wenn man definiert:* $(gN)(hN) := ghN$ *für* $g, h \in G$.
(5) *Es existieren eine Gruppe* H *und ein Homomorphismus* $f : G \to H$ *mit* $N = \mathrm{Ker}(f)$.

Beweis. Algebra. □

Definition. Gegebenenfalls nennt man N eine *normale* Untergruppe oder einen *Normalteiler* von G, und man schreibt: $N \trianglelefteq G$ (bzw. $N \triangleleft G$ im Fall $N \neq G$). Man bezeichnet G/N $(= N\backslash G)$ als *Faktorgruppe* von G nach N. Statt $gN = hN$ schreibt man auch: $g \equiv h \pmod N$.

Bemerkung. Für jeden Normalteiler N von G ist die Abbildung $f : G \to G/N,\ g \mapsto gN$ ein Homomorphismus, den man den *kanonischen* oder den *natürlichen* Epimorphismus von G nach G/N nennt. Daher ist $1_{G/N} = f(1_G) = 1_G N = N$ und $(gN)^{-1} = g^{-1}N$ für $g \in G$.

Beispiel.

(i) Für jede Gruppe G sind 1 und G normal in G. Ist $G \neq 1$ und sind 1 und G die einzigen Normalteiler von G, so nennt man G *einfach*. Nach dem Satz von Lagrange sind z.B. Gruppen von Primzahlordnung stets einfach und zyklisch. Die Bestimmung aller endlichen einfachen Gruppen war eines der bisher größten Projekte in der Mathematik. Beteiligt waren ca. 50–100 Mathematiker. Die entsprechenden Arbeiten haben einen Umfang von ca. 10000 Seiten. Das Projekt wurde ca. 1980 erfolgreich abgeschlossen. Zwei Bücher von D. Gorenstein informieren über die wichtigsten Schritte.

(ii) In jeder Gruppe G ist jede Untergruppe von $Z(G)$ normal wegen (3); insbesondere ist $Z(G) \trianglelefteq G$. Speziell in abelschen Gruppen ist jede Untergruppe normal.

(iii) Ist G Gruppe und $H \leq G$ mit $|G : H| = 2$, so ist $H \trianglelefteq G$.

(iv) Für jede Untergruppe H einer Gruppe G ist nach Definition stets $H \trianglelefteq N_G(H)$.

(v) Für jede Teilmenge X einer Gruppe ist $C_G(X) \trianglelefteq N_G(X)$; denn $C_G(X)$ ist der Kern der durch ${}^g x := gxg^{-1}$ für $g \in N_G(X)$ und $x \in X$ definierten Operation von $N_G(X)$ auf X.

(vi) Für jede Untergruppe H einer Gruppe G ist $\mathrm{Core}_G(H) = \bigcap_{g\in G} gHg^{-1}$ als Kern einer Operation normal in G. Offenbar ist $\mathrm{Core}_G(H) \subseteq H$, und für jeden Normalteiler N von G mit $N \subseteq H$ gilt:

$$N = \bigcap_{g\in G} gNg^{-1} \subseteq \bigcap_{g\in G} gHg^{-1} = \mathrm{Core}_G(H).$$

Daher ist $\mathrm{Core}_G(H)$ der „größte“ in H enthaltene Normalteiler in G. Analog ist

$$\langle gHg^{-1} : g \in G\rangle := \langle \bigcup_{g\in G} gHg^{-1}\rangle \trianglelefteq G;$$

für $X := \bigcup_{g\in G} gHg^{-1}$ und $x \in G$ ist nämlich:

$$xXx^{-1} = \bigcup_{g\in G} xgHg^{-1}x^{-1} = \bigcup_{y\in G} yHy^{-1} = X,$$

also auch $x\langle X\rangle x^{-1} = \langle xXx^{-1}\rangle = \langle X\rangle$. Man nennt $\langle gHg^{-1} : g \in G\rangle$ den *normalen Abschluß* von H in G. Ist $N \trianglelefteq G$ mit $H \subseteq N$, so ist auch $gHg^{-1} \subseteq gNg^{-1} = N$ für $g \in G$, also $\langle gHg^{-1} : g \in G\rangle \subseteq N$. Daher ist $\langle gHg^{-1} : g \in G\rangle$ der „kleinste“ Normalteiler von G, der H enthält.

(vii) Für $n \in \mathbb{N}$ und jeden Körper K ist $\mathrm{SL}(n,K) = \mathrm{Ker}(\det) \trianglelefteq \mathrm{GL}(n,K)$ und $\mathrm{Alt}(n) = \mathrm{Ker}(\mathrm{sgn}) \trianglelefteq \mathrm{Sym}(n)$.

(viii) Für jeden Homomorphismus von Gruppen $f : G \to H$ und jeden Normalteiler N von H ist $f^{-1}(N) \trianglelefteq G$. Umgekehrt gilt für jeden Normalteiler M von G $f(M) \trianglelefteq f(G)$, aber nicht notwendig $f(M) \trianglelefteq H$.

(ix) Ist $G = \mathrm{Sym}(3)$ und

$$H = \langle \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \rangle = \{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \},$$

so ist $H \not\trianglelefteq G$ wegen

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & \cdot & \cdot \end{pmatrix} \notin H.$$

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

(xi) Für jede Gruppe G, jeden Automorphismus α von G und beliebige $a, b \in G$ gilt:

$$\alpha(a\alpha^{-1}(b)a^{-1}) = \alpha(a)\alpha(\alpha^{-1}(b))\alpha(a)^{-1} = \alpha(a)b\alpha(a)^{-1}.$$

Bezeichnet man den von einem Element $g \in G$ induzierten inneren Automorphismus von G mit f_g, so ist also $\alpha \circ f_a \circ \alpha^{-1} = f_{\alpha(a)} \in \mathrm{Inn}(G)$. Insbesondere ist $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$. Man nennt die Faktorgruppe $\mathrm{Aut}(G)/\mathrm{Inn}(G) =: \mathrm{Out}(G)$ die *äußere Automorphismengruppe* von G.

3.2. Satz (Homomorphiesatz)**.** *Für jeden Homomorphismus von Gruppen $f : G \to H$ ist die Abbildung $F : G/\mathrm{Ker}(f) \to f(G)$, $g\,\mathrm{Ker}(f) \mapsto f(g)$ wohldefiniert und ein Isomorphismus; insbesondere ist $G/\mathrm{Ker}(f) \cong f(G)$ und $|G/\mathrm{Ker}(f)| = |f(G)|$.*

Beweis. Algebra. □

Beispiel. Als leichte Anwendung erhält man:

(i) Für jede zyklische Gruppe $G = \langle g\rangle = \{g^n : n \in \mathbb{Z}\}$ ist die Abbildung $f : \mathbb{Z} \to G$, $z \mapsto g^z$ ein Epimorphismus. Im Fall $\mathrm{Ker}(f) = 0$ ist also $G \cong \mathbb{Z}$, und im Fall $\mathrm{Ker}(f) = n\mathbb{Z}$ für ein $n \in \mathbb{N}$ ist $G \cong \mathbb{Z}/n\mathbb{Z}$.

(ii) Für jede Untergruppe H einer Gruppe G induziert nach Beispiel 2.6(v) die Operation von G auf G/H durch Linksmultiplikation einen Homomorphismus $f : G \to \mathrm{Sym}(G/H)$ mit Kern $\mathrm{Core}_G(H)$ (vgl. 2.6(ii)). Insbesondere ist $G/\mathrm{Core}_G(H) \cong f(G) \leq \mathrm{Sym}(G/H)$. Im Fall $|G : H| < \infty$ ist also

$$|G : H| \;\big|\; |G : \mathrm{Core}_G(H)| = |f(G)| \;\big|\; |\mathrm{Sym}(G/H)| = |G : H|! < \infty.$$

Im Fall $H = 1$ ist $\mathrm{Core}_G(H) = 1$, d.h. G ist zu einer Untergruppe von $\mathrm{Sym}(G)$ isomorph (Satz von Cayley). Ist G endlich und $|G : H|$ der kleinste Primteiler p von $|G|$, so folgt: $p \;\big|\; |G : \mathrm{Core}_G(H)| \;\big|\; \mathrm{ggT}(p!, |G|) = p$, d.h. $p = |G : H| = |G : \mathrm{Core}_G(H)|$ und damit $H = \mathrm{Core}_G(H) \trianglelefteq G$.

(iii) Für $n \in \mathbb{N}$ mit $n \geq 2$ ist $\mathrm{sgn} : \mathrm{Sym}(n) \to \{\pm 1\}$ ein Epimorphismus. Daher ist $|\mathrm{Sym}(n) : \mathrm{Alt}(n)| = 2$ und $|\mathrm{Alt}(n)| = \frac{n!}{2}$.

(iv) Für $n \in \mathbb{N}$ und jeden endlichen Körper K ist bekanntlich $|\mathrm{GL}(n,K)| = (q^n - 1)(q^n - q)\dots(q^n - q^{n-1})$ mit $q := |K|$. Da $\det : \mathrm{GL}(n,K) \to K\setminus\{0\}$ surjektiv ist, folgt: $|\mathrm{GL}(n,K) : \mathrm{SL}(n,K)| = q-1$ und $|\mathrm{SL}(n,K)| = (q^n - 1)(q^n - q)\dots(q^n - q^{n-1}) \;/\; (q-1)$.

(v) Für jede Untergruppe H einer Gruppe G operiert $N_G(H)$ auf H durch Konjugation (vgl. Beispiel 3.1(v)). Der Kern dieser Operation ist $C_G(H)$, und das Bild der zugehörigen Abbildung $\tau : N_G(H) \to \mathrm{Sym}(H)$ ist eine Untergruppe von $\mathrm{Aut}(H)$. Daher ist $N_G(H)/C_G(H)$ zu einer Untergruppe von $\mathrm{Aut}(H)$ isomorph. Im Spezialfall $H = G$ ist $N_G(H) = G$, $C_G(H) = Z(G)$ und $\tau(G) = \mathrm{Inn}(G)$. Daher ist $G/Z(G) \cong \mathrm{Inn}(G)$.

3.3. Satz (Erster Isomorphiesatz)**.** *Für jede Gruppe G, jede Untergruppe H von G und jeden Normalteiler N von G ist $HN \leq G,\ N \trianglelefteq HN,\ H \cap N \trianglelefteq H$ und $H/H \cap N \cong HN/N$.*

Beweis. Algebra. □

Bemerkung. Im Fall $H \trianglelefteq G$ ist $HN \trianglelefteq G$.

3.4. Satz. *Für jede Menge π von Primzahlen und jede Gruppe G gilt:*

(i) *Ist G π-Gruppe, so auch jede Untergruppe von G.*
(ii) *Für jeden Normalteiler N von G gilt: G π-Gruppe $\Leftrightarrow N, G/N$ π-Gruppen.*
(iii) *G, H π-Gruppen $\Rightarrow G \times H$ π-Gruppe.*
(iv) *H π-Untergruppe, N π-Normalteiler von $G \Rightarrow HN$ π-Untergruppe von G.*
(v) *M, N π-Normalteiler von $G \Rightarrow MN$ π-Normalteiler von G.*
(vi) *$O_\pi(G) := \langle N : N$ π-Normalteiler von $G\rangle$ ist π-Normalteiler von G.*

Beweis.

(i) Trivial.
(ii) $\Rightarrow$: Für $g \in G$ ist $(gN)^{|\langle g\rangle|} = g^{|\langle g\rangle|}N = 1N = N$, also $|\langle gN\rangle| \mid |\langle g\rangle|$.
$\Leftarrow$: Für $g \in G$ ist $g^{|\langle gN\rangle|}N = (gN)^{|\langle gN\rangle|} = 1_{G/N} = N$, also $h := g^{|\langle gN\rangle|} \in N$ und $g^{|\langle gN\rangle|\cdot|\langle h\rangle|} = h^{|\langle h\rangle|} = 1$. Daher ist $|\langle g\rangle| \mid |\langle gN\rangle| \cdot |\langle h\rangle|$.
(iii) $g \in G,\ h \in H \ \Rightarrow\ (g,h)^{|\langle g\rangle|\cdot|\langle h\rangle|} = (g^{|\langle g\rangle|\cdot|\langle h\rangle|}, h^{|\langle g\rangle|\cdot|\langle h\rangle|}) = (1,1) = 1 \ \Rightarrow\ |\langle (g,h)\rangle| \mid |\langle g\rangle| \cdot |\langle h\rangle|$.
(iv) H π-Untergruppe, N π-Normalteiler von $G \ \Rightarrow\ HN/N \overset{3.3}{\cong} H/H \cap N$ π-Gruppe nach (ii) $\overset{(ii)}{\Rightarrow}\ HN$ π-Gruppe.
(v) Klar (auch für endlich viele Faktoren).
(vi) Offenbar ist $O_\pi(G) \trianglelefteq G$. Für $g \in O_\pi(G)$ existieren endlich viele π-Normalteiler $N_1, \ldots, N_r$ von G und Elemente $g_1 \in N_1, \ldots, g_r \in N_r$ mit $g = g_1 \ldots g_r \in N_1 \ldots N_r$. Nach (v) ist $N_1 \ldots N_r$ π-Gruppe, also g π-Element.

□

Definition. Man nennt $O_\pi(G)$ den *π-Kern* oder das *π-Radikal* von G.

3.5. Satz (Zweiter Isomorphiesatz)**.** *Für jede Gruppe G und jeden Normalteiler N von G ist die Abbildung $H \mapsto H/N$ eine Bijektion zwischen der Menge aller Untergruppen von G, die N enthalten, und der Menge aller Untergruppen von G/N. Eine Untergruppe H von G, die N enthält, ist genau dann normal in G, wenn H/N normal in G/N ist. In diesem Fall ist $(G/N)/(H/N) \cong G/H$.*

Beweis. Algebra. □

Bemerkung. Als Anwendung erhält man:

(i) In jeder unendlichen zyklischen Gruppe $G = \langle g\rangle$ existiert für $n \in \mathbb{N}$ genau eine Untergruppe vom Index n, und zwar $\langle g^n\rangle$. Auf diese Weise erhält man alle nichttrivialen Untergruppen von G.
(ii) In jeder endlichen zyklischen Gruppe $G = \langle g\rangle$ existiert zu jedem Teiler n von $|G|$ genau eine Untergruppe vom Index n, nämlich $\langle g^n\rangle$.

3.6. Satz (Dritter Isomorphiesatz, Zassenhaus)**.** *Für jede Gruppe G, beliebige Untergruppen U, V von G und beliebige Normalteiler U_0 von U, V_0 von V gilt:*
$U_0(U \cap V_0) \trianglelefteq U_0(U \cap V),\ V_0(V \cap U_0) \trianglelefteq V_0(V \cap U),\ (U_0 \cap V)(V_0 \cap U) \trianglelefteq U \cap V$ *und*

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

Beweis. Algebra. □

3.7. Bemerkung. Für jede Familie $(N_i)_{i\in I}$ von Normalteilern einer Gruppe G ist die Abbildung $G \to \bigtimes_{i\in I}(G/N_i),\ g \mapsto (gN_i)_{i\in I}$ ein Homomorphismus mit Kern $\bigcap_{i\in I} N_i$; insbesondere ist die Abbildung $G/\bigcap_{i\in I} N_i \to \bigtimes_{i\in I}(G/N_i),\ g(\bigcap_{i\in I} N_i) \mapsto (gN_i)_{i\in I}$ nach dem Homomorpiesatz ein Monomorphismus.

Satz. *Sind M, N Normalteiler einer Gruppe G mit $M \cap N = 1$, so ist jedes Element in M mit jedem Element in N vertauschbar.*

Beweis. Nach der Bemerkung ist die Abbildung $f : G \to G/M \times G/N,\ g \mapsto (gM, gN)$ ein Monomorphismus. Für $m \in M,\ n \in N$ gilt also:

$$\begin{aligned} f(mn) &= (mnM, mnN) = (Mmn, mN) = (Mn, mN) = (nM, Nm) = \\ &= (nM, Nnm) = (nmM, nmN) = f(nm), \end{aligned}$$

d.h. $mn = nm$. □

3.8. Bemerkung. Für jede Primzahlenmenge π, jede endliche Gruppe G und beliebige Normalteiler N_1, $\ldots, N_r$ von G gilt nach 3.7 und 3.4: Ist G/N_i π-Gruppe für $i = 1, \ldots, r$, so auch $G/N_1 \cap \ldots \cap N_r$. Insbesondere ist der Durchschnitt aller Normalteiler N von G mit der Eigenschaft, daß G/N eine π-Gruppe ist, ein Normalteiler $O^\pi(G)$, und $G/O^\pi(G)$ eine π-Gruppe. Man nennt $O^\pi(G)$ das *π-Residuum* von G.

KAPITEL 4

Normalreihen und Gruppen mit Operatoren

4.1. Definition. Unter einer *Subnormalreihe* einer Gruppe G versteht man eine endliche Folge

$$G = G_0 \trianglerighteq G_1 \trianglerighteq G_2 \trianglerighteq \ldots \trianglerighteq G_l = 1$$

von Untergruppen von G mit $G_i \trianglelefteq G_{i-1}$ für $i = 1, \ldots, l$. Ist sogar $G_i \trianglelefteq G$ für $i = 1, \ldots, l$, so spricht man von einer *Normalreihe* von G. Die Faktorgruppen G_{i-1}/G_i $(i = 1, \ldots, l)$ nennt man die *Faktoren* und ihre Anzahl l die *Länge* dieser (Sub-)Normalreihe. Ist $G_{i-1} \neq G_i$ für $i = 1, \ldots, l$, so spricht man von einer (Sub-)Normalreihe *ohne Wiederholungen*. Eine (Sub-)Normalreihe $G = H_0 \trianglerighteq H_1 \trianglerighteq \ldots \trianglerighteq H_m = 1$ von G nennt man eine *Verfeinerung* der obigen (Sub-)Normalreihe, falls eine injektive Abbildung $f : \{1, \ldots, l\} \to \{1, \ldots, m\}$ existiert mit $G_i = H_{f(i)}$ für $i = 1, \ldots, l$. Im Fall $m > l$ spricht man von einer *echten* Verfeinerung.

Beispiel. $\mathrm{Sym}(4) \trianglerighteq \mathrm{Alt}(4) \trianglerighteq V_4 \trianglerighteq \langle (\begin{smallmatrix}1&2&3&4\\2&1&4&3\end{smallmatrix}) \rangle \trianglerighteq 1$ ist eine Subnormalreihe, wobei $V_4 := \langle (\begin{smallmatrix}1&2&3&4\\2&1&4&3\end{smallmatrix}), (\begin{smallmatrix}1&2&3&4\\3&4&1&2\end{smallmatrix}) \rangle$ die *Kleinsche Vierergruppe* ist. Diese Subnormalreihe ist wegen $\langle (\begin{smallmatrix}1&2&3&4\\2&1&4&3\end{smallmatrix}) \rangle \not\trianglelefteq \mathrm{Sym}(4)$ keine Normalreihe. Dagegen ist $\mathrm{Sym}(4) \trianglerighteq \mathrm{Alt}(4) \trianglerighteq V_4 \trianglerighteq 1$ eine Normalreihe.

4.2. Definition. Zwei Subnormalreihen $G = G_0 \trianglerighteq G_1 \trianglerighteq \ldots \trianglerighteq G_l = 1$ und $G = H_0 \trianglerighteq H_1 \trianglerighteq \ldots \trianglerighteq H_m = 1$ nennt man *isomorph*, wenn $l = m$ ist und ein $f \in \mathrm{Sym}(l)$ existiert mit $G_{i-1}/G_i \cong H_{f(i)-1}/H_{f(i)}$ für $i = 1, \ldots, l$.

Beispiel. $\mathbb{Z}/6\mathbb{Z}$ hat isomorphe Subnormalreihen:

$$\mathbb{Z}/6\mathbb{Z} \trianglerighteq 2\mathbb{Z}/6\mathbb{Z} \trianglerighteq 1 \quad \text{und} \quad \mathbb{Z}/6\mathbb{Z} \trianglerighteq 3\mathbb{Z}/6\mathbb{Z} \trianglerighteq 1.$$

Satz (Verfeinerungssatz, Schreier)**.** *Je zwei Subnormalreihen einer Gruppe G besitzen isomorphe Verfeinerungen.*

Beweis. Algebra. □

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

Beispiel. $\mathbb{Z}$ besitzt keine Kompositionsreihe; denn jede Subnormalreihe $\mathbb{Z} \trianglerighteq n_1\mathbb{Z} \trianglerighteq n_2\mathbb{Z} \trianglerighteq \ldots \trianglerighteq n_i\mathbb{Z} \trianglerighteq 0$ läßt sich zu $\mathbb{Z} \trianglerighteq n_1\mathbb{Z} \trianglerighteq \ldots \trianglerighteq n_i\mathbb{Z} \trianglerighteq 2n_i\mathbb{Z} \trianglerighteq 0$ verfeinern. Andrerseits besitzt jede endliche Gruppe eine Kompositionsreihe.

Bemerkung. Nach dem 2. Isomorphiesatz ist eine Subnormalreihe genau dann eine Kompositionsreihe, wenn alle ihre Faktoren einfache Gruppen sind.

Satz (Jordan-Hölder)**.** *Besitzt eine Gruppe G eine Kompositionsreihe, so sind je zwei Kompositionsreihen von G isomorph.*

Beweis. Algebra. □

4.4. Definition. Die Faktoren einer Kompositionsreihe einer Gruppe G nennt man *Kompositionsfaktoren* von G und die Länge einer Kompositionsreihe die *Kompositionslänge* von G.

Bemerkung. Nach Jordan-Hölder bestimmt eine Gruppe G ihre Kompositionslänge eindeutig und ihre Kompositionsfaktoren eindeutig bis auf Isomorphie.

4.5. Definition. Gegeben sei eine Menge Ω. Eine Ω-*Gruppe* ist ein Paar, das aus einer Gruppe G und einer Abbildung $\Omega \times G \to G,\ (\omega, g) \mapsto {}^{\omega}g$ mit folgender Eigenschaft besteht: Für $g, h \in G$ und $\omega \in \Omega$ ist ${}^{\omega}(gh) = ({}^{\omega}g)({}^{\omega}h)$. Die Elemente in Ω nennt man *Operatoren* für G, und man sagt kurz: G ist Ω-Gruppe.

Bemerkung. Für $\omega \in \Omega$ ist dann die Abbildung $G \to G,\ g \mapsto {}^{\omega}g$ ein Endomorphismus von G; dabei ist zugelassen, daß verschiedene Elemente in Ω den gleichen Endomorphismus liefern.

Beispiel.

(i) Jeder Vektorraum V über einem Körper Ω läßt sich als Ω-Gruppe mit ${}^{\omega}v := \omega v$ für $\omega \in \Omega,\ v \in V$ auffassen.
(ii) G beliebig, $\Omega = \mathrm{End}(G),\ {}^{\omega}g := \omega(g)$ für $\omega \in \Omega,\ g \in G$; analog für $\Omega = \mathrm{Aut}(G)$ oder $\Omega = \mathrm{Inn}(G)$.
(iii) G beliebig, $\Omega \leq G,\ {}^{\omega}g := \omega g \omega^{-1}$ für $\omega \in \Omega,\ g \in G$.
(iv) Für jede Familie $(G_i)_{i\in I}$ von Ω-Gruppen ist auch $\bigtimes_{i\in I} G_i$ eine Ω-Gruppe, wenn man definiert: ${}^{\omega}(g_i)_{i\in I} := ({}^{\omega}g_i)_{i\in I}$ für $\omega \in \Omega,\ (g_i)_{i\in I} \in \bigtimes_{i\in I} G_i$.

4.6. Definition. Gegeben seien eine Menge Ω und eine Ω-Gruppe G. Eine Untergruppe H von G mit ${}^{\omega}h \in H$ für alle $\omega \in \Omega,\ h \in H$ nennt man eine Ω-*Untergruppe* von G.

Bemerkung.

(i) In diesem Fall wird H selbst zu einer Ω-Gruppe.
(ii) Ist G beliebig und $\Omega = \mathrm{End}(G)$ wie oben, so nennt man Ω-Untergruppen auch *vollinvariante* Untergruppen von G.
(iii) Ist G beliebig und $\Omega = \mathrm{Aut}(G)$ wie oben, so nennt man Ω-Untergruppen auch *charakteristische* Untergruppen von G.
(iv) Ist G beliebig und $\Omega = \mathrm{Inn}(G)$ wie oben, so sind die Ω-Untergruppen von G genau die Normalteiler von G.

Beispiel. Für jede Gruppe G ist $Z(G)$ charakteristisch, aber nicht notwendig vollinvariant in G.

Satz. *Für Untergruppen H, K einer Gruppe G mit $K \leq H \leq G$ gilt:*

(i) *K charakteristisch (vollinvariant) in H $\wedge$ H charakteristisch (vollinvariant) in G $\Rightarrow$ K charakteristisch (vollinvariant) in G.*
(ii) *K charakteristisch in H $\wedge$ $H \trianglelefteq G$ $\Rightarrow$ $K \trianglelefteq G$.*

Beweis.

(i) Sei K charakteristisch in H, H charakteristisch in G und $\alpha \in \mathrm{Aut}(G)$. Dann ist $\alpha(H) \subseteq H = \alpha(\alpha^{-1}(H)) \subseteq \alpha(H)$, also $\alpha(H) = H$. Daher ist die Einschränkung α' von α ein Automorphismus von H. Folglich ist $\alpha(K) = \alpha'(K) \subseteq K$.
Analog für vollinvariante Untergruppen.
(ii) Sei K charakteristisch in H, $H \trianglelefteq G$ und $g \in G$. Dann ist die Abbildung $\alpha : H \to H,\ h \mapsto ghg^{-1}$ ein Automorphismus von H. Also ist $gKg^{-1} = \alpha(K) \subseteq K$.

□

4.7. Definition. Gegeben seien eine Menge Ω und Ω-Gruppen G, H. Einen Homomorphismus $f : G \to H$ mit $f({}^{\omega}g) = {}^{\omega}f(g)$ für alle $\omega \in \Omega,\ g \in G$ nennt man einen Ω-*Homomorphismus*. Wie üblich hat man auch die Begriffe „ Ω-Monomorphismus“, ..., „ Ω-isomorph“ und die Notationen $\cong_\Omega$, $\mathrm{Hom}_\Omega(G, H)$, $\mathrm{End}_\Omega(G)$, $\mathrm{Aut}_\Omega(G)$.

Bemerkung.

(i) Für jeden Ω-*Normalteiler* N von G (d.h. N ist Ω-Untergruppe von G und $N \trianglelefteq G$) wird G/N zu einer Ω-Gruppe, wenn man definiert: ${}^{\omega}(gN) = ({}^{\omega}g)N$ für $\omega \in \Omega,\ g \in G$; dies rechnet man leicht nach. Der kanonische Epimorphismus $G \to G/N,\ g \mapsto gN$ ist dann ein Ω-Epimorphismus.

(ii) Bild und Kern von Ω-Homomorphismen sind Ω-Untergruppen, und jeder Ω-Homomorphismus f von einer Ω-Gruppe G in eine Ω-Gruppe H induziert einen Ω-Isomorphismus $G/\operatorname{Ker}(f) \to f(G)$ (Homomorphiesatz für Ω-Gruppen); dies rechnet man leicht nach. Analog übertragen sich die anderen Isomorphiesätze auf Ω-Gruppen. Wir verwenden diese im folgenden ohne Kommentar.

4.8. Definition. Gegeben seien eine Menge Ω und eine Ω-Gruppe $G \neq 1$. Man nennt G eine *einfache* Ω-Gruppe, wenn 1 und G die einzigen Ω-Normalteiler von G sind. Im Fall $\Omega = \operatorname{Aut}(G)$ nennt man G *charakteristisch einfach.*

Bemerkung. Es ist klar, wie man Ω-(Sub-)Normalreihen und Ω-Kompositionsreihen definiert. Die Sätze von Schreier und Jordan-Hölder übertragen sich. Im Fall $\Omega = \operatorname{Inn}(G)$ spricht man von *Hauptreihen* und im Fall $\Omega = \operatorname{Aut}(G)$ von *charakteristischen Reihen* statt von Ω-Kompositionsreihen. Die Faktoren einer Hauptreihe nennt man *Hauptfaktoren.* Nach Satz 4.6(ii) sind diese charakteristisch einfach.

Satz. *Gegeben sei eine Menge Ω, eine Ω-Gruppe G, eine Ω-Subnormalreihe $G_0 \trianglerighteq G_1 \trianglerighteq \ldots \trianglerighteq G_r$ von G und eine Ω-Untergruppe H von G. Setzt man $H_i := H \cap G_i$ für $i = 0, \ldots, r$, so ist $H_0 \trianglerighteq H_1 \trianglerighteq \ldots \trianglerighteq H_r$ eine Ω-Subnormalreihe von H mit*

$$H_{i-1}/H_i \cong_\Omega (H \cap G_{i-1})G_i/G_i \leq G_{i-1}/G_i \quad \text{für } i = 1, \ldots, r.$$

Beweis. Für $i = 1, \ldots, r$ ist $H_i = H \cap G_i = (H \cap G_{i-1}) \cap G_i \trianglelefteq H \cap G_{i-1} = H_{i-1}$ und $H_{i-1}/H_i = (H \cap G_{i-1})/(H \cap G_{i-1}) \cap G_i \cong_\Omega (H \cap G_{i-1})G_i/G_i$ nach dem 1. Isomorphiesatz. □

4.9. Satz. *Gegeben seien eine Menge Ω, eine Ω-Gruppe G und Ω-Normalteiler M, N von G. Besitzen G/M und G/N Ω-Kompositionsreihen, so auch $G/M \cap N$, und jeder Ω-Kompositionsfaktor von $G/M \cap N$ ist zu einem Ω-Kompositionsfaktor von G/M oder G/N isomorph.*

Beweis. Wegen $(G/M \cap N)/(M/M \cap N) \cong_\Omega G/M$ und $(G/M \cap N)/(N/M \cap N) \cong_\Omega G/N$ kann man zu $G/M \cap N$ statt G übergehen und daher $M \cap N = 1$ annehmen. Nach dem 1. Isomorphiesatz ist $M/M \cap N$ Ω-isomorph zu dem Ω-Normalteiler MN/N von G/N, besitzt also eine Ω-Kompositionsreihe, deren Faktoren zu Ω-Kompositionsfaktoren von G/N Ω-isomorph sind. Sind $G/M = G_0/M \trianglerighteq \ldots \trianglerighteq G_r/M = M/M$ und $M = M_0 \trianglerighteq \ldots \trianglerighteq M_s = 1$ Ω-Kompositionsreihen von G/M bzw. M, so ist

$$\begin{array}{ccccccccccc} G_0 & \trianglerighteq & \ldots & \trianglerighteq & G_r & = & M_0 & \trianglerighteq & \ldots & \trianglerighteq & M_s \\ \| & & & & \| & & \| & & & & \| \\ G & & & & M & & M & & & & 1 \end{array}$$

eine Ω-Kompositionsreihe von G mit den gewünschten Eigenschaften. □

KAPITEL 5

Direkte Summen und Produkte

5.1. Bemerkung. Es ist plausibel, daß man viele Eigenschaften eines direkten Produkts $G_1 \times \ldots \times G_n$ von Gruppen G_i an den Eigenschaften der Faktoren G_i ablesen kann. Es ist daher wichtig, bei einer vorgegebenen Gruppe G erkennen zu können, ob sie zu einem direkten Produkt $G_1 \times \ldots \times G_n$ isomorph ist.

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

(i) $\langle G_i : i \in I\rangle = G$.
(ii) $G_i \cap \langle G_j : j \in I \setminus \{i\}\rangle = 1$ für $i \in I$.

Dann nennt man G eine *direkte Summe* der Familie $(G_i)_{i\in I}$ und schreibt: $G = \bigoplus_{i\in I} G_i$.

5.2. Bemerkung.

(i) Die Gruppe G sei direkte Summe der Familie $(G_i)_{i\in I}$ von Normalteilern von G. Für verschiedene $i, j \in I$ ist dann $G_i \cap G_j = 1$ wegen (ii). Nach 3.7 ist also jedes Element in G_i mit jedem Element in G_j vertauschbar. Zu jedem $g \in G$ existieren also nach (i) Elemente $i_1, \ldots, i_n \in I$, $g_{i_1} \in G_{i_1}, \ldots, g_{i_n} \in G_{i_n}$ mit $g = g_{i_1} \ldots g_{i_n}$, wobei o.B.d.A. $i_1, \ldots, i_n$ paarweise verschieden sind. Auf die Reihenfolge der Faktoren kommt es dabei nicht an. Wir setzen $g_i := 1$ für $i \in I \setminus \{i_1, \ldots, i_n\}$ und schreiben dieses Produkt dann auch in der Form $g = \prod_{i\in I} g_i$. Hat man eine weitere Familie $(h_i)_{i\in I}$ von Elementen $h_i \in G_i$ mit $|\{i \in I : h_i \neq 1\}| < \infty$ und $g = \prod_{i\in I} h_i$, so ist $g_i = h_i$ für $i \in I$; im Fall $g_j \neq h_j$ für ein $j \in I$ wäre nämlich $1 \neq g_j^{-1}h_j = \prod_{i\in I\setminus\{j\}} g_i h_i^{-1} \in G_j \cap \langle G_i : i \in I \setminus \{j\}\rangle = 1$. Widerspruch. Daher läßt sich jedes Element $g \in G$ 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. Es folgt leicht, daß die Abbildung $\coprod_{i\in I} G_i \to G$, $(g_i)_{i\in I} \mapsto \prod_{i\in I} g_i$ ein Isomorphismus ist. Man identifiziert daher häufig $\bigoplus_{i\in I} G_i$ mit $\coprod_{i\in I} G_i$ und schreibt z.B. im Fall $I = \{1, \ldots, n\}$ auch $G_1 \times \ldots \times G_n$ statt $G_1 \oplus \ldots \oplus G_n$.

(ii) Hat man umgekehrt eine Familie $(G_i)_{i\in I}$ von Gruppen vorgegeben und setzt man $G := \coprod_{i\in I} G_i$, $\hat{G}_j := \{(g_i)_{i\in I} : g_i = 1 \text{ für } i \neq j\}$ für $j \in I$, so ist $G = \bigoplus_{j\in I} \hat{G}_j$, wie man leicht nachrechnet.

5.3. Satz. *Gegeben seien Normalteiler $G_1, \ldots, G_n$ einer Gruppe G mit $G = G_1 \ldots G_n$ und $G_i \cap G_1 \ldots G_{i-1} = 1$ für $i = 2, \ldots, n$. Dann ist $G = G_1 \oplus \ldots \oplus G_n$.*

Beweis. Sei $i \in \{1, \ldots, n\}$ und $1 \neq g \in G_i \cap \langle G_1, \ldots, G_{i-1}, G_{i+1}, \ldots, G_n\rangle = G_i \cap G_1 \ldots G_{i-1}G_{i+1} \ldots G_n$. Dann existieren $g_1 \in G_1, \ldots, g_n \in G_n$ mit $g_i^{-1} = g = g_1 \ldots g_{i-1}g_{i+1} \ldots g_n$. Für $j, k = 1, \ldots, n$ mit $j \neq k$ ist $G_j \cap G_k = 1$, also jedes Element in G_j mit jedem Element in G_k vertauschbar. Daher ist $1 = g_1 \ldots g_{i-1}g_ig_{i+1} \ldots g_n$. Sei $j \in \{1, \ldots, n\}$ maximal mit $g_j \neq 1$. Dann ist $1 \neq g_j^{-1} = g_1 \ldots g_{j-1} \in G_j \cap G_1 \ldots G_{j-1}$ im Widerspruch zur Voraussetzung. □

5.4. Satz. *Gegeben seien Normalteiler $G_1, \ldots, G_n$ einer endlichen Gruppe G mit $|G| = |G_1| \ldots |G_n|$ und $\mathrm{ggT}(|G_i|, |G_j|) = 1$ für $i \neq j$. Dann ist $G = G_1 \oplus \ldots \oplus G_n$.*

Beweis. Wir zeigen durch Induktion nach i, daß $G_i \cap G_1 \ldots G_{i-1} = 1$ und $|G_1 \ldots G_i| = |G_1| \ldots |G_i|$ ist. Für $i = 2$ ist $|G_1 \cap G_2| \mid \mathrm{ggT}(|G_1|, |G_2|) = 1$, also $G_1 \cap G_2 = 1$ und $|G_1G_2| = |G_1| \cdot |G_2|$. Ist die Aussage für i bereits bewiesen, so ist

$$|G_{i+1} \cap G_1 \ldots G_i| \mid \mathrm{ggT}(|G_{i+1}|, |G_1 \ldots G_i|) = \mathrm{ggT}(|G_{i+1}|, |G_1| \ldots |G_i|) = 1$$

und

$$|G_1 \dots G_i G_{i+1}| = |G_1 \dots G_i| \cdot |G_{i+1}| = |G_1| \dots |G_i| \cdot |G_{i+1}|.$$

Schließlich ist $|G| = |G_1| \dots |G_n| = |G_1 \dots G_n|$, also $G = G_1 \dots G_n$. Wende 5.3 an. □

5.5. Definition. Ein *minimaler (maximaler)* Normalteiler einer Gruppe G ist ein Normalteiler $N \neq 1$ ($N \neq G$) von G mit der Eigenschaft, daß kein Normalteiler M von G existiert mit $1 \neq M < N$ ($N < M \neq G$).

Satz.

(i) *Jede endliche charakteristisch einfache Gruppe G ist direkte Summe isomorpher einfacher Gruppen.*

(ii) *Sind $G_1, \dots, G_n$ nichtabelsche einfache Normalteiler einer Gruppe G mit $G = G_1 \oplus \dots \oplus G_n$, so sind die Teilsummen $G_{i_1} \oplus \dots \oplus G_{i_k}$ die einzigen Normalteiler von G, und zu jedem Normalteiler N von G exstiert ein Normalteiler M von G mit $G = N \oplus M$.*

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

Beweis.

(i) Sei G endlich und charakteristisch einfach und N ein minimaler Normalteiler von G. Für $\alpha \in \mathrm{Aut}(G)$ ist dann auch $\alpha(N)$ ein minimaler Normalteiler von G. Wir wählen eine möglichst große Untergruppe M von G, die direkte Summe einiger $\alpha(N)$ ist. Offenbar ist $M \trianglelefteq G$.
Annahme: $\beta(N) \not\subseteq M$ für ein $\beta \in \mathrm{Aut}(G)$. Dann ist $M \cap \beta(N) \trianglelefteq G$ und $M \cap \beta(N) < \beta(N)$, also $M \cap \beta(N) = 1$ wegen der Minimalität von $\beta(N)$. Folglich ist $M\beta(N) = M \oplus \beta(N)$ im Widerspruch zur Wahl von M.
Daher ist $M = \langle \beta(N) : \beta \in \mathrm{Aut}(G) \rangle$ charakteristische Untergruppe von G, also $M = G$. Folglich existieren $\alpha_1, \dots, \alpha_n \in \mathrm{Aut}(G)$ mit $G = \alpha_1(N) \oplus \dots \oplus \alpha_n(N)$. Da für $i \neq j$ jedes Element in $\alpha_i(N)$ mit jedem Element in $\alpha_j(N)$ vertauschbar ist, ist für $i = 1, \dots, n$ jeder Normalteiler K von $\alpha_i(N)$ auch einer von G, also $K \in \{1, \alpha_i(N)\}$ wegen der Minimalität von $\alpha_i(N)$. Daher sind $\alpha_1(N), \dots, \alpha_n(N)$ einfache Gruppen.

(ii) Seien $G_1, \dots, G_n$ einfache nichtabelsche Normalteiler einer Gruppe G mit $G = G_1 \oplus \dots \oplus G_n$, sei $N \trianglelefteq G$ und $g \in N$, $g = g_1 \dots g_n$ mit $g_1 \in G_1, \dots, g_n \in G_n$. Es genügt zu zeigen: Ist $i \in \{1, \dots, n\}$ mit $g_i \neq 1$, so ist $G_i \subseteq N$. Sei also $i \in \{1, \dots, n\}$ und $g_i \neq 1$. Da G_i einfach und nichtabelsch ist, ist $Z(G_i) = 1$; insbesondere ist $g_i \notin Z(G_i)$. Also existiert ein $h \in G_i$ mit $hg_i \neq g_i h$, d.h

$$1 \neq hg_ih^{-1}g_i^{-1} = \underbrace{h\overbrace{gh^{-1}}^{\in G_i}g^{-1}}_{\in N} \in G_i \cap N.$$

Folglich ist $1 \neq G_i \cap N \trianglelefteq G_i$, also $G_i = G_i \cap N \subseteq N$.

(iii) Sei H eine einfache Gruppe, $n \in \mathbb{N}$ und $G := H^n = \underbrace{H \times \dots \times H}_{n}$.

Fall 1: H nichtabelsch. Dann ist $G = H_1 \oplus \dots \oplus H_n$, wobei

$$H_i := 1 \times \dots \times 1 \times \overset{\overset{i}{\downarrow}}{H} \times 1 \times \dots \times 1 \cong H \qquad \text{für } i = 1, \dots, n.$$

Jede charakteristische Untergruppe $N \neq 1$ von G enthält nach (ii) ein H_i. Für $f \in \mathrm{Sym}(n)$ ist aber die Abbildung $\alpha : G \to G$, $(g_1, \dots, g_n) \mapsto (g_{f(1)}, \dots, g_{f(n)})$ ein Automorphismus von G. Also ist $\alpha(H_i) \subseteq N$ und $H_j \subseteq N$ für $j = 1, \dots, n$, d.h. $N = G$.
Fall 2: H abelsch, also $H \cong \mathbb{Z}/p\mathbb{Z}$ für eine Primzahl p. Also ist $G \cong (\mathbb{Z}/p\mathbb{Z})^n$, o.B.d.A. $G = (\mathbb{Z}/p\mathbb{Z})^n$. Jeder Automorphismus des $\mathbb{Z}/p\mathbb{Z}$-Vektorraumes $(\mathbb{Z}/p\mathbb{Z})^n$ ist auch ein Automorphismus der Gruppe $(\mathbb{Z}/p\mathbb{Z})^n$. Wie man in der Linearen Algebra zeigt, existiert für je zwei Elemente $x, y \in G \setminus \{1\}$ ein Vektorraum-Automorphismus α von G mit $\alpha(x) = y$. Folglich ist G charakteristisch einfach.

□

5.6. Satz (Hauptsatz über endlich erzeugte abelsche Gruppen)**.**

(i) *Zu jeder endlich erzeugten abelschen Gruppe G existieren eindeutig bestimmte $n_1, \ldots, n_r \in \mathbb{N}_0$ mit $n_1 \mid n_2 \mid \ldots \mid n_r$ und $G \cong \mathbb{Z}/n_1\mathbb{Z} \times \ldots \times \mathbb{Z}/n_r\mathbb{Z}$.*

(ii) *Zu jeder endlich erzeugten abelschen Gruppe G existieren eindeutig bestimmte Primzahlpotenzen $q_1 = p_1^{a_1}, \ldots, q_s = p_s^{a_s}$ und ein eindeutig bestimmtes $t \in \mathbb{N}_0$ mit $G \cong \mathbb{Z}/q_1\mathbb{Z} \times \ldots \times \mathbb{Z}/q_s\mathbb{Z} \times \underbrace{\mathbb{Z} \times \ldots \times \mathbb{Z}}_{t}$.*

Beweis. Algebra. □

5.7. Definition. Einen Endomorphismus α einer Gruppe G mit $\alpha(xyx^{-1}) = x\alpha(y)x^{-1}$ für alle $x, y \in G$ nennt man *normal*.

Bemerkung.

(i) Mit $\Omega := \mathrm{Inn}(G)$ sind also die normalen Endomorphismen genau die Ω-Endomorphismen.

(ii) Ist α normal, so ist $x^{-1}\alpha(x)\alpha(y)\alpha(x)^{-1}x = \alpha(y)$ für $x, y \in G$, also $x^{-1}\alpha(x) \in C_G(\alpha(G))$ für $x \in G$. Im Fall $\alpha \in \mathrm{Aut}(G)$ ist also $x^{-1}\alpha(x) \in Z(G)$ für $x \in G$.

Beispiel. Die *Nullabbildung* $0 = 0_G : G \to G,\ g \mapsto 1$ ist für jede Gruppe G ein normaler Endomorphismus.

Satz (Schurs Lemma)**.** *Gegeben sei eine Menge Ω, eine einfache Ω-Gruppe G und ein normaler Ω-Endomorphismus $\alpha \neq 0$ von G. Dann ist $\alpha \in \mathrm{Aut}_\Omega(G)$.*

Beweis. Offenbar ist $\alpha(G)$ ein Ω-Normalteiler von G. Wegen $\alpha \neq 0$ ist $\alpha(G) \neq 1$, also $\alpha(G) = G$, d.h. α ist surjektiv. Analog ist $\mathrm{Ker}(\alpha)$ ein Ω-Normalteiler von G mit $\mathrm{Ker}(\alpha) \neq G$ wegen $\alpha \neq 0$, also $\mathrm{Ker}(\alpha) = 1$, d.h. α ist injektiv. □

5.8. Definition. Gegeben sei eine Menge Ω und eine Ω-Gruppe G. Man sagt, daß G die *Minimalbedingung* (bzw. *Maximalbedingung*) für Ω-Untergruppen erfüllt, falls jede nichtleere Menge $\mathcal{M}$ von Ω-Untergruppen von G ein minimales (bzw. maximales) Element M enthält, d.h. es existiert kein $H \in \mathcal{M}$ mit $H < M$ (bzw. $M < H$).

Satz (Fitting)**.** *Gegeben seien eine Menge Ω und eine Ω-Gruppe G mit Minimal- und Maximalbedingung für Ω-Untergruppen. Zu jedem normalen Ω-Endomorphismus α von G existiert dann ein $k \in \mathbb{N}$ mit:*

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

(ii) $1 \leq \mathrm{Ker}(\alpha) \leq \mathrm{Ker}(\alpha^2) \leq \ldots \leq \mathrm{Ker}(\alpha^k) = \mathrm{Ker}(\alpha^{k+1}) = \ldots$

Für jedes solche k ist $G = \mathrm{Ker}(\alpha^k) \oplus \alpha^k(G)$.

Beweis. (i) und (ii) folgen aus der Minimal- und Maximalbedingung. Offenbar sind $\mathrm{Ker}(\alpha^k)$ und $\alpha^k(G)$ Normalteiler von G. Für $g \in \mathrm{Ker}(\alpha^k) \cap \alpha^k(G)$ existiert ein $h \in G$ mit $g = \alpha^k(h)$, und es ist $1 = \alpha^k(g) = \alpha^{2k}(h)$, also $h \in \mathrm{Ker}(\alpha^{2k}) = \mathrm{Ker}(\alpha^k)$. Damit ist $g = \alpha^k(h) = 1$. Für $g \in G$ ist andrerseits $\alpha^k(g) \in \alpha^k(G) = \alpha^{2k}(G)$, also $\alpha^k(g) = \alpha^{2k}(h)$ für ein $h \in G$. Dann ist $1 = \alpha^k(g)\alpha^{2k}(h)^{-1} = \alpha^k(g\alpha^k(h^{-1}))$, also $g\alpha^k(h^{-1}) \in \mathrm{Ker}(\alpha^k)$ und $g = g\alpha^k(h^{-1})\alpha^k(h) \in \mathrm{Ker}(\alpha^k)\alpha^k(G)$. □

Bemerkung. Im Fall $\mathrm{Ker}(\alpha^k) = 1$ ist also $G = \alpha^k(G)$, d.h. α^k und α sind bijektiv. Im Fall $\mathrm{Ker}(\alpha^k) = G$ ist $\alpha^k = 0$, und man nennt α *nilpotent*.

5.9. Definition. Gegeben seien eine Menge Ω und eine Ω-Gruppe $G \neq 1$. Man nennt G *unzerlegbar*, falls es keine echten Ω-Normalteiler M, N von G mit $G = M \oplus N$ gibt.

Bemerkung. Jeder normale Ω-Endomorphismus einer unzerlegbaren Ω-Gruppe mit Minimal- und Maximalbedingung für Ω-Untergruppen ist nach 5.8 entweder nilpotent oder bijektiv.

KAPITEL 6

Direkte Zerlegungen

6.1. Definition. Zwei Endomorphismen α, β einer Gruppe G nennt man *addierbar*, falls die Abbildung $G \to G,\ g \mapsto \alpha(g)\beta(g)$ ein Endomorphismus von G ist. Gegebenenfalls bezeichnet man diese Abbildung mit $\alpha + \beta$.

Satz. *Zwei Endomorphismen α, β einer Gruppe G sind genau dann addierbar, wenn jedes Element in $\alpha(G)$ mit jedem Element in $\beta(G)$ vertauschbar ist. In diesem Fall gilt also $\alpha + \beta = \beta + \alpha$.*

Beweis.

$\Rightarrow$: Sind α, β addierbar, so gilt für $g, h \in G$:

$$\begin{aligned}\alpha(g)\beta(g)\alpha(h)\beta(h) &= (\alpha+\beta)(g)(\alpha+\beta)(h) = (\alpha+\beta)(gh) = \alpha(gh)\beta(gh) = \\ &= \alpha(g)\alpha(h)\beta(g)\beta(h),\end{aligned}$$

also $\beta(g)\alpha(h) = \alpha(h)\beta(g)$.

$\Leftarrow$: Für $g, h \in G$ mit $\beta(g)\alpha(h) = \alpha(h)\beta(g)$ ist

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

□

Bemerkung.

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

$$(\alpha + \beta) \circ \gamma = \alpha \circ \gamma + \beta \circ \gamma, \quad \gamma \circ (\alpha + \beta) = \gamma \circ \alpha + \gamma \circ \beta;$$

denn für $g \in G$ gilt:

$$\begin{aligned}((\alpha+\beta)\circ\gamma)(g) &= \alpha(\gamma(g))\beta(\gamma(g)) = (\alpha\circ\gamma + \beta\circ\gamma)(g)\\ (\gamma\circ(\alpha+\beta))(g) &= \gamma(\alpha(g)\beta(g)) = \gamma(\alpha(g))\gamma(\beta(g)) = (\gamma\circ\alpha + \gamma\circ\beta)(g).\end{aligned}$$

(ii) Ist Ω eine Menge, G eine Ω-Gruppe und sind $\alpha, \beta \in \mathrm{End}_\Omega(G)$ addierbar, so 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) Endomorphismen $\alpha_1, \ldots, \alpha_n$ einer Gruppe G heißen *paarweise addierbar*, falls α_i und α_j für alle $i, j = 1, \ldots, n$ mit $i \neq j$ addierbar sind. In diesem Fall ist die Abbildung $\alpha_1 + \ldots + \alpha_n : G \to G,\ g \mapsto \alpha_1(g) \ldots \alpha_n(g)$ ein Endomorphismus von G, und für $m = 1, \ldots, n-1$ gilt: $\alpha_1 + \ldots + \alpha_n = (\alpha_1 + \ldots + \alpha_m) + (\alpha_{m+1} + \ldots + \alpha_n)$.

6.2. Satz. *Gegeben seien eine Menge Ω, eine unzerlegbare Ω-Gruppe G mit Minimal- und Maximalbedingung für Ω-Untergruppen und addierbare normale Ω-Endomorphismen α, β von G 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 6.1 sind $\alpha' := (\alpha+\beta)^{-1} \circ \alpha,\ \beta' := (\alpha+\beta)^{-1} \circ \beta \in \mathrm{End}_\Omega(G)$ addierbar mit $\alpha' + \beta' = (\alpha+\beta)^{-1}(\alpha+\beta) = \mathrm{id}_G$. Für $g \in G$ ist also

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

Im Fall $\alpha', \beta' \notin \mathrm{Aut}_\Omega(G)$ wären beide nilpotent nach 5.8, also $(\alpha')^n = 0 = (\beta')^n$ für ein $n \in \mathbb{N}$. Dann wäre $\mathrm{id}_G = (\alpha'+\beta')^{2n} = \sum_{j=0}^{2n} \binom{2n}{j} (\alpha')^j (\beta')^{2n-j} = 0$ ein Widerspruch zu $G \neq 1$. Daher ist $\alpha' \in \mathrm{Aut}_\Omega(G)$ oder $\beta' \in \mathrm{Aut}_\Omega(G)$, also $\alpha \in \mathrm{Aut}_\Omega(G)$ oder $\beta \in \mathrm{Aut}_\Omega(G)$. □

6.3. Satz. *Gegeben seien eine Menge Ω und Ω-Normalteiler $G_1, \ldots, G_n$ einer Ω-Gruppe G mit $G = G_1 \oplus \ldots \oplus G_n$. Für $i = 1, \ldots, n$ sei $\varepsilon_i : G \to G$ definiert durch $\varepsilon_i(g_1 \ldots g_n) := g_i$ für $g_1 \in G_1, \ldots, g_n \in G_n$. Dann sind $\varepsilon_1, \ldots, \varepsilon_n$ paarweise addierbare normale Ω-Endomorphismen von G mit $\varepsilon_i^2 = \varepsilon_i$ für $i = 1, \ldots, n$, $\varepsilon_i \circ \varepsilon_j = 0$ für $i \neq j$ und $\varepsilon_1 + \ldots + \varepsilon_n = \mathrm{id}_G$.*

Beweis. Für $i = 1, \ldots, n$ ist ε_i nach Definition der direkten Summe wohldefiniert, und für Elemente $g_1, h_1 \in G_1, \ldots, g_n, h_n \in G_n,\ \omega \in \Omega,\ g \in G$ gilt:

$$\begin{aligned}
\varepsilon_i((g_1 \ldots g_n)(h_1 \ldots h_n)) &= \varepsilon_i(g_1 h_1 \ldots g_n h_n) = g_i h_i = \varepsilon_i(g_1 \ldots g_n)\varepsilon_i(h_1 \ldots h_n), \\
\varepsilon_i({}^\omega(g_1 \ldots g_n)) &= \varepsilon_i({}^\omega g_1 \ldots {}^\omega g_n) = {}^\omega g_i = {}^\omega \varepsilon_i(g_1 \ldots g_n), \\
\varepsilon_i(g(g_1 \ldots g_n)g^{-1}) &= \varepsilon_i((gg_1g^{-1}) \ldots (gg_ng^{-1})) = gg_ig^{-1} = g\varepsilon_i(g_1 \ldots g_n)g^{-1}.
\end{aligned}$$

Wegen $\varepsilon_i(G) = G_i$ für $i = 1, \ldots, n$ sind ε_i und ε_j für $i \neq j$ addierbar, und der Rest ist klar. □

6.4. Satz. *Gegeben seien eine Menge Ω und eine Ω-Gruppe G mit Minimalbedingung für Ω-Untergruppen. Ferner enthalte Ω alle inneren Automorphismen von G. Dann existieren endlich viele unzerlegbare Ω-Normalteiler $G_1, \ldots, G_n$ von G mit $G = G_1 \oplus \ldots \oplus G_n$.*

Beweis. Ist die Aussage falsch, so ist die Menge $\mathcal{M}$ aller Ω-Untergruppen von G, die sich nicht als direkte Summe von endlich vielen unzerlegbaren Ω-Untergruppen von G schreiben lassen, nichtleer und enthält daher ein minimales Element M. Dann ist $M \neq 1$, und M ist selbst keine unzerlegbare Ω-Untergruppe von G. Daher existieren echte Ω-Untergruppen M_1, M_2 von M mit $M = M_1 \oplus M_2$. Nach Wahl von M sind M_1, M_2 beide direkte Summe von endlich vielen unzerlegbaren Ω-Untergruppen von G, also auch M. Widerspruch. □

6.5. Satz (Krull-Remak-Schmidt)**.** *Gegeben seien eine Menge Ω und eine Ω-Gruppe G mit Minimal- und Maximalbedingung für Ω-Untergruppen. Ferner enthalte Ω alle inneren Automorphismen von G, und es sei $G = G_1 \oplus \ldots \oplus G_r = H_1 \oplus \ldots \oplus H_s$ mit unzerlegbaren Ω-Untergruppen $G_1, \ldots, G_r, H_1, \ldots, H_s$ von G. Dann ist $r = s$, nach geeigneter Umnumerierung von $H_1, \ldots, H_s$ ist $G = H_1 \oplus \ldots \oplus H_{i-1} \oplus G_i \oplus \ldots \oplus G_r$ für $i = 2, \ldots, r$, und es existiert ein 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 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 geeigneter Numerierung von $H_1, \ldots, H_s$). Für $i = 1$ setzt man $\alpha_1 := \mathrm{id}_G$. Sei nun α_i für ein $i \in \{1, \ldots, r\}$ schon definiert. Dann ist

$$\begin{aligned}
G &= \alpha_i(G) = \alpha_i(G_1 \oplus \ldots \oplus G_r) = \alpha_i(G_1) \oplus \ldots \oplus \alpha_i(G_r) = \\
&= H_1 \oplus \ldots \oplus H_{i-1} \oplus G_i \oplus \ldots \oplus G_r.
\end{aligned}$$

Zu dieser Zerlegung hat man $\varepsilon_1, \ldots, \varepsilon_r \in \mathrm{End}_\Omega(G)$ wie in 6.3, und analog hat man $\eta_1, \ldots, \eta_s \in \mathrm{End}_\Omega(G)$ zur Zerlegung $G = H_1 \oplus \ldots \oplus H_s$. Für $i = 1, \ldots, r$ ist

$$\varepsilon_i = \varepsilon_i \circ \mathrm{id}_G = \varepsilon_i \circ \sum_{j=1}^{s} \eta_j = \sum_{j=1}^{s} \varepsilon_i \circ \eta_j.$$

Dabei ist $\eta_j(G) = H_j$ für $j = 1, \ldots, s$, also $\varepsilon_j \circ \eta_j = \eta_j$ und $\varepsilon_i \circ \eta_j = 0$ für $j = 1, \ldots, i-1$. Daher ist $\varepsilon_i = \sum_{j=i}^{s} \varepsilon_i \circ \eta_j$ mit paarweise addierbaren Ω-Endomorphismen $\varepsilon_i \circ \eta_i, \ldots, \varepsilon_i \circ \eta_s$. Für jeden Endomorphismus β von G mit $\beta(G_i) \subseteq G_i$ sei $\overline{\beta} : G_i \to G_i$ die Einschränkung von β. Dann ist $\mathrm{id}_{G_i} = \overline{\varepsilon_i} = \sum_{j=1}^{s} \overline{\varepsilon_i \circ \eta_j}$. Da G_i unzerlegbar ist, folgt aus 6.2, daß sich unter $\overline{\varepsilon_i \circ \eta_i}, \ldots, \overline{\varepsilon_i \circ \eta_s}$ ein Automorphismus von G_i befindet. Nach Umnumerierung von $H_i, \ldots, H_s$ kann man $\overline{\varepsilon_i \circ \eta_i} \in \mathrm{Aut}_\Omega(G)$ annehmen.
Beh.: $H_i = \eta_i(G_i) \oplus (\mathrm{Ker}(\varepsilon_i) \cap H_i)$.
Bew.: Da ε_i und η_i Ω-Homomorphismen sind und Ω alle inneren Automorphismen von G enthält, sind $\eta_i(G_i)$ und $\mathrm{Ker}(\varepsilon_i) \cap H_i$ Ω-Normalteiler von G. Für $g \in G_i$ mit $1 = \varepsilon_i(\eta_i(g)) = (\overline{\varepsilon_i \circ \eta_i})(g)$ ist $g = 1$, also $\eta_i(g) = 1$. Daher ist $\eta_i(G_i) \cap \mathrm{Ker}(\varepsilon_i) \cap H_i = 1$. Für $h \in H_i$ ist $\varepsilon_i(h) \in G_i = (\overline{\varepsilon_i \circ \eta_i})(G_i) = \varepsilon_i(\eta_i(G_i))$,

also $\varepsilon_i(h) = \varepsilon_i(\eta_i(k))$ für ein $k \in G_i$. Daher ist $1 = \varepsilon_i(\eta_i(k^{-1}))\varepsilon_i(h) = \varepsilon_i(\eta_i(k^{-1})h)$, d.h. $\eta_i(k^{-1}h) \in \mathrm{Ker}(\varepsilon_i) \cap H_i$ und $h = \eta_i(k)\eta_i(k^{-1})h \in \eta_i(G_i)(\mathrm{Ker}(\varepsilon_i) \cap H_i)$.
Da H_i unzerlegbar und $\eta_i(G_i) \neq 1$ ist, folgt: $\mathrm{Ker}(\varepsilon_i) \cap H_i = 1$ und $H_i = \eta_i(G_i)$. Für $j = 1, \ldots, i-1$ ist $\varepsilon_j(G) = H_j$, es ist $\eta_i(\varepsilon_i(G)) = \eta_i(G_i) = H_i$, 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 $g_i \in G_i = \varepsilon_i(G),\ g_j \in G_j,\ i \neq j$. Daher sind $\varepsilon_1, \ldots, \varepsilon_{i-1}, \eta_i \circ \varepsilon_i, \varepsilon_{i+1}, \ldots, \varepsilon_r$ paarweise addierbar. Folglich ist $\delta := \varepsilon_1 + \ldots + \varepsilon_{i-1} + (\eta_i \circ \varepsilon_i) + \varepsilon_{i+1} + \ldots + \varepsilon_r \in \mathrm{End}_\Omega(G)$ mit

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

Daher ist $\delta(G) = \delta(H_1 \ldots H_{i-1} G_i G_{i+1} \ldots G_r) = H_1 \ldots H_{i-1} H_i G_{i+1} \ldots G_r$. Dabei ist

$$H_1 \ldots H_{i-1} G_{i+1} \ldots G_r = H_1 \oplus \ldots \oplus H_{i-1} \oplus G_{i+1} \oplus \ldots \oplus G_r = \mathrm{Ker}(\varepsilon_i)$$

und $H_i \cap \mathrm{Ker}(\varepsilon_i) = 1$, also

$$H_1 \ldots H_{i-1} H_i G_{i+1} \ldots G_r = H_1 \oplus \ldots \oplus H_{i-1} \oplus H_i \oplus G_{i+1} \oplus \ldots \oplus G_r.$$

Hat man Elemente $h_1 \in H_1, \ldots, h_{i-1} \in H_{i-1}, g_i \in G_i, \ldots, g_r \in G_r$ mit $1 = \delta(h_1 \ldots h_{i-1} g_i \ldots g_r) = h_1 \ldots h_{i-1} \eta_i(g_i) g_{i+1} \ldots g_r$, so folgt $1 = h_1 = \ldots = h_{i-1} = \eta_i(g_i) = g_{i+1} = \ldots = g_r$. Wegen $\overline{\varepsilon_i \circ \eta_i} \in \mathrm{Aut}_\Omega(G)$ ist dann auch $g_i = 1$. Daher ist δ injektiv. Nach Bemerkung 5.8 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 $\alpha_{i+1} := \delta \circ \alpha_i \in \mathrm{Aut}_\Omega(G)$ wie gewünscht. Für $i = r$ erhält man schließlich einen Ω-Automorphismus α_{r+1} von G mit $\alpha_{r+1}(G_1) = H_1, \ldots, \alpha_{r+1}(G_r) = H_r$, und es folgt $r = s$. □

6.6. Satz. *Gegeben sei eine Gruppe G mit Minimal- und Maximalbedingung für Normalteiler.*

(i) *Dann besitzt G eine Zerlegung $G = G_1 \oplus \ldots \oplus G_r$ mit unzerlegbaren Gruppen $G_1, \ldots, G_r$.*
(ii) *Ist $G = H_1 \oplus \ldots \oplus H_s$ eine weitere Zerlegung mit unzerlegbaren Gruppen $H_1, \ldots, H_s$, so ist $r = s$, und es gibt einen normalen Automorphismus α von G mit $\alpha(G_i) = H_i$ für $i = 1, \ldots, r$ (bei geeigneter Numerierung).*
(iii) *Die Zerlegung $G = G_1 \oplus \ldots \oplus G_r$ ist genau dann eindeutig (bis auf die Reihenfolge von $G_1, \ldots, G_r$), wenn für alle $i, j \in \{1, \ldots r\}$ mit $i \neq j$ nur der triviale Homomorphismus $G_i \to Z(G_j)$ existiert.*

Beweis.

(i),(ii) sind Spezialfälle von 6.4, 6.5.

(iii) Seien $G = G_1 \oplus \ldots \oplus G_r = H_1 \oplus \ldots \oplus H_r$ Zerlegungen in unzerlegbare Gruppen $G_1, H_1, \ldots, G_r, H_r$, wobei o.B.d.A. $G_1 \notin \{H_1, \ldots, H_r\}$. Nach geeigneter Umnumerierung existiert ein normaler Automorphismus α von G mit $\alpha(G_1) = H_1, \ldots, \alpha(G_r) = H_r$. Für $x \in G_1$ gilt nach Bemerkung 5.7: $x^{-1}\alpha(x) \in Z(G) = Z(G_1) \oplus \ldots \oplus Z(G_r)$, also $x^{-1}\alpha(x) = z_1 \ldots z_r$ mit eindeutig bestimmten $z_1 \in Z(G_1), \ldots, z_r \in Z(G_r)$. Indem man x auf z_i abbildet, erhält man für $i = 1, \ldots, r$ eine Abbildung $\tau_i : G_1 \to Z(G_i)$. Ist auch $\tilde{x} \in G_1$ und $\tilde{x}^{-1}\alpha(\tilde{x}) = \tilde{z}_1 \ldots \tilde{z}_r$ mit $\tilde{z}_1 \in Z(G_1), \ldots, \tilde{z}_r \in Z(G_r)$, so ist

$$\begin{aligned} (x\tilde{x})^{-1}\alpha(x\tilde{x}) &= \tilde{x}^{-1}x^{-1}\alpha(x)\alpha(\tilde{x}) = x^{-1}\alpha(x)\tilde{x}^{-1}\alpha(\tilde{x}) = \\ &= z_1 \ldots z_r \tilde{z}_1 \ldots \tilde{z}_r = z_1\tilde{z}_1 \ldots z_r\tilde{z}_r. \end{aligned}$$

Daher ist τ_i ein Homomorphismus. Wäre $\tau_i(x) = 1$ für $x \in G_1$, und $i = 2, \ldots, r$, so wäre $x^{-1}\alpha(x) \in Z(G_1)$ für $x \in G_1$, und damit $H_1 = \alpha(G_1) \subseteq G_1$. Nach Fitting wäre dann sogar $H_1 = \alpha(G_1) = G_1$. Daher ist mindestens einer der Homomorphismen $\tau_2, \ldots, \tau_r$ nichttrivial.
Sei umgekehrt $\tau : G_1 \to Z(G_2)$ ein nichttrivialer Homomorphismus und $\tilde{G}_1 := \{g_1\tau(g_1) : g_1 \in G_1\}$. Dann ist $\tilde{G}_1 \trianglelefteq G$; denn es ist $1 \in \tilde{G}_1$, und für $g_1, g_1' \in G_1,\ g \in G$ ist

$$\begin{aligned} &g_1'\tau(g_1')(g_1\tau(g_1))^{-1} = g_1'\tau(g_1')\tau(g_1^{-1})g_1^{-1} = g_1'g_1^{-1}\tau(g_1'g_1^{-1}) \in \tilde{G}_1 \qquad \text{und} \\ &gg_1\tau(g_1)g^{-1} = gg_1g^{-1}\tau(g_1) = gg_1g^{-1}\tau(g)\tau(g_1)\tau(g)^{-1} = \underbrace{(gg_1g^{-1})}_{\in G_1}\tau(gg_1g^{-1}) \in \tilde{G}_1. \end{aligned}$$

Ferner ist $G_1 \neq \tilde{G}_1$, und jedes Element $g \in G$ läßt sich in der Form

$$g = g_1 \dots g_r = \underbrace{g_1 \tau(g_1)}_{\in \tilde{G}_1} \underbrace{\tau(g_1^{-1}) g_2}_{\in G_2} g_3 \dots g_r$$

mit $g_1 \in G_1, \dots, g_r \in G_r$ schreiben. Ist $g_1 \in G_1$ mit $g_1 \tau(g_1) \in G_2 \oplus \dots \oplus G_r$, so ist $g_1 \in G_2 \oplus \dots \oplus G_r$, also $g_1 = 1$. Folglich gilt $G = \tilde{G}_1 \oplus G_2 \oplus \dots \oplus G_r$.

□

KAPITEL 7

Kommutatoren

7.1. Definition. Für Elemente x, y einer Gruppe G bezeichnet man $[x, y] := xyx^{-1}y^{-1}$ als *Kommutator* von x und y.

Bemerkung.

(i) In manchen Büchern definiert man $[x, y]$ durch $x^{-1}y^{-1}xy$.
(ii) Offenbar ist $xy = [x, y]yx,\ [x, y]^{-1} = [y, x]$ und $[x, y] = (xyx^{-1})y^{-1} = x(yx^{-1}y^{-1})$.
(iii) Ist H eine Gruppe und $f : G \to H$ ein Homomorphismus, so ist $f([x, y]) = [f(x), f(y)]$ für $x, y \in G$.
(iv) Für $x, y \in G$ ist

$$[xy, z] = xyzy^{-1}x^{-1}z^{-1} = x[y, z]zx^{-1}z^{-1} = (x[y, z]x^{-1})[x, z],$$
$$[x, yz] = xyzx^{-1}z^{-1}y^{-1} = [x, y]yxzx^{-1}z^{-1}y^{-1} = [x, y](y[x, z]y^{-1}).$$

7.2. Definition. 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.

(i) Manche Bücher bevorzugen linksnormierte Kommutatoren.
(ii) Für $x, y, z \in G$ gilt nach Bemerkung 7.1:

$$[xy, z] = [x, y, z][y, z][x, z]$$
$$[x, yz] = [x, y][y, x, z][x, z].$$

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

Satz (Witt-Identität)**.** *Für Elemente x, y, z einer Gruppe G gilt stets:*

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

Beweis. Wegen

$$y[x, y^{-1}, z]y^{-1} = yx[y^{-1}, z]x^{-1}[z, y^{-1}]y^{-1} = yxy^{-1}zyz^{-1}x^{-1}zy^{-1}z^{-1}yy^{-1}$$

ist die linke Seite der Identität gleich

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

□

7.3. Definition. Für Teilmengen A, B einer Gruppe G setzt man $[A, B] := \langle [a, b] : a \in A,\ b \in B \rangle$.

Bemerkung.

(i) Nach Bemerkung 7.1(ii) ist $[A, B] = [B, A]$.
(ii) Für jede Gruppe H und jeden Homomorphismus $f : G \to H$ ist $f([A, B]) = [f(A), f(B)]$; insbesondere ist mit A, B auch $[A, B]$ eine normale bzw. charakteristische Untergruppe von G.
(iii) $[A, B] = 1 \ \Leftrightarrow\ \forall a \in A,\ b \in B : ab = ba$.

Satz. *Für Untergruppen A, B einer Gruppe G gilt:*

(i) $[A, B] \trianglelefteq \langle A, B \rangle$.
(ii) $[A, B] \leq A \ \Leftrightarrow\ B \leq N_G(A)$.

Beweis.

(i) Nach Bemerkung 7.1(iv) ist $a[a',b]a^{-1} = [aa',b][a,b]^{-1} \in [A,B]$ für $a,a' \in A,\ b \in B$. Folglich ist $a[A,B]a^{-1} \subseteq [A,B]$.

(ii) $$\begin{aligned}[A,B] \leq A &\Leftrightarrow \forall a \in A,\ b \in B : [a,b] = aba^{-1}b^{-1} \in A \\ &\Leftrightarrow \forall a \in A,\ b \in B : ba^{-1}b^{-1} \in A \\ &\Leftrightarrow B \leq N_G(A).\end{aligned}$$

□

7.4. Definition. Für Teilmengen $X_1, \ldots, X_n$ einer Gruppe G definiert man induktiv: $[X_1, \ldots, X_n] := [X_1, [X_2, \ldots, X_n]]$.

Bemerkung.

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

(ii) Für jede Gruppe G und jeden Homomorphismus $f : G \to H$ ist $f([X_1, \ldots, X_n]) = [f(X_1), \ldots, f(X_n)]$.

Satz. *Für Untergruppen A, B, C einer Gruppe G gilt:*

(i) $B \leq N_G(A) \cap N_G(C) \ \Rightarrow\ [A, BC] = [A,B][A,C]$.

(ii) *(Drei-Untergruppen-Lemma)*
$[A,B,C] = 1 = [B,C,A] \ \Rightarrow\ [C,A,B] = 1$.

Beweis.

(i) Sei $B \leq N_G(A) \cap N_G(C)$. Wegen $C \trianglelefteq N_G(C)$ ist $BC \leq N_G(C)$. Nach Satz 7.3 ist $[A,C] \trianglelefteq \langle A, C\rangle$ und $[A,B] \leq A \leq N_G([A,C])$. Wegen $[A,C] \trianglelefteq N_G([A,C])$ ist daher $[A,B][A,C] \leq N_G([A,C])$. Für $a \in A,\ b \in B,\ c \in C$ gilt nach 7.1:

$$[a,bc] = [a,b]b[a,c]b^{-1} = [a,b][\underbrace{bab^{-1}}_{\in A}, \underbrace{bcb^{-1}}_{\in C}] \in [A,B][A,C].$$

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

(ii) Aus $[A,B,C] = 1 = [B,C,A]$ folgt mit der Witt-Identität: $[c,[a,b]] = 1$ für alle $a \in A,\ b \in B,\ c \in C$. Folglich ist $C \leq C_G([A,B])$ nach Bemerkung 7.3(iii), d.h. $[C,[A,B]] = 1$.

□

7.5. Definition. Für jede Gruppe G und $n \in \mathbb{N}$ definiert man induktiv: $G^1 := G,\ G^2 := [G,G],\ G^{n+1} := [G, G^n]$.

Bemerkung.

(i) Es ist also $G^n = [\underbrace{G, \ldots, G}_{n}]$ für $n \in \mathbb{N}$.

(ii) Man zeigt leicht, daß $U^n \leq G^n$ für $n \in \mathbb{N}$ und jede Untergruppe U von G gilt.

(iii) Nach Bemerkung 7.4(ii) ist $f(G^n) = f(G)^n \leq H^n$ für jeden Homomorphismus f von G in eine Gruppe H; insbesondere ist G^n vollinvariant in G.

(iv) Nach (iii) ist $G^n \trianglelefteq G$, also $G^{n+1} \leq G^n$ nach 7.3. Man erhält so eine Folge von vollinvarianten Untergruppen $G = G^1 \geq G^2 \geq G^3 \geq \ldots$; diese Folge nennt man die *absteigende Zentralfolge* von G. Wir setzen $G^\infty := \bigcap_{i \in \mathbb{N}} G^i$.

(v) Für $n \in \mathbb{N}$ gilt nach Bemerkung 7.4: $[G/G^{n+1}, G^n/G^{n+1}] = [G,G^n]G^{n+1}/G^{n+1} = G^{n+1}/G^{n+1} = 1$, d.h. $G^n/G^{n+1} \leq Z(G/G^{n+1})$.

Satz. *Für $n \in \mathbb{N}$ mit $n \geq 2$ ist $G^n = \langle [g_1, \ldots, g_n] : g_1, \ldots, g_n \in G\rangle$.*

Beweis. (Induktion nach n) O.B.d.A. sei $n \geq 3$. Offenbar ist $N := \langle [g_1, \ldots, g_n] : g_1, \ldots, g_n \in G\rangle \trianglelefteq G$ und $N \subseteq G^n$. Nach Induktion dürfen wir $G^{n-1} = \langle [g_2, \ldots, g_n] : g_2, \ldots, g_n \in G\rangle$ voraussetzen. Dann ist $G^{n-1}/N = \langle [g_2, \ldots, g_n]N : g_2, \ldots, g_n \in G\rangle$, und für $g_1, \ldots, g_n \in G$ gilt: $[g_1N, [g_2, \ldots, g_n]N] =$

$[g_1, [g_2, \ldots, g_n]]N = 1$. Folglich ist $G^{n-1}/N \subseteq Z(G/N)$ und $G^n/N = [G, G^{n-1}]/N = [G/N, G^{n-1}/N] = 1$, d.h. $G^n = N$. □

7.6. Satz. *Für $m, n \in \mathbb{N}$ und jede Gruppe G ist $[G^m, G^n] \subseteq G^{m+n}$.*

Beweis. (Induktion nach n) Im Fall $n = 1$ ist $[G^m, G] = [G, G^m] = G^{m+1}$. Sei also $n \geq 2$ und die Aussage für $n-1$ bereits bewiesen. Mit $H := G/G^{m+n}$ gilt dann:

$$[G^m, G^n]G^{m+n}/G^{m+n} = [G^m/G^{m+n}, G^n/G^{m+n}] = [H^m, H^n] = [H^m, [H, H^{n-1}]].$$

Wegen

$$[H, [H^{n-1}, H^m]] = [H, [H^m, H^{n-1}]] \overset{\text{Ind.}}{\subseteq} [H, H^{m+n-1}] = H^{m+n} = G^{m+n}/G^{m+n} = 1$$

und

$$[H^{n-1}, [H^m, H]] = [[H, H^m], H^{n-1}] = [H^{m+1}, H^{n-1}] \overset{\text{Ind.}}{\subseteq} H^{m+n} = 1$$

folgt aus dem Drei-Untergruppen-Lemma:

$$[G^m, G^n]G^{m+n}/G^{m+n} = [H^m, [H, H^{n-1}]] = 1,$$

also $[G^m, G^n] \subseteq G^{m+n}$. □

7.7. Definition. Für jede Gruppe G nennt man $G' := G^2 = [G, G]$ die *Kommutatorgruppe* von G.

Bemerkung.

(i) Nach 7.5 ist G' vollinvariant in G. Ist $G = G'$, so nennt man G *perfekt*.
(ii) Eine Untergruppe U einer Gruppe G ist genau dann ein Normalteiler in G mit abelscher Faktorgruppe G/U, wenn $G' \subseteq U$ gilt. Daher ist G' der „kleinste“ Normalteiler von G mit abelscher Faktorgruppe.

7.8. Definition. Die *höheren Kommutatorgruppen* einer Gruppe G definiert man induktiv durch $G^{(0)} := G,\ G^{(1)} := G',\ G^{(2)} := G'' := [G', G'],\ G^{(i+1)} := [G^{(i)}, G^{(i)}]$ für $i \in \mathbb{N}$.

Bemerkung.

(i) Für $i \in \mathbb{N}_0$ und jede Untergruppe U von G ist $U^{(i)} \leq G^{(i)}$.
(ii) Analog ist $f(G^{(i)}) = f(G)^{(i)}$ für jeden Homomorphismus f von G in eine Gruppe H; insbesondere ist $G^{(i)}$ vollinvariant in G für $i \in \mathbb{N}_0$.
(iii) Offenbar ist $G = G^{(0)} \supseteq G^{(1)} \supseteq G^{(2)} \supseteq \ldots$; wir setzen $G^{(\infty)} := \bigcap_{i \in \mathbb{N}} G^{(i)}$.

Satz. *Für $n \in \mathbb{N}_0$ und jede Gruppe G ist $G^{(n)} \subseteq G^{2^n}$.*

Beweis. (Induktion nach n) Wegen $G^{(0)} = G = G^1 = G^{2^0}$ sei o.B.d.A. $n \in \mathbb{N}$ und $G^{(n-1)} \subseteq G^{2^{n-1}}$. Nach 7.6 ist dann $G^{(n)} = [G^{(n-1)}, G^{(n-1)}] \subseteq [G^{2^{n-1}}, G^{2^{n-1}}] \subseteq G^{2^n}$. □

KAPITEL 8

Auflösbare und nilpotente Gruppen

8.1. Definition. Eine Gruppe G mit $G^{(s)} = 1$ für ein $s \in \mathbb{N}_0$ nennt man *auflösbar*; gegebenenfalls nennt man das kleinste s mit $G^{(s)} = 1$ die *(Auflösbarkeits-)Stufe* von G.

Bemerkung.

(i) $s = 0 \Leftrightarrow G = 1$.
$s \leq 1 \Leftrightarrow G' = 1 \Leftrightarrow G$ abelsch.
$s \leq 2 \Leftrightarrow$: G *metabelsch.*

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

(iii) Hat man umgekehrt eine Subnormalreihe $G = G_0 \trianglerighteq G_1 \trianglerighteq \ldots \trianglerighteq G_t = 1$ einer Gruppe G mit abelschen Faktoren, so ist $G^{(i)} \subseteq G_i$ für $i = 0, \ldots, t$; insbesondere ist $G^{(t)} = 1$, d.h. G ist auflösbar, und die Stufe von G ist höchstens t.

(iv) Für jede Gruppe G gilt also: G ist auflösbar $\Leftrightarrow$ G besitzt eine Normalreihe mit abelschen Faktoren $\Leftrightarrow$ G besitzt eine Subnormalreihe mit abelschen Faktoren.

(v) Für jede endliche Gruppe G gilt: G ist auflösbar $\Leftrightarrow$ alle Kompositionsfaktoren haben Primzahlordnung. Da Hauptfaktoren stets charakteristisch einfach sind, ergibt sich mit 5.5: G ist auflösbar $\Leftrightarrow$ alle Hauptfaktoren von G sind direkte Summen von isomorphen Gruppen von Primzahlordnung.

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

(vii) Für jeden Normalteiler N einer Gruppe G gilt: G auflösbar $\Leftrightarrow$ $N, G/N$ auflösbar.

(viii) Burnside hat 1904 gezeigt, daß für beliebige Primzahlen p, q und beliebige $a, b \in \mathbb{N}_0$ Gruppen der Ordnung $p^a q^b$ auflösbar sind. Er vermutete auch, daß Gruppen ungerader Ordnung stets auflösbar sind. Dies haben W. Feit und J. Thompson 1963 bewiesen. Ihr Beweis ist ca. 250 Seiten lang. Beide Beweise verwenden wesentlich die Darstellungstheorie endlicher Gruppen.

(ix) Sind die Gruppen G, H auflösbar, so auch $G \times H$; denn für $i \in \mathbb{N}_0$ gilt offenbar: $(G \times H)^{(i)} = G^{(i)} \times H^{(i)}$.

(x) Sind M, N Normalteiler einer Gruppe G mit auflösbaren Faktorgruppen G/M und G/N, so ist $G/M \cap N$ auflösbar; denn nach 3.7 ist $G/M \cap N$ isomorph zu einer Untergruppe von $G/M \times G/N$.

(xi) Für auflösbare Normalteiler M, N einer Gruppe G ist auch MN auflösbar; dies folgt aus (vii) wegen $MN/N \cong M/M \cap N$. In einer endlichen Gruppe G ist also das Produkt aller auflösbaren Normalteiler ein auflösbarer Normalteiler S von G. Man nennt S das *auflösbare Radikal* von G.

Beispiel.

(i) $\mathrm{Sym}(n)$ ist auflösbar $\Leftrightarrow$ $n \leq 4$. Kompositionsreihen von $\mathrm{Sym}(3)$ und $\mathrm{Sym}(4)$ sind:

$$\mathrm{Sym}(3) \trianglerighteq \mathrm{Alt}(3) \trianglerighteq 1,$$
$$\mathrm{Sym}(4) \trianglerighteq \mathrm{Alt}(4) \trianglerighteq V_4 \trianglerighteq \langle \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \rangle \trianglerighteq 1.$$

(ii) Gruppen von Primzahlpotenzordnung sind auflösbar.

(iii) Für beliebige Primzahlen p, q, r sind Gruppen der Ordnungen pq und pqr stets auflösbar.

(iv) Gruppen der Ordnungen $1, \ldots, 59$ sind auflösbar.

8.2. Definition. Für jede Gruppe G definiert man die *aufsteigende Zentralfolge* induktiv durch $Z_0(G) := 1$, $Z_1(G) := Z(G)$, $Z_i(G)/Z_{i-1}(G) := Z(G/Z_{i-1}(G))$ für $i \in \mathbb{N}$.

Bemerkung. Für $i \in \mathbb{N}_0$ ist $Z_i(G)$ charakteristisch in G; dies ist klar für $i = 0, 1$, und ist $Z_{i-1}(G)$ charakteristisch in G für ein $i \in \mathbb{N}$, so induziert jeder Automorphismus α von G einen Automorphismus $\overline{\alpha}$ von $G/Z_{i-1}(G)$, wenn man definiert: $\overline{\alpha}(gZ_{i-1}(G)) := \alpha(g)Z_{i-1}(G)$ für $g \in G$. Da $Z(G/Z_{i-1}(G))$ charakteristisch in $G/Z_{i-1}(G)$ ist, folgt: $\overline{\alpha}(Z_i(G)/Z_{i-1}(G)) = Z_i(G)/Z_{i-1}(G)$. Folglich ist $\alpha(g) \in Z_i(G)$ für $g \in Z_i(G)$.
Man hat $1 = Z_0(G) \subseteq Z_1(G) \subseteq Z_2(G) \subseteq \ldots$, und man nennt $Z_\infty(G) := \bigcup_{i\in\mathbb{N}} Z_i(G)$ das *Hyperzentrum* von G.

8.3. Definition. Eine Gruppe G mit $Z_c(G) = G$ für ein $c \in \mathbb{N}_0$ nennt man *nilpotent*; gegebenenfalls nennt man das kleinste c mit $Z_c(G) = G$ die *(Nilpotenz-)Klasse* von G.

Bemerkung. $c = 0 \Leftrightarrow G = 1$, $c \leq 1 \Leftrightarrow G$ abelsch.

8.4. Definition. 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 $i = 1, \ldots, r$ nennt man eine *Zentralreihe* von G.

Beispiel. 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 von G. Diese nennt man die *aufsteigende* oder *obere Zentralreihe* von G.

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

(1) *$G_0 \trianglerighteq \ldots \trianglerighteq G_r$ ist eine Zentralreihe von G.*
(2) *$[G, G_{i-1}] \subseteq G_i$ für $i = 1, \ldots, r$.*

Beweis.

(1)⇒(2): Ist (1) erfüllt, so gilt für $i = 1, \ldots, r$: $[G, G_{i-1}]G_i/G_i = [G/G_i, G_{i-1}/G_i] = 1$, d.h. $[G, G_{i-1}] \subseteq G_i$.
(2)⇒(1): Für $i = 1, \ldots, r$ sei $[G, G_{i-1}] \subseteq G_i \subseteq G_{i-1}$. Dann ist $G_{i-1} \trianglelefteq G$, d.h. es liegt eine Normalreihe vor. Ferner ist $[G/G_i, G_{i-1}/G_i] = [G, G_{i-1}]G_i/G_i = 1$, also $G_{i-1}/G_i \subseteq Z(G/G_i)$.

□

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

8.5. Satz. *Ist $G_0 \trianglerighteq \ldots \trianglerighteq G_r$ eine Zentralreihe einer Gruppe G, so ist $G_{r-i} \subseteq Z_i(G)$ und $G^{i+1} \subseteq G_i$ für $i = 0, \ldots, r$; 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. (Induktion nach i) Wegen $G_r = 1 = Z_0(G)$ und $G^1 = G = G_0$ sei o.B.d.A. $i > 0$ und bereits $G_{r-i+1} \subseteq Z_{i-1}(G)$, $G^i \subseteq G_{i-1}$ bewiesen. Dann ist

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

also

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

d.h. $G_{r-i} \subseteq Z_i(G)$. Ferner ist $G^{i+1} = [G, G^i] \subseteq [G, G_{i-1}] \subseteq G_i$. □

Bemerkung.

(i) Nach 8.4 und 8.5 ist eine Gruppe G genau dann nilpotent, wenn sie eine Zentralreihe besitzt. Gegebenenfalls ist die Klasse von G durch die Länge einer Zentralreihe beschränkt.
(ii) Ist G eine nilpotente Gruppe der Klasse c, so ist $G^{c+1} = 1$. Daher ist $G = G^1 \trianglerighteq G^2 \trianglerighteq \ldots \trianglerighteq G^{c+1} = 1$ eine Zentralreihe von G. Diese nennt man die *absteigende* oder *untere Zentralreihe* von G. Nach (i) ist ferner $G^c \neq 1$.
(iii) Eine Gruppe G ist also genau dann nilpotent, wenn $G^s = 1$ für ein $s \in \mathbb{N}$ ist.
(iv) Untergruppen und Faktorgruppen einer nilpotenten Gruppe sind nilpotent; ihre Klasse ist jeweils durch die Klasse von G beschränkt.
(v) Offenbar ist jede nilpotente Gruppe auflösbar.

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

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

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

Beweis. Da G nilpotent ist, existiert ein $n \in \mathbb{N}$ mit $G^n = 1 \subseteq U$. Wir wählen $m \in \mathbb{N}$ minimal mit $G^m \subseteq U$. Wegen $G^1 = G \not\subseteq U$ ist $m \geq 2$. Wegen $[U, G^{m-1}] \subseteq [G, G^{m-1}] = G^m \subseteq U$ ist $G^{m-1} \subseteq N_G(U)$, aber $G^{m-1} \not\subseteq U$. □

Bemerkung. Wir werden später sehen, daß man 8.6 für endliche Gruppen umkehren kann.

8.7. Satz. *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 induktiv $N_1 := N$, $N_{i+1} := [G, N_i]$ für $i \in \mathbb{N}$. Dann ist $N_i \trianglelefteq G$, $N_i \leq N$ und $N_i \subseteq G^i$ für $i \in \mathbb{N}$. Da G nilpotent ist, folgt $1 = G^m = N_m$ für ein $m \in \mathbb{N}$. Dann ist $N_2 = [G, N] < N$; denn im Fall $N_2 = N$ wäre auch $N_3 = [G, N_2] = [G, N] = N_2 = N$, usw. Wir wählen $n \in \mathbb{N}$ mit $N_n = 1 \neq N_{n-1}$. Dann ist $[G, N_{n-1}] = N_n = 1$, also $N_{n-1} \subseteq Z(G) \cap N$. □

8.8. Satz. *Sind A und B nilpotente Normalteiler einer Gruppe G, so auch AB. Hat A die Klasse a und B die Klasse b, so hat AB höchstens die Klasse $a + b$.*

Beweis. Für Normalteiler L, M, N von G ist $[L, MN] = [L, M][L, N]$ und $[LM, N] = [L, N][M, N]$ nach 7.4. Daraus folgt leicht, 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. Wir zeigen, daß jede dieser Gruppen trivial ist; dann folgt die Behauptung aus Bemerkung 8.5(iii). Zum Beweis von $[H_0, \ldots, H_{a+b}] = 1$ setzen wir $m := |\{i : 0 \leq i \leq a + b,\ H_i = A\}|$, $n := |\{i : 0 \leq i \leq a + b,\ H_i = B\}|$. Dann ist $a + b + 1 = n + m$, also $m > a$ oder $n > b$, o.B.d.A. $m > a$. Offenbar ist dann $[H_0, \ldots, H_{a+b}] \subseteq A^m \subseteq A^{a+1} = 1$. □

Bemerkung. Für jede endliche Gruppe G ist das Produkt aller nilpotenten Normalteiler ein nilpotenter Normalteiler $F(G)$ von G. Man nennt $F(G)$ die *Fittinggruppe* von G (Fitting 1906–1938). Offenbar ist $F(G)$ charakteristisch in G.

8.9. Satz. *Für jede endliche Gruppe G ist das auflösbare Radikal von $C_G(F(G))F(G)/F(G)$ trivial. Ist G auflösbar, so ist also $C_G(F(G)) \subseteq F(G)$, d.h. $C_G(F(G)) = Z(F(G))$.*

Beweis. Wir bezeichnen mit S das auflösbare Radikal von $C_G(F(G))F(G)/F(G)$ und nehmen $S \neq 1$ an. Dann wählen wir $n \in \mathbb{N}$ minimal mit $S^{(n)} = 1$. Dann ist $S^{(n-1)}$ ein nichttrivialer abelscher Normalteiler von $G/F(G)$ mit $S^{(n-1)} \subseteq C_G(F(G))F(G)/F(G)$. Wir schreiben $S^{(n-1)} = N/F(G)$ mit einem Normalteiler N von G mit $F(G) \subsetneqq N \subseteq C_G(F(G))F(G)$. Nach Dedekind ist $N = N \cap C_G(F(G))F(G) = CF(G)$ mit $C := N \cap C_G(F(G)) \trianglelefteq N$. Wegen $N/C \subseteq F(G)C/C \cong F(G)/F(G) \cap C$ ist N/C nilpotent. Es existiert also ein $k \in \mathbb{N}$ mit $1 = (N/C)^k = N^kC/C$, d.h. $N^k \subseteq C$. Da $N/F(G)$ abelsch ist, ist andrerseits $N' \subseteq F(G)$, also

$$N^{k+1} \subseteq C \cap F(G) \subseteq Z(F(G)) \leq N \cap C_G(N) = Z(N)$$

und damit $N^{k+2} = [N, N^{k+1}] = 1$. Folglich ist N nilpotent, und man erhält den Widerspruch $N \subseteq F(G)$. □

Bemerkung. Jede endliche auflösbare Gruppe G setzt sich also zusammen aus der abelschen Gruppe $Z(F(G))$ und der Faktorgruppe $G/Z(F(G)) = G/C_G(F(G))$, die zu einer Untergruppe der Automorphismengruppe der nilpotenten Gruppe $F(G)$ isomorph ist.

8.10. Satz. *Für jeden minimalen Normalteiler N einer endlichen Gruppe G ist $F(G) \subseteq C_G(N)$.*

Beweis. Fall 1: N nicht nilpotent. Dann ist $N \not\subseteq F(G)$, also $N \cap F(G) < N$. Aus der Minimalität von N folgt dann $N \cap F(G) = 1$. Nach 3.7 ist also $F(G) \subseteq C_G(N)$.
Fall 2: N nilpotent, also $N \trianglelefteq F(G)$. Nach 8.7 ist $1 \neq N \cap Z(F(G)) \subseteq N$, also $N = N \cap Z(F(G)) \subseteq Z(F(G))$ wegen der Minimalität von N. Folglich ist $F(G) \subseteq C_G(N)$. □

8.11. Definition. Für Normalteiler K, H einer Gruppe G mit $K \subseteq H$ definiert man den Normalteiler $C_G(H/K)$ von G mit $K \subseteq C_G(H/K)$ durch $C_G(H/K)/K := C_{G/K}(H/K)$.

Satz. *Für jede Hauptreihe $G_0 \trianglerighteq \ldots \trianglerighteq G_r$ einer endlichen Gruppe G ist $F(G) = \bigcap_{i=1}^{r} C_G(G_{i-1}/G_i)$.*

Bemerkung. Nach 3.7 ist also $G/F(G)$ isomorph zu einer Untergruppe von

$$\begin{aligned} \bigtimes_{i=1}^{r} G/C_G(G_{i-1}/G_i) &\cong \bigtimes_{i=1}^{r} (G/G_i)/(C_G(G_{i-1}/G_i)/G_i) = \\ &= \bigtimes_{i=1}^{r} \underbrace{(G/G_i)/C_{G/G_i}(G_{i-1}/G_i)}_{\text{isom. zu einer Ugr. von } \mathrm{Aut}(G_{i-1}/G_i)}, \end{aligned}$$

wobei jedes G_{i-1}/G_i charakteristisch einfach, also direkte Summe isomorpher einfacher Gruppen ist. Auf diese Weise baut sich jede endliche Gruppe auf aus der nilpotenten Gruppe $F(G)$ und einer Untergruppe eines direkten Produkts von Automorphismengruppen charakteristisch einfacher Gruppen.

Beweis. Wir setzen $D := \bigcap_{i=1}^{r} C_G(G_{i-1}/G_i)$ und $D_i := D \cap G_i$ für $i = 0, \ldots, r$. Dann ist $D = D_0 \trianglerighteq D_1 \trianglerighteq \ldots \trianglerighteq D_r = 1$, und für $i = 1, \ldots, r$ gilt:

$$\begin{aligned} [D, D_{i-1}]G_i/G_i &\subseteq [C_G(G_{i-1}/G_i), G_{i-1}]G_i/G_i = [C_G(G_{i-1}/G_i)/G_i, G_{i-1}/G_i] = \\ &= [C_{G/G_i}(G_{i-1}/G_i), G_{i-1}/G_i] = 1, \end{aligned}$$

also $[D, D_{i-1}] \subseteq D \cap G_i = D_i$. Folglich liegt eine Zentralreihe von D vor, d.h. D ist nilpotent. Wegen $D \trianglelefteq G$ ist also $D \subseteq F(G)$.
Umgekehrt ist G_{i-1}/G_i für $i = 1, \ldots, r$ ein minimaler Normalteiler von G/G_i. Ferner ist $F(G)G_i/G_i \cong F(G)/F(G) \cap G_i$ nilpotent, also

$$F(G)G_i/G_i \subseteq F(G/G_i) \subseteq C_{G/G_i}(G_{i-1}/G_i) = C_G(G_{i-1}/G_i)/G_i$$

nach 8.10; insbesondere ist $F(G) \subseteq C_G(G_{i-1}/G_i)$. □

KAPITEL 9

Sylowgruppen

9.1. Satz (Sylow)**.** *Gegeben seien eine endliche Gruppe G, eine Primzahl p und eine Zahl $a \in \mathbb{N}_0$ mit $p^a \mid |G|$. Dann enthält G eine Untergruppe der Ordnung p^a, und für die Anzahl $z_G(p^a)$ dieser Untergruppen gilt: $z_G(p^a) \equiv 1 \pmod{p}$.*

Beweis. Algebra. □

9.2. Korollar (Cauchy)**.** *Zu jedem Primteiler p der Ordnung einer endlichen Gruppe G enthält G ein Element der Ordnung p.*

Beweis. 9.1 mit $a = 1$. □

Bemerkung. Aus dem Satz von Cauchy folgt unmittelbar, daß für jede endliche Gruppe G und jede Menge π von Primzahlen gilt: G π-Gruppe $\Leftrightarrow$ alle Primteiler von $|G|$ liegen in π. Insbesondere gilt für jede endliche Gruppe G und jede Primzahl p: G p-Gruppe $\Leftrightarrow$ $|G|$ Potenz von p.

9.3. Definition. Sei G endliche Gruppe, p Primzahl, $|G| = p^a m$ mit $a \in \mathbb{N}_0$, $m \in \mathbb{N}$, $p \nmid m$. Untergruppen der Ordnung p^a von G nennt man dann *p-Sylowgruppen* von G.

Satz (Sylow)**.** *Für jede endliche Gruppe G und jede Primzahl p gilt:*

(i) *G enthält eine p-Sylowgruppe.*
(ii) *Je zwei p-Sylowgruppen von G sind in G konjugiert.*
(iii) *Für jede p-Sylowgruppe P von G enthält G genau $|G : N_G(P)|$ p-Sylowgruppen.*
(iv) *Für jede p-Sylowgruppe P von G ist $|G : N_G(P)| \equiv 1 \pmod{p}$.*
(v) *Jede p-Untergruppe von G ist in einer p-Sylowgruppe von G enthalten.*

Beweis. Algebra. □

Bemerkung. Für jede endliche Gruppe G, jede Primzahl p, jede p-Sylowgruppe P von G und jeden Normalteiler N von G gilt nach Aufgabe 1 von Blatt 3: $P \cap N$ ist p-Sylowgruppe von N, und PN/N ist p-Sylowgruppe von G/N.

9.4. Satz (Frattini-Argument (Frattini, 1852–1925))**.**
Gegeben seien eine endliche Gruppe G, ein Normalteiler H von G, eine Primzahl p und eine p-Sylowgruppe P von H. Dann ist $G = N_G(P)H$.

Beweis. Für $x \in G$ ist $xPx^{-1} \subseteq xHx^{-1} = H$, d.h. xPx^{-1} ist auch p-Sylowgruppe von H. Daher operieren G und H transitiv durch Konjugation auf der Menge Ω aller p-Sylowgruppen von H. Nach 2.10 ist $G = N_G(P)H$. □

9.5. Satz. *Für jede endliche Gruppe G, jede Primzahl p, jede p-Sylowgruppe P von G und jede Untergruppe U von G mit $N_G(P) \leq U$ ist $N_G(U) = U$.*

Bemerkung. Vergleiche Aufgabe 1 von Blatt 3.

Beweis. Unter den gegebenen Voraussetzungen ist P auch p-Sylowgruppe von U. Wegen $U \trianglelefteq N_G(U)$ gilt nach 9.4: $N_G(U) = N_{N_G(U)}(P)U \subseteq N_G(P)U \subseteq U \subseteq N_G(U)$. □

9.6. Satz (Burnside, 1852–1927)**.** *Gegeben seien eine endliche Gruppe G, eine Primzahl p, eine p-Sylowgruppe P von G und Teilmengen K, L von G mit $xKx^{-1} = K$, $xLx^{-1} = L$ für $x \in P$. Existiert ein Element $g \in G$ mit $gKg^{-1} = L$, so auch ein $h \in N_G(P)$ mit $hKh^{-1} = L$.*

Beweis. Sei $g \in G$ mit $gKg^{-1} = L$. Dann ist $P \leq N_G(K)$ und $P \leq N_G(L) = N_G(gKg^{-1}) = gN_G(K)g^{-1}$, also $g^{-1}Pg \leq N_G(K)$. Nach Sylow existiert ein $y \in N_G(K)$ mit $yg^{-1}Pgy^{-1} = P$. Folglich ist $gy^{-1} \in N_G(P)$ und $gy^{-1}Kyg^{-1} = gKg^{-1} = L$. □

9.7. Satz (Frobenius)**.** *Für jede endliche Gruppe G, jede Konjugationsklasse C von G und $n \in \mathbb{N}$ ist die Anzahl der Elemente $g \in G$ mit $g^n \in C$ durch* $\mathrm{ggT}(n|C|, |G|)$ *teilbar.*

Beweis. Für jede Teilmenge X von G setzen wir $F_G(X, n) := \{g \in G : g^n \in X\}$ und $f_G(X, n) := |F_G(X, n)|$. Die Aussage ist trivial, falls $|G| = 1$ oder $n = 1$. Wir argumentieren im folgenden mit Induktion nach $|G| + n$. Offenbar ist

$$F_G(C, n) = \dot{\bigcup_{c \in C}} F_G(\{c\}, n) = \dot{\bigcup_{c \in C}} F_{C_G(c)}(\{c\}, n)$$

und

$$F_G(\{xcx^{-1}\}, n) = xF_G(\{c\}, n)x^{-1}$$

für $c \in C,\ x \in G$. Daher ist $f_G(C, n) = |C| f_{C_G(c)}(\{c\}, n)$; dabei ist $\{c\}$ eine Konjugationsklasse von $C_G(c)$.
Im Fall $G \neq C_G(c)$ kann man mit Induktion voraussetzen:

$$\mathrm{ggT}(n, |C_G(c)|) \mid f_{C_G(c)}(\{c\}, n).$$

Wegen $|G| = |G : C_G(c)| \cdot |C_G(c)| = |C| \cdot |C_G(c)|$ ergibt sich daraus:

$$\mathrm{ggT}(n|C|, |G|) = |C| \cdot \mathrm{ggT}(n, |C_G(c)|) \mid |C| f_{C_G(c)}(\{c\}, n) = f_G(C, n).$$

Es bleibt also der Fall $G = C_G(c)$. In diesem Fall ist $c \in Z(G)$ und $C = \{c\}$, und wir müssen $\mathrm{ggT}(n, |G|) \mid f_G(C, n)$ zeigen.
Wir betrachten zunächst den Spezialfall, daß $n = n_1 n_2$ mit teilerfremden $n_1, n_2 \in \mathbb{N} \setminus \{1\}$ ist, und setzen $D := F_G(C, n_2)$. Offenbar ist $F_G(C, n) = F_G(D, n_1)$, und D ist disjunkte Vereinigung von Konjugationsklassen $C_1, \ldots, C_t$ von G. Daher ist

$$F_G(D, n_1) = F_G(C_1, n_1) \dot{\cup} \ldots \dot{\cup} F_G(C_t, n_1)$$

und

$$f_G(D, n_1) = f_G(C_1, n_1) + \ldots + f_G(C_t, n_1).$$

Nach Induktion kann man $\mathrm{ggT}(n_1|C_i|, |G|) \mid f_G(C_i, n_1)$ für $i = 1, \ldots, t$ annehmen. Dann ist

$$\mathrm{ggT}(n_1, |G|) \mid f_G(D, n_1) = f_G(C, n).$$

Analog ist $\mathrm{ggT}(n_2, |G|) \mid f_G(C, n)$, also auch $\mathrm{ggT}(n, |G|) \mid f_G(C, n)$.
Wir brauchen also nur noch den Fall zu betrachten, daß $n = p^m$ für ein $m \in \mathbb{N}$ und eine Primzahl p ist. Sei zunächst $p \mid \alpha := |\langle c \rangle|$. Für $x \in F_G(C, n)$ ist $x^{p^m \alpha} = c^\alpha = 1$, also $|\langle x \rangle| \mid p^m \alpha$. Wegen $p \mid \alpha$ ist $x^{p^{m-1}\alpha} = c^{\alpha/p} \neq 1$, und für jeden echten Teiler β von α ist $x^{p^m \beta} = c^\beta \neq 1$. Dies zeigt, daß alle Elemente in $F_G(C, n)$ die Ordnung $p^m \alpha$ haben. Daher ist $F_G(C, n)$ die disjunkte Vereinigung aller $F_H(C, n)$, wobei H alle zyklischen Untergruppen von G durchläuft, die von einem Element aus $F_G(C, n)$ erzeugt werden. Für ein Element $x \in F_G(C, n)$ und ein Element $y \in \langle x \rangle$ gilt dabei:

$$xy \in F_G(C, n) \ \Leftrightarrow\ (xy)^{p^m} = c \ \Leftrightarrow\ x^{p^m} y^{p^m} = c \ \Leftrightarrow\ y^{p^m} = 1 \ \Leftrightarrow\ y \in \langle x^\alpha \rangle.$$

Daher ist $f_{\langle x \rangle}(C, n) = |\langle x^\alpha \rangle| = p^m$. Insbesondere ist $p^m \mid f_G(C, n)$.
Es bleibt der Fall $p \nmid \alpha$ übrig. In diesem Fall ist $\mathrm{ggT}(p^m, \alpha) = 1$, d.h. es existieren $k, l \in \mathbb{Z}$ mit $kp^m + l\alpha = 1$. Setzt man $d := c^k$, so ist

$$d^{p^m} = c^{kp^m} = c^{kp^m} c^{l\alpha} = c^{kp^m + l\alpha} = c^1 = c.$$

Für ein Element $x \in G$ gilt also: $x^{p^m} = c \ \Leftrightarrow (xd^{-1})^{p^m} = 1$. Folglich ist $F_G(\{c\}, n) = F_G(\{1\}, n)d$ und $f_G(C, n) = f_G(\{1\}, n)$. Offenbar ist $Z := \{z \in Z(G) : p \nmid |\langle z \rangle|\} \leq G$. Bezeichnet man mit $\mathcal{K}$ die Menge aller Konjugationsklassen von G, so ist

$$|G| = \sum_{K \in \mathcal{K}} f_G(K, n) = \sum_{K \in \mathcal{K}, K \not\subseteq Z} f_G(K, n) + |Z| f_G(\{c\}, n).$$

Nach den erledigten Fällen ist $\mathrm{ggT}(n, |G|) \mid f_G(K, n)$ für $K \not\subseteq Z$. Also gilt auch: $\mathrm{ggT}(n, |G|) \mid |Z| f_G(C, n)$. Nach Cauchy ist $p \nmid |Z|$. Folglich ist $\mathrm{ggT}(n, |G|) \mid f_G(C, n)$. □

Bemerkung. Für jede endliche Gruppe G und jeden Teiler n von $|G|$ ist also insbesondere die Anzahl der Elemente $g \in G$ mit $g^n = 1$ durch n teilbar. Frobenius hat vermutet, daß im Fall $|\{g \in G : g^n = 1\}| = n$ die Elemente $g \in G$ mit $g^n = 1$ eine Untergruppe bilden, und dies in mehreren Fällen auch bewiesen.

KAPITEL 10

Einfache Anwendungen der Sylow-Sätze

10.1. Lemma. *Für $n \in \mathbb{N}$, jede Primzahl p und jede Gruppe G der Ordnung p^n ist $Z(G) \neq 1$.*

Beweis. Algebra. □

10.2. Satz. *Für $n \in \mathbb{N}_0$ und jede Primzahl p ist jede Gruppe G der Ordnung p^n nilpotent.*

Beweis. (Induktion nach n) O.B.d.A. sei $n \neq 0$. Sei die Behauptung für Gruppen kleinerer Ordnung bewiesen. Nach 10.1 ist $Z(G) \neq 1$, also $|G/Z(G)| = p^m$ für ein $m \in \mathbb{N}_0$ und $m < n$. Nach Induktion ist $G/Z(G)$ nilpotent. Daher existiert ein $k \in \mathbb{N}$ mit $1 = (G/Z(G))^k = G^k Z(G)/Z(G)$, d.h. $G^k \subseteq Z(G)$. Folglich ist $G^{k+1} = [G, G^k] \subseteq [G, Z(G)] = 1$, d.h. G ist nilpotent. □

10.3. Satz. *Für eine endliche Gruppe G sind äquivalent:*

(1) *G ist nilpotent.*
(2) *Für jede echte Untergruppe U von G ist $U < N_G(U)$.*
(3) *Jede maximale Untergruppe ist normal in G.*
(4) *Für jeden Primteiler p von $|G|$ enthält G genau eine p-Sylowgruppe.*
(5) *G ist direkte Summe seiner Sylowgruppen.*

Beweis.

(1)⇒(2): 8.6.
(2)⇒(3): Trivial.
(3)⇒(4): Sei (3) erfüllt, p ein Primteiler von $|G|$ und P eine p-Sylowgruppe von G. Wäre $G \neq N_G(P)$, so gäbe es eine maximale Untergruppe M von G mit $N_G(P) \leq M$. Nach 9.5 wäre dann $M = N_G(M)$, was (3) widerspricht. Also ist $G = N_G(P)$. Nach Sylow ist P die einzige p-Sylowgruppe von G.
(4)⇒(5): Ist (4) erfüllt, so ist jede Sylowgruppe normal in G. Mit 5.4 folgt die Behauptung.
(5)⇒(1): Nach 10.2 ist jede Sylowgruppe von G nilpotent, und offenbar sind direkte Produkte von nilpotenten Gruppen wieder nilpotent.

□

10.4. Satz. *Gegeben seien eine endliche Gruppe G und eine Primzahl p. Eine p-Untergruppe P von G ist genau dann eine p-Sylowgruppe von G, wenn P eine p-Sylowgruppe von $N_G(P)$ ist.*

Beweis.

⇒: Trivial.
⇐: Aufgabe 1(iii) von Blatt 5.

□

10.5. Satz. *Für $n \in \mathbb{N}$ und beliebige Primzahlen p, q ist jede Gruppe G der Ordnung $p^n q$ auflösbar.*

Bemerkung. Dies ist ein Spezialfall eines früher erwähnten Satzes von Burnside.

Beweis. Wir nehmen an, daß die Aussage falsch ist, und wählen ein Gegenbeispiel möglichst kleiner Ordnung. Wegen 10.2 ist $p \neq q$. Für jede p-Sylowgruppe P von G ist $|G : N_G(P)| \mid q$. Im Fall $|G : N_G(P)| = 1$ wäre $P \trianglelefteq G$. Nach 10.2 wären daher P und G/P auflösbar, also auch G. Folglich ist $|G : N_G(P)| = q$. Wir wählen zwei verschiedene p-Sylowgruppen P_1, P_2 von G so, daß $|P_1 \cap P_2|$ möglichst groß ist.

Fall 1: $P_1 \cap P_2 = 1$. Dann haben je zwei verschiedene p-Sylowgruppen von G den Durchschnitt 1. Daher enthält G genau $1 + q(p^n - 1) = |G| - q + 1$ p-Elemente. Die übrigen $q - 1$ Elemente bilden zusammen mit dem Einselement eine q-Sylowgruppe Q von G. Offenbar ist Q die einzige q-Sylowgruppe von G, also ist $Q \trianglelefteq G$. Nach 10.2 sind Q und G/Q auflösbar, also auch G.
Fall 2: $D := P_1 \cap P_2 \neq 1$. Für $i = 1, 2$ gilt nach 10.2 und 10.3: $D < N_{P_i}(D) =: V_i \leq P_i$. Folglich ist $D \trianglelefteq \langle V_1, V_2 \rangle =: T$.
Annahme: $|T| = p^t$ für ein $t \in \mathbb{N}$. Nach Sylow existiert dann eine p-Sylowgruppe P_3 von G mit $T \subseteq P_3$. Folglich ist $P_i \cap P_3 \geq P_i \cap T \geq V_i > D$. Nach Wahl von D ist also $P_i = P_3$. Man erhält den Widerspruch $P_1 = P_2$.
Also ist $|T| = p^t q$ für ein $t \in \mathbb{N}$. Für jede q-Sylowgruppe Q von T ist $|P_1 Q| = p^n q = |G|$, also $G = P_1 Q$. Ist $g \in G$ und $g = xy$ mit $x \in P_1$ und $y \in Q \subseteq T \subseteq N_G(D)$, so ist $gDg^{-1} = xyDy^{-1}x^{-1} = xDx^{-1} \subseteq P_1$. Folglich ist $K := \langle gDg^{-1} : g \in G \rangle \subseteq P_1$ und $D \leq K \trianglelefteq G$. Weder K noch G/K sind Gegenbeispiele für unsere Behauptung. Folglich sind K und G/K auflösbar, also auch G. □

10.6. Satz (O. Schmidt)**.** *Für jede endliche nichtnilpotente Gruppe G, in der jede echte Untergruppe nilpotent ist, gilt:*

(i) *G ist auflösbar.*
(ii) *Es existieren Primzahlen p, q und $a, b \in \mathbb{N}$, so daß $|G| = p^a q^b$ ist, und G eine zyklische p-Sylowgruppe und eine normale q-Sylowgruppe enthält.*

Beweis.

(i) Sei G ein Gegenbeispiel minimaler Ordnung. Ist G nicht einfach und $1 \neq N \lhd G$, so ist nach den Isomorphiesätzen jede echte Untergruppe von G/N nilpotent. Da G/N kein Gegenbeispiel mehr ist, ist G/N auflösbar. Wegen $N \neq G$ ist N nilpotent, also G auflösbar. Daher können wir voraussetzen, daß G einfach ist. Wir wählen zwei verschiedene maximale Untergruppen M_1, M_2 von G so, 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:

$$D < N_{M_i}(D) =: V_i \leq N_G(D) < G.$$

Daher existiert eine maximale Untergruppe M_3 von G mit $N_G(D) \subseteq M_3$. Dann ist $D < V_i \leq M_i \cap M_3$, also $M_i = M_3$ nach Wahl von M_1, M_2. Man erhält so den Widerspruch $M_1 = M_2$.
Folglich ist $M \cap N = 1$ für je zwei verschiedene maximale Untergruppen M, N von G. Ferner ist $N_G(M) = M$ wegen der Einfachheit von G; insbesondere besitzt M genau $|G : M|$ Konjugierte in G. Sind $M_1, \ldots, M_s$ Repräsentanten für die Konjugationsklassen maximaler Untergruppen von G, so ist also

$$|G| = 1 + \sum_{i=1}^{s} (|M_i| - 1)|G : M_i| = 1 + s|G| - \sum_{i=1}^{s} |G : M_i|.$$

Wegen $|G : M_i| \leq \frac{|G|}{2}$ für $i = 1, \ldots, s$ folgt:

$$|G| \geq 1 + s|G| - \frac{s|G|}{2} = 1 + \frac{s|G|}{2},$$

d.h. $s = 1$. Dann ist aber $|G| = 1 + |G| - |G : M_1|$, und man erhält den Widerspruch $|G : M_1| = 1$.

(ii) Sei $|G| = p_1^{a_1} \ldots p_r^{a_r}$ mit $a_1, \ldots, a_r \in \mathbb{N}$ und paarweise verschiedenen Primzahlen $p_1, \ldots, p_r$, und sei H maximaler Normalteiler von G. Nach (i) ist $|G : H|$ Primzahl. O.B.d.A. sei $|G : H| = p_1$. Nach Voraussetzung ist H nilpotent, besitzt also für $i = 2, \ldots, r$ genau eine p_i-Sylowgruppe P_i. Diese ist charakteristisch in H, also normal in G und eine p_i-Sylowgruppe in G. Ferner sei P_1 eine p_1-Sylowgruppe von G.
Annahme: $r \geq 3$. Für $i = 2, \ldots, r$ ist $P_1 P_i$ eine echte Untergruppe von G, also nilpotent; insbesondere ist $P_i \subseteq N_G(P_1)$. Wegen $P_1 \subseteq N_G(P_1)$ ist also $|G| = p_1^{a_1} \ldots p_r^{a_r} \mid |N_G(P_1)|$. Folglich ist $P_1 \trianglelefteq G$. Nach 10.3 ist also G nilpotent. Widerspruch.
Also ist $r = 2$.
Annahme: P_1 nicht zyklisch. Für $x \in P_1$ ist dann $\langle x \rangle P_2$ eine echte Untergruppe von G, also

nilpotent; insbesondere ist $P_2 \subseteq C_G(P_1) \subseteq N_G(P_1)$, also wieder $P_1 \trianglelefteq G$, und man hat einen Widerspruch wie oben.

□

10.7. Definition. Eine Untergruppe H einer endlichen Gruppe G mit $\mathrm{ggT}(|H|, |G:H|) = 1$ nennt man eine *Hallgruppe* von G.

Beispiel. Sylowgruppen sind stets Hallgruppen.

Bemerkung. Für jede Hallgruppe einer endlichen Gruppe G und jeden Normalteiler N von G ist $H \cap N$ eine Hallgruppe von N und HN/N eine Hallgruppe von G/N nach Aufgabe 1 von Blatt 3.

Satz (Wielandt)**.** *Gegeben seien eine nilpotente Hallgruppe H einer endlichen Gruppe G und eine Untergruppe U von G mit $|U| \mid |H|$. Dann ist $gUg^{-1} \subseteq H$ für ein $g \in G$.*

Beweis. (Induktion nach $|U|$) Der Fall $|U| = 1$ ist trivial. Sei also $|U| > 1$ und die Behauptung richtig für jede echte Untergruppe V von U. Zu jeder echten Untergruppe V von U existiert also ein $h \in G$ mit $hVh^{-1} \subseteq H$; wegen $V \cong hVh^{-1}$ ist also V nilpotent.
Ist U nicht nilpotent, so enthält U nach 10.6 für eine Primzahl q eine normale q-Sylowgruppe $Q \neq 1$, und U/Q ist eine endliche p-Gruppe für eine Primzahl $p \neq q$. Wir bezeichnen mit P eine p-Sylowgruppe von U. Dann ist $U = PQ$.
Ist U nilpotent, p ein beliebiger Primteiler von $|U|$ und P die einzige p-Sylowgruppe von U, so existiert eine Untergruppe Q von U mit $U = P \oplus Q$.
In beiden Fällen ist $Q \trianglelefteq U$. Da H nilpotent ist, existiert eine Zerlegung $H = H_1 \oplus H_2$, wobei H_1 die p-Sylowgruppe von H ist. Nach Induktion existiert ein $x \in G$ mit $xQx^{-1} \subseteq H$, also $xQx^{-1} \subseteq H_2$. Wegen $Q \trianglelefteq U$ ist $N_G(xQx^{-1}) \geq \langle H_1, xUx^{-1} \rangle$. Offenbar ist H_1 eine p-Sylowgruppe von G, also auch von $N_G(xQx^{-1})$. Zu der p-Untergruppe xPx^{-1} von $N_G(xQx^{-1})$ existiert nach Sylow ein $y \in N_G(xQx^{-1})$ mit $yxPx^{-1}y^{-1} \subseteq H_1$. Wegen $yxQx^{-1}y^{-1} = xQx^{-1} \subseteq H_2$ ist also

$$yxUx^{-1}y^{-1} = yxPQx^{-1}y^{-1} = (yxPx^{-1}y^{-1})(yxQx^{-1}y^{-1}) \subseteq H_1H_2 = H.$$

□

10.8. Definition. Gegeben sei eine Untergruppe H einer Gruppe G. Eine Untergruppe K von G mit $H \cap K = 1$ und $HK = G$ nennt man ein *Komplement* von H in G.

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

Satz (Galois)**.** *Jeder minimale Normalteiler M einer endlichen auflösbaren Gruppe G mit $M = C_G(M)$ besitzt ein Komplement in G, und je zwei Komplemente von M in G sind in G konjugiert.*

Beweis. Nach Bemerkung 8.1(v) ist $M \cong (\mathbb{Z}/p\mathbb{Z})^m$ für ein $m \in \mathbb{N}$ und eine Primzahl p. Sei o.B.d.A. $G \neq M$ und N/M ein minimaler Normalteiler von G/M. Dann ist analog $N/M \cong (\mathbb{Z}/q\mathbb{Z})^n$ für ein $n \in \mathbb{N}$ und eine Primzahl q.
Im Fall $p = q$ wäre N eine p-Gruppe, also nilpotent. Folglich wäre $1 \neq Z(N) \cap M \trianglelefteq G$, also $M = Z(N) \cap M \subseteq Z(N)$ wegen der Minimalität von M. Dies widerspricht aber der Voraussetzung $M = C_G(M)$. Also ist $p \neq q$. Ist Q eine q-Sylowgruppe von N, so ist $N = QM$ und $G = N_G(Q)N = N_G(Q)QM = N_G(Q)M$ nach Frattini. Offenbar ist $N_G(Q) \cap M \trianglelefteq N_G(Q)$ und $N_G(Q) \cap M \trianglelefteq M$ wegen der Kommutativität von M. Daher ist auch $N_G(Q) \cap M \trianglelefteq N_G(Q)M = G$. Wegen der Minimalität von M ist also $N_G(Q) \cap M \in \{1, M\}$.
Im Fall $M = N_G(Q) \cap M \subseteq N_G(Q)$ wäre $G = N_G(Q)$, d.h. $Q \trianglelefteq G$. Wegen $M \cap Q = 1$ wäre $Q \subseteq C_G(M) = M$, was nicht geht. Also ist $N_G(Q) \cap M = 1$, d.h. $N_G(Q)$ ist Komplement von M in G.
Sei nun H ein beliebiges Komplement von M in G und $R := H \cap N$, also $R \trianglelefteq H$. Nach Dedekind ist $N = MH \cap N = M(H \cap N) = MR$ und $M \cap R \subseteq M \cap H = 1$. Folglich ist $|R| = |N:M| = |Q|$, d.h. R ist auch q-Sylowgruppe von N. Folglich existiert ein $g \in G$ mit $R = gQg^{-1}$, und es ergibt sich

$$H \leq N_G(R) = N_G(gQg^{-1}) = gN_G(Q)g^{-1}.$$

Andererseits ist

$$|H| = \frac{|G|}{|M|} = |N_G(Q)| = |gN_G(Q)g^{-1}|,$$

also $H = gN_G(Q)g^{-1}$. □

10.9. Satz (P. Hall)**.** *Jede endliche auflösbare Gruppe G der Ordnung rs mit teilerfremden $r, s \in \mathbb{N}$ besitzt eine Untergruppe der Ordnung r (eine Hallgruppe von G).*

Beweis. (Induktion nach $|G|$) O.B.d.A. sei $G \neq 1$. Sei M minimaler Normalteiler von G, also $M \cong (\mathbb{Z}/p\mathbb{Z})^m$ für ein $m \in \mathbb{N}$ und eine Primzahl p.
Im Fall $p^m \mid r$ ist $|G/M| = r's$ mit teilerfremden $r' := \frac{r}{p^m}, s \in \mathbb{N}$. Nach Induktion enthält G/M eine Untergruppe H/M der Ordnung r'. Dann ist $H \leq G$ und $|H| = p^m r' = r$.
Sei also $p^m \nmid r$, d.h. $p^m \mid s$ wegen $\mathrm{ggT}(r, s) = 1$. Dann ist $|G/M| = rs'$ mit teilerfremden $r, s' := \frac{s}{p^m} \in \mathbb{N}$. Nach Induktion enthält G/M eine Untergruppe H/M der Ordnung r. Dann ist $H \leq G$ und $|H| = p^m r$ mit teilerfremden p^m, r. Im Fall $H \neq G$ enthält H nach Induktion eine Untergruppe der Ordnung r.
Sei also $H = G$, d.h. $s = p^m$. Dann ist M die einzige p-Sylowgruppe von G. Im Fall $M \neq F(G)$ existiert ein minimaler Normalteiler $N \neq M$ von G. Offenbar ist $|N| \mid r$. Daher kann man die Argumentation zu Beginn des Beweises mit N statt M wiederholen und erhält so die Behauptung.
Sei also $M = F(G)$ und daher $M = C_G(M)$. Nach Galois besitzt M in diesem Fall ein Komplement K. Dann ist $|K| = r$, und wir sind fertig. □

10.10. Satz (P. Hall)**.** *Gegeben seien eine endliche auflösbare Gruppe G, eine Hallgruppe H von G und eine Untergruppe U von G mit $|U| \mid |H|$. Dann existiert ein $g \in G$ mit $gUg^{-1} \subseteq H$.*

Beweis. (Induktion nach $|G|$) O.B.d.A. sei $G \neq 1$. Sei M minimaler Normalteiler von G, also $M \cong (\mathbb{Z}/p\mathbb{Z})^m$ für ein $m \in \mathbb{N}$ und eine Primzahl p. Dann ist HM/M eine Hallgruppe von G/M, und UM/M ist eine Untergruppe von G/M mit

$$\mathrm{ggT}(|UM/M|, |G/M : HM/M|) = \mathrm{ggT}(|U : U \cap M|, |G : HM|) \mid \mathrm{ggT}(|U|, |G : H|) = 1,$$

also $|UM/M| \mid |HM/M|$. Nach Induktion existiert $xM \in G/M$ mit

$$HM/M \supseteq (xM)(UM/M)(xM)^{-1} = (xUx^{-1})M/M,$$

also $(xUx^{-1})M \subseteq HM$. Offenbar ist H auch Hallgruppe von HM, und $xUx^{-1} \leq HM$, $|xUx^{-1}| = |U| \mid |H|$. Im Fall $HM < G$ existiert nach Induktion ein $y \in G$ mit $yxUx^{-1}y^{-1} \subseteq H$, und wir sind fertig.
Sei also $HM = G$ und o.B.d.A. $M \not\subseteq H$. Dann ist $p \nmid |H|$, also $H \cap M = 1$. Daher ist M die einzige p-Sylowgruppe von G. Im Fall $M \neq F(G)$ existiert ein minimaler Normalteiler $N \neq M$ von G. Offenbar ist $|N| \mid |H|$. Daher kann man die Argumentation zu Beginn des Beweises mit N statt M wiederholen und erhält so die Behauptung.
Sei also $M = F(G)$ und daher $M = C_G(M)$. Nach Dedekind ist

$$xUx^{-1}M = (xUx^{-1})M \cap HM = ((xUx^{-1})M \cap H)M$$

und $xUx^{-1} \cap M = 1$, $(xUx^{-1})M \cap H \cap M = 1$. Daher sind xUx^{-1} und $(xUx^{-1})M \cap H$ Hallgruppen der gleichen Ordnung von $(xUx^{-1})M$.
Im Fall $(xUx^{-1})M < G$ existiert also ein $y \in (xUx^{-1})M$ mit $yxUx^{-1}y^{-1} = (xUx^{-1})M \cap H \subseteq H$, und wir sind fertig.
Sei daher $G = (xUx^{-1})M$. Dann sind H und xUx^{-1} Komplemente von M in G. Nach Galois existiert also ein Element $y \in G$ mit $yxUx^{-1}y^{-1} = H$. □

KAPITEL 11

Die Frattinigruppe

11.1. Definition. Den Durchschnitt $\Phi(G)$ aller maximalen Untergruppen einer Gruppe G nennt man die *Frattinigruppe* von G.

Bemerkung.

(i) Besitzt G keine maximale Untergruppen, so setzt man $\Phi(G) := G$.
(ii) Stets ist $\Phi(G)$ charakteristisch in G.

Satz. *Eine Teilmenge X einer endlichen Gruppe G liegt genau dann in $\Phi(G)$, wenn gilt: Ist Y eine Teilmenge von G mit $G = \langle X, Y\rangle$, so ist $G = \langle Y\rangle$.*

Beweis.

$\Rightarrow$: Sei $X \subseteq \Phi(G),\ Y \subseteq G$ und $G = \langle X, Y\rangle$. Im Fall $G \neq \langle Y\rangle$ gäbe es eine maximale Untergruppe M von G mit $\langle Y\rangle \subseteq M$. Wegen $\Phi(G) \subseteq M$ wäre dann aber auch $G = \langle X, Y\rangle \subseteq M$. Widerspruch.
$\Leftarrow$: Sei $X \subseteq G$ und $X \not\subseteq \Phi(G)$, also $X \not\subseteq M$ für eine maximale Untergruppe M von G. Dann ist $\langle X, M\rangle = G$, aber $G \neq M = \langle M\rangle$.

□

11.2. Satz. *Ein Normalteiler N einer endlichen Gruppe G liegt genau dann nicht in $\Phi(G)$, wenn eine echte Untergruppe H von G mit $G = NH$ existiert.*

Beweis.

$\Rightarrow$: Sei $N \trianglelefteq G$ und $N \not\subseteq \Phi(G)$, also $N \not\subseteq M$ für eine maximale Untergruppe M von G. Dann ist $NM = G$.
$\Leftarrow$: Sei $N \trianglelefteq G,\ N \subseteq \Phi(G)$ und $H \leq G$ mit $G = NH = \langle N, H\rangle$. Nach 11.1 ist dann $G = \langle H\rangle = H$.

□

11.3. Satz. *Für jeden Normalteiler N einer endlichen Gruppe G gilt:*

(i) *Ist $N \subseteq \Phi(U)$ für eine Untergruppe U von G, so ist auch $N \subseteq \Phi(G)$.*
(ii) $\Phi(N) \trianglelefteq \Phi(G)$.
(iii) $\Phi(G)N/N \subseteq \Phi(G/N)$.
(iv) $N \subseteq \Phi(G) \ \Rightarrow\ \Phi(G/N) = \Phi(G)/N$.

Beweis.

(i) Sei $U \leq G$ und $N \subseteq \Phi(U)$. Ist die Behauptung falsch, so existiert nach 11.2 eine echte Untergruppe H von G mit $G = NH$. Nach Dedekind ist dann $U = NH \cap U = N(H \cap U)$. Aus 11.2 folgt also $U = H \cap U \subseteq H$, und man hat den Widerspruch $G = NH = UH \subseteq H$.
(ii) Als charakteristische Untergruppe von N ist $\Phi(N)$ normal in G. In (i) ersetze man also N durch $\Phi(N)$ und U durch N.
(iii) Nach den Isomorphiesätzen hat jede maximale Untergruppe von G/N die Form M/N, wobei M eine maximale Untergruppe von G mit $N \subseteq M$ ist. Für jedes solche M ist $\Phi(G) \subseteq M$, also auch $\Phi(G)N/N \subseteq M/N$, und die Behauptung folgt.
(iv) Im Fall $N \subseteq \Phi(G)$ ist $N \subseteq M$ für jede maximale Untergruppe M von G. Folglich ist $\Phi(G/N) \subseteq M/N$ für jedes solche M, und die Behauptung folgt.

□

11.4. Satz (Frattini)**.** *Für jede endliche Gruppe G gilt:*

(i) $\Phi(G)$ *ist nilpotent.*
(ii) *Ist* $G/\Phi(G)$ *nilpotent, so auch* G*.*
(iii) $G' \cap Z(G) \subseteq \Phi(G)$*.*

Beweis.

(i) Für jede Primzahl p und jede p-Sylowgruppe P von $\Phi(G)$ ist $G = N_G(P)\Phi(G)$ nach 9.4. Aus 11.2 folgt $G = N_G(P)$, d.h. $P \trianglelefteq G$; insbesondere ist $P \trianglelefteq \Phi(G)$, und die Behauptung folgt mit 10.3.
(ii) Sei $G/\Phi(G)$ nilpotent, p Primzahl und P eine p-Sylowgruppe von G. Dann ist $P\Phi(G)/\Phi(G)$ p-Sylowgruppe in $G/\Phi(G)$, also $P\Phi(G)/\Phi(G) \trianglelefteq G/\Phi(G)$. Folglich ist $P\Phi(G) \trianglelefteq G$. Aus 9.4 und 11.2 folgt: $G = N_G(P)P\Phi(G) = N_G(P)\Phi(G) = N_G(P)$, d.h. $P \trianglelefteq G$.
(iii) Im Fall $D := G' \cap Z(G) \not\subseteq \Phi(G)$ gibt es nach 11.2 eine maximale Untergruppe M von G mit $G = DM$. Für $d \in D$, $m \in M$ ist aber $dmMm^{-1}d^{-1} = dMd^{-1} = M$. Folglich ist $M \trianglelefteq G$, also G/M zyklisch von Primzahlordnung. Insbesondere ist $G' \subseteq M$, also $G = DM \subseteq M$. Widerspruch.

□

11.5. Satz (Wielandt)**.** *Eine endliche Gruppe G ist genau dann nilpotent, wenn $G' \subseteq \Phi(G)$ gilt.*

Beweis.

⇒: Ist G nilpotent, so ist jede maximale Untergruppe M von G normal in G. Folglich hat G/M Primzahlordnung; insbesondere ist $G' \subseteq M$. Daher ist auch $G' \subseteq \Phi(G)$.
⇐: Ist $G' \subseteq \Phi(G)$, so ist $G/\Phi(G)$ abelsch, also G nilpotent nach 11.4(ii).

□

11.6. Definition. Für jede Primzahl p nennt man eine endliche abelsche p-Gruppe E mit $x^p = 1$ für alle $x \in E$ *elementarabelsch.*

Bemerkung. Man zeigt leicht, daß E in diesem Fall zu einem Vektorraum über dem Körper $\mathbb{Z}/p\mathbb{Z}$ wird, wenn man definiert: $(k + p\mathbb{Z})x := x^k$ für $k \in \mathbb{Z}$, $x \in E$. Folglich ist E für ein $n \in \mathbb{N}$ isomorph zu $(\mathbb{Z}/p\mathbb{Z})^n$ als Vektorraum, also auch als Gruppe. Offenbar ist jede Untergruppe E auch ein Untervektorraum von E, und jeder Homomorphismus zwischen elementarabelschen p-Gruppen ist auch $\mathbb{Z}/p\mathbb{Z}$-linear. Für jede Teilmenge X von E ist $\langle X\rangle = \mathrm{Span}_{\mathbf{Z}/p\mathbf{Z}}(X)$.

Satz. *Für jede Primzahl p und jede endliche p-Gruppe G ist $\Phi(G) = \langle [a,b], c^p : a,b,c \in G\rangle$; insbesondere ist $G/\Phi(G)$ elementarabelsch. Ist umgekehrt N ein Normalteiler von G mit elementarabelscher Faktorgruppe G/N, so ist $\Phi(G) \subseteq N$. Folglich ist $\Phi(G)$ der „kleinste" Normalteiler in G mit elementarabelscher Faktorgruppe.*

Beweis. Nach 11.5 ist $[a,b] \in \Phi(G)$ für $a,b \in G$. Da G nilpotent ist, ist jede maximale Untergruppe M normal in G. Folglich ist $|G/M| = p$. Für $c \in G$ ist also $1 = (cM)^p = c^pM$, also $c^p \in M$. Dies zeigt: $D := \langle [a,b], c^p : a,b,c \in G\rangle \subseteq \Phi(G)$.
Sei $N \trianglelefteq G$ und G/N elementarabelsch. Wäre $\Phi(G) \not\subseteq N$, so wäre $x \notin N$ für ein $x \in \Phi(G)$. Wegen $xN \neq 1$ gäbe es dann eine $\mathbb{Z}/p\mathbb{Z}$-Basis von G/N der Form $x_1N = xN, x_2N, \ldots, x_nN$. Dann wäre aber $G = \langle x_1, \ldots, x_n, N\rangle = \langle x_2, \ldots, x_n, N\rangle$ nach 11.1, also $G/N = \langle x_2N, \ldots, x_nN\rangle$ im Widerspruch zur Tatsache, daß $x_1N, \ldots, x_nN$ eine Basis von G/N bilden. Dies zeigt: $\Phi(G) \subseteq N$.
Offenbar ist $D \trianglelefteq G$ und G/D elementarabelsch. Daher ist insbesondere $\Phi(G) \subseteq D$. □

11.7. Satz (Burnsides Basissatz)**.** *Gegeben seien eine Primzahl p, eine endliche p-Gruppe G und Elemente $x_1, \ldots, x_n \in G$. Genau dann ist $G = \langle x_1, \ldots, x_n\rangle$, wenn $G/\Phi(G) = \mathrm{Span}_{\mathbb{Z}/p\mathbb{Z}}(x_1\Phi(G), \ldots, x_n\Phi(G))$ ist. Ist also $|G/\Phi(G)| = p^d$, so besitzt G ein Erzeugendensystem aus d Elementen, aber keines aus $d-1$ Elementen.*

Beweis. $G = \langle x_1, \ldots, x_n\rangle \Leftrightarrow G = \langle x_1, \ldots, x_n, \Phi(G)\rangle \Leftrightarrow G/\Phi(G) = \langle x_1\Phi(G), \ldots, x_n\Phi(G)\rangle$. □

11.8. Satz. *Gegeben sei eine endliche Gruppe G mit genau einer maximalen Untergruppe M. Dann ist G zyklisch von Primzahlpotenzordnung.*

Beweis. Offenbar ist $M = \Phi(G)$. Wäre $|G|$ keine Primzahlpotenz, so läge jede Sylowgruppe von G in M. Dann wäre also $M = G$, was nicht geht. Daher ist G eine p-Gruppe für eine Primzahl p. Wegen $|G/\Phi(G)| = |G/M| = p$ ist G nach 11.7 zyklisch. □

11.9. Satz. *Gegeben sei ein Automorphismus α einer endlichen Gruppe G mit* $\mathrm{ggT}(|\langle\alpha\rangle|,\ |\Phi(G)|) = 1$, *und $\alpha(g)\Phi(G) = g\Phi(G)$ für $g \in G$. Dann ist $\alpha = \mathrm{id}_G$.*

Beweis. Wir wählen ein Erzeugendensystem $\{x_1, \ldots, x_d\}$ von G und setzen $\Omega := \{(x_1y_1, \ldots, x_dy_d) : y_1, \ldots, y_d \in \Phi(G)\}$. Nach Voraussetzung operiert $\langle\alpha\rangle$ auf Ω durch $\beta(z_1, \ldots, z_d) := (\beta(z_1), \ldots, \beta(z_d))$ für $\beta \in \langle\alpha\rangle$, $(z_1, \ldots, z_d) \in \Omega$. Sei Δ eine Bahn von Ω unter $\langle\alpha\rangle$ und $\omega = (z_1, \ldots, z_d) \in \Delta$. Wegen $G = \langle z_1, \ldots, z_d\rangle$ ist $\mathrm{Stb}_{\langle\alpha\rangle}(\omega) = 1$, also $|\Delta| = |\langle\alpha\rangle|$. Für die Anzahl k der Bahnen von $\langle\alpha\rangle$ auf Ω gilt also: $|\Omega| = k|\langle\alpha\rangle|$. Andrerseits ist $|\Omega| = |\Phi(G)|^d$, d.h. $|\langle\alpha\rangle| \mid |\Phi(G)|^d$. Nach Voraussetzung ist also $|\langle\alpha\rangle| = 1$, d.h. $\alpha = \mathrm{id}_G$. □

Bemerkung. Aus diesem Satz folgt sofort: Ist p eine Primzahl, G eine endliche p-Gruppe und $\alpha \in \mathrm{Aut}(G)$ mit $\alpha(g)\Phi(G) = g\Phi(G)$ für $g \in G$, so ist $|\langle\alpha\rangle|$ eine Potenz von p.

KAPITEL 12

Gruppenerweiterungen

12.1. Bemerkung. Gegeben seien Gruppen G und K. Wir wenden uns dem Problem zu, alle Gruppen H zu bestimmen, die einen zu K isomorphen Normalteiler N mit zu G isomorpher Faktorgruppe H/N besitzen. Dazu führen wir den folgenden Begriff ein.

Definition. Gegeben seien Gruppen G und K. Eine *Erweiterung* von G mit K ist ein Tripel (H, ε, ν), das aus einer Gruppe H, einem Monomorphismus $\varepsilon : K \to H$ und einem Epimorphismus $\nu : H \to G$ mit $\mathrm{Ker}(\nu) = \varepsilon(K)$ besteht. Wir schreiben diese Erweiterung meist in der Form

$$K \xrightarrow{\varepsilon} H \xrightarrow{\nu} G.$$

Beispiel. Jeder Normalteiler N einer Gruppe H liefert eine Erweiterung $N \xrightarrow{\varepsilon} H \xrightarrow{\nu} H/N$, wobei ε die Inklusionsabbildung und ν der kanonische Epimorphismus ist. Für eine beliebige Erweiterung $K \xrightarrow{\varepsilon} H \xrightarrow{\nu} G$ ist umgekehrt $K \cong \varepsilon(K) = \mathrm{Ker}(\nu) \trianglelefteq H$ und $H/\mathrm{Ker}(\nu) \cong \nu(H) = G$.

Satz. *Gegeben sei eine Gruppenerweiterung $K \xrightarrow{\varepsilon} H \xrightarrow{\nu} G$. Zu jedem Element $x \in G$ wählen wir ein festes Urbild $h_x \in H$ unter ν. Dann gilt:*

(i) *Zu jedem Element $h \in H$ existieren eindeutig bestimmte Elemente $x \in G$ und $a \in K$ mit $h = \varepsilon(a)h_x$.*
(ii) *Für $x \in G$ und $a \in K$ existiert genau ein Element $\alpha_x(a) \in K$ mit $\varepsilon(\alpha_x(a)) = h_x\varepsilon(a)h_x^{-1}$.*
(iii) *Für $x \in G$ ist die durch (ii) definierte Abbildung $\alpha_x : K \to K$ ein Automorphismus.*
(iv) *Für $x, y \in G$ existiert genau ein Element $\kappa(x, y) \in K$ mit $h_xh_y = \varepsilon(\kappa(x, y))h_{xy}$.*
(v) *Für $x, y \in G$ ist $\alpha_x \circ \alpha_y = \iota_{\kappa(x,y)} \circ \alpha_{xy}$; dabei ist ι_a der von einem Element $a \in K$ induzierte innere Automorphismus von K.*
(vi) *Für $x, y, z \in G$ ist $\kappa(x, y)\kappa(xy, z) = \alpha_x(\kappa(y, z))\kappa(x, yz)$.*

Beweis.

(i) Sei $h \in H$ und $x := \nu(h) \in G$. Dann ist $\nu(hh_x^{-1}) = \nu(h)\nu(h_x)^{-1} = xx^{-1} = 1$, also $hh_x^{-1} \in \mathrm{Ker}(\nu) = \varepsilon(K)$. Daher existiert ein Element $a \in K$ mit $hh_x^{-1} = \varepsilon(a)$, d.h. $h = \varepsilon(a)h_x$. Sind auch $b \in K$ und $y \in G$ mit $h = \varepsilon(b)h_y$, so ist $x = \nu(h) = \nu(\varepsilon(b)h_y) = \nu(\varepsilon(b))\nu(h_y) = 1 \cdot y = y$. Daher ist $h_x = h_y,\ \varepsilon(a) = \varepsilon(b),\ a = b$.

(ii) Für $x \in G$ und $a \in K$ ist $h_x\varepsilon(a)h_x^{-1} \subseteq \varepsilon(K)$ wegen $\varepsilon(K) = \mathrm{Ker}(\nu) \trianglelefteq H$. Da ε injektiv ist, folgt die Behauptung.

(iii) Für $a, b \in K$ ist $\alpha_x(a)\alpha_x(b) \in K$ mit

$$\begin{aligned}\varepsilon(\alpha_x(a)\alpha_x(b)) &= \varepsilon(\alpha_x(a))\varepsilon(\alpha_x(b)) = h_x\varepsilon(a)h_x^{-1}h_x\varepsilon(b)h_x^{-1} = \\ &= h_x\varepsilon(ab)h_x^{-1} = \varepsilon(\alpha_x(ab)).\end{aligned}$$

Da ε injektiv ist, folgt $\alpha_x(ab) = \alpha_x(a)\alpha_x(b)$.
Ist $a \in K$ mit $\alpha_x(a) = 1$, so ist $1 = \varepsilon(\alpha_x(a)) = h_x\varepsilon(a)h_x^{-1}$, also auch $\varepsilon(a) = 1$ und $a = 1$. Folglich ist α_x injektiv.
Ist $b \in K$ beliebig, so ist $h_x^{-1}\varepsilon(b)h_x \in h_x^{-1}\varepsilon(K)h_x = \varepsilon(K)$. Daher existiert ein Element $a \in K$ mit $h_x^{-1}\varepsilon(b)h_x = \varepsilon(a)$. Dann ist $\varepsilon(\alpha_x(a)) = h_x\varepsilon(a)h_x^{-1} = \varepsilon(b)$, also $\alpha_x(a) = b$. Folglich ist α_x surjektiv.

(iv) Für $x, y \in G$ ist $\nu(h_xh_yh_{xy}^{-1}) = \nu(h_x)\nu(h_y)\nu(h_{xy})^{-1} = xy(xy)^{-1} = 1$, also $h_xh_yh_{xy}^{-1} \in \mathrm{Ker}(\nu) = \varepsilon(K)$. Wegen der Injektivität von ε existiert also genau ein Element $\kappa(x, y) \in K$ mit $h_xh_yh_{xy}^{-1} = \varepsilon(\kappa(x, y))$.

(v) Für $x, y \in G$ und $a \in K$ ist

$$\begin{aligned}\varepsilon(\alpha_x(\alpha_y(a))) &= h_x\varepsilon(\alpha_y(a))h_x^{-1} = h_xh_y\varepsilon(a)h_y^{-1}h_x^{-1} = \\ &= \varepsilon(\kappa(x,y))h_{xy}\varepsilon(a)h_{xy}^{-1}\varepsilon(\kappa(x,y))^{-1} = \\ &= \varepsilon(\kappa(x,y))\varepsilon(\alpha_{xy}(a))\varepsilon(\kappa(x,y))^{-1} = \\ &= \varepsilon(\kappa(x,y)\alpha_{xy}(a)\kappa(x,y)^{-1}),\end{aligned}$$

also $(\alpha_x \circ \alpha_y)(a) = \kappa(x,y)\alpha_{xy}(a)\kappa(x,y)^{-1}$.

(vi) Für $x, y, z \in G$ ist

$$\begin{aligned}\varepsilon(\kappa(x,y)\kappa(xy,z))h_{xyz} &= \varepsilon(\kappa(x,y))\varepsilon(\kappa(xy,z))h_{(xy)z} = \varepsilon(\kappa(x,y))h_{xy}h_z = \\ &= h_xh_yh_z = h_x\varepsilon(\kappa(y,z))h_{yz} = \\ &= h_x\varepsilon(\kappa(y,z))h_x^{-1}h_xh_{yz} = \\ &= \varepsilon(\alpha_x(\kappa(y,z)))\varepsilon(\kappa(x,yz))h_{x(yz)} = \\ &= \varepsilon(\alpha_x(\kappa(y,z))\kappa(x,yz))h_{xyz},\end{aligned}$$

und aus der Injektivität von ε folgt die Behauptung.

□

12.2. Definition. Gegeben seien Gruppen G und K. Ein *Parametersystem* von G in K ist ein Paar (α, κ) von Abbildungen $\alpha : G \to \mathrm{Aut}(K),\ x \mapsto \alpha_x$ und $\kappa : G \times G \to K,\ (x,y) \mapsto \kappa(x,y)$ mit folgenden Eigenschaften:

(i) Für $x, y \in G$ ist $\alpha_x \circ \alpha_y = \iota_{\kappa(x,y)} \circ \alpha_{xy}$; dabei ist ι_a für $a \in K$ der von a induzierte innere Automorphismus von K.

(ii) Für $x, y, z \in G$ ist $\kappa(x,y)\kappa(xy,z) = \alpha_x(\kappa(y,z))\kappa(x,yz)$.

Man nennt α das *Automorphismensystem* und κ das *Faktorensystem* von (α, κ).

Beispiel. Nach 12.1 induziert jede Gruppenerweiterung $K \xrightarrow{\varepsilon} H \xrightarrow{\nu} G$ nach Wahl eines Urbildes $h_x \in H$ zu jedem Element $x \in G$ ein Parametersystem (α, κ) von G in K. Man nennt (α, κ) das durch $K \xrightarrow{\varepsilon} H \xrightarrow{\nu} G$ und $(h_x)_{x\in G}$ definierte Parametersystem. Wir werden bald die Abhängigkeit von (α, κ) von $(h_x)_{x\in G}$ untersuchen.

Satz. *Gegeben seien Gruppen G und K und ein Parametersystem (α, κ) von G in K. Dann gilt:*

(i) $\alpha_1 = \iota_{\kappa(1,1)}$.

(ii) $\kappa(1,1) = \kappa(1,z)$ *für* $z \in G$.

(iii) $\kappa(x,1) = \alpha_x(\kappa(1,1))$ *für* $x \in G$.

Beweis.

(i) Wegen $\alpha_1 \circ \alpha_1 = \iota_{\kappa(1,1)} \circ \alpha_1$ ist $\alpha_1 = \iota_{\kappa(1,1)}$.

(ii) Für $z \in G$ gilt nach (i):

$$\kappa(1,1)\kappa(1\cdot 1, z) = \alpha_1(\kappa(1,z))\kappa(1,1\cdot z) = \kappa(1,1)\kappa(1,z)\kappa(1,1)^{-1}\kappa(1,z).$$

(iii) Für $x \in G$ ist $\kappa(x,1)\kappa(x1,1) = \alpha_x(\kappa(1,1))\kappa(x,1\cdot 1)$.

□

12.3. Satz. *Gegeben seien Gruppen G und K und ein Parametersystem (α, κ) von G in K. Dann existiert eine Gruppenerweiterung $K \xrightarrow{\varepsilon} H \xrightarrow{\nu} G$, die (α, κ) definiert.*

Beweis. Wir definieren eine Verknüpfung auf der Menge $H := K \times G$ durch

$$(a,x)(b,y) := (a\alpha_x(b)\kappa(x,y), xy) \qquad \text{für } a, b \in K,\ x, y \in G.$$

Dann gilt für $a,b,c \in K,\ x,y,z \in G$:

$$\begin{aligned}
[(a,x)(b,y)](c,z) &= (a\alpha_x(b)\kappa(x,y),xy)(c,z) \ = \\
&= (a\alpha_x(b)\kappa(x,y)\alpha_{xy}(c)\kappa(xy,z),xyz) \ = \\
&= (a\alpha_x(b)\kappa(x,y)\alpha_{xy}(c)\kappa(x,y)^{-1}\kappa(x,y)\kappa(xy,z),xyz) \ = \\
&= (a\alpha_x(b)\alpha_x(\alpha_y(c))\alpha_x(\kappa(y,z))\kappa(x,yz),xyz) \ = \\
&= (a\alpha_x(b\alpha_y(c)\kappa(y,z))\kappa(x,yz),xyz) \ = \\
&= (a,x)(b\alpha_y(c)\kappa(y,z),yz) \ = \\
&= (a,x)[(b,y)(c,z)].
\end{aligned}$$

Für $b \in K$ und $y \in G$ gilt außerdem nach 12.2:

$$\begin{aligned}
(\kappa(1,1)^{-1},1)(b,y) &= (\kappa(1,1)^{-1}\alpha_1(b)\kappa(1,y),1\cdot y) \ = \\
&= (\kappa(1,1)^{-1}\kappa(1,1)b\kappa(1,1)^{-1}\kappa(1,y),y) \ = \\
&= (b,y)
\end{aligned}$$

und

$$\begin{aligned}
&(\kappa(1,1)^{-1}\kappa(y^{-1},y)^{-1}\alpha_{y^{-1}}(b)^{-1},y^{-1})(b,y) \ = \\
&\qquad = (\kappa(1,1)^{-1}\kappa(y^{-1},y)^{-1}\alpha_{y^{-1}}(b)^{-1}\alpha_{y^{-1}}(b)\kappa(y^{-1},y),y^{-1}y) \ = \\
&\qquad = (\kappa(1,1)^{-1},1).
\end{aligned}$$

Daher ist H eine Gruppe mit neutralem Element $(\kappa(1,1)^{-1},1)$ und inversen Elementen $(b,y)^{-1} = (\kappa(1,1)^{-1}\kappa(y^{-1},y)^{-1}\alpha_{y^{-1}}(b)^{-1},y^{-1})$ für $b \in K,\ y \in G$.
Wir definieren Abbildungen $\varepsilon : K \to H$ und $\nu : H \to G$ durch

$$\varepsilon(a) := (\kappa(1,1)^{-1}a,1) \quad \text{und} \quad \nu(a,x) := x \qquad \text{für } a \in K,\ x \in G.$$

Für $a,b \in K,\ x,y \in G$ ist dann:

$$\begin{aligned}
\varepsilon(a)\varepsilon(b) &= (\kappa(1,1)^{-1}a,1)(\kappa(1,1)^{-1}b,1) \ = \\
&= (\kappa(1,1)^{-1}a\alpha_1(\kappa(1,1)^{-1}b)\kappa(1,1),1\cdot 1) \ = \\
&= (\kappa(1,1)^{-1}a\kappa(1,1)\kappa(1,1)^{-1}b\kappa(1,1)^{-1}\kappa(1,1),1) \ = \\
&= (\kappa(1,1)^{-1}ab,1) \ = \\
&= \varepsilon(ab)
\end{aligned}$$

und

$$\nu((a,x)(b,y)) \ = \ \nu(a\alpha_x(b)\kappa(x,y),xy) \ = \ xy \ = \ \nu(a,x)\nu(b,y).$$

Daher sind ε und ν Homomorphismen. Offenbar ist ε injektiv und ν surjektiv, und für $a \in K,\ x \in G$ gilt:

$$(a,x) \in \mathrm{Ker}(\nu) \ \Leftrightarrow \ x = 1 \ \Leftrightarrow \ (a,x) \in \varepsilon(K).$$

Folglich ist $K \xrightarrow{\varepsilon} H \xrightarrow{\nu} G$ eine Gruppenerweiterung.
Für $x \in G$ ist $h_x := (\kappa(1,1)^{-1}\kappa(x,1),x) \in H$ ein Urbild von x unter ν, und für $x,y \in G,\ a \in K$ gilt:

$$\begin{aligned}
h_x\varepsilon(a) &= (\kappa(1,1)^{-1}\kappa(x,1),x)(\kappa(1,1)^{-1}a,1) \ = \\
&= (\kappa(1,1)^{-1}\kappa(x,1)\alpha_x(\kappa(1,1)^{-1}a)\kappa(x,1),x1) \ = \\
&= (\kappa(1,1)^{-1}\kappa(x,1)\alpha_x(\kappa(1,1))^{-1}\alpha_x(a)\kappa(x,1),x) \ = \\
&= (\kappa(1,1)^{-1}\alpha_x(a)\kappa(1,1)\kappa(1,1)^{-1}\kappa(x,1)\kappa(1,1)^{-1}\kappa(1,x),x) \ = \\
&= (\kappa(1,1)^{-1}\alpha_x(a)\alpha_1(\kappa(1,1)^{-1}\kappa(x,1))\kappa(1,x),1\cdot x) \ = \\
&= (\kappa(1,1)^{-1}\alpha_x(a),1)(\kappa(1,1)^{-1}\kappa(x,1),x) \ = \\
&= \varepsilon(\alpha_x(a))h_x
\end{aligned}$$

und

$$\begin{aligned} h_xh_y &= (\kappa(1,1)^{-1}\kappa(x,1),x)(\kappa(1,1)^{-1}\kappa(y,1),y) = \\ &= (\kappa(1,1)^{-1}\kappa(x,1)\alpha_x(\kappa(1,1)^{-1}\kappa(y,1))\kappa(x,y),xy) = \\ &= (\kappa(1,1)^{-1}\kappa(x,1)\alpha_x(\kappa(1,1))^{-1}\alpha_x(\kappa(y,1))\kappa(x,y),xy) = \\ &= (\kappa(1,1)^{-1}\kappa(x,y)\kappa(xy,1),xy) = \\ &= (\kappa(1,1)^{-1}\kappa(x,y)\kappa(1,1)\kappa(1,1)^{-1}\kappa(xy,1)\kappa(1,1)^{-1}\kappa(1,xy),xy) = \\ &= (\kappa(1,1)^{-1}\kappa(x,y)\alpha_1(\kappa(1,1)^{-1}\kappa(xy,1))\kappa(1,xy),xy) = \\ &= (\kappa(1,1)^{-1}\kappa(x,y),1)(\kappa(1,1)^{-1}\kappa(xy,1),xy) = \\ &= \varepsilon(\kappa(x,y))h_{xy}. \end{aligned}$$

Daher wird (α,κ) durch $K \xrightarrow{\varepsilon} H \xrightarrow{\nu} G$ und $(h_x)_{x\in G}$ definiert. □

Bemerkung. Wir haben gesehen, daß zu jeder Gruppenerweiterung ein Parametersystem und zu jedem Parametersystem eine Gruppenerweiterung gehört. Im folgenden wenden wir uns der Eindeutigkeit dieser Beziehung zu.

12.4. Satz. *Gegeben seien Gruppen G und K. Die Menge $\mathrm{Abb}(G,K)$ aller Abbildungen $\varphi: G \to K$ bildet eine Gruppe, wenn man $\psi\varphi$ für $\psi,\varphi \in \mathrm{Abb}(G,K)$ durch $(\psi\varphi)(x) := \psi(x)\varphi(x)$ für $x \in G$ definiert. Diese Gruppe operiert auf der Menge $\mathrm{Par}(G,K)$ aller Parametersysteme von G in K durch ${}^{\varphi}(\alpha,\kappa) := (\alpha',\kappa')$ für $\varphi \in \mathrm{Abb}(G,K)$ und $(\alpha,\kappa) \in \mathrm{Par}(G,K)$, wobei man*

$$\alpha'_x := \iota_{\varphi(x)} \circ \alpha_x \quad \text{und} \quad \kappa'(x,y) := \varphi(x)\alpha_x(\varphi(y))\kappa(x,y)\varphi(xy)^{-1}$$

für $x,y \in G$ setzt.

Beweis. Die erste Aussage ist klar wegen $\mathrm{Abb}(G,K) = \bigtimes_{x\in G} K$.
Seien also $\varphi,\psi \in \mathrm{Abb}(G,K)$, $(\alpha,\kappa) \in \mathrm{Par}(G,K)$ und ${}^{\varphi}(\alpha,\kappa) = (\alpha',\kappa')$, ${}^{\psi}({}^{\varphi}(\alpha,\kappa)) = (\alpha'',\kappa'')$. Dann gilt für $x,y \in G$:

$$\alpha''_x = \iota_{\psi(x)} \circ \alpha'_x = \iota_{\psi(x)} \circ \iota_{\varphi(x)} \circ \alpha_x = \iota_{\psi(x)\varphi(x)} \circ \alpha_x = \iota_{(\psi\varphi)(x)} \circ \alpha_x$$

und

$$\begin{aligned} \kappa''(x,y) &= \psi(x)\alpha'_x(\psi(y))\kappa'(x,y)\psi(xy)^{-1} = \\ &= \psi(x)\varphi(x)\alpha_x(\psi(y))\varphi(x)^{-1}\varphi(x)\alpha_x(\varphi(y))\kappa(x,y)\varphi(xy)^{-1}\psi(xy)^{-1} = \\ &= (\psi\varphi)(x)\cdot\alpha_x((\psi\varphi)(y))\cdot\kappa(x,y)\cdot(\psi\varphi)(xy)^{-1}. \end{aligned}$$

Daher ist ${}^{\psi}({}^{\varphi}(\alpha,\kappa)) = {}^{\psi\varphi}(\alpha,\kappa)$. Im Fall $\varphi = 1$, d.h. $\varphi(x) = 1$ für $x \in G$, ist offenbar $\alpha'_x = \alpha_x$ und $\kappa'(x,y) = \kappa(x,y)$ für $x,y \in G$, also ${}^{1}(\alpha,\kappa) = (\alpha,\kappa)$. Im allgemeinen Fall ist ${}^{\varphi}(\alpha,\kappa) = (\alpha',\kappa') \in \mathrm{Par}(G,K)$; denn für $x,y,z \in G$ gilt:

$$\begin{aligned} \alpha'_x \circ \alpha'_y &= \iota_{\varphi(x)} \circ \alpha_x \circ \iota_{\varphi(y)} \circ \alpha_y = \\ &= \iota_{\varphi(x)} \circ \alpha_x \circ \iota_{\varphi(y)} \circ \alpha_x^{-1} \circ \alpha_x \circ \alpha_y = \\ &= \iota_{\varphi(x)} \circ \iota_{\alpha_x(\varphi(y))} \circ \iota_{\kappa(x,y)} \circ \alpha_{xy} = \\ &= \iota_{\varphi(x)\alpha_x(\varphi(y))\kappa(x,y)} \circ \iota^{-1}_{\varphi(xy)} \circ \alpha'_{xy} = \\ &= \iota_{\kappa'(x,y)} \circ \alpha'_{xy} \end{aligned}$$

und

$$\begin{aligned}
\kappa'(x,y)\kappa'(xy,z) &= \varphi(x)\alpha_x(\varphi(y))\kappa(x,y)\varphi(xy)^{-1}\varphi(xy)\alpha_{xy}(\varphi(z))\kappa(xy,z)\varphi(xyz)^{-1} = \\
&= \varphi(x)\alpha_x(\varphi(y))\kappa(x,y)\alpha_{xy}(\varphi(z))\kappa(x,y)^{-1}\kappa(x,y)\kappa(xy,z)\varphi(xyz)^{-1} = \\
&= \varphi(x)\alpha_x(\varphi(y))\alpha_x(\alpha_y(\varphi(z)))\alpha_x(\kappa(y,z))\kappa(x,yz)\varphi(xyz)^{-1} = \\
&= \varphi(x)\alpha_x(\varphi(y)\alpha_y(\varphi(z))\kappa(y,z)\varphi(yz)^{-1})\alpha_x(\varphi(yz))\kappa(x,yz)\varphi(xyz)^{-1} = \\
&= \alpha'_x(\kappa'(y,z))\varphi(x)\alpha_x(\varphi(yz))\kappa(x,yz)\varphi(xyz)^{-1} = \\
&= \alpha'_x(\kappa'(y,z))\kappa'(x,yz).
\end{aligned}$$

□

Definition. Gegeben seien Gruppen G und K. Zwei Parametersysteme (α,κ), (β,λ) von G in K nennt man *äquivalent*, falls sie in der gleichen Bahn unter $\mathrm{Abb}(G,K)$ liegen. Die Menge aller Äquivalenzklassen von Parametersystemen von G in K bezeichnen wir mit $\overline{\mathrm{Par}}(G,K)$.

12.5. Satz. *Die durch eine feste Gruppenerweiterung $K \xrightarrow{\varepsilon} H \xrightarrow{\nu} G$ definierten Parametersysteme von G in K bilden genau eine Äquivalenzklasse.*

Beweis. Für $x \in G$ seien $h_x, h'_x \in H$ Urbilder von x unter ν. Dann ist $\nu(h'_x h_x^{-1}) = \nu(h'_x)\nu(h_x)^{-1} = xx^{-1} = 1$, also $h'_x h_x^{-1} \in \mathrm{Ker}(\nu) = \varepsilon(K)$. Daher existiert ein Element $\varphi(x) \in K$ mit $h'_x h_x^{-1} = \varepsilon(\varphi(x))$, d.h. $h'_x = \varepsilon(\varphi(x))h_x$. Wir bezeichnen mit (α,κ) und (α',κ') die entsprechenden Parametersysteme. Für $x \in G$ und $a \in K$ ist dann:

$$\begin{aligned}
\varepsilon(\alpha'_x(a)) &= h'_x\varepsilon(a)(h'_x)^{-1} = \\
&= \varepsilon(\varphi(x))h_x\varepsilon(a)h_x^{-1}\varepsilon(\varphi(x))^{-1} = \\
&= \varepsilon(\varphi(x))\varepsilon(\alpha_x(a))\varepsilon(\varphi(x))^{-1} = \\
&= \varepsilon(\varphi(x)\alpha_x(a)\varphi(x)^{-1}).
\end{aligned}$$

Daher ist $\alpha'_x = \iota_{\varphi(x)} \circ \alpha_x$ für $x \in G$. Für $x, y \in G$ ist außerdem

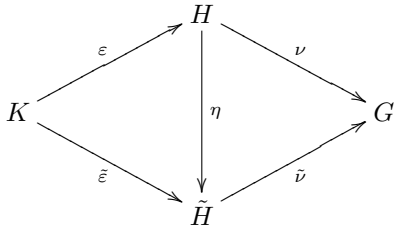
$$\begin{aligned}
\varepsilon(\kappa'(x,y))h'_{xy} &= h'_x h'_y = \varepsilon(\varphi(x))h_x\varepsilon(\varphi(y))h_y = \\
&= \varepsilon(\varphi(x))h_x\varepsilon(\varphi(y))h_x^{-1}h_x h_y = \\
&= \varepsilon(\varphi(x))\varepsilon(\alpha_x(\varphi(y)))\varepsilon(\kappa(x,y))h_{xy} = \\
&= \varepsilon(\varphi(x)\alpha_x(\varphi(y))\kappa(x,y)\varphi(xy)^{-1})\varepsilon(\varphi(xy))h_{xy} = \\
&= \varepsilon(\varphi(x)\alpha_x(\varphi(y))\kappa(x,y)\varphi(xy)^{-1})h'_{xy},
\end{aligned}$$

also $\kappa'(x,y) = \varphi(x)\alpha_x(\varphi(y))\kappa(x,y)\varphi(xy)^{-1}$. Dies zeigt, daß je zwei durch $K \xrightarrow{\varepsilon} H \xrightarrow{\nu} G$ definierte Parametersysteme äquivalent sind.
Sei umgekehrt (α,κ) ein durch $K \xrightarrow{\varepsilon} H \xrightarrow{\nu} G$ nach Wahl eines Urbildes $h_x \in H$ zu jedem Element $x \in G$ definiertes Parametersystem, und sei (α',κ') ein zu (α,κ) äquivalentes Parametersystem. Dann existiert eine Abbildung $\varphi : G \to K$ mit $\alpha'_x = \iota_{\varphi(x)} \circ \alpha_x$ und $\kappa'(x,y) = \varphi(x)\alpha_x(\varphi(y))\kappa(x,y)\varphi(xy)^{-1}$ für $x, y \in G$. Für $x \in G$ ist daher $h'_x := \varepsilon(\varphi(x))h_x \in H$ mit $\nu(h'_x) = \nu(\varepsilon(\varphi(x)))\nu(h_x) = x$. Die obigen Rechnungen zeigen, daß (α',κ') durch $(h'_x)_{x\in G}$ definiert wird. □

Bemerkung. Als nächstes halten wir ein Parametersystem (α,κ) fest und untersuchen den Zusammenhang zwischen allen Gruppenerweiterungen, die (α,κ) definieren.

12.6. Definition. Gegeben seien Gruppen G und K. Zwei Erweiterungen $K \xrightarrow{\varepsilon} H \xrightarrow{\nu} G$ und $K \xrightarrow{\tilde\varepsilon} \tilde H \xrightarrow{\tilde\nu} G$ von G mit K nennt man *äquivalent*, falls ein Homomorphismus $\eta : H \to \tilde H$ existiert mit $\eta\circ\varepsilon = \tilde\varepsilon$

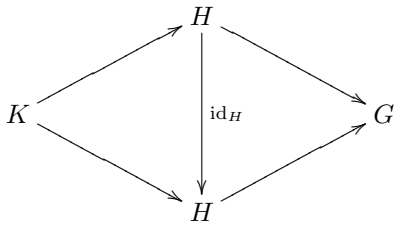
und $\tilde{\nu} \circ \eta = \nu$.

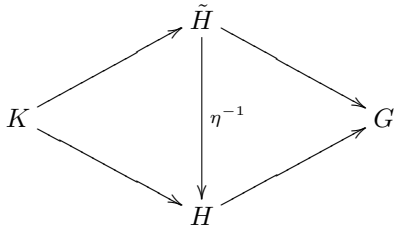


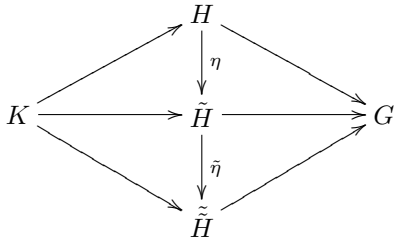
Bemerkung.

(i) Gegebenenfalls ist η bijektiv; ist nämlich $h \in H$ mit $\eta(h) = 1$, so ist auch $1 = \tilde{\nu}(\eta(h)) = \nu(h)$, also $h \in \mathrm{Ker}(\nu) = \varepsilon(K)$. Folglich existiert ein Element $a \in K$ mit $h = \varepsilon(a)$, und man erhält $1 = \eta(\varepsilon(a)) = \tilde{\varepsilon}(a)$, also $a = 1$. Damit ist aber auch $h = \varepsilon(a) = 1$.
Ist ferner $\tilde{h} \in \tilde{H}$ gegeben, so ist $\tilde{\nu}(\tilde{h}) \in G$. Folglich existiert ein Element $h \in H$ mit $\tilde{\nu}(\tilde{h}) = \nu(h)$. Dann ist $\eta(h)\tilde{h}^{-1} \in \tilde{H}$ mit $\tilde{\nu}(\eta(h)\tilde{h}^{-1}) = \tilde{\nu}(\eta(h))\tilde{\nu}(\tilde{h})^{-1} = \nu(h)\tilde{\nu}(\tilde{h})^{-1} = 1$. Folglich ist $\eta(h)\tilde{h}^{-1} \in \mathrm{Ker}(\tilde{\nu}) = \tilde{\varepsilon}(K)$. Daher existiert ein Element $a \in K$ mit $\eta(h)\tilde{h}^{-1} = \tilde{\varepsilon}(a)$. Dann ist $\varepsilon(a)^{-1}h \in H$ mit $\eta(\varepsilon(a)^{-1}h) = \eta(\varepsilon(a))^{-1}\eta(h) = \tilde{\varepsilon}(a)^{-1}\eta(h) = \tilde{h}$.

(ii) Aus (i) folgt leicht, daß die Äquivalenz von Gruppenerweiterungen eine Äquivalenzrelation ist:







Satz. *Äquivalente Gruppenerweiterungen* $K \xrightarrow{\varepsilon} H \xrightarrow{\nu} G$ *und* $K \xrightarrow{\tilde{\varepsilon}} \tilde{H} \xrightarrow{\tilde{\nu}} G$ *definieren die gleichen Parametersysteme.*

Beweis. Sei $\eta : H \to \tilde{H}$ ein Isomorphismus mit $\eta \circ \varepsilon = \tilde{\varepsilon}$ und $\tilde{\nu} \circ \eta = \nu$, und für $x \in G$ sei $h_x \in H$ ein Urbild von x unter ν. Dann ist $\tilde{h}_x := \eta(h_x) \in \tilde{H}$ mit

$$\tilde{\nu}(\tilde{h}_x) = \tilde{\nu}(\eta(h_x)) = \nu(h_x) = x.$$

Wir bezeichnen mit (α,κ) bzw. $(\tilde\alpha,\tilde\kappa)$ die entsprechenden Parametersysteme von G in K. Für $x,y\in G$ und $a\in K$ ist offenbar:

$$\begin{aligned}\tilde\varepsilon(\tilde\alpha_x(a)) &= \tilde h_x\tilde\varepsilon(a)\tilde h_x^{-1} = \eta(h_x)\eta(\varepsilon(a))\eta(h_x)^{-1} = \\ &= \eta(h_x\varepsilon(a)h_x^{-1}) = \eta(\varepsilon(\alpha_x(a))) = \\ &= \tilde\varepsilon(\alpha_x(a))\end{aligned}$$

und

$$\begin{aligned}\tilde\varepsilon(\tilde\kappa(x,y))\tilde h_{xy} &= \tilde h_x\tilde h_y = \eta(h_x)\eta(h_y) = \eta(h_xh_y) = \\ &= \eta(\varepsilon(\kappa(x,y))h_{xy}) = \eta(\varepsilon(\kappa(x,y)))\eta(h_{xy}) = \\ &= \tilde\varepsilon(\kappa(x,y))\tilde h_{xy}.\end{aligned}$$

Daher ist $(\alpha,\kappa)=(\tilde\alpha,\tilde\kappa)$, und die Behauptung ist gezeigt. □

12.7. Satz. *Gegeben seien durch Gruppenerweiterungen $K\xrightarrow{\varepsilon}H\xrightarrow{\nu}G$ und $K\xrightarrow{\tilde\varepsilon}\tilde H\xrightarrow{\tilde\nu}G$ definierte Parametersysteme (α,κ) bzw. $(\tilde\alpha,\tilde\kappa)$. Sind (α,κ) und $(\tilde\alpha,\tilde\kappa)$ äquivalent, so auch $K\xrightarrow{\varepsilon}H\xrightarrow{\nu}G$ und $K\xrightarrow{\tilde\varepsilon}\tilde H\xrightarrow{\tilde\nu}G$.*

Beweis. Wir wählen eine Familie $(h_x)_{x\in G}$ von Urbildern $h_x\in H$ der Elemente $x\in G$ mit der Eigenschaft, daß (α,κ) durch $(h_x)_{x\in G}$ definiert wird. Nach 12.1 läßt sich jedes Element in H in der Form $\varepsilon(a)h_x$ mit eindeutig bestimmten Elementen $a\in K,\ x\in G$ schreiben. Für $a,b\in K$ und $x,y\in G$ gilt dabei:

$$\begin{aligned}\varepsilon(a)h_x\cdot\varepsilon(b)h_y &= \varepsilon(a)h_x\varepsilon(b)h_x^{-1}h_xh_y = \\ &= \varepsilon(a)\varepsilon(\alpha_x(b))\varepsilon(\kappa(x,y))h_{xy} = \\ &= \varepsilon(a\alpha_x(b)\kappa(x,y))h_{xy}.\end{aligned}$$

Definiert die Gruppenerweiterung $K\xrightarrow{\tilde\varepsilon}\tilde H\xrightarrow{\tilde\nu}G$ ein zu (α,κ) äquivalentes Parametersystem, so definiert sie auch (α,κ) nach 12.5. Daher existiert eine Familie $(\tilde h_x)_{x\in G}$ von Urbildern $\tilde h_x\in\tilde H$ der Elemente $x\in G$ mit der Eigenschaft, daß (α,κ) durch $(\tilde h_x)_{x\in G}$ definiert wird. Wieder läßt sich jedes Element in $\tilde H$ in der Form $\tilde\varepsilon(a)\tilde h_x$ mit eindeutig bestimmten Elementen $a\in K,\ x\in G$ schreiben, und für $a,b\in K,\ x,y\in G$ gilt:

$$\tilde\varepsilon(a)\tilde h_x\cdot\tilde\varepsilon(b)\tilde h_y = \tilde\varepsilon(a\alpha_x(b)\kappa(x,y))\tilde h_{xy}.$$

Daher ist die Abbildung $\eta:H\to\tilde H$, die einem Element der Form $\varepsilon(a)h_x\in H$ das Element $\tilde\varepsilon(a)\tilde h_x\in\tilde H$ zuordnet, ein Isomorphismus. Wegen $\eta(h_1)=\eta(\varepsilon(1)h_1)=\tilde\varepsilon(1)\tilde h_1=\tilde h_1$ ist

$$\begin{aligned}\eta(\varepsilon(a)) &= \eta(\varepsilon(a)h_1h_1^{-1}) = \eta(\varepsilon(a)h_1)\eta(h_1)^{-1} = \\ &= \tilde\varepsilon(a)\tilde h_1\tilde h_1^{-1} = \tilde\varepsilon(a)\end{aligned}$$

und

$$\begin{aligned}\tilde\nu(\eta(\varepsilon(a)h_x)) &= \tilde\nu(\tilde\varepsilon(a)\tilde h_x) = \tilde\nu(\tilde\varepsilon(a))\tilde\nu(\tilde h_x) = \\ &= x = \nu(\varepsilon(a))\nu(h_x) = \nu(\varepsilon(a)h_x)\end{aligned}$$

für $a\in K,\ x\in G$. □

12.8. Satz (Schreier)**.** *Gegeben seien Gruppen G und K. Indem man jeder Erweiterung von G mit K die dadurch definierten Parametersysteme zuordnet, erhält man eine Bijektion zwischen der Menge der Äquivalenzklassen von Erweiterungen von G mit K und der Menge der Äquivalenzklassen von Parametersystemen von G in K.*

Beweis. 12.1 – 12.7. □

Definition. Wir bezeichnen mit $\mathrm{Erw}(G,K)$ die Gesamtheit aller Erweiterungen von G mit K und mit $\overline{\mathrm{Erw}}(G,K)$ die Menge der entsprechenden Äquivalenzklassen.

12.9. Satz. *Für eine Gruppenerweiterung $K\xrightarrow{\varepsilon}H\xrightarrow{\nu}G$ sind äquivalent:*

(1) *Es existiert ein Homomorphismus $\sigma:G\to H$ mit $\nu\circ\sigma=\mathrm{id}_G$.*

(2) *$\varepsilon(K)$ besitzt ein Komplement in H.*

Definition. Gegebenenfalls sagt man, die Erweiterung *zerfällt*.

Beweis.

(1)⇒(2): Sei $\sigma : G \to H$ ein Homomorphismus mit $\nu \circ \sigma = \mathrm{id}_G$. Wir zeigen, daß $\sigma(G)$ ein Komplement von $\varepsilon(K) = \mathrm{Ker}(\nu)$ ist. Ist nämlich $h \in \mathrm{Ker}(\nu) \cap \sigma(G)$ und $h = \sigma(x)$ mit $x \in G$, so ist $1 = \nu(h) = \nu(\sigma(x)) = x$, also auch $h = \sigma(x) = 1$. Daher ist $\mathrm{Ker}(\nu) \cap \sigma(G) = 1$. Für $h \in H$ ist $\sigma(\nu(h)) \in H$ mit

$$\nu(h\sigma(\nu(h))^{-1}) \;=\; \nu(h)\nu(\sigma(\nu(h)))^{-1} \;=\; \nu(h)\nu(h)^{-1} \;=\; 1.$$

Folglich ist $h\sigma(\nu(h))^{-1} \in \mathrm{Ker}(\nu)$ und $h \in \mathrm{Ker}(\nu) \cdot \sigma(G)$. Dies zeigt $H = \mathrm{Ker}(\nu)\sigma(G)$.

(2)⇒(1): Sei C ein Komplement von $\varepsilon(K)$ in H, also $H = C\varepsilon(K)$ und $C \cap \varepsilon(K) = 1$. Dann ist die Abbildung $\gamma : C \to H/\varepsilon(K),\ c \mapsto c\,\varepsilon(K)$ ein Isomorphismus. Nach dem Homomorphiesatz ist auch die Abbildung $\overline{\nu} : H/\varepsilon(K) \to G,\ h\varepsilon(K) \mapsto \nu(h)$ ein Isomorphismus mit $\overline{\nu}(\gamma(c)) = \overline{\nu}(c\,\varepsilon(K)) = \nu(c)$ für $c \in C$. Daher ist die Abbildung $\sigma : G \to H,\ x \mapsto \gamma^{-1}(\overline{\nu}^{-1}(x)) \in C$ ein Homomorphismus mit $\nu(\sigma(x)) = \overline{\nu}(\gamma(\gamma^{-1}(\overline{\nu}^{-1}(x)))) = x$ für $x \in G$.

□

Bemerkung.

(i) Gegeben seien eine zerfallende Gruppenerweiterung $K \xrightarrow{\varepsilon} H \xrightarrow{\nu} G$ und ein Homomorphismus $\sigma : G \to H$ mit $\nu \circ \sigma = \mathrm{id}_G$. Für $x \in G$ ist dann $h_x := \sigma(x) \in H$ ein Urbild von x unter ν. Für $x, y \in G$ ist also $h_x h_y = \sigma(x)\sigma(y) = \sigma(xy) = h_{xy}$, d.h. das zugehörige Parametersystem ist von der Form (α, κ) mit $\kappa(x, y) = 1$ für $x, y \in G$. Daher ist auch $\alpha_x \circ \alpha_y = \alpha_{xy}$ für $x, y \in G$, d.h. $\alpha : G \to \mathrm{Aut}(K),\ x \mapsto \alpha_x$ ist ein Homomorphismus.

(ii) Sind umgekehrt Gruppen G und K und ein Homomorphismus $\alpha : G \to \mathrm{Aut}(K),\ x \mapsto \alpha_x$ gegeben, so erhält man ein Parametersystem von G in K, indem man $\kappa(x, y) = 1$ für $x, y \in G$ setzt. Eine entsprechende Gruppenerweiterung ergibt sich wie im Beweis von 12.3 dadurch, daß man auf der Menge $H := K \times G$ eine Verknüpfung durch

$$(a, x)(b, y) := (a\alpha_x(b), xy) \qquad \text{für } a, b \in K,\ x, y \in G$$

definiert. Man nennt die so definierte Gruppe H das *semidirekte Produkt* von G mit K bzgl. α. Die entsprechenden Homomorphismen $\varepsilon : K \to H,\ \nu : H \to G$ werden gegeben durch $\varepsilon(a) := (a, 1)$ und $\nu(a, x) := x$ für $a \in K,\ x \in G$. Die Gruppenerweiterung $K \xrightarrow{\varepsilon} H \xrightarrow{\nu} G$ zerfällt, denn die Abbildung $\sigma : G \to H,\ x \mapsto (1, x)$ erfüllt $\sigma(x)\sigma(y) = (1, x)(1, y) = (1\alpha_x(1), xy) = (1, xy) = \sigma(xy)$ und $\nu(\sigma(x)) = \nu(1, x) = x$ für $x, y \in G$. Oft identifiziert man K mit $\varepsilon(K)$ und G mit $\sigma(G)$. Dann ist $K \trianglelefteq H,\ G \leq H,\ K \cap G = 1$ und $KG = H$.

Beispiel. Ist $\alpha_x = \mathrm{id}_K$ für $x \in G$, so ist das semidirekte Produkt von G mit K bzgl. α genau das direkte Produkt von G und K.

KAPITEL 13

Erweiterungen mit abelschem Kern

13.1. Bemerkung. In diesem Abschnitt betrachten wir Erweiterungen einer Gruppe G mit einer abelschen Gruppe $K = A$. Ein Parametersystem von G in A ist in diesem Fall ein Paar (α, κ) von Abbildungen $\alpha : G \to \mathrm{Aut}(A),\ x \mapsto \alpha_x$ und $\kappa : G \times G \to A,\ (x, y) \mapsto \kappa(x, y)$ mit

$$\alpha_x \circ \alpha_y = \alpha_{xy} \quad \text{und} \quad \kappa(x, y)\kappa(xy, z) = \alpha_x(\kappa(y, z))\kappa(x, yz) \quad \text{für } x, y, z \in G.$$

Folglich ist α ein Homomorphismus, und jedes zu (α, κ) äquivalente Parametersystem hat ebenfalls α als Automorphismensystem. Nach Schreier definiert also jede Erweiterung $A \xrightarrow{\varepsilon} H \xrightarrow{\nu} G$ von G mit A genau ein Automorphismensystem, und äquivalente Gruppenerweiterungen definieren das gleiche Automorphismensystem. Für einen beliebigen Homomorphismus $\alpha : G \to \mathrm{Aut}(A),\ x \mapsto \alpha_x$ bezeichnen wir mit $\mathrm{Fak}(\alpha)$ die Menge aller Faktorensysteme zu α, d.h. die Menge aller Abbildungen $\kappa : G \times G \to A$ mit $\kappa(x, y)\kappa(xy, z) = \alpha_x(\kappa(y, z))\kappa(x, yz)$ für $x, y, z \in G$. Zwei Elemente $\kappa, \lambda \in \mathrm{Fak}(\alpha)$ nennen wir *äquivalent*, falls (α, κ) und (α, λ) äquivalente Parametersysteme sind, d.h. wenn es eine Abbildung $\varphi : G \to A$ gibt mit $\lambda(x, y) = \varphi(x)\alpha_x(\varphi(y))\kappa(x, y)\varphi(xy)^{-1}$ für $x, y \in G$. Mit $\overline{\mathrm{Fak}}(\alpha)$ bezeichnen wir die Menge aller Äquivalenzklassen von Faktorensystemen in $\mathrm{Fak}(\alpha)$. Ferner bezeichnen wir mit $\mathrm{Erw}(\alpha)$ die Gesamtheit aller Erweiterungen von G mit A zum Automorphismensystem α und mit $\overline{\mathrm{Erw}}(\alpha)$ die Menge der entsprechenden Äquivalenzklassen. Offenbar ist

$$\mathrm{Erw}(G, A) = \dot{\bigcup_{\alpha \in \mathrm{Hom}(G, \mathrm{Aut}(A))}} \mathrm{Erw}(\alpha)$$

und

$$\overline{\mathrm{Erw}}(G, A) = \dot{\bigcup_{\alpha \in \mathrm{Hom}(G, \mathrm{Aut}(A))}} \overline{\mathrm{Erw}}(\alpha),$$

und der Satz von Schreier liefert für $\alpha \in \mathrm{Hom}(G, \mathrm{Aut}(A))$ eine Bijektion zwischen $\overline{\mathrm{Erw}}(\alpha)$ und $\overline{\mathrm{Fak}}(\alpha)$. Im folgenden halten wir einen Homomorphismus $\alpha : G \to \mathrm{Aut}(A)$ fest und studieren $\overline{\mathrm{Fak}}(\alpha)$ (und damit $\overline{\mathrm{Erw}}(\alpha)$) genauer.

Satz. *Gegeben seien eine Gruppe G, eine abelsche Gruppe A und ein Homomorphismus $\alpha : G \to \mathrm{Aut}(A),\ x \mapsto \alpha_x$. Dann wird $\mathrm{Abb}(G \times G, A)$ zu einer abelschen Gruppe, wenn man $\gamma\delta \in \mathrm{Abb}(G \times G, A)$ durch $(\gamma\delta)(x, y) := \gamma(x, y)\delta(x, y)$ für $x, y \in G$ definiert. Ferner ist $\mathrm{Fak}(\alpha)$ eine Untergruppe von $\mathrm{Abb}(G \times G, A)$, und die zu 1 äquivalenten Faktorensysteme bilden eine Untergruppe $\mathrm{Pri}(\alpha)$ von $\mathrm{Fak}(\alpha)$. Zwei Elemente $\kappa, \lambda \in \mathrm{Fak}(\alpha)$ sind genau dann äquivalent, wenn $\kappa \equiv \lambda \pmod{\mathrm{Pri}(\alpha)}$ ist; insbesondere ist $\overline{\mathrm{Fak}}(\alpha) = \mathrm{Fak}(\alpha)/\mathrm{Pri}(\alpha)$. Auf diese Weise wird also $\overline{\mathrm{Fak}}(\alpha)$ zu einer abelschen Gruppe.*

Beweis. Die erste Aussage ist klar wegen $\mathrm{Abb}(G \times G, A) = \bigtimes_{x,y \in G} A$.
Offenbar ist $1 \in \mathrm{Pri}(\alpha) \subseteq \mathrm{Fak}(\alpha)$. Für $\kappa, \lambda \in \mathrm{Fak}(\alpha)$ ist auch $\kappa\lambda^{-1} \in \mathrm{Fak}(\alpha)$, wie man leicht nachrechnet. Im Fall $\kappa, \lambda \in \mathrm{Pri}(\alpha)$ existieren Abbildungen $\varphi, \psi : G \to A$ mit $\kappa(x, y) = \varphi(x)\alpha_x(\varphi(y))\varphi(xy)^{-1}$ und $\lambda(x, y) = \psi(x)\alpha_x(\psi(y))\psi(xy)^{-1}$ für $x, y \in G$. Daher ist $\varphi\psi^{-1} : G \to A, x \mapsto \varphi(x)\psi(x)^{-1}$ eine Abbildung mit

$$(\kappa\lambda^{-1})(x, y) \ = \ (\varphi\psi^{-1})(x) \cdot \alpha_x((\varphi\psi^{-1})(y)) \cdot ((\varphi\psi^{-1})(xy))^{-1}$$

für $x, y \in G$. Dies zeigt: $\mathrm{Pri}(\alpha) \leq \mathrm{Fak}(\alpha) \leq \mathrm{Abb}(G \times G, A)$. Für $\kappa, \lambda \in \mathrm{Fak}(\alpha)$ gilt ferner:

$$\begin{aligned} \kappa \text{ ist äquivalent zu } \lambda &\Leftrightarrow \exists \varphi : G \to A : \forall x, y \in G : \lambda(x,y) = \varphi(x)\alpha_x(\varphi(y))\kappa(x,y)\varphi(xy)^{-1} \\ &\Leftrightarrow \exists \varphi : G \to A : \forall x, y \in G : \lambda(x,y) = \kappa(x,y)\varphi(x)\alpha_x(\varphi(y))\varphi(xy)^{-1} \\ &\Leftrightarrow \lambda \equiv \kappa \pmod{\mathrm{Pri}(\alpha)}. \end{aligned}$$

□

Definition. Die Elemente in $\mathrm{Pri}(\alpha)$ nennt man *prinzipale* Faktorensysteme.

13.2. Bemerkung. Gegeben sei eine Gruppe G, eine abelsche Gruppe A und ein Homomorphismus $\alpha : G \to \mathrm{Aut}(A)$.

(i) Nach 12.9 ist ein Faktorensystem in $\mathrm{Fak}(\alpha)$ genau dann prinzipal, wenn die entsprechende Erweiterung zerfällt.

(ii) Die Gruppe $\overline{\mathrm{Fak}}(\alpha)$ ist ein Beispiel für eine Kohomologiegruppe; Kohomologiegruppen werden in der Homologischen Algebra behandelt und haben Anwendungen in Gruppentheorie, Zahlentheorie, Topologie, etc. Wir vermeiden die sonst übliche Bezeichnung $H^2(G, A)$, da sie die Abhängigkeit von α nicht deutlich macht.

13.3. Satz. *Gegeben seien eine endliche Gruppe G, eine abelsche Gruppe A und ein Homomorphismus $\alpha : G \to \mathrm{Aut}(A)$, $x \mapsto \alpha_x$. Dann ist $c^{|G|} = 1$ für $c \in \overline{\mathrm{Fak}}(\alpha)$; insbesondere ist $\overline{\mathrm{Fak}}(\alpha)$ eine Torsionsgruppe.*

Beweis. Für $x, y, z \in G$ und $\kappa \in \mathrm{Fak}(\alpha)$ ist $\kappa(x,y) = \alpha_x(\kappa(y,z))\kappa(x,yz)\kappa(xy,z)^{-1}$, also

$$\kappa(x,y)^{|G|} = \prod_{z \in G} \alpha_x(\kappa(y,z)) \prod_{z \in G} \kappa(x,yz) \prod_{z \in G} \kappa(xy,z)^{-1}.$$

Setzt man $\varphi(x) := \prod_{z \in G} \kappa(x,z)$ für $x \in G$, so ist $\varphi : G \to A$ eine Abbildung mit

$$\kappa(x,y)^{|G|} = \alpha_x(\varphi(y))\varphi(x)\varphi(xy)^{-1} \qquad \text{für } x, y \in G,$$

d.h. $\kappa^{|G|} \in \mathrm{Pri}(\alpha)$. □

Bemerkung. Ist auch A endlich, so ist außerdem $c^{|A|} = 1$ für $c \in \overline{\mathrm{Fak}}(\alpha)$; denn es ist $\gamma^{|A|} = 1$ für alle $\gamma \in \mathrm{Abb}(G \times G, A)$. Sind ferner $|G|$ und $|A|$ teilerfremd, so ist $\overline{\mathrm{Fak}}(\alpha) = 1$. In diesem Fall zerfällt daher jede Erweiterung von G mit A. Diese Beobachtung verallgemeinert der folgende Satz.

13.4. Satz (Schur-Zassenhaus)**.** *Gegeben sei ein Normalteiler K einer endlichen Gruppe H mit* $\mathrm{ggT}(|K|, |H/K|) = 1$ *(d.h. ein Hallnormalteiler von G).*

(i) *Dann hat K ein Komplement in H.*

(ii) *Ist K oder H/K auflösbar, so sind je zwei Komplemente von K in H konjugiert.*

Bemerkung. Wegen $\mathrm{ggT}(|K|, |H/K|) = 1$ ist $|K|$ oder $|H/K|$ ungerade. Nach dem Satz von Feit-Thompson ist also K oder H/K auflösbar. Daher ist die Voraussetzung unter (ii) entbehrlich, wenn man den Satz von Feit-Thompson bewiesen hat.

Beweis.

(i) Es genügt zu zeigen, daß H eine Untergruppe C der Ordnung $|H/K|$ enthält; denn dann ist $|K \cap C| \mid \mathrm{ggT}(|K|, |C|) = 1$, also $K \cap C = 1$, und $|KC| = |K| \cdot |C| = |H|$, also $KC = H$.
Die Sache ist trivial im Fall $K = 1$. Daher nehmen wir $|K| > 1$ an und argumentieren durch Induktion nach $|K|$. Sei p ein Primteiler von $|K|$ und P eine p-Sylowgruppe von K. Nach Frattini ist dann $H = N_H(P)K$, also $N_H(P) \cap K \trianglelefteq N_H(P)$ und $N_H(P)/N_H(P) \cap K \cong N_H(P)K/K = H/K$. Folglich ist $N_H(P) \cap K/P \trianglelefteq N_H(P)/P$ und $|N_H(P)/P : N_H(P) \cap K/P| = |H/K|$. Nach Induktion enthält $N_H(P)/P$ eine Untergruppe L/P mit $|L/P| = |H/K|$. Wegen $P \neq 1$ ist $Z := Z(P) \neq 1$. Daher ist $P/Z \trianglelefteq L/Z$ und $|L/Z : P/Z| = |L : P| = |H/K|$. Nach Induktion enthält L/Z eine Untergruppe U/Z mit $|U/Z| = |H/K|$. Nach Bemerkung 13.3 zerfällt die Erweiterung $Z \longrightarrow U \longrightarrow U/Z$; insbesondere enthält U eine Untergruppe der Ordnung $|U/Z| = |H/K|$, und wir sind fertig.

(ii) Seien C, D Komplemente von K in H, und sei zunächst K abelsch. Dann zerfällt die Erweiterung $K \longrightarrow H \longrightarrow H/K =: G$. Wie im Beweis von 12.9 existieren also Homomorphismen $\sigma, \tau : G \to H$ mit $\sigma(G) = C,\ \tau(G) = D$. Zu den Elementen $h_x := \sigma(x),\ \tilde{h}_x := \tau(x)$ $(x \in G)$ gehören Parametersysteme (α, κ) bzw. $(\alpha, \tilde{\kappa})$ von G in K mit $\kappa(x, y) = 1 = \tilde{\kappa}(x, y)$ für $x, y \in G$. Schreibt man $\tilde{h}_x = \varphi(x)h_x$ mit $\varphi(x) \in K$ für $x \in G$, so ist $\varphi(x)\alpha_x(\varphi(y)) = \varphi(xy)$ für $x, y \in G$. Folglich gilt für $x \in G$:

$$\varphi(x)^{|G|} \ = \ \prod_{y\in G} \alpha_x(\varphi(y))^{-1} \prod_{y\in G} \varphi(xy) \ = \ \alpha_x(a)^{-1}a$$

mit $a := \prod_{y\in G} \varphi(y)$. Wegen $\mathrm{ggT}(|K|, |G|) = 1$ existiert ein $z \in \mathbb{Z}$ mit $|G|z \equiv 1 \pmod{|K|}$. Mit $b := a^z$ ist also $\varphi(x) = \varphi(x)^{|G|z} = \alpha_x(b^{-1})b$, d.h.

$$\tau(x) \ = \ \tilde{h}_x \ = \ \varphi(x)h_x \ = \ b\alpha_x(b^{-1})h_x \ = \ bh_xb^{-1}h_x^{-1}h_x \ = \ b\sigma(x)b^{-1}$$

für $x \in G$. Insbesondere ist $D = \tau(G) = b\sigma(G)b^{-1} = bCb^{-1}$.
Als nächstes sei K auflösbar. Wir argumentieren durch Induktion nach $|K|$ und können $K \neq 1$ annehmen. Dann ist $K' < K$, und $CK'/K',\ DK'/K'$ sind Komplemente von K/K' in H/K'. Da K/K' abelsch ist, existiert ein $h \in H$ mit $DK'/K' = (hK')(CK'/K')(hK')^{-1} = (hCh^{-1})K'/K'$. Daher sind D und hCh^{-1} Komplemente von K' in DK'. Nach Induktion sind also D und hCh^{-1} in DK' konjugiert, und wir sind in diesem Fall fertig.
Schließlich sei H/K auflösbar. Wegen $C \cong H/K \cong D$ sind auch C, D auflösbar. Wir wählen einen minimalen Normalteiler M von C. Dann ist $M \cong (\mathbb{Z}/p\mathbb{Z})^m$ für ein $m \in \mathbb{Z}$ und eine Primzahl p. Nach Dedekind ist $MK = MK \cap DK = (MK \cap D)K$ und $N := MK \cap D \trianglelefteq D$. Im Fall $MK = H$ sind $M = C$ und $N = D$ p-Sylowgruppen von H, also in H konjugiert. Sei daher $MK \neq H$. Wir argumentieren durch Induktion nach $|H|$ und können dann voraussetzen, daß ein $x \in MK$ existiert mit $xMx^{-1} = N$. Dann ist $xCx^{-1} \subseteq xN_H(M)x^{-1} = N_H(xMx^{-1}) = N_H(N)$ und $D \subseteq N_H(N)$. Ferner sind xCx^{-1}/N und D/N Komplemente von $N_H(N) \cap K/N$ in $N_H(N)/N$. Nach Induktion sind also xCx^{-1}/N und D/N in $N_H(N)/N$ konjugiert, also auch xCx^{-1} und D in $N_H(N)$.

□

13.5. Bemerkung. Der folgende Satz verallgemeinert 13.3.

Satz. *Gegeben seien eine Untergruppe U einer endlichen Gruppe G, eine abelsche Gruppe A, ein Homomorphismus $\alpha : G \to \mathrm{Aut}(A),\ x \mapsto \alpha_x$ und ein Element $\kappa \in \mathrm{Fak}(\alpha)$. Ist die Einschränkung $\kappa_U : U \times U \to A$ von $\kappa : G \times G \to A$ prinzipal, so auch $\kappa^{|G:U|}$.*

Beweis. Wir wählen eine Gruppenerweiterung $A \xrightarrow{\varepsilon} H \xrightarrow{\nu} G$, die (α, κ) definiert. Dann ist $A \xrightarrow{\varepsilon_U} V := \nu^{-1}(U) \xrightarrow{\nu_U} U$ eine Gruppenerweiterung, die das eingeschränkte Parametersystem (α_U, κ_U) definiert; dabei sind $\varepsilon_U, \nu_U, \alpha_U$ entsprechend eingeschränkte Abbildungen. Nach Voraussetzung zerfällt die Erweiterung $A \xrightarrow{\varepsilon_U} V \xrightarrow{\nu_U} U$, d.h. es existiert ein Homomorphismus $\sigma : U \to V$ mit $\nu_U \circ \sigma = \mathrm{id}_U$. Für $x \in U$ ist dann $h_x := \sigma(x) \in V$ ein Urbild von x unter ν_U. Wir wählen ein Repräsentantensystem R für die Linksnebenklassen von G nach U, wobei o.B.d.A. $1 \in R$. Dann ist also $G = \dot{\bigcup}_{r\in R} rU$ und man kann jedes Element $x \in G$ in der Form $x = \overline{x}\underline{x}$ mit eindeutig bestimmten Elementen $\overline{x} \in R,\ \underline{x} \in U$ schreiben. Für $r \in R \setminus \{1\}$ wählen wir ein beliebiges Urbild $h_r \in H$ von r unter ν. Für ein beliebiges Element $x \in G$ ist dann $h_x := h_{\overline{x}}h_{\underline{x}}$ ein Urbild von x unter ν. (Diese Definition ist verträglich mit den Wahlen von h_x für $x \in U \cup R$ wegen $h_1 = \sigma(1) = 1$.) Wir bezeichnen mit γ das entsprechende Faktorensystem, d.h. für $x, y \in G$ ist $h_xh_y = \varepsilon(\gamma(x, y))h_{xy}$. Für $x, y \in U$ ist

$$h_xh_y \ = \ \sigma(x)\sigma(y) \ = \ \sigma(xy) = h_{xy},$$

also $\gamma(x,y)=1$. Für $x\in G$ und $y\in U$ ist daher

$$\begin{aligned}\varepsilon(\gamma(x,y)) &= h_xh_yh_{xy}^{-1} = h_{\overline{x}\underline{x}}h_yh_{\overline{x}\underline{x}y}^{-1} = \\ &= h_{\overline{x}}h_{\underline{x}}h_y(h_{\overline{x}}h_{\underline{x}y})^{-1} = \\ &= h_{\overline{x}}h_{\underline{x}}h_yh_{\underline{x}y}^{-1}h_{\overline{x}}^{-1} = \\ &= h_{\overline{x}}\varepsilon(\underbrace{\gamma(\underline{x},y)}_{=1})h_{\overline{x}}^{-1} = \\ &= 1,\end{aligned}$$

d.h. $\gamma(x,y)=1$. Für $x,y\in G$ ist daher

$$\begin{aligned}\varepsilon(\gamma(x,y)) &= h_xh_yh_{xy}^{-1} = h_xh_{\overline{y}\underline{y}}h_{xy}^{-1} = \\ &= h_xh_{\overline{y}}h_{\underline{y}}h_{xy}^{-1} = \\ &= \varepsilon(\gamma(x,\overline{y}))h_{x\overline{y}}h_{\underline{y}}h_{xy}^{-1} = \\ &= \varepsilon(\gamma(x,\overline{y}))\varepsilon(\underbrace{\gamma(x\overline{y},\underline{y})}_{=1})h_{x\overline{y}\underline{y}}h_{xy}^{-1} = \\ &= \varepsilon(\gamma(x,\overline{y})),\end{aligned}$$

d.h. $\gamma(x,y)=\gamma(x,\overline{y})$. Für $x,y,z\in G$ ist also

$$\begin{aligned}\gamma(x,y) &= \alpha_x(\gamma(y,z))\gamma(x,yz)\gamma(xy,z)^{-1} = \\ &= \alpha_x(\gamma(y,\overline{z}))\gamma(x,\overline{yz})\gamma(xy,\overline{z})^{-1}.\end{aligned}$$

Wir setzen $\delta(x):=\prod_{z\in R}\gamma(x,z)$ für $x\in G$ und erhalten:

$$\gamma(x,y)^{|R|} = \alpha_x(\delta(y))\delta(x)\delta(xy)^{-1}$$

für $x,y\in G$. Dies zeigt, daß $\gamma^{|R|}$ prinzipal ist. Da κ zu γ äquivalent ist, ist auch $\kappa^{|R|}$ prinzipal. □

13.6. Satz. *Gegeben seien eine endliche Gruppe G, eine abelsche Gruppe A, ein Homomorphismus $\alpha: G\to \mathrm{Aut}(A),\ x\mapsto\alpha_x$ und ein Element $\kappa\in\mathrm{Fak}(\alpha)$.*

(i) *Ist κ prinzipal, so auch die Einschränkung $\kappa_U: U\times U\to A$ von κ für jede Untergruppe U von G.*

(ii) *Existiert zu jedem Primteiler p von $|G|$ eine p-Sylowgruppe P von G mit der Eigenschaft, daß die Einschränkung $\kappa_P: P\times P\to A$ von κ prinzipal ist, so ist auch κ prinzipal.*

Beweis.

(i) Trivial.

(ii) Nach 13.5 folgt aus der Voraussetzung in (ii), daß $\kappa^{|G:P|}+\mathrm{Pri}(\alpha)=1$, d.h. $|\langle\kappa+\mathrm{Pri}(\alpha)\rangle|\ \big|\ |G:P|$ für jedes solche P ist. Da die Indizes $|G:P|$ insgesamt teilerfremd sind, folgt $|\langle\kappa+\mathrm{Pri}(\alpha)\rangle|=1$, d.h. $\kappa\in\mathrm{Pri}(\alpha)$.

□

13.7. Satz (Gaschütz)**.** *Eine Gruppenerweiterung $A\xrightarrow{\varepsilon}H\xrightarrow{\nu}G$, wobei A abelsch und G endlich ist, zerfällt genau dann, wenn zu jedem Primteiler p von $|G|$ eine p-Sylowgruppe P von G existiert mit der Eigenschaft, daß die eingeschränkte Erweiterung $A\longrightarrow\nu^{-1}(P)\longrightarrow P$ zerfällt.*

Beweis. 13.6 und Schreier. □

Bemerkung. Im Gegensatz zum Satz von Schur-Zassenhaus gilt der Satz von Gaschütz i.a. nicht für nichtabelsches A.

KAPITEL 14

Erweiterungen mit nichtabelschem Kern

14.1. Bemerkung. Gegeben seien Gruppen G und K und ein Parametersystem (α, κ) von G in K. Wegen $\alpha_x \circ \alpha_y = \iota_{\kappa(x,y)} \circ \alpha_{xy}$ für $x, y \in G$ ist die Abbildung $\omega : G \to \mathrm{Out}(K) = \mathrm{Aut}(K)/\mathrm{Inn}(K),\ x \mapsto \alpha_x \mathrm{Inn}(K)$ ein Homomorphismus. Wir nennen ω die durch (α, κ) definierte *Paarung*. Ist (α', κ') ein zu (α, κ) äquivalentes Parametersystem, so existiert eine Abbildung $\varphi : G \to K$ mit $\alpha'_x = \iota_{\varphi(x)} \circ \alpha_x$ und $\kappa'(x, y) = \varphi(x)\alpha_x(\varphi(y))\kappa(x, y)\varphi(xy)^{-1}$ für $x, y \in G$. Daher definiert (α', κ') die gleiche Paarung wie (α, κ). Folglich definiert auch jede Äquivalenzklasse von Parametersystemen von G in K eine Paarung. Nach Schreier definiert also auch jede Erweiterung von G mit K eine Paarung, und äquivalente Erweiterungen definieren die gleiche Paarung. (Ist K abelsch, so ist $\mathrm{Inn}(K) = 1$, also $\mathrm{Aut}(K) \cong \mathrm{Out}(K)$, und man braucht nicht zwischen Automorphismensystemen und Paarungen zu unterscheiden.)
Für jeden Homomorphismus $\omega : G \to \mathrm{Out}(K)$ bezeichnen wir mit $\mathrm{Erw}(\omega)$ die Gesamtheit aller Erweiterungen und mit $\mathrm{Par}(\omega)$ die Menge aller Parametersysteme von G in K zur Paarung ω. Ferner bezeichnen wir mit $\overline{\mathrm{Erw}}(\omega)$ und $\overline{\mathrm{Par}}(\omega)$ die Mengen der entsprechenden Äquivalenzklassen. Dann ist also

$$\begin{aligned}
\mathrm{Erw}(G, K) &= \dot{\bigcup_{\omega \in \mathrm{Hom}(G, \mathrm{Out}(K))}} \mathrm{Erw}(\omega), \\
\mathrm{Par}(G, K) &= \dot{\bigcup_{\omega \in \mathrm{Hom}(G, \mathrm{Out}(K))}} \mathrm{Par}(\omega), \\
\overline{\mathrm{Erw}}(G, K) &= \dot{\bigcup_{\omega \in \mathrm{Hom}(G, \mathrm{Out}(K))}} \overline{\mathrm{Erw}}(\omega), \\
\overline{\mathrm{Par}}(G, K) &= \dot{\bigcup_{\omega \in \mathrm{Hom}(G, \mathrm{Out}(K))}} \overline{\mathrm{Par}}(\omega).
\end{aligned}$$

Ferner liefert der Satz von Schreier für jeden Homomorphismus $\omega : G \to \mathrm{Out}(K)$ eine Bijektion zwischen $\overline{\mathrm{Erw}}(\omega)$ und $\overline{\mathrm{Par}}(\omega)$. Im folgenden halten wir ω fest und untersuchen $\overline{\mathrm{Erw}}(\omega)$ und $\overline{\mathrm{Par}}(\omega)$. Im Unterschied zum vorigen Kapitel kann es durchaus vorkommen, daß $\mathrm{Erw}(\omega)$ leer ist. Wir werden u.a. feststellen, wann das passiert.
Für jeden Automorphismus α von K ist die Einschränkung $\mathrm{res}^K_{Z(K)}(\alpha)$ von α auf $Z(K)$ ein Automorphismus von $Z(K)$. Auf diese Weise erhält man einen Homomorphismus $\mathrm{res}^K_{Z(K)} : \mathrm{Aut}(K) \to \mathrm{Aut}(Z(K))$. Offenbar ist $\mathrm{res}^K_{Z(K)}(\iota) = \mathrm{id}_{Z(K)}$ für alle $\iota \in \mathrm{Inn}(K)$. Daher induziert $\mathrm{res}^K_{Z(K)}$ einen Homomorphismus $\mathrm{Out}(K) = \mathrm{Aut}(K)/\mathrm{Inn}(K) \to \mathrm{Aut}(Z(K)),\ \alpha \mathrm{Inn}(K) \mapsto \mathrm{res}^K_{Z(K)}(\alpha)$; diesen bezeichnen wir ebenfalls mit $\mathrm{res}^K_{Z(K)}$. Für jeden Homomorphismus $\omega : G \to \mathrm{Out}(K)$ ist also $\zeta := \mathrm{res}^K_{Z(K)} \circ \omega : G \to \mathrm{Out}(K) \to \mathrm{Aut}(Z(K))$ ein Homomorphismus, d.h. ein Automorphismensystem von G in die abelsche Gruppe $Z(K)$. Es wird sich herausstellen, daß ein enger Zusammenhang zwischen $\overline{\mathrm{Par}}(\omega)$ und $\overline{\mathrm{Fak}}(\zeta)$ besteht.

14.2. Satz. *Gegeben seien Gruppen G und K und ein Homomorphismus $\omega : G \to \mathrm{Out}(K)$ mit $\mathrm{Par}(\omega) \neq \emptyset$. Setzt man $\zeta := \mathrm{res}^K_{Z(K)} \circ \omega : G \to \mathrm{Aut}(Z(K))$, so gilt:*

(i) *Für $(\alpha, \kappa) \in \mathrm{Par}(\omega)$ und $\gamma \in \mathrm{Fak}(\zeta)$ ist auch $(\alpha, \gamma\kappa) \in \mathrm{Par}(\omega)$; dabei ist $\gamma\kappa : G \times G \to K$ definiert durch $(\gamma\kappa)(x, y) := \gamma(x, y)\kappa(x, y)$ für $x, y \in G$.*

(ii) *Durch (i) erhält man eine Operation von* $\mathrm{Fak}(\zeta)$ *auf* $\mathrm{Par}(\omega)$*:* ${}^{\gamma}(\alpha,\kappa) := (\alpha,\gamma\kappa)$ *für* $\gamma \in \mathrm{Fak}(\zeta)$, $(\alpha,\kappa) \in \mathrm{Par}(\omega)$.

(iii) *Sind* $(\alpha,\kappa),(\alpha',\kappa') \in \mathrm{Par}(\omega)$ *äquivalent, so auch* ${}^{\gamma}(\alpha,\kappa)$ *und* ${}^{\gamma}(\alpha',\kappa')$ *für* $\gamma \in \mathrm{Fak}(\zeta)$*. Daher induziert die Operation in (ii) eine Operation von* $\mathrm{Fak}(\zeta)$ *auf* $\overline{\mathrm{Par}}(\omega)$*:* ${}^{\gamma}[\alpha,\kappa] := [\alpha,\gamma\kappa]$ *für* $\gamma \in \mathrm{Fak}(\zeta)$, $(\alpha,\kappa) \in \mathrm{Par}(\omega)$, $[\alpha,\kappa]$ *die Äquivalenzklasse von* (α,κ).

(iv) *Für* $(\alpha,\kappa) \in \mathrm{Par}(\omega)$ *und* $\delta \in \mathrm{Pri}(\zeta)$ *ist* ${}^{\delta}(\alpha,\kappa)$ *äquivalent zu* (α,κ)*. Daher operiert* $\mathrm{Pri}(\zeta)$ *trivial auf* $\overline{\mathrm{Par}}(\omega)$*, und die Operation von (iii) induziert eine Operation von* $\overline{\mathrm{Fak}}(\zeta)$ *auf* $\overline{\mathrm{Par}}(\omega)$*:* ${}^{\gamma\,\mathrm{Pri}(\zeta)}[\alpha,\kappa] := [\alpha,\gamma\kappa]$ *für* $\gamma \in \mathrm{Fak}(\zeta)$, $(\alpha,\kappa) \in \mathrm{Par}(\omega)$.

(v) *Für* $(\alpha,\kappa) \in \mathrm{Par}(\omega)$ *ist die Abbildung* $\overline{\mathrm{Fak}}(\zeta) \to \overline{\mathrm{Par}}(\omega)$, $\gamma\,\mathrm{Pri}(\zeta) \mapsto {}^{\gamma\,\mathrm{Pri}(\zeta)}[\alpha,\kappa]$ *bijektiv.*

Bemerkung.

(i) Nach Schreier gibt es also im Fall $\mathrm{Par}(\omega) \neq \emptyset$ eine Bijektion zwischen $\overline{\mathrm{Erw}}(\omega)$ und $\overline{\mathrm{Erw}}(\zeta)$. Man kann daher oft Fragen über Erweiterungen von G mit K zurückführen auf Fragen über Erweiterungen von G mit $Z(K)$.

(ii) Die Bijektion $\overline{\mathrm{Fak}}(\zeta) \to \overline{\mathrm{Par}}(\omega)$ hängt ab von der Wahl von $(\alpha,\kappa) \in \mathrm{Par}(\omega)$. Es gibt i.a. keine besonders ausgezeichnete Wahl für (α,κ). (Die Situation hier ist ähnlich zur Situation bei linearen Gleichungssystemen, wo im Fall der Existenz einer Lösung die Lösungen des inhomogenen Systems in (nicht kanonischer) Bijektion zu den Lösungen des entsprechenden homogenen Systems stehen.)

Beweis.

(i) Für $x,y,z \in G$ ist

$$\begin{aligned}(\gamma\kappa)(x,y)\cdot(\gamma\kappa)(xy,z) &= \gamma(x,y)\kappa(x,y)\gamma(xy,z)\kappa(xy,z) = \\ &= \gamma(x,y)\gamma(xy,z)\kappa(x,y)\kappa(xy,z) = \\ &= \zeta_x(\gamma(y,z))\gamma(x,yz)\alpha_x(\kappa(y,z))\kappa(x,yz) = \\ &= \alpha_x(\gamma(y,z))\alpha_x(\kappa(y,z))\gamma(x,yz)\kappa(x,yz) = \\ &= \alpha_x((\gamma\kappa)(y,z))\cdot(\gamma\kappa)(x,yz)\end{aligned}$$

und

$$\begin{aligned}\iota_{(\gamma\kappa)(x,y)}\circ\alpha_{xy} &= \iota_{\gamma(x,y)\kappa(x,y)}\circ\alpha_{xy} = \\ &= \iota_{\gamma(x,y)}\circ\iota_{\kappa(x,y)}\circ\alpha_{xy} = \\ &= \iota_{\kappa(x,y)}\circ\alpha_{xy} = \\ &= \alpha_x\circ\alpha_y.\end{aligned}$$

(ii) Für $(\alpha,\kappa) \in \mathrm{Par}(\omega)$ und $\gamma,\delta \in \mathrm{Fak}(\zeta)$ ist offenbar

$${}^{\delta}({}^{\gamma}(\alpha,\kappa)) = {}^{\delta}(\alpha,\gamma\kappa) = (\alpha,\delta\gamma\kappa) = {}^{\delta\gamma}(\alpha,\kappa)$$

und ${}^{1}(\alpha,\kappa) = (\alpha,\kappa)$.

(iii) Seien $(\alpha,\kappa),(\alpha',\kappa') \in \mathrm{Par}(\omega)$ äquivalent, und sei $\varphi \in \mathrm{Abb}(G,K)$ mit $\alpha'_x = \iota_{\varphi(x)}\circ\alpha_x$ und $\kappa'(x,y) = \varphi(x)\alpha_x(\varphi(y))\kappa(x,y)\varphi(xy)^{-1}$ für $x,y \in G$. Multiplikation mit $\gamma(x,y)$ ergibt:

$$\gamma(x,y)\kappa'(x,y) = \varphi(x)\alpha_x(\varphi(y))\gamma(x,y)\kappa(x,y)\varphi(xy)^{-1}$$

für $x,y \in G$. Daher sind ${}^{\gamma}(\alpha,\kappa) = (\alpha,\gamma\kappa)$ und ${}^{\gamma}(\alpha',\kappa') = (\alpha',\gamma\kappa')$ äquivalent.

(iv) Seien $(\alpha,\kappa) \in \mathrm{Par}(\omega)$, $\delta \in \mathrm{Pri}(\zeta)$ und $\varphi \in \mathrm{Abb}(G,Z(K))$ mit $\delta(x,y) = \varphi(x)\zeta_x(\varphi(y))\varphi(xy)^{-1}$. Dann ist $\alpha_x = \iota_{\varphi(x)}\circ\alpha_x$ und

$$(\delta\kappa)(x,y) = \delta(x,y)\kappa(x,y) = \varphi(x)\alpha_x(\varphi(y))\kappa(x,y)\varphi(xy)^{-1}$$

für $x,y \in G$, d.h. ${}^{\delta}(\alpha,\kappa)$ ist äquivalent zu (α,κ).

(v) Seien $(\alpha,\kappa) \in \mathrm{Par}(\omega)$ und $\gamma_1,\gamma_2 \in \mathrm{Fak}(\zeta)$ mit ${}^{\gamma_1}[\alpha,\kappa] = {}^{\gamma_2}[\alpha,\kappa]$. Dann ist $\gamma := \gamma_1^{-1}\gamma_2 \in \mathrm{Fak}(\zeta)$ mit ${}^{\gamma}[\alpha,\kappa] = [\alpha,\kappa]$, d.h. (α,κ) ist äquivalent zu $(\alpha,\gamma\kappa)$. Folglich existiert eine Abbildung $\varphi : G \to K$ mit $\alpha_x = \iota_{\varphi(x)}\circ\alpha_x$ und $\gamma(x,y)\kappa(x,y) = \varphi(x)\alpha_x(\varphi(y))\kappa(x,y)\varphi(xy)^{-1}$ für $x,y \in G$. Für $x \in G$ ist also $\iota_{\varphi(x)} = \mathrm{id}_K$, d.h. $\varphi(x) \in Z(K)$. Folglich ist $\gamma(x,y) = \varphi(x)\alpha_x(\varphi(y))\varphi(xy)^{-1}$ für $x,y \in G$, d.h. $\gamma \in \mathrm{Pri}(\zeta)$. Dann ist $\gamma_1\,\mathrm{Pri}(\zeta) = \gamma_2\,\mathrm{Pri}(\zeta)$, und die Injektivität ist gezeigt.

Zum Beweis der Surjektivität seien $(\alpha,\kappa),(\beta,\lambda)\in \mathrm{Par}(\omega)$. Wir beweisen die Existenz eines $\gamma\in \mathrm{Fak}(\zeta)$, so daß (α,κ) zu ${}^{\gamma}(\beta,\lambda)$ äquivalent ist. Für $x\in G$ existiert wegen $\alpha_x\,\mathrm{Inn}(K)=\omega(x)=\beta_x\,\mathrm{Inn}(K)$ ein Element $\varphi(x)\in K$ mit $\iota_{\varphi(x)}\circ\alpha_x=\beta_x$. Wir setzen $\kappa'(x,y):=\varphi(x)\alpha_x(\varphi(y))\kappa(x,y)\,\varphi(xy)^{-1}\in K$ für $x,y\in G$. Dann ist (α,κ) äquivalent zu (β,κ'). Für $x,y\in G$ ist $\iota_{\kappa'(x,y)}\circ\beta_{xy}=\beta_x\circ\beta_y=\iota_{\lambda(x,y)}\circ\beta_{xy}$, also $\iota_{\kappa'(x,y)}=\iota_{\lambda(x,y)}$. Daher ist $\gamma(x,y):=\kappa'(x,y)\lambda(x,y)^{-1}\in Z(K)$, und für $x,y\in G$ gilt:

$$\begin{aligned}
\gamma(x,y)\gamma(xy,z) &= \kappa'(x,y)\lambda(x,y)^{-1}\gamma(xy,z) \;=\\
&= \kappa'(x,y)\gamma(xy,z)\lambda(x,y)^{-1} \;=\\
&= \kappa'(x,y)\kappa'(xy,z)\lambda(xy,z)^{-1}\lambda(x,y)^{-1} \;=\\
&= \beta_x(\kappa'(y,z))\kappa'(x,yz)\lambda(x,yz)^{-1}\beta_x(\lambda(y,z))^{-1} \;=\\
&= \beta_x(\kappa'(y,z))\gamma(x,yz)\beta_x(\lambda(y,z))^{-1} \;=\\
&= \beta_x(\kappa'(y,z)\lambda(y,z)^{-1})\gamma(x,yz) \;=\\
&= \zeta_x(\gamma(y,z))\gamma(x,yz).
\end{aligned}$$

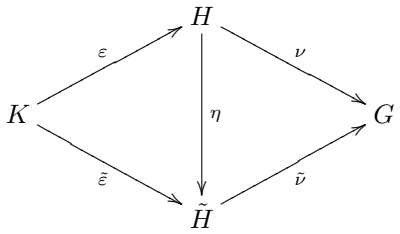
Daher ist $\gamma\in\mathrm{Fak}(\zeta)$ und $\kappa'=\gamma\lambda$, d.h. $(\beta,\kappa')={}^{\gamma}(\beta,\lambda)$. Damit ist (α,κ) äquivalent zu $(\beta,\kappa')={}^{\gamma}(\beta,\lambda)$.

□

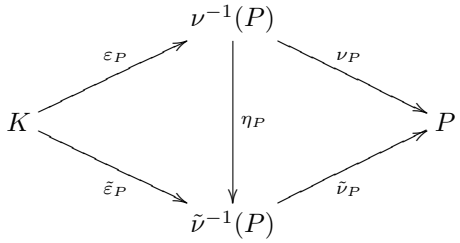
14.3. Satz (Johnson-Zassenhaus)**.** *Zwei Erweiterungen $K\xrightarrow{\varepsilon}H\xrightarrow{\nu}G$, $K\xrightarrow{\tilde\varepsilon}\tilde H\xrightarrow{\tilde\nu}G$ einer endlichen Gruppe G mit einer beliebigen Gruppe K sind genau dann äquivalent, wenn zu jedem Primteiler p von $|G|$ eine p-Sylowgruppe P von G existiert mit der Eigenschaft, daß die eingeschränkten Erweiterungen $K\xrightarrow{\varepsilon_P}\nu^{-1}(P)\xrightarrow{\nu_P}P$, $K\xrightarrow{\tilde\varepsilon_P}\tilde\nu^{-1}(P)\xrightarrow{\tilde\nu_P}P$ äquivalent sind.*

Beweis.

⇒: Seien $K\xrightarrow{\varepsilon}H\xrightarrow{\nu}G$, $K\xrightarrow{\tilde\varepsilon}\tilde H\xrightarrow{\tilde\nu}G$ äquivalent, $\eta: H\to\tilde H$ ein Isomorphismus mit $\eta\circ\varepsilon=\tilde\varepsilon$, $\tilde\nu\circ\eta=\nu$, p ein Primteiler von $|G|$ und P eine p-Sylowgruppe von G.



Dann ist $\eta(\nu^{-1}(P))\subseteq\tilde\nu^{-1}(P)$; denn für $h\in\nu^{-1}(P)$ ist $\tilde\nu(\eta(h))=\nu(h)\in P$. Durch Einschränken erhält man ein Diagramm der Form



⇐: Zu jedem Primteiler p von $|G|$ existiere jetzt umgekehrt eine p-Sylowgruppe P von G mit der Eigenschaft, daß die Erweiterungen $K\xrightarrow{\varepsilon_P}\nu^{-1}(P)\xrightarrow{\nu_P}P$ und $K\xrightarrow{\tilde\varepsilon_P}\tilde\nu^{-1}(P)\xrightarrow{\tilde\nu_P}P$ äquivalent sind. Wir bezeichnen mit ω und $\tilde\omega$ die durch $K\xrightarrow{\varepsilon}H\xrightarrow{\nu}G$ bzw. $K\xrightarrow{\tilde\varepsilon}\tilde H\xrightarrow{\tilde\nu}G$ definierten Paarungen. Dann sind die durch $K\xrightarrow{\varepsilon_P}\nu^{-1}(P)\xrightarrow{\nu_P}P$ und $K\xrightarrow{\tilde\varepsilon_P}\tilde\nu^{-1}(P)\xrightarrow{\tilde\nu_P}P$ definierten Paarungen gerade die Einschränkungen $\omega_P,\tilde\omega_P$ von ω bzw. $\tilde\omega$. Aus der Voraussetzung folgt, daß $\omega_P=\tilde\omega_P$ ist. Da G durch seine Sylowgruppen erzeugt wird, folgt: $\omega=\tilde\omega$. Wir bezeichnen mit (α,κ) und

$(\tilde\alpha,\tilde\kappa)$ die durch $K \xrightarrow{\varepsilon} H \xrightarrow{\nu} G$ bzw. $K \xrightarrow{\tilde\varepsilon} \tilde H \xrightarrow{\tilde\nu} G$ definierten Parametersysteme und setzen $\zeta := \mathrm{res}^K_{Z(K)} \circ \omega$. Nach 14.2 existiert ein $\gamma \in \mathrm{Fak}(\zeta)$, so daß ${}^\gamma(\alpha,\kappa)$ zu $(\tilde\alpha,\tilde\kappa)$ äquivalent ist, und das Element $\gamma\,\mathrm{Pri}(\zeta)$ ist dabei eindeutig bestimmt. Offenbar werden die entsprechend eingeschränkten Parametersysteme $(\alpha_P,\kappa_P),(\tilde\alpha_P,\tilde\kappa_P)$ durch $K \xrightarrow{\varepsilon_P} \nu^{-1}(P) \xrightarrow{\nu_P} P$ bzw. $K \xrightarrow{\tilde\varepsilon_P} \tilde\nu^{-1}(P) \xrightarrow{\tilde\nu_P} P$ definiert. Für das entsprechend eingeschränkte Element $\gamma_P \in \mathrm{Fak}(\zeta_P)$ ist ${}^{\gamma_P}(\alpha_P,\kappa_P)$ äquivalent zu $(\tilde\alpha_P,\tilde\kappa_P)$, und $\gamma_P\,\mathrm{Pri}(\zeta_P)$ ist dabei eindeutig bestimmt. Aus der Voraussetzung folgt andrerseits, daß (α_P,κ_P) zu $(\tilde\alpha_P,\tilde\kappa_P)$ äquivalent ist, d.h. $\gamma_P \in \mathrm{Pri}(\zeta_P)$. Mit 13.6 ergibt sich daraus $\gamma \in \mathrm{Pri}(\zeta)$. Folglich ist (α,κ) äquivalent zu $(\tilde\alpha,\tilde\kappa)$, und Schreier liefert die Behauptung.

□

14.4. Satz. *Gegeben seien Gruppen G und K und ein Homomorphismus $\omega : G \to \mathrm{Out}(K)$. Ist $Z(K) = 1$, so existiert bis auf Äquivalenz genau eine Erweiterung von G mit K zur Paarung ω.*

Beweis. Wir schreiben $\omega(x) = \alpha_x\,\mathrm{Inn}(K)$ für $x \in G$. Für $x,y \in G$ ist dann $\alpha_x\alpha_y\,\mathrm{Inn}(K) = \omega(x)\omega(y) = \omega(xy) = \alpha_{xy}\,\mathrm{Inn}(K)$. Daher existiert ein Element $\kappa(x,y) \in K$ mit $\alpha_x \circ \alpha_y = \iota_{\kappa(x,y)} \circ \alpha_{xy}$. Für $x,y,z \in G$ ist also

$$\begin{aligned}
\iota_{\kappa(x,y)\kappa(xy,z)} \circ \alpha_{xyz} &= \iota_{\kappa(x,y)} \circ \iota_{\kappa(xy,z)} \circ \alpha_{(xy)z} = \\
&= \iota_{\kappa(x,y)} \circ \alpha_{xy} \circ \alpha_z = \\
&= \alpha_x \circ \alpha_y \circ \alpha_z = \\
&= \alpha_x \circ \iota_{\kappa(y,z)} \circ \alpha_{yz} = \\
&= \alpha_x \circ \iota_{\kappa(y,z)} \circ \alpha_x^{-1} \circ \alpha_x \circ \alpha_{yz} = \\
&= \iota_{\alpha_x(\kappa(y,z))} \circ \iota_{\kappa(x,yz)} \circ \alpha_{x(yz)} = \\
&= \iota_{\alpha_x(\kappa(y,z))\kappa(x,yz)} \circ \alpha_{xyz},
\end{aligned}$$

d.h. $\iota_{\kappa(x,y)\kappa(xy,z)} = \iota_{\alpha_x(\kappa(y,z))\kappa(x,yz)}$. Wegen $Z(K) = 1$ ist die Abbildung $K \to \mathrm{Inn}(K)$, $a \mapsto \iota_a$ ein Isomorphismus. Daher ist $\kappa(x,y)\kappa(xy,z) = \alpha_x(\kappa(y,z))\kappa(x,yz)$, d.h. (α,κ) ist ein Parametersystem zur Paarung ω. Wir setzen $\zeta := \mathrm{res}^K_{Z(K)} \circ \omega : G \to \mathrm{Aut}(Z(K)) = 1$. Nach 14.2 ist dann $|\overline{\mathrm{Erw}}(\omega)| = |\overline{\mathrm{Par}}(\omega)| = |\overline{\mathrm{Fak}}(\zeta)| = 1$. □

Bemerkung. Im folgenden versuchen wir, das obige Argument zu verallgemeinern, um entscheiden können, wann zu einem gegebenen Homomorphismus $\omega : G \to \mathrm{Out}(K)$ eine Erweiterung von G mit K zur Paarung ω existiert.

14.5. Satz. *Gegeben seien Gruppen G und K und ein Homomorphismus $\omega : G \to \mathrm{Out}(K)$. Wir setzen $\zeta := \mathrm{res}^K_{Z(K)} \circ \omega$ und schreiben $\omega(x) = \alpha_x\,\mathrm{Inn}(K)$ mit $\alpha_x \in \mathrm{Aut}(K)$ für $x \in G$. Dann gilt:*

(i) *Für $x,y \in G$ existiert ein Element $\chi(x,y) \in K$ mit $\alpha_x \circ \alpha_y = \iota_{\chi(x,y)} \circ \alpha_{xy}$.*
(ii) *Für $x,y,z \in G$ ist $\vartheta(x,y,z) := \alpha_x(\chi(y,z))\chi(x,yz)\chi(xy,z)^{-1}\chi(x,y)^{-1} \in Z(K)$.*
(iii) *Für $x,y,z,w \in G$ ist $\zeta_x(\vartheta(y,z,w))\vartheta(x,yz,w)\vartheta(x,y,z) = \vartheta(xy,z,w)\vartheta(x,y,zw)$.*

Beweis.

(i) Für $x,y \in G$ ist
$$\alpha_x\alpha_y\,\mathrm{Inn}(K) = \omega(x)\omega(y) = \omega(xy) = \alpha_{xy}\,\mathrm{Inn}(K),$$
d.h. $\alpha_x\alpha_y\alpha_{xy}^{-1} \in \mathrm{Inn}(K)$.

(ii) Für $x,y,z \in G$ ist
$$\begin{aligned}
\iota_{\vartheta(x,y,z)} &= \iota_{\alpha_x(\chi(y,z))} \circ \iota_{\chi(x,yz)} \circ \iota^{-1}_{\chi(xy,z)} \circ \iota^{-1}_{\chi(x,y)} = \\
&= \alpha_x \circ \iota_{\chi(y,z)} \circ \alpha_x^{-1} \circ \alpha_x \circ \alpha_{yz} \circ \alpha_{xyz}^{-1} \circ \alpha_{xyz} \circ \alpha_z^{-1} \circ \alpha_{xy}^{-1} \circ \alpha_{xy} \circ \alpha_y^{-1} \circ \alpha_x^{-1} = \\
&= \alpha_x \circ \alpha_y \circ \alpha_z \circ \alpha_{yz}^{-1} \circ \alpha_{yz} \circ \alpha_z^{-1} \circ \alpha_y^{-1} \circ \alpha_x^{-1} = \\
&= \mathrm{id}_K,
\end{aligned}$$
d.h. $\vartheta(x,y,z) \in Z(K)$.

(iii) Für $x,y,z,w \in G$ ist

$$\begin{aligned}
&\zeta_x(\vartheta(y,z,w))\vartheta(x,yz,w)\vartheta(x,y,z) \;=\\
&= \alpha_x(\alpha_y(\chi(z,w)))\alpha_x(\chi(y,zw))\alpha_x(\chi(yz,w))^{-1}\alpha_x(\chi(y,z))^{-1}\vartheta(x,yz,w)\vartheta(x,y,z) \;=\\
&= \alpha_x(\alpha_y(\chi(z,w)))\alpha_x(\chi(y,zw))\alpha_x(\chi(yz,w))^{-1}\vartheta(x,yz,w)\alpha_x(\chi(y,z))^{-1}\vartheta(x,y,z) \;=\\
&= \alpha_x(\alpha_y(\chi(z,w)))\alpha_x(\chi(y,zw))\alpha_x(\chi(yz,w))^{-1}\alpha_x(\chi(yz,w))\chi(x,yzw)\chi(xyz,w)^{-1}\\
&\quad \chi(x,yz)^{-1}\alpha_x(\chi(y,z))^{-1}\alpha_x(\chi(y,z))\chi(x,yz)\chi(xy,z)^{-1}\chi(x,y)^{-1} \;=\\
&= \alpha_x(\alpha_y(\chi(z,w)))\alpha_x(\chi(y,zw))\chi(x,yzw)\chi(xyz,w)^{-1}\chi(xy,z)^{-1}\chi(x,y)^{-1} \;=\\
&= \alpha_x(\alpha_y(\chi(z,w)))\alpha_x(\chi(y,zw))\chi(x,yzw)\chi(xy,zw)^{-1}\chi(x,y)^{-1}\chi(x,y)\chi(xy,zw)\\
&\quad \chi(xyz,w)^{-1}\chi(xy,z)^{-1}\chi(x,y)^{-1} \;=\\
&= \alpha_x(\alpha_y(\chi(z,w)))\vartheta(x,y,zw)\chi(x,y)\chi(xy,zw)\chi(xyz,w)^{-1}\chi(xy,z)^{-1}\chi(x,y)^{-1} \;=\\
&= \chi(x,y)\alpha_{xy}(\chi(z,w))\chi(x,y)^{-1}\chi(x,y)\chi(xy,zw)\chi(xyz,w)^{-1}\chi(xy,z)^{-1}\chi(x,y)^{-1}\\
&\quad \vartheta(x,y,zw) \;=\\
&= \chi(x,y)\vartheta(xy,z,w)\chi(x,y)^{-1}\vartheta(x,y,zw) \;=\\
&= \vartheta(xy,z,w)\vartheta(x,y,zw).
\end{aligned}$$

□

14.6. Definition. Gegeben seien eine Gruppe G, eine abelsche Gruppe A und ein Homomorphismus $\alpha : G \to \mathrm{Aut}(A),\ x \mapsto \alpha_x$. Eine *Obstruktion* zu α ist eine Abbildung $\vartheta : G \times G \times G \to A$ mit $\alpha_x(\vartheta(y,z,w))\vartheta(x,yz,w)\vartheta(x,y,z) = \vartheta(xy,z,w)\vartheta(x,y,zw)$ für alle $x,y,z,w \in G$. Mit $\mathrm{Obs}(\alpha)$ bezeichnen wir die Menge aller Obstruktionen zu α.

Beispiel. Gegeben seien Gruppen G und K und ein Homomorphismus $\omega : G \to \mathrm{Out}(K)$. Dann ist $\zeta := \mathrm{res}^K_{Z(K)} \circ \omega : G \to \mathrm{Aut}(Z(K))$ ein Homomorphismus, und nach Wahl von Elementen $\alpha_x \in \mathrm{Aut}(K)$ und $\chi(x,y) \in K$ für $x,y \in G$ erhält man wie in 14.5 eine Obstruktion ϑ zu ζ. Man nennt ϑ die durch ω, $(\alpha_x)_{x\in G}$ und $(\chi(x,y))_{x,y\in G}$ definierte Obstruktion.

14.7. Satz.

(i) *Für jede Gruppe G und jede abelsche Gruppe A wird* $\mathrm{Abb}(G\times G\times G, A)$ *zu einer abelschen Gruppe, wenn man $\varphi\psi$ für $\varphi,\psi \in \mathrm{Abb}(G\times G\times G, A)$ durch $(\varphi\psi)(x,y,z) := \varphi(x,y,z)\psi(x,y,z)$ für $x,y,z \in G$ definiert.*

(ii) *Für jeden Homomorphismus $\alpha : G \to \mathrm{Aut}(A), x \mapsto \alpha_x$ ist* $\mathrm{Obs}(\alpha)$ *eine Untergruppe von* $\mathrm{Abb}(G\times G\times G, A)$.

(iii) *Für jede Abbildung $\varphi : G\times G \to A$ ist die Abbildung $\partial\varphi : G\times G\times G \to A$, $(x,y,z) \mapsto \alpha_x(\varphi(y,z))\varphi(x,yz)\varphi(xy,z)^{-1}\varphi(x,y)^{-1}$ eine Obstruktion zu α.*

(iv) *Die durch (iii) definierte Abbildung $\partial = \partial_\alpha : \mathrm{Abb}(G\times G, A) \to \mathrm{Obs}(\alpha)$ ist ein Homomorphismus.*

Beweis.

(i) Klar wegen $\mathrm{Abb}(G\times G\times G, A) = \bigtimes_{x,y,z\in G} A$.

(ii) Folgt unmittelbar aus der Definition der Obstruktionen.

(iii) Für $x,y,z,w \in G$ gilt:

$$\begin{aligned}
&\alpha_x((\partial\varphi)(y,z,w))\cdot(\partial\varphi)(x,yz,w)\cdot(\partial\varphi)(x,y,z) \;=\\
&= \alpha_x(\alpha_y(\varphi(z,w)))\alpha_x(\varphi(y,zw))\alpha_x(\varphi(yz,w))^{-1}\alpha_x(\varphi(y,z))^{-1}\\
&\quad \alpha_x(\varphi(yz,w))\varphi(x,yzw)\varphi(xyz,w)^{-1}\varphi(x,yz)^{-1}\\
&\quad \alpha_x(\varphi(y,z))\varphi(x,yz)\varphi(xy,z)^{-1}\varphi(x,y)^{-1} \;=\\
&= \alpha_{xy}(\varphi(z,w))\varphi(xy,zw)\varphi(xyz,w)^{-1}\varphi(xy,z)^{-1}\alpha_x(\varphi(y,zw))\varphi(x,yzw)\\
&\quad \varphi(xy,zw)^{-1}\varphi(x,y)^{-1} \;=\\
&= (\partial\varphi)(xy,z,w)\cdot(\partial\varphi)(x,y,zw).
\end{aligned}$$

(iv) Klar.

□

Bemerkung. Man setzt $\overline{\mathrm{Obs}}(\alpha) := \mathrm{Obs}(\alpha)/\mathrm{Bild}(\partial_\alpha)$. (Dies ist eine i.a. mit $H^3(G,A)$ bezeichnete Kohomologiegruppe.)

14.8. Satz. *Gegeben seien Gruppen G und K und ein Homomorphismus $\omega : G \to \mathrm{Out}(K)$. Wir setzen $\zeta := \mathrm{res}^K_{Z(K)} \circ \omega$. Dann bilden die durch ω definierten Obstruktionen genau eine Nebenklasse nach* $\mathrm{Bild}(\partial_\zeta)$ *in* $\mathrm{Obs}(\zeta)$.

Beweis. Für $x, y \in G$ wählen wir $\alpha_x \in \mathrm{Aut}(K)$ mit $\omega(x) = \alpha_x \mathrm{Inn}(K)$ und $\chi(x,y) \in K$ mit $\alpha_x \circ \alpha_y = \iota_{\chi(x,y)} \circ \alpha_{xy}$. Dann ist die Abbildung $\vartheta : G \times G \times G \to Z(K),\ (x,y,z) \mapsto \alpha_x(\chi(y,z))\chi(x,yz)\chi(xy,z)^{-1}\chi(x,y)^{-1}$ eine durch ω definierte Obstruktion. Jede weitere durch ω definierte Obstruktion wird durch andere Wahlen von $(\alpha_x)_{x\in G}$ und $(\chi(x,y))_{x,y\in G}$ definiert. Man kann $\chi(x,y)$ durch ein Element der Form $\chi'(x,y) := \varphi(x,y)\chi(x,y)$ ersetzen, wobei $\varphi(x,y) \in Z(K)$ beliebig ist. Dann ist

$$\begin{aligned}
\vartheta'(x,y,z) &:= \alpha_x(\chi'(y,z))\chi'(x,yz)\chi'(xy,z)^{-1}\chi'(x,y)^{-1} = \\
&= \alpha_x(\varphi(y,z))\alpha_x(\chi(y,z))\varphi(x,yz)\chi(x,yz)\varphi(xy,z)^{-1}\chi(xy,z)^{-1} \\
&\quad \varphi(x,y)^{-1}\chi(x,y)^{-1} = \\
&= \zeta_x(\varphi(y,z))\varphi(x,yz)\varphi(xy,z)^{-1}\varphi(x,y)^{-1}\vartheta(x,y,z) = \\
&= (\partial\varphi)(x,y,z)\cdot\vartheta(x,y,z).
\end{aligned}$$

Analog kann man jedes α_x durch ein Element $\alpha''_x := \iota_{\psi(x)} \circ \alpha_x$ ersetzen, wobei $\psi(x) \in K$ beliebig ist. Für $x, y \in G$ ist dann

$$\begin{aligned}
\alpha''_x \circ \alpha''_y &= \iota_{\psi(x)} \circ \alpha_x \circ \iota_{\psi(y)} \circ \alpha_y = \\
&= \iota_{\psi(x)} \circ \alpha_x \circ \iota_{\psi(y)} \circ \alpha_x^{-1} \circ \alpha_x \circ \alpha_y = \\
&= \iota_{\psi(x)} \circ \iota_{\alpha_x(\psi(y))} \circ \iota_{\chi(x,y)} \circ \alpha_{xy} = \\
&= \iota_{\psi(x)\alpha_x(\psi(y))\chi(x,y)} \circ \iota^{-1}_{\psi(xy)} \circ \alpha''_{xy} = \\
&= \iota_{\psi(x)\alpha_x(\psi(y))\chi(x,y)\psi(xy)^{-1}} \circ \alpha''_{xy}.
\end{aligned}$$

Setzt man $\chi''(x,y) := \psi(x)\alpha_x(\psi(y))\chi(x,y)\psi(xy)^{-1}$ für $x, y \in G$, so gilt für $x, y, z \in G$:

$$\begin{aligned}
\vartheta''(x,y,z) &:= \alpha''_x(\chi''(y,z))\chi''(x,yz)\chi''(xy,z)^{-1}\chi''(x,y)^{-1} = \\
&= \psi(x)\alpha_x(\psi(y)\alpha_y(\psi(z))\chi(y,z)\psi(yz)^{-1})\psi(x)^{-1} \\
&\quad \psi(x)\alpha_x(\psi(yz))\chi(x,yz)\psi(xyz)^{-1} \\
&\quad \psi(xyz)\chi(xy,z)^{-1}\alpha_{xy}(\psi(z))^{-1}\psi(xy)^{-1} \\
&\quad \psi(xy)\chi(x,y)^{-1}\alpha_x(\psi(y))^{-1}\psi(x)^{-1} = \\
&= \psi(x)\alpha_x(\psi(y))\alpha_x(\alpha_y(\psi(z)))\alpha_x(\chi(y,z))\chi(x,yz)\chi(xy,z)^{-1}\alpha_{xy}(\psi(z))^{-1} \\
&\quad \chi(x,y)^{-1}\alpha_x(\psi(y))^{-1}\psi(x)^{-1} = \\
&= \psi(x)\alpha_x(\psi(y))\chi(x,y)\alpha_{xy}(\psi(z))\chi(x,y)^{-1}\vartheta(x,y,z)\chi(x,y)\alpha_{xy}(\psi(z))^{-1} \\
&\quad \chi(x,y)^{-1}\alpha_x(\psi(y))^{-1}\psi(x)^{-1} = \\
&= \vartheta(x,y,z).
\end{aligned}$$

□

Bemerkung. Jeder Homomorphismus $\omega : G \to \mathrm{Out}(K)$ definiert also genau ein Element in $\overline{\mathrm{Obs}}(\zeta)$.

14.9. Satz. *Gegeben seien Gruppen G und K und ein Homomorphismus $\omega : G \to \mathrm{Out}(K)$. Wir setzen $\zeta := \mathrm{res}^K_{Z(K)} \circ \omega$. Genau dann ist* $\mathrm{Par}(\omega) \neq \emptyset$, *wenn das durch ω definierte Element in* $\overline{\mathrm{Obs}}(\zeta)$ *trivial ist.*

Beweis.

$\Rightarrow$: Sei $\mathrm{Par}(\omega) \neq \emptyset$ und $(\alpha, \kappa) \in \mathrm{Par}(\omega)$. Dann ist $\omega(x) = \alpha_x \mathrm{Inn}(K)$, $\alpha_x \circ \alpha_y = \iota_{\kappa(x,y)} \circ \alpha_{xy}$ und $\alpha_x(\kappa(y,z))\kappa(x,yz)\kappa(xy,z)^{-1}\kappa(x,y)^{-1} = 1$. Daher ist die durch ω, $(\alpha_x)_{x\in G}$, $(\kappa(x,y))_{x,y\in G}$ definierte Obstruktion trivial.

$\Leftarrow$: Wir wählen Elemente $\alpha_x \in \mathrm{Aut}(K)$ und $\chi(x,y) \in K$ mit $\omega(x) = \alpha_x \mathrm{Inn}(K)$ und $\alpha_x \circ \alpha_y = \iota_{\chi(x,y)} \circ \alpha_{xy}$ für $x, y \in G$. Dann ist die Abbildung $\vartheta : G \times G \times G \to Z(K)$, $(x,y,z) \mapsto \alpha_x(\chi(y,z))\chi(x,yz)\chi(xy,z)^{-1}\chi(x,y)^{-1}$ eine durch ω definierte Obstruktion. Ist $\vartheta\,\mathrm{Bild}(\partial_\zeta) = 1$, so ist $\vartheta \in \mathrm{Bild}(\partial_\zeta)$, d.h. $\vartheta = \partial_\zeta\varphi$ für eine Abbildung $\varphi : G \times G \to Z(K)$. Wir setzen $\kappa(x,y) := \varphi(x,y)^{-1}\chi(x,y)$ für $x, y \in G$ und zeigen, daß dann (α, κ) ein Parametersystem zur Paarung ω ist. Für $x, y, z \in G$ ist nämlich

$$\alpha_x \circ \alpha_y \;=\; \iota_{\kappa(x,y)} \circ \alpha_{xy}$$

und

$$\begin{aligned}
\kappa(x,y)\kappa(xy,z) &= \varphi(x,y)^{-1}\chi(x,y)\varphi(xy,z)^{-1}\chi(xy,z) \;= \\
&= \varphi(x,y)^{-1}\varphi(xy,z)^{-1}\chi(x,y)\chi(xy,z) \;= \\
&= \varphi(x,yz)^{-1}\alpha_x(\varphi(y,z))^{-1}\underbrace{(\partial_\zeta\varphi)}_{=\vartheta}(x,y,z)\chi(x,y)\chi(xy,z) \;= \\
&= \varphi(x,yz)^{-1}\alpha_x(\varphi(y,z))^{-1}\alpha_x(\chi(y,z))\chi(x,yz) \;= \\
&= \alpha_x(\kappa(y,z))\kappa(x,yz).
\end{aligned}$$

□

KAPITEL 15

Freie Gruppen

15.1. Bemerkung.

(i) Gegeben sei eine nichtleere Menge X. Wir setzen $X^+ := \{(x,1) : x \in X\},\ X^- := \{(x,-1) : x \in X\}$. Dann bezeichnen wir mit W das freie Monoid über dem Alphabet $X^+ \cup X^-$ (vgl. Beispiel 1.3). Jedes Element $w \in W$ läßt sich also in der Form $w = a_1 \dots a_n$ mit eindeutig bestimmten $n \in \mathbb{N}_0,\ a_1, \dots, a_n \in X^+ \cup X^-$ schreiben.
Unter einer *elementaren Umformung* verstehen wir das Einfügen oder Weglassen von $(x,1)(x,-1)$ oder $(x,-1)(x,1)$ für ein $x \in X$. Wir nennen zwei Elemente $v, w \in W$ *äquivalent* und schreiben $v \sim w$, falls v aus w durch endlich viele elementare Umformungen entsteht. Dann ist $\sim$ eine Äquivalenzrelation auf W. Wir bezeichnen mit $[w]$ die Äquivalenzklasse von $w \in W$ und setzen $F := \{[w] : w \in W\}$. Für Worte $v, v', w, w' \in W$ mit $v \sim v',\ w \sim w'$ ist offenbar $vw \sim v'w'$. Daher kann man durch $[v][w] := [vw]$ für $v, w \in W$ eine Verknüpfung auf F definieren. Auf diese Weise wird F zu einem Monoid mit neutralem Element $[1]$. Ferner gilt für $n \in \mathbb{N},\ x_1, \dots, x_n \in X,\ \delta_1, \dots, \delta_n \in \{\pm 1\}$:

$$\begin{aligned}[(x_1,\delta_1)\dots(x_n,\delta_n)][(x_n,-\delta_n)\dots(x_1,-\delta_1)] \ &= \\ = \ [(x_1,\delta_1)\dots(x_n,\delta_n)(x_n,-\delta_n)\dots(x_1,-\delta_1)] \ &= \ [1]\end{aligned}$$

Daher ist F eine Gruppe mit $F = \langle [(x,1)] : x \in X \rangle$. Man nennt F die *freie Gruppe* über dem Alphabet X. Zusätzlich definiert man $\{1\}$ als freie Gruppe über dem leeren Alphabet $\emptyset$.

(ii) Ein Element $w = (x_1,\delta_1)\dots(x_n,\delta_n) \in W$ nennt man *reduziert*, falls für $i = 2, \dots, n$ gilt: $x_{i-1} = x_i \ \Rightarrow\ \delta_{i-1} = \delta_i$. Für ein beliebiges Element $w = (x_1,\delta_1)\dots(x_n,\delta_n) \in W$ definieren wir $w_0 := 1$, und ist w_i für ein $i \in \{0, \dots, n-1\}$ bereis definiert, so setzen wir

$$w_{i+1} := \begin{cases} w_{i-1} & \text{falls } (x_{i+1}, -\delta_{i+1}) \text{ der letzte Buchstabe von } w_i \text{ ist,} \\ w_i(x_{i+1},\delta_{i+1}) & \text{sonst.} \end{cases}$$

Dann ist $\overline{w} := w_n$ ein reduziertes Wort mit $w \sim \overline{w}$. Sei $r \in \{0, \dots, n\},\ x \in X,\ \delta \in \{\pm 1\}$ und $v := (x_1,\delta_1)\dots(x_r,\delta_r)(x,\delta)(x,-\delta)(x_{r+1},\delta_{r+1})\dots(x_n,\delta_n)$. Dann ist $v_0 = w_0,\ \dots,\ v_r = w_r$. Ist $(x,-\delta)$ der letzte Buchstabe von $v_r = w_r$, so ist $v_{r+1} = w_{r-1},\ v_{r+2} = v_{r-1}(x,-\delta) = w_r,\ \dots,\ v_{n+2} = w_n$. Ist $(x,-\delta)$ nicht der letzte Buchstabe von $v_r = w_r$, so ist $v_{r+1} = v_r(x,\delta),\ v_{r+2} = v_r = w_r,\ \dots,\ v_{n+2} = w_n$. In jedem Fall ist $\overline{v} = \overline{w}$. Für beliebige Elemente $y, z \in W$ mit $y \sim z$ ist also $\overline{y} = \overline{z}$. Dies zeigt, daß jede Äquivalenzklasse genau ein reduziertes Wort enthält. Insbesondere sind die Elemente $[(x,1)]$ mit $x \in X$ paarweise verschieden. Wir können also jedes Element $x \in X$ mit $[(x,1)]$ identifizieren. Dann ist $F = \langle X \rangle$, und jedes Element in F läßt sich in der Form $x_1^{k_1} \dots x_t^{k_t}$ mit $x_1, \dots, x_t \in X,\ k_1, \dots, k_t \in \mathbb{Z}$ und $x_1 \neq x_2 \neq \dots \neq x_t$ schreiben; dabei sind $x_1, \dots, x_t$ und $k_1, \dots, k_t$ eindeutig.

Beispiel. Ist $X = \{x\}$ einelementig, so ist $F = \{x^k : k \in \mathbb{Z}\}$ eine unendliche zyklische Gruppe, also zu $\mathbb{Z}$ isomorph. Im Fall $|X| \geq 2$ ist F nichtabelsch wegen $xx' \neq x'x$ für verschiedene $x, x' \in X$.

15.2. Satz (Universelle Eigenschaft freier Gruppen)**.** *Gegeben seien eine Menge X, die freie Gruppe F über X und eine beliebige Gruppe G. Dann kann man jede Abbildung $f : X \to G$ zu genau einem Homomorphismus $g : F \to G$ fortsetzen.*

Beweis. Sei W die freie Halbgruppe über $X^+ \cup X^-$ wie oben. Wir definieren eine Abbildung $\tilde{f} : W \to G$ durch $\tilde{f}((x_1,\delta_1)\dots(x_n,\delta_n)) := f(x_1)^{\delta_1} \dots f(x_n)^{\delta_n}$ für $x_1, \dots, x_n \in X,\ \delta_1, \dots, \delta_n \in \{\pm 1\}$. Für $v, w \in W$

gilt dann $\tilde{f}(vw) = \tilde{f}(v)\tilde{f}(w)$ und $\tilde{f}(1) = 1$, d.h. $\tilde{f}$ ist ein Homomorphismus von Monoiden. Für $v, w \in W$ gilt ferner: $v \sim w \;\Rightarrow\; \tilde{f}(v) = \tilde{f}(w)$. Daher kann man eine Abbildung $g : F \to G$ definieren durch $g([v]) := \tilde{f}(v)$ für $v \in W$. Offenbar ist g ein Homomorphismus von Gruppen mit $g(x) = \tilde{f}(x, 1) = f(x)$ für $x \in X$. Wegen $F = \langle X \rangle$ ist g die einzige Fortsetzung von f zu einem Homomorphismus $F \to G$. □

Bemerkung. Aus dem Satz folgt insbesondere, daß für gleichmächtige Mengen X, Y (d.h. es existiert eine Bijektion $f : X \to Y$) die freien Gruppen über X und Y isomorph sind.

15.3. Satz. *Gegeben sei ein Erzeugendensystem X einer Gruppe G mit der Eigenschaft, daß sich jede Abbildung f von X in eine Gruppe H zu einem Homomorphismus $g : G \to H$ fortsetzen läßt. Dann ist G zur freien Gruppe F über X isomorph.*

Beweis. Nach Voraussetzung existiert ein Homomorphismus $g : G \to F$ mit $g(x) = x$ für $x \in X$. Nach 15.2 existiert ein Homomorphismus $h : F \to G$ mit $h(x) = x$ für $x \in X$. Wegen $(g \circ h)(x) = x$ für $x \in X$ und $F = \langle X \rangle$ ist $g \circ h = \mathrm{id}_F$. Analog ist $h \circ g = \mathrm{id}_G$. □

15.4. Satz. *Für endliche Mengen X, Y mit $|X| \neq |Y|$ sind die freien Gruppen über X und Y nicht isomorph.*

Beweis. Sei $|X| = n$. Dann existieren genau 2^n Abbildungen $X \to \mathbb{Z}/2\mathbb{Z}$. Nach 15.2 existieren also genau 2^n Homomorphismen von der freien Gruppe F über X in $\mathbb{Z}/2\mathbb{Z}$. □

Bemerkung. Der Satz gilt auch für unendliche Mengen. Sein Beweis erfordert etwas mehr Mengenlehre. Man nennt $|X|$ auch den *Rang* der freien Gruppe F über X.

15.5. Satz. *Jede Gruppe G ist zu einer Faktorgruppe einer freien Gruppe isomorph. Läßt sich G durch m Elemente erzeugen, so ist G zu einer Faktorgruppe einer freien Gruppe des Ranges m isomorph.*

Beweis. Sei X ein Erzeugendensystem von G (notfalls $X = G$). Sei F die freie Gruppe über X. Nach 15.2 läßt sich die Abbildung $X \to G,\ x \mapsto x$ zu einem Homomorphismus $f : F \to G$ fortsetzen. Wegen $G = \langle X \rangle$ ist f surjektiv, also $G \cong F/\operatorname{Ker}(f)$. □

Bemerkung.

(i) Sei X Erzeugendensystem einer Gruppe G, F die freie Gruppe über X und $f : F \to G$ der Homomorphismus mit $f(x) = x$ für $x \in X$. Die Elemente in $\operatorname{Ker}(f)$ nennt man *Relatoren* für G und X. Ein Element $x_1^{\delta_1} \dots x_n^{\delta_n} \in F$ mit $x_1, \dots, x_n \in X,\ \delta_1, \dots, \delta_n \in \{\pm 1\}$ ist also genau dann ein Relator für G und X, wenn das Bild von $x_1^{\delta_1} \dots x_n^{\delta_n}$ in G gleich 1 ist, d.h. wenn $x_1^{\delta_1} \dots x_n^{\delta_n} = 1$ in G ist. (Unsere Schreibweise unterscheidet das Produkt $x_1^{\delta_1} \dots x_n^{\delta_n}$ in F nicht von dem Produkt $x_1^{\delta_1} \dots x_n^{\delta_n}$ in G; dies ist zwar schlampig, aber üblich und bequem.) Für jeden Relator $x_1^{\delta_1} \dots x_n^{\delta_n} \in F$ nennt man die Gleichung $x_1^{\delta_1} \dots x_n^{\delta_n} = 1$ eine *Relation* für G und X. Eine Menge R von Relatoren für G und X nennt man ein *System definierender Relatoren* für G und X, falls $\operatorname{Ker}(f)$ der normale Abschluß von $\langle R \rangle$ in F ist. In diesem Fall nennt man auch die Gleichungen $r = 1$ $(r \in R)$ ein *System definierender Relationen* für G und X.

(ii) Sei umgekehrt X eine Menge, F die freie Gruppe über X, R eine Teilmenge von F und N der normale Abschluß von $\langle R \rangle$ in F. Dann nennt man die Faktorgruppe $\langle X | R \rangle := F/N$ die durch X mit den Relatoren R erzeugte Gruppe.

Beispiel. $G := \langle a, b | a^3, b^2, baba \rangle$.
Man schreibt auch $G := \langle a, b | a^3 = b^2 = baba = 1 \rangle$ und unterscheidet dabei nicht zwischen dem Rechnen in der von a und b erzeugten freien Gruppe F und dem Rechnen in der Faktorgruppe G von F. Wegen $ba = a^{-1}b^{-1} = a^{-1}b$ läßt sich jedes Element in G auf die Form $a^m b^n$ mit $m, n \in \mathbb{Z}$ bringen. Wegen $a^3 = 1 = b^2$ kann man o.B.d.A. $m \in \{0, 1, 2\},\ n \in \{0, 1\}$ annehmen. Daher ist $|G| \leq 6$. I.a. ist es schwierig, die Struktur einer durch Erzeugende und Relationen definierte Gruppe genau zu bestimmen. Es gibt z.B. kein allgemeines Verfahren, um zu entscheiden, ob eine solche Gruppe trivial ist oder nicht. In unserem Fall ist die Sache einfach. In Sym(3) erfüllen die Elemente $\alpha = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{smallmatrix}\right),\ \beta = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{smallmatrix}\right)$ die Relationen $\alpha^3 = \beta^2 = \alpha\beta\alpha\beta = 1$, wie man leicht nachrechnet. Außerdem ist $\mathrm{Sym}(3) = \langle \alpha, \beta \rangle$. Der folgende Satz wird

zeigen, daß es dann einen Epimorphismus $f : G \to \mathrm{Sym}(3)$ gibt. Folglich ist $6 = |\mathrm{Sym}(3)| \leq |G| \leq 6$, also $|G| = 6$, und f ist injektiv, d.h. $G \cong \mathrm{Sym}(3)$. Die Gruppe $\mathrm{Sym}(3)$ wird also von den Elementen α, β mit den Relationen $\alpha^3 = \beta^2 = \alpha\beta\alpha\beta = 1$ erzeugt.

15.6. Satz. *Gegeben seien Gruppen G und H mit Erzeugendensystemen $X = \{g_\lambda : \lambda \in \Lambda\}$ bzw. $Y = \{h_\lambda : \lambda \in \Lambda\}$. Für jede Relation $g_{\lambda_1}^{\varepsilon_1} \dots g_{\lambda_n}^{\varepsilon_n} = 1$ für G und X sei $h_{\lambda_1}^{\varepsilon_1} \dots h_{\lambda_n}^{\varepsilon_n} = 1$ eine Relation für H und Y. Dann existiert ein Epimorphismus $f : G \to H$ mit $f(g_\lambda) = h_\lambda$ für $\lambda \in \Lambda$.*

Beweis. Sei F die freie Gruppe über Λ. Dann existieren Epimorphismen $\varphi : F \to G,\ \psi : F \to H$ mit $\varphi(\lambda) = g_\lambda,\ \psi(\lambda) = h_\lambda$ für $\lambda \in \Lambda$. Die Voraussetzung bedeutet $\mathrm{Ker}(\varphi) \subseteq \mathrm{Ker}(\psi)$. Daher ist die Abbildung $F/\mathrm{Ker}(\varphi) \to F/\mathrm{Ker}(\psi),\ x\,\mathrm{Ker}(\varphi) \mapsto x\,\mathrm{Ker}(\psi)$ wohldefiniert und ein Epimorphismus. Setzt man diesen mit den Isomorphismen $F/\mathrm{Ker}(\varphi) \to G,\ x\,\mathrm{Ker}(\varphi) \mapsto \varphi(x)$ und $F/\mathrm{Ker}(\psi) \to H,\ x\,\mathrm{Ker}(\psi) \mapsto \psi(x)$ zusammen, so erhält man die Behauptung. □

KAPITEL 16

Endliche p-Gruppen

Sei p Primzahl.

16.1. Bemerkung. Nach Aufgabe 4 von Blatt 5 ist $G/Z(G)$ für eine nichtabelsche Gruppe G niemals zyklisch. Für eine nichtabelsche endliche p-Gruppe G ist also stets $p^2 \mid |G/Z(G)|$; insbesondere sind Gruppen der Ordnung p^2 stets abelsch nach 10.1.

Satz. *Ist N ein Normalteiler einer Gruppe G mit $|G/N| = p^2$, so ist $G' \subseteq N$.*

Beweis. $|G/N| = p^2 \Rightarrow G/N$ abelsch $\Rightarrow G' \subseteq N$. □

Beispiel. In einer nichtabelschen Gruppe der Ordnung p^3 ist $Z(G) \neq 1$ nach 10.1. Wegen $p^2 \mid |G/Z(G)|$ ist also $|Z(G)| = p$. Folglich ist $G' \subseteq Z(G)$. Wegen $G' \neq 1$ ist $G' = Z(G)$.

16.2. Satz.

(i) *Ist p ungerade und $n \in \mathbb{N}$, so ist $(\mathbb{Z}/p^n\mathbb{Z})^\times$ zyklisch der Ordnung $p^{n-1}(p-1)$. Die p-Sylowgruppe von $(\mathbb{Z}/p^n\mathbb{Z})^\times$ wird von $1+p+p^n\mathbb{Z}$ erzeugt.*

(ii) *Für $n \in \mathbb{N}$, $n \geq 2$ ist $(\mathbb{Z}/2^n\mathbb{Z})^\times = \langle -1+2^n\mathbb{Z}\rangle \oplus \langle 5+2^n\mathbb{Z}\rangle$ mit $|\langle -1+2^n\mathbb{Z}\rangle| = 2$ und $|\langle 5+2^n\mathbb{Z}\rangle| = 2^{n-2}$; insbesondere ist $|(\mathbb{Z}/2^n\mathbb{Z})^\times| = 2^{n-1}$.*

Beweis. Algebra. □

Bemerkung. Nach Aufgabe 3 von Blatt 3 ist für $k \in \mathbb{Z}$ die Abbildung $(\mathbb{Z}/k\mathbb{Z})^\times \to \mathrm{Aut}(\mathbb{Z}/k\mathbb{Z})$, $l+k\mathbb{Z} \mapsto (\mathbb{Z}/k\mathbb{Z} \to \mathbb{Z}/k\mathbb{Z},\ z \mapsto lz)$ ein Isomorphismus.

16.3. Satz. *Für $n \in \mathbb{N}$ ist jede nichtabelsche Gruppe H der Ordnung p^{n+1}, die eine zyklische Untergruppe K der Ordnung p^n enthält, zu einer der folgenden Gruppen isomorph:*

(I) $\langle a,b \mid a^{p^n} = b^p = 1,\ bab^{-1} = a^{1+p^{n-1}}\rangle$, *$p$ ungerade, $n \geq 2$.*
(II) $\langle a,b \mid a^{2^n} = b^2 = 1,\ bab^{-1} = a^{-1}\rangle$, $p = 2,\ n \geq 2$.
(III) $\langle a,b \mid a^{2^n} = 1,\ b^2 = a^{2^{n-1}},\ bab^{-1} = a^{-1}\rangle$, $p = 2,\ n \geq 2$.
(IV) $\langle a,b \mid a^{2^n} = b^2 = 1,\ bab^{-1} = a^{1+2^{n-1}}\rangle$, $p = 2,\ n \geq 3$.
(V) $\langle a,b \mid a^{2^n} = b^2 = 1,\ bab^{-1} = a^{-1+2^{n-1}}\rangle$, $p = 2,\ n \geq 3$.

Beweis. Wir betrachten die Gruppenerweiterung $K = \langle k\rangle \longrightarrow H \longrightarrow G := H/K \cong \mathbb{Z}/p\mathbb{Z}$ und bezeichnen mit α das entsprechende Automorphismensystem. Wäre $\alpha_x = \mathrm{id}_K$ für $x \in G$, so wäre $K \subseteq Z(H)$, also $|H/Z(H)| \mid p$ und damit H abelsch. Also ist $\alpha_x \neq \mathrm{id}_K$ für ein $x \in G$.
Sei zunächst $p \neq 2$. Da $\mathrm{Aut}(K)$ zyklisch der Ordnung $p^{n-1}(p-1)$ ist, ist $\mathrm{Bild}(\alpha)$ die einzige Untergruppe der Ordnung p von $\mathrm{Aut}(K)$. Diese wird von der Abbildung

$$\beta : K \to K,\ a \mapsto a^{(1+p)^{p^{n-2}}} = a^{1+p^{n-1}}$$

erzeugt. Daher genügt es zu zeigen, daß $\overline{\mathrm{Fak}}(\alpha) = 1$ ist. Für $a \in K$ gilt:

$$\beta(a) = a \ \Leftrightarrow\ a^{1+p^{n-1}} = a \ \Leftrightarrow\ a^{p^{n-1}} = 1$$

und

$$\begin{aligned} a\beta(a)\beta^2(a)\dots\beta^{p-1}(a) &= aa^{1+p^{n-1}}a^{(1+p^{n-1})^2}\dots a^{(1+p^{n-1})^{p-1}} = \\ &= a^{1+(1+p^{n-1})+(1+2p^{n-1})+\dots+(1+(p-1)p^{n-1})} = \\ &= a^{p+\frac{p(p-1)}{2}p^{n-1}} = a^p. \end{aligned}$$

Mit den Bezeichnungen aus Aufgabe 2 von Blatt 8 ist also $K_\alpha = \langle k^p \rangle = N_\alpha(K)$, also $\overline{\mathrm{Fak}}(\alpha) \cong K_\alpha/N_\alpha(K) = 1$.
Sei also $p = 2$. In diesem Fall hat K nach 16.2 genau drei Automorphismen $\beta_1, \beta_2, \beta_3$ der Ordnung 2. Diese werden gegeben durch $\beta_1(a) = a^{-1}$, $\beta_2(a) = a^{1+2^{n-1}}$, $\beta_3(a) = a^{-1+2^{n-1}}$ für $a \in K$. Der Fall $\mathrm{Bild}(\alpha) = \langle \beta_1 \rangle$ folgt aus Aufgabe 3 von Blatt 8. Im Fall $n = 2$ ist $\beta_2 = \beta_1$ und $\beta_3 = 1$. Sei also $n \geq 3$. Im Fall $\mathrm{Bild}(\alpha) = \langle \beta_2 \rangle$ gilt für $a \in K$:

$$\beta_2(a) = a \;\Leftrightarrow\; a^{1+2^{n-1}} = a \;\Leftrightarrow\; a^{2^{n-1}} = 1$$

und

$$N_\alpha(a) \;=\; a\beta_2(a) \;=\; a^{2+2^{n-1}}.$$

Also ist $K_\alpha = \langle k^2 \rangle = N_\alpha(K)$ und $\overline{\mathrm{Fak}}(\alpha) \cong K_\alpha/N_\alpha(K) = 1$. Im Fall $\mathrm{Bild}(\alpha) = \langle \beta_3 \rangle$ gilt für $a \in K$:

$$\beta_3(a) = a \;\Leftrightarrow\; a^{2^{n-1}} = a^2 \;\Leftrightarrow\; a^2 = 1 \qquad \text{(wegen } n \geq 3\text{)}$$

und

$$N_\alpha(a) \;=\; aa^{-1+2^{n-1}} \;=\; a^{2^{n-1}}.$$

Also ist wieder $K_\alpha = \langle k^{2^{n-1}} \rangle = N_\alpha(K)$ und $\overline{\mathrm{Fak}}(\alpha) \cong K_\alpha/N_\alpha(K) = 1$. □

Bemerkung.

(i) Gruppen vom Typ (II) sind *Diedergruppen*, Gruppen vom Typ (III) *Quaternionengruppen* (vgl. Aufgabe 3 von Blatt 8). Gruppen vom Typ (V) nennt man *Semidiedergruppen*.
(ii) Man kann leicht zeigen, daß die Gruppen (I)–(V) paarweise nichtisomorph sind (vgl. Aufgabe 1 von Blatt 9).
(iii) Die abelschen Gruppen der Ordnung p^{n+1}, die eine zyklische Untergruppe der Ordnung p^n enthalten, sind nach Satz 5.6 zu $\mathbb{Z}/p^{n+1}\mathbb{Z}$ oder zu $\mathbb{Z}/p^n\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ isomorph.

16.4. Satz. *Gegeben sei eine endliche nichtzyklische p-Gruppe G, in der jeder abelsche Normalteiler zyklisch ist. Dann ist $p = 2$, und G ist eine Diedergruppe, eine Semidiedergruppe oder eine Quaternionengruppe.*

Beweis. Wir wählen einen maximalen abelschen Normalteiler A von G. Dann ist A zyklisch, also $A \neq G$. Nach Aufgabe 4 von Blatt 6 ist $A = C_G(A)$. Daher ist $G/A = G/C_G(A)$ isomorph zu einer Untergruppe von $\mathrm{Aut}(A)$. Im Fall $|A| = p$ wäre $|\mathrm{Aut}(A)| = p - 1$, also $G/A = 1$. Daher ist $|A| \geq p^2$. Wir bezeichnen mit B die einzige Untergruppe der Ordnung p^2 von A. Dann ist $B \trianglelefteq G$, $A \subseteq C_G(B) =: C \trianglelefteq G$, und G/C ist isomorph zu einer Untergruppe von $\mathrm{Aut}(B)$. Nach 16.2 ist $|\mathrm{Aut}(B)| = p(p-1)$, also $|G/C| \leq p$. *Annahme:* $A \neq C$. Da G nilpotent ist, existiert ein $D \trianglelefteq G$ mit $A \subseteq D \subseteq C$ und $|D : A| = p$. Nach Wahl von A ist D nichtabelsch mit einem zyklischen Normalteiler A vom Index p. Daher ist D eine der Gruppen in 16.3. Offenbar ist $B \subseteq Z(D)$, also $|Z(D)| \geq p^2$. Man rechnet leicht nach, daß dies die Typen (II), (III), (V) ausschließt. In Gruppen vom Typ (I) oder (IV) erzeugen aber die Elemente der Ordnung p eine nichtzyklische charakteristische Untergruppe der Ordnung p^2, wie man leicht nachrechnet (vgl. Aufgabe 1 von Blatt 9). Widerspruch.
Also ist $A = C$ und damit $|G/A| \leq p$. Daher ist G eine der Gruppen in 16.3. Wie oben kann man die Fälle (I) und (IV) ausschließen. □

16.5. Satz. *Für eine endliche p-Gruppe G sind äquivalent:*

(1) *Jede abelsche Untergruppe von G ist zyklisch.*
(2) *G enthält genau eine Untergruppe der Ordnung p.*
(3) *G ist zyklisch oder eine Quaternionengruppe.*

Beweis.

(3)⇒(2): Nachrechnen!
(2)⇒(1): Hauptsatz über endliche abelsche Gruppen.
(1)⇒(3): Ist (1) erfüllt, so ist G nach 16.4 zyklisch, eine Diedergruppe, eine Quaternionengruppe oder eine Semidiedergruppe. Man zeigt leicht, daß Dieder- und Semidiedergruppen nichtzyklische abelsche Untergruppen enthalten.

□

16.6. Satz. *Jede nichtabelsche Gruppe G der Ordnung p^3 ist zu einer der folgenden Gruppen isomorph:*

(I) $\langle a, b \mid a^4 = b^2 = 1,\ bab^{-1} = a^{-1}\rangle$, $p = 2$.
(II) $\langle a, b \mid a^4 = 1,\ b^2 = a^2,\ bab^{-1} = a^{-1}\rangle$, $p = 2$.
(III) $\langle a, b \mid a^{p^2} = 1 = b^p,\ bab^{-1} = a^{1+p}\rangle$, $p \neq 2$.
(IV) $\langle a, b, c \mid a^p = b^p = c^p = 1,\ c = aba^{-1}b^{-1},\ ac = ca,\ bc = cb\rangle$, $p \neq 2$.

Beweis. Enthält G ein Element der Ordnung p^2, so folgt die Behauptung aus 16.3. Daher können wir $g^p = 1$ für alle $g \in G$ annehmen. Dann ist $p \neq 2$; denn sonst ist $gh = gh(hg)^2 = ghhghg = hg$ für alle $g, h \in G$. Nach 16.1 ist $|Z(G)| = p$, etwa $Z(G) = \langle c\rangle$. Für $b \in G \setminus Z(G)$ ist $\langle b, c\rangle$ abelsch der Ordnung p^2; insbesondere ist $\langle b, c\rangle \trianglelefteq G$. Wir wählen $a \in G \setminus \langle b, c\rangle$. Dann ist $G = \langle a, b, c\rangle$. Nach 16.1 ist $G/Z(G)$ abelsch; insbesondere ist $aba^{-1}Z(G) = bZ(G)$, also $aba^{-1} = bc^i$ für ein $i \in \mathbb{N}$; dabei ist $p \nmid i$, da sonst $b \in Z(G)$. Wir ersetzen also c durch c^i und erhalten die angegebenen Relationen. □

Bemerkung. Man kann sich leicht überlegen, daß die angegebenen Gruppen existieren und paarweise nichtisomorph sind (vgl. Aufgabe 2 von Blatt 9).

16.7. Definition. Eine endliche p-Gruppe G mit $\Phi(G) = G' = Z(G)$ und $|G'| = p$ nennt man *extraspeziell*.

Beispiel. Nichtabelsche Gruppen der Ordnung p^3 sind extraspeziell nach 16.1.

Bemerkung. Jede extraspezielle p-Gruppe ist nilpotent der Klasse 2 mit $\exp(G) \leq p^2$. Für $g, h, k \in G$ gilt nach 7.1: $[gh, k] = [g, k][h, k]$, $[g, hk] = [g, h][g, k]$. Für $z \in Z(G)$ ist ferner $[gz, h] = [g, h] = [g, hz]$. Wegen $Z(G) \cong \mathbb{Z}/p\mathbb{Z}$ ist also die Abbildung

$$\beta : G/\Phi(G) \times G/\Phi(G) \to Z(G) \cong \mathbb{Z}/p\mathbb{Z},\ (g\Phi(G), h\Phi(G)) \mapsto [g, h]$$

eine Bilinearform auf dem $\mathbb{Z}/p\mathbb{Z}$-Vektorraum $G/\Phi(G)$. Wegen $[g, g] = 1$ für $g \in G$ ist diese Bilinearform symplektisch, d.h. $\beta(x, x) = 0$ für alle x. Ist $g \in G$ mit $[g, h] = 1$ für alle $h \in G$, so ist $g \in Z(G)$. Daher ist β nichtausgeartet. Aus der Linearen Algebra sollte bekannt sein, daß $G/\Phi(G)$ eine Basis $x_1, y_1, \ldots, x_n, y_n$ mit $\beta(x_i, y_i) = 1$ für $i = 1, \ldots, n$, $\beta(x_i, y_j) = 0$ für $i \neq j$ und $\beta(x_i, x_j) = 0 = \beta(y_i, y_j)$ für $i, j = 1, \ldots, n$ besitzt. Wir schreiben $x_i = g_i\Phi(G)$, $y_i = h_i\Phi(G)$, $z = [g_i, h_i]$. Dann ist $G = \langle g_1, h_1, \ldots, g_n, h_n, z\rangle$, $[g_i, h_i] = z$ für $i = 1, \ldots, n$, $[g_i, h_j] = 1$ für $i \neq j$ und $[g_i, g_j] = 1 = [h_i, h_j]$ für $i, j = 1, \ldots, n$. Für $i = 1, \ldots, n$ ist also $\langle g_i, h_i, z\rangle$ ein Normalteiler der Ordnung p^3 von G. Ferner ist $|G| = p^{2n+1}$.
Sei zunächst $p \neq 2$. Hat G den Exponenten p, so auch $\langle g_i, h_i, z\rangle$ für $i = 1, \ldots, n$. Es ist also $g_i^p = h_i^p = z^p = 1$ für $i = 1, \ldots, n$. Damit ist in diesem Fall der Isomorphie-Typ von G eindeutig festgelegt.
Hat G den Exponenten p^2, so hat mindestens eine der Gruppen $\langle g_i, h_i, z\rangle$ den Exponenten p^2, o.B.d.A. $\langle g_1, h_1, z\rangle$. Wir können annehmen: $g_1^p = z$, $h_1^p = z^p = 1$. Hat auch $\langle g_2, h_2, z\rangle$ den Exponenten p^2, so können wir auch $g_2^p = z$, $h_2^p = z^p = 1$ annehmen. Wir setzen $\tilde{h}_1 := h_1h_2$ und $\tilde{g}_2 := g_1^{-1}g_2$. Dann ist $\langle g_1, h_1, g_2, h_2, z\rangle = \langle g_1, \tilde{h}_1, \tilde{g}_2, h_2, z\rangle$ und $\tilde{g}_2^p = g_1^{-p}g_2^p = z^{-1}z = 1$. Es folgt leicht, daß $\langle \tilde{g}_2, h_2, z\rangle$ den Exponenten p hat. Wegen $[\langle g_1, \tilde{h}_1, z\rangle, \langle \tilde{g}_2, h_2, z\rangle] = 1$ hat also $\langle g_1, \tilde{h}_1, z\rangle$ den Exponenten p^2. Ersetzt man also $\langle g_1, h_1, z\rangle$ durch $\langle g_1, \tilde{h}_1, z\rangle$ und $\langle g_2, h_2, z\rangle$ durch $\langle \tilde{g}_2, h_2, z\rangle$, so kann man annehmen, daß $\langle g_2, h_2, z\rangle$ den Exponenten p hat. Analog kann man annehmen, daß $\langle g_i, h_i, z\rangle$ für $i = 2, \ldots, n$ den Exponenten p hat. Damit ist der Isomorphie-Typ eindeutig festgelegt.
Für $p \neq 2$ und $n \in \mathbb{N}$ existieren also bis auf Isomorphie höchstens zwei extraspezielle p-Gruppen der Ordnung p^{2n+1}. Man kann sich leicht überlegen, daß diese auch tatsächlich existieren (vgl. Aufgabe 3 von Blatt 9).
Sei jetzt $p = 2$. Für $i = 1, \ldots, n$ ist dann $\langle g_i, h_i, z\rangle$ eine Diedergruppe oder eine Quaternionengruppe der Ordnung 8. Wir betrachten zunächst den Fall, daß $\langle g_1, h_1, z\rangle$ und $\langle g_2, h_2, z\rangle$ Quaternionengruppen sind. Dann ist $g_1^2 = g_2^2 = h_1^2 = h_2^2 = z$, $h_1g_1h_1^{-1} = g_1^{-1}$, $h_2g_2h_2^{-1} = g_2^{-1}$. Wir setzen $\tilde{h}_1 := h_1g_2$ und $\tilde{h}_2 := h_2g_1$. Dann ist $\langle g_1, h_1, g_2, h_2, z\rangle = \langle g_1, \tilde{h}_1, g_2, \tilde{h}_2, z\rangle$, $\tilde{h}_1^2 = h_1^2g_2^2 = z^2 = 1$, $\tilde{h}_2^2 = h_2^2g_1^2 = z^2 = 1$ und

$$\begin{aligned}[\tilde{h}_1, \tilde{h}_2] &= h_1g_2h_2g_1g_2^{-1}h_1^{-1}g_1^{-1}h_2^{-1} = h_1g_1g_2h_2g_2^{-1}h_2^{-1}h_1^{-1}g_1^{-1} = \\ &= h_1g_1zh_1^{-1}g_1^{-1} = zh_1g_1h_1^{-1}g_1^{-1} = z^2 = 1,\end{aligned}$$

also $[\langle g_1, \tilde{h}_1, z\rangle, \langle g_2, \tilde{h}_2, z\rangle] = 1$. Ferner sind $\langle g_1, \tilde{h}_1, z\rangle$ und $\langle g_2, \tilde{h}_2, z\rangle$ Diedergruppen. Daher kann man annehmen, daß $\langle g_i, h_i, z\rangle$ für $i = 2, \ldots, n$ eine Diedergruppe ist. Damit gibt es auch für $p = 2$ höchstens zwei extraspezielle Gruppen der Ordnung p^{2n+1}. Man kann sich wieder überlegen, daß es tatsächlich für $n \in \mathbb{N}$ bis auf Isomorphie genau zwei extraspezielle Gruppen der Ordnung 2^{2n+1} gibt (vgl. Aufgabe 3 von Blatt 9).

Satz. *Für $n \in \mathbb{N}$ existieren bis auf Isomorphie genau zwei extraspezielle Gruppen der Ordnung p^{2n+1}.*

16.8. Satz. *Jeder Automorphismus α einer extraspeziellen p-Gruppe G mit $\alpha(g)Z(G) = gZ(G)$ für $g \in G$ liegt in* $\mathrm{Inn}(G)$.

Beweis. Sei $|G/Z(G)| = p^d$, also $|\mathrm{Inn}(G)| = p^d$. Jeder innere Automorphismus hat die gewünschte Eigenschaft. Daher genügt es zu zeigen, daß es höchstens p^d Automorphismen α mit der gewünschten Eigenschaft gibt. Wegen $Z(G) = \Phi(G)$ existieren $x_1, \ldots, x_d \in G$ mit $G = \langle x_1, \ldots, x_d\rangle$. Für jeden solchen Automorphismus α und $i = 1, \ldots, d$ existiert ein Element $z_i \in Z(G)$ mit $\alpha(x_i) = x_i z_i$. Da α durch $\alpha(x_1), \ldots, \alpha(x_d)$ eindeutig bestimmt ist, gibt es höchstens p^d Möglichkeiten für α. □

16.9. Satz. *Ist E eine extraspezielle p-Untergruppe einer Gruppe G mit $[E, G] \subseteq Z(E)$, so ist $G = EC_G(E)$.*

Beweis. Wegen $[E, G] \subseteq Z(E) \subseteq E$ ist $E \trianglelefteq G$. Für $g \in G$ ist also die Abbildung $\alpha : E \to E,\ x \mapsto gxg^{-1}$ ein Automorphismus von E mit $\alpha(x)Z(E) = gxg^{-1}Z(E) = xx^{-1}gxg^{-1}Z(E) = x[x^{-1}, g]Z(E) = xZ(E)$ für $x \in E$. Nach 16.8 existiert also ein $e \in E$ mit $exe^{-1} = \alpha(x) = gxg^{-1}$ für $x \in E$. Folglich ist $e^{-1}g \in C_G(E)$ und $g = ee^{-1}g \in EC_G(E)$. □

KAPITEL 17

Permutationsgruppen

17.1. Satz. *Für eine transitive Operation einer Gruppe G auf einer nichtleeren Menge Ω sind äquivalent:*

(1) *Es existiert ein $\alpha \in \Omega$ mit $\mathrm{Stb}_G(\alpha) = 1$.*
(2) *Für alle Elemente $\beta \in \Omega$ ist $\mathrm{Stb}_G(\beta) = 1$.*
(3) *Zu je zwei Elementen $\alpha, \beta \in \Omega$ existiert genau ein Element $g \in G$ mit ${}^g\alpha = \beta$.*

Beweis.

(1)⇒(2): Sei (1) erfüllt und $\beta \in \Omega$. Dann existiert ein $g \in G$ mit ${}^g\alpha = \beta$. Folglich ist $\mathrm{Stb}_G(\beta) = g\,\mathrm{Stb}_G(\alpha)g^{-1} = g1g^{-1} = 1$.

(2)⇒(3): Sei (2) erfüllt. Wegen der Transitivität von G existiert dann für $\alpha, \beta \in \Omega$ ein Element $g \in G$ mit ${}^g\alpha = \beta$. Ist auch $h \in G$ mit ${}^h\alpha = \beta$, so ist ${}^{g^{-1}h}\alpha = {}^{g^{-1}}\beta = \alpha$, d.h. $g^{-1}h \in \mathrm{Stb}_G(\alpha) = 1$ und $g = h$.

(3)⇒(1): Sei (3) erfüllt und $\alpha \in \Omega$. Dann existiert genau ein Element $g \in G$ mit ${}^g\alpha = \alpha$. Folglich ist $|\,\mathrm{Stb}_G(\alpha)| = 1$, also $\mathrm{Stb}_G(\alpha) = 1$.

□

Definition. Sind (1)–(3) erfüllt, so nennt man die Operation *regulär*.

Bemerkung.

(i) In diesem Fall ist für $\alpha \in \Omega$ die Abbildung $G \to \Omega,\ g \mapsto {}^g\alpha$ bijektiv; insbesondere ist $|\Omega| = |G|$.
(ii) Ist umgekehrt $|G| = |\Omega| < \infty$ und operiert G transitiv auf Ω, so auch regulär; denn für $\alpha \in \Omega$ ist $|G| = |\Omega| = |G : \mathrm{Stb}_G(\alpha)|$, also $|\,\mathrm{Stb}_G(\alpha)| = 1$.
(iii) Ist G abelsch, transitiv und treu auf Ω, so auch regulär; denn wäre $\mathrm{Stb}_G(\alpha) \neq 1$ für ein $\alpha \in \Omega$ und $x \in \mathrm{Stb}_G(\alpha) \setminus \{1\}$, so wäre $x = gxg^{-1} \in \mathrm{Stb}_G({}^g\alpha)$ für $g \in G$, also x im Kern der Operation wegen ihrer Transitivität.

17.2. Satz. *Für eine transitive Operation einer Gruppe G auf einer Menge Ω mit $|\Omega| \geq 2$ sind äquivalent:*

(1) *Es existiert eine echte Teilmenge Δ von Ω mit der Eigenschaft, daß $|\Delta| > 1$ und für $g \in G$ entweder ${}^g\Delta = \Delta$ oder ${}^g\Delta \cap \Delta = \emptyset$ ist.*
(2) *Es existiert eine disjunkte Zerlegung $\Omega = \dot{\bigcup}_{\Lambda \in \mathcal{L}} \Lambda$, wobei $\Lambda \subsetneqq \Omega$, $|\Lambda| > 1$ und ${}^g\Lambda \in \mathcal{L}$ für alle $\Lambda \in \mathcal{L}$, $g \in G$ ist.*

Beweis.

(1)⇒(2): Sei (1) erfüllt, $\delta \in \Delta$ und $\mathcal{L} = \{{}^g\Delta : g \in G\}$. Für $\omega \in \Omega$ existiert dann ein Element $g \in G$ mit $\omega = {}^g\delta \in {}^g\Delta$. Daher ist $\Omega = \bigcup_{\Lambda \in \mathcal{L}} \Lambda$. Sind $g, h \in G$ mit ${}^g\Delta \cap {}^h\Delta \neq \emptyset$, so ist $\emptyset \neq {}^{h^{-1}}({}^g\Delta \cap {}^h\Delta) = {}^{h^{-1}g}\Delta \cap \Delta$, also ${}^{h^{-1}g}\Delta = \Delta$ und ${}^g\Delta = {}^h\Delta$. Daher ist $\Omega = \dot{\bigcup}_{\Lambda \in \mathcal{L}} \Lambda$. Für $g \in G$ ist offenbar ${}^g\Delta \subsetneqq \Omega$, $|{}^g\Delta| > 1$ und ${}^h({}^g\Delta) = {}^{hg}\Delta \in \mathcal{L}$ für $g \in G$.

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

□

Bemerkung. Unter den obigen Voraussetzungen operiert G auch transitiv auf $\mathcal{L}$; sind nämlich $\Lambda, \Delta \in \mathcal{L}$, so wähle man $\alpha \in \Lambda$, $\beta \in \Delta$ und ein $g \in G$ mit ${}^g\alpha = \beta$. Dann ist ${}^g\Lambda \cap \Delta \neq \emptyset$, also ${}^g\Lambda = \Delta$. Für $\Lambda \in \mathcal{L}$ ist $|\mathcal{L}| = |G : \mathrm{Stb}_G(\Lambda)|$ und $|\Omega| = |\Lambda| \cdot |G : \mathrm{Stb}_G(\Lambda)|$. Für $\omega \in \Lambda$ ist $\mathrm{Stb}_G(\omega) \subseteq \mathrm{Stb}_G(\Lambda)$; für $g \in \mathrm{Stb}_G(\omega)$ ist nämlich $\omega = {}^g\omega \in \Lambda \cap {}^g\Lambda$, also ${}^g\Lambda = \Lambda$.

Definition. Sind (1) und (2) erfüllt, so nennt man die Operation *imprimitiv*, andernfalls *primitiv*.

Beispiel. Ist $|\Omega|$ eine Primzahl und operiert G transitiv auf Ω, so auch primitiv; denn die Bedingungen $|\Omega| \neq |\Lambda| \neq 1$ und $|\Lambda| \mid |\Omega|$ widersprechen sich.

17.3. Satz. *Für eine transitive Operation einer endlichen Gruppe G auf einer Menge Ω mit $|\Omega| \geq 2$ sind äquivalent:*

(1) *G operiert primitiv auf Ω.*
(2) *Für jedes $\omega \in \Omega$ ist $\mathrm{Stb}_G(\omega)$ eine maximale Untergruppe von G.*
(3) *Es existiert ein $\omega \in \Omega$, so daß $\mathrm{Stb}_G(\omega)$ eine maximale Untergruppe von G ist.*

Beweis.

(1)⇒(2): Sei (1) erfüllt und $\omega \in \Omega$. Wegen $2 \leq |\Omega| = |G : \mathrm{Stb}_G(\omega)|$ ist $G \neq \mathrm{Stb}_G(\omega)$. Wir nehmen an, daß eine Untergruppe H von G existiert mit $\mathrm{Stb}_G(\omega) < H < G$. Für $\Delta := \mathrm{Orb}_H(\omega)$ gilt dann: $1 < |\Delta| = |H : \mathrm{Stb}_G(\omega)| < |G : \mathrm{Stb}_G(\omega)| = |\Omega|$. Ist $g \in G$ mit ${}^g\Delta \cap \Delta \neq \emptyset$, so existieren $h, h' \in H$ mit ${}^h\omega = {}^{gh'}\omega$, also $h^{-1}gh' \in \mathrm{Stb}_G(\omega) \leq H$ und damit $g \in H$. Folglich ist ${}^g\Delta = \Delta$. Dies zeigt, daß G imprimitiv auf Ω operiert. Widerspruch.

(2)⇒(3): Trivial.

(3)⇒(1): Sei (3) erfüllt. Wir nehmen an, daß G imprimitiv auf Ω operiert, und übernehmen die Bezeichnungen aus 17.2. Ist $\Lambda \in \mathcal{L}$ mit $\omega \in \Lambda$, so ist also $\mathrm{Stb}_G(\omega) \subseteq \mathrm{Stb}_G(\Lambda) \subseteq G$ und $|G : \mathrm{Stb}_G(\omega)| = |\Omega| > |\mathcal{L}| = |G : \mathrm{Stb}_G(\Lambda)| > 1$, d.h. $\mathrm{Stb}_G(\omega) < \mathrm{Stb}_G(\Lambda) < G$. Widerspruch.

□

17.4. Satz. *Gegeben sei eine primitive Operation einer Gruppe G auf einer Menge Ω. Dann operiert jeder Normalteiler N von G 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 $gNg^{-1} = N$, also ${}^g\Delta = \Delta$ oder ${}^g\Delta \cap \Delta = \emptyset$. Aus der Primitivität von G folgt also $|\Delta| = 1$. Daher operiert N trivial auf Ω. □

17.5. Satz. *Gegeben sei eine endliche auflösbare Gruppe G, die treu und primitiv auf einer Menge Ω operiert. Dann enthält G genau einen minimalen Normalteiler M. Dieser operiert regulär auf Ω; insbesondere ist $|\Omega| = |M| = p^m$ für ein $m \in \mathbb{N}$ und eine Primzahl p. Ferner ist $M = C_G(M)$. Im Fall $m = 1$ ist G metabelsch.*

Beweis. Sei M ein minimaler Normalteiler von G, also $M \cong (\mathbb{Z}/p\mathbb{Z})^m$ für ein $m \in \mathbb{N}$ und eine Primzahl p. Nach 17.4 operiert M transitiv auf Ω, nach 17.1 also sogar regulär. Daher ist $|\Omega| = |M| = p^m$.
Setzt man $C := C_G(M)$, so gilt nach Frattini für $\alpha \in \Omega$: $C = M\,\mathrm{Stb}_C(\alpha)$. Für $g \in M$ ist also $\mathrm{Stb}_C(\alpha) = g\,\mathrm{Stb}_C(\alpha)g^{-1} = \mathrm{Stb}_C({}^g\alpha)$. Also operiert $\mathrm{Stb}_C(\alpha)$ trivial auf Ω, d.h. $\mathrm{Stb}_C(\alpha) = 1$ und $C = M$. Ist $N \neq M$ ein weiterer minimaler Normalteiler von G, so ist $M \cap N = 1$, also $N \subseteq C_G(M) = M$. Widerspruch.
Im Fall $m = 1$ ist $G/M = G/C_G(M)$ isomorph zu einer Untergruppe von $\mathrm{Aut}(M) \cong (\mathbb{Z}/p\mathbb{Z})^\times$. □

Bemerkung. Auf G kann man also den Satz von Galois anwenden. Umgekehrt zeigt man leicht, daß die Gruppe im Satz von Galois primitiv auf den Nebenklassen nach einem Komplement des minimalen Normalteilers operiert.

17.6. Definition. Gegeben seien eine Operation einer Gruppe G auf einer Menge Ω und ein $n \in \mathbb{N}$ mit $n \leq |\Omega|$. Wir sagen, daß G *n-transitiv* auf Ω operiert, falls zu je zwei n-Tupeln $(\alpha_1, \ldots, \alpha_n)$, $(\beta_1, \ldots, \beta_n)$ paarweise verschiedener Elemente in Ω ein Element $g \in G$ existiert mit ${}^g\alpha_1 = \beta_1, \ldots, {}^g\alpha_n = \beta_n$.

Bemerkung. Vgl. Aufgabe 6 von Blatt 2.

Satz. *Operiert eine Gruppe G n-transitiv auf einer Menge Ω mit $n \geq 2$, so auch primitiv.*

Beweis. Wir nehmen an, daß G imprimitiv auf Ω operiert, und wählen eine echte Teilmenge Δ von Ω mit $|\Delta| > 1$ und ${}^g\Delta = \Delta$ oder ${}^g\Delta \cap \Delta = \emptyset$ für $g \in G$. Ferner wählen wir $\alpha, \beta \in \Delta$ mit $\alpha \neq \beta$ und $\gamma \in \Omega \setminus \Delta$. Wegen $n \geq 2$ existiert ein $g \in G$ mit ${}^g\alpha = \alpha$ und ${}^g\beta = \gamma$. Dann ist $\alpha \in {}^g\Delta$, also ${}^g\Delta = \Delta$ im Widerspruch zu ${}^g\beta = \gamma \notin \Delta$. □

Beispiel. Für $n \geq 3$ operiert $\mathrm{Alt}(n)$ $(n-2)$-transitiv auf $\{1,\dots,n\}$; denn für paarweise verschiedene $\alpha_1,\dots,\alpha_n \in \{1,\dots,n\}$ liegt

$$\begin{pmatrix} 1 & \dots & n-2 & n-1 & n \\ \alpha_1 & \dots & \alpha_{n-2} & \alpha_{n-1} & \alpha_n \end{pmatrix} \quad \text{oder} \quad \begin{pmatrix} 1 & \dots & n-2 & n-1 & n \\ \alpha_1 & \dots & \alpha_{n-2} & \alpha_n & \alpha_{n-1} \end{pmatrix}$$

in $\mathrm{Alt}(n)$.

17.7. Satz. *Gegeben sei ein Normalteiler $N \neq 1$ einer endlichen Gruppe G. Dann operiert G auf $N \setminus \{1\}$ durch Konjugation. Ist diese Operation transitiv, so ist N eine elementarabelsche p-Gruppe für eine Primzahl p. Ist die Operation sogar 2-transitiv, so ist $p = 2$ oder $|N| = 3$. Ist sie 3-transitiv, so ist $|N| = 4$. Sie ist nie 4-transitiv.*

Beweis. Sei p ein Primteiler von $|N|$. Nach Cauchy enthält N ein Element der Ordnung p. Operiert G transitiv auf $N \setminus \{1\}$, so hat also jedes Element in N Ordnung p, d.h. N ist eine p-Gruppe. Andrerseits ist N charakteristisch einfach, also insgesamt elementarabelsch.
Sei G 2-transitiv auf $N \setminus \{1\}$, $x \in N \setminus \{1\}$ und $p \neq 2$. Dann ist $x^{-1} \neq x$. Für alle $g \in G$ mit $gxg^{-1} = x$ ist $gx^{-1}g^{-1} = x^{-1}$. Daher ist $N = \{1, x, x^{-1}\}$, d.h. $|N| = 3$.
Sei G 3-transitiv auf $N \setminus \{1\}$, also $|N| \geq 4$. Da N elementarabelsch ist, enthält N eine Untergruppe U der Ordnung 4. Es gibt kein Element in G, das die drei Elemente in $U \setminus \{1\}$ auf drei Elemente abbildet, die nicht in einer Untergruppe der Ordnung 4 liegen. Also ist $|N| = 4$. □

17.8. Definition. Operationen einer Gruppe G auf Mengen Ω, Ω' nennt man *ähnlich* oder *isomorph*, falls es eine Bijektion $\varphi : \Omega \to \Omega'$ gibt mit ${}^g\varphi(\omega) = \varphi({}^g\omega)$ für alle $g \in G,\ \omega \in \Omega$.

Bemerkung. Gegebenenfalls operiert G genau dann treu (transitiv, regulär, ...) auf Ω', wenn G treu (transitiv, regulär, ...) auf Ω operiert.

Satz. *Gegeben seien eine Operation einer Gruppe G auf einer Menge Ω, ein Element $\omega \in \Omega$ und ein Normalteiler N von G, der regulär auf Ω operiert. Dann ist die Operation von $\mathrm{Stb}_G(\omega)$ auf $\Omega \setminus \{\omega\}$ ähnlich zu der Operation von $\mathrm{Stb}_G(\omega)$ auf $N \setminus \{1\}$ (durch Konjugation).*

Beweis. Da N regulär auf Ω operiert, existiert zu jedem $\alpha \in \Omega$ genau ein Element $\varphi(\alpha) \in N$ mit ${}^{\varphi(\alpha)}\omega = \alpha$. Für $g \in \mathrm{Stb}_G(\omega)$ ist dann ${}^{g\varphi(\alpha)g^{-1}}\omega = {}^{g\varphi(\alpha)}\omega = {}^g\alpha$, also $\varphi({}^g\alpha) = g\varphi(\alpha)g^{-1}$. Daher ist $\varphi : \Omega \setminus \{\omega\} \to N \setminus \{1\}$ eine Bijektion mit den gewünschten Eigenschaften. □

17.9. Satz. *Für $n \geq 5$ ist $\mathrm{Alt}(n)$ einfach.*

Beweis. (Induktion nach n) Der Fall $n = 5$ ist bereits erledigt. Sei also $n \geq 6$ und die Aussage für $n-1$ bewiesen. Wir identifizieren die einfache Gruppe $\mathrm{Alt}(n-1)$ mit dem Stabilisator von n in $\mathrm{Alt}(n)$. Für jeden minimalen Normalteiler N von $\mathrm{Alt}(n)$ ist $\mathrm{Alt}(n-1) \cap N \trianglelefteq \mathrm{Alt}(n-1)$, also $\mathrm{Alt}(n-1) \cap N \in \{1, \mathrm{Alt}(n-1)\}$. Nach 17.6 operiert $\mathrm{Alt}(n)$ $(n-2)$-transitiv und damit primitiv auf $\{1,\dots,n\}$. Nach 17.4 operiert also N transitiv auf $\{1,\dots,n\}$. Im Fall $\mathrm{Alt}(n-1) \cap N = 1$ operiert N sogar regulär auf $\{1,\dots,n\}$. Nach 17.8 sind die Operationen von $\mathrm{Alt}(n-1)$ auf $\{1,\dots,n-1\}$ und auf $N \setminus \{1\}$ ähnlich; insbesondere operiert $\mathrm{Alt}(n-1)$ $(n-3)$-transitiv auf $N \setminus \{1\}$. Nach 17.7 ist dann $n \leq 6$, d.h. $n = 6$. Das widerspricht aber auch 17.7. Also ist $\mathrm{Alt}(n-1) = \mathrm{Alt}(n-1) \cap N \subseteq N$; insbesondere ist $|N| = n \cdot |\mathrm{Alt}(n-1)| = |\mathrm{Alt}(n)|$, d.h. $N = \mathrm{Alt}(n)$. Dies zeigt, daß $\mathrm{Alt}(n)$ einfach ist. □

17.10. Satz. *Für $n \geq 5$ sind 1, $\mathrm{Alt}(n)$ und $\mathrm{Sym}(n)$ die einzigen Normalteiler von $\mathrm{Sym}(n)$.*

Beweis. Sei N ein von diesen verschiedener Normalteiler in $\mathrm{Sym}(n)$. Dann ist $N \cap \mathrm{Alt}(n) \trianglelefteq \mathrm{Alt}(n)$, also $N \cap \mathrm{Alt}(n) \in \{1, \mathrm{Alt}(n)\}$ nach 17.9. Im Fall $\mathrm{Alt}(n) = N \cap \mathrm{Alt}(n) \subseteq N \subseteq \mathrm{Sym}(n)$ wäre $N \in \{\mathrm{Alt}(n), \mathrm{Sym}(n)\}$. Also ist $N \cap \mathrm{Alt}(n) = 1$ und

$$|N| \cdot \underbrace{|\mathrm{Alt}(n)|}_{n!/2} = |N\,\mathrm{Alt}(n)| \;\big|\; |\mathrm{Sym}(n)| = n!,$$

d.h. $|N| \leq 2$. Andererseits ist N nach 17.6 und 17.4 transitiv auf $\{1,\dots,n\}$, also $n \;\big|\; |N|$. Widerspruch. □

KAPITEL 18

Die Verlagerung

18.1. Bemerkung. Gegeben seien eine endliche Gruppe G, eine Untergruppe H von G, ein Normalteiler K von H mit abelscher Faktorgruppe H/K und ein Repräsentantensystem R für die Linksnebenklassen von G nach H, d.h. $G = \dot{\bigcup}_{r\in R} rH$. Für $g \in G$ und $r \in R$ existiert dann genau ein $\rho_g(r) \in R$ mit $grH = \rho_g(r)H$. Dann ist $\eta_g(r) := \rho_g(r)^{-1}gr \in H$. Wir setzen

$$V^G_{H/K}(g) \;:=\; \prod_{r\in R} \eta_g(r)K$$

und erhalten so eine Abbildung $V^G_{H/K} : G \to H/K$. (Da H/K abelsch ist, kommt es beim Produkt nicht auf die Reihenfolge der Faktoren an.)

Satz. *$V^G_{H/K}$ ist unabhängig von der Wahl von R und ein Homomorphismus.*

Beweis. Jedes weitere Repräsentantensystem für G/H hat die Form $R' = \{rh_r : r \in R\}$, wobei $h_r \in H$ beliebig für $r \in R$ ist. Für $g \in G,\ r \in R$ ist dann

$$grh_rH \;=\; grH \;=\; \rho_g(r)H \;=\; \rho_g(r)h_{\rho_g(r)}H.$$

Definiert man $\eta'_g(r)$ analog, so ist also

$$\eta'_g(r) \;=\; h^{-1}_{\rho_g(r)}\rho_g(r)^{-1}grh_r \;=\; h^{-1}_{\rho_g(r)}\eta_g(r)h_r$$

und

$$\prod_{r\in R} \eta'_g(r)K \;=\; \prod_{r\in R} h^{-1}_{\rho_g(r)}\eta_g(r)h_rK \;=\; \prod_{r\in R} \eta_g(r)K,$$

da H/K abelsch und die Abbildung $R \to R,\ r \mapsto \rho_g(r)$ für $g \in G$ bijektiv ist.
Für $f, g \in G,\ r \in R$ ist

$$fgrH \;=\; f\rho_g(r)H \;=\; \rho_f(\rho_g(r))H,$$

also

$$\begin{aligned} V^G_{H/K}(fg) \;&=\; \prod_{r\in R} \rho_f(\rho_g(r))^{-1}fgrK \;= \\ &=\; \prod_{r\in R} \rho_f(\rho_g(r))^{-1}f\rho_g(r)\cdot\rho_g(r)^{-1}grK \;= \\ &=\; V^G_{H/K}(f)\cdot V^G_{H/K}(g). \end{aligned}$$

□

Definition. Man nennt $V^G_{H/K}$ die *Verlagerung* (transfer) von G nach H/K.

18.2. Bemerkung. Gegeben seien eine endliche Gruppe G, eine Untergruppe H von G, ein Normalteiler K von H mit abelscher Faktorgruppe H/K und ein Element $g \in G$. Zur Berechnung von $V^G_{H/K}$ können wir ein Repräsentantensystem für G/H wählen, das von g abhängt. Die zyklische Gruppe $\langle g\rangle$ operiert auf G/H durch Linksmultiplikation. Wir bezeichnen mit $\Delta_1, \ldots, \Delta_s$ die Bahnen und wählen $r_1H \in \Delta_1, \ldots, r_sH \in \Delta_s$. Für $i = 1, \ldots, s$ sei $d_i := |\Delta_i|$, also $\Delta_i = \{r_iH, gr_iH, g^2r_iH, \ldots, g^{d_i-1}r_iH\}$ und $g^{d_i}r_iH = r_iH$. Dann ist

$$R \;:=\; \{r_1, gr_1, \ldots, g^{d_1-1}r_1, r_2, gr_2, \ldots, g^{d_2-1}r_2, \ldots, r_s, gr_s, \ldots, g^{d_s-1}r_s\}$$

ein Repräsentantensystem für G/H und

$$V_{H/K}^G(g) \;=\; \prod_{i=1}^{s} r_i^{-1} g^{d_i} r_i K;$$

dabei ist $d_1 + \ldots + d_s = |G : H|$ und $r_i^{-1} g^{d_i} r_i \in H$ für $i = 1, \ldots, s$. In den Anwendungen ist oft $r_i^{-1} g^{d_i} r_i K = g^{d_i} K$ für $i = 1, \ldots, s$; in diesem Fall ist $V_{H/K}^G(g) = g^{|G:H|} K$.

Beispiel.

(i) Für $g \in Z(G)$ ist also $V_{H/K}^G(g) = g^{|G:H|} K$.

(ii) Faßt man $V_{Z(G)/1}^G$ als Abbildung in $Z(G)$ auf, so ist $V_{Z(G)/1}^G(g) = g^{|G:Z(G)|}$ für alle $g \in G$. Daher ist die Abbildung $G \to Z(G),\ g \mapsto g^{|G:Z(G)|}$ ein Homomorphismus.

18.3. Definition. Für eine endliche Gruppe G und eine Untergruppe H von G nennt man $\mathrm{Foc}_G(H) := \langle [g,h] : g \in G,\ h \in H,\ [g,h] \in H \rangle$ die *Fokalgruppe* von H in G.

Bemerkung. Dann ist $H' \subseteq F := \mathrm{Foc}_G(H) \subseteq H \cap G'$; insbesondere ist $F \trianglelefteq H$ mit abelscher Faktorgruppe H/F, und für alle Elemente $g \in G,\ h \in H$ mit $[g,h] \in H$ ist $ghg^{-1}F = ghg^{-1}h^{-1}Fh = [g,h]Fh = Fh = hF$. Folglich ist $V_{H/F}^G(h) = h^{|G:H|} F$ für $h \in H$.

Satz. *Sei G eine endliche Gruppe, $H \leq G$ und $F := \mathrm{Foc}_G(H)$. Im Fall* $\mathrm{ggT}(|G : H|, |H : F|) = 1$ *gilt dann:*

(i) $H \cap \mathrm{Ker}(V_{H/F}^G) = H \cap G' = \mathrm{Foc}_G(H)$.

(ii) $H \,\mathrm{Ker}(V_{H/F}^G) = G$.

(iii) $G/G' = HG'/G' \oplus \mathrm{Ker}(V_{H/F}^G)/G'$.

(iv) $G/\,\mathrm{Ker}(V_{H/F}^G) \cong H/\,\mathrm{Foc}_G(H)$.

Beweis.

(i) Offenbar ist $G' \subseteq \mathrm{Ker}(V_{H/F}^G) =: N$, also $F \subseteq H \cap G' \subseteq H \cap N$. Für $h \in H \cap N$ ist andrerseits $1 = V_{H/F}^G(h) = h^{|G:H|} F$. Außerdem ist $h^{|H:F|} F = 1$ nach Fermat. Also ist $hF = 1$ wegen $\mathrm{ggT}(|G : H|, |H : F|) = 1$. Daher ist $h \in F$, und wir haben $H \cap N \subseteq F$ bewiesen.

(ii) Nach (i) ist $|G/N| \geq |HN/N| = |H/H \cap N| = |H/F| \geq |G/N|$. Daher ist $G = HN$.

(iii) Nach (ii) ist $G/G' = (HG'/G')(N/G')$, und nach (i) ist $N \cap HG' = (N \cap H)G' = G'$.

(iv) Der Beweis von (ii) zeigt, daß $V_{H/F}^G$ surjektiv ist.

□

Beispiel. Die Voraussetzung $\mathrm{ggT}(|G : H|, |H : F|) = 1$ ist z.B. erfüllt, wenn H eine Hallgruppe von G ist.

18.4. Definition. Sei H Untergruppe einer endlichen Gruppe G. Wir setzen induktiv $H_1 := H$ und $H_{n+1} := \mathrm{Foc}_G(H_n)$ für $n \in \mathbb{N}$ und nennen H *hyperfokal* in G, falls $H_m = 1$ für ein $m \in \mathbb{N}$ ist.

Bemerkung. Dann ist jede Untergruppe K von H wegen $\mathrm{Foc}_G(K) \subseteq \mathrm{Foc}_G(H)$ auch hyperfokal in G. Ferner ist H auch hyperfokal in jeder Untergruppe U von G mit $H \subseteq U$ wegen $\mathrm{Foc}_U(H) \subseteq \mathrm{Foc}_G(H)$. Schließlich ist H nilpotent wegen $H^n \subseteq H_n$ für alle $n \in \mathbb{N}$.

Satz. *Jede hyperfokale Hallgruppe H einer endlichen Gruppe G besitzt ein normales Komplement in G.*

Beweis. (Induktion nach $|G|$) O.B.d.A. sei $H \neq 1$. Dann ist $F := \mathrm{Foc}_G(H) < H$. Nach 18.3 ist $N := \mathrm{Ker}(V_{H/F}^G) \trianglelefteq G$ mit $G/N \cong H/F \neq 1$. Die Hallgruppe $H \cap N$ von N ist nach der obigen Bemerkung hyperfokal in G und in N. Nach Induktion besitzt $H \cap N$ ein normales Komplement K in N. Als Hallgruppe von N ist K charakteristisch in N und damit normal in G. Ferner ist $HK = H(H \cap N)K = HN = G$ nach 18.3 und $H \cap K = H \cap N \cap K = 1$. □

18.5. Satz. *Gegeben sei eine nilpotente Hallgruppe H einer endlichen Gruppe G. Sind je zwei Elemente in H, die in G konjugiert sind, auch bereits in H konjugiert, so besitzt H ein normales Komplement in G.*

Beweis. Wir setzen $H_1 := H$ und $H_{n+1} := \mathrm{Foc}_G(H_n)$ für $n \in \mathbb{N}$. Nach 18.4 genügt es zu zeigen, daß aus der Voraussetzung $H_n = H^n$ für $n \in \mathbb{N}$ folgt. Dies geschieht durch Induktion nach n. Im Fall $n = 1$ ist $H_1 = H = H^1$. Sei also $n \in \mathbb{N}$ fest mit $H_n = H^n$. Nach Bemerkung 18.4 ist $H^{n+1} \subseteq H_{n+1}$. Für $g \in G,\ h \in H_n$ mit $ghg^{-1}h^{-1} = [g,h] \in H_n$ ist umgekehrt $ghg^{-1} \in H_n \subseteq H$. Nach Voraussetzung existiert also ein $k \in H$ mit $ghg^{-1} = khk^{-1}$. Folglich ist

$$[g,h] = ghg^{-1}h^{-1} = khk^{-1}h^{-1} = [k,h] \in [H,H_n] = [H,H^n] = H^{n+1}.$$

Dies zeigt: $H_{n+1} = \langle [g,h] : g \in G,\ h \in H_n,\ [g,h] \in H_n \rangle \subseteq H^{n+1}$. □

Beispiel. Insbesondere besitzt also eine p-Sylowgruppe P einer endlichen Gruppe G ein normales Komplement, falls je zwei Elemente in P, die in G konjugiert sind, auch bereits in P konjugiert sind.

Bemerkung. Mit Methoden der Darstellungstheorie werden wir 18.5 im nächsten Semester verallgemeinern.

18.6. Satz (Burnside)**.** *Eine p-Sylowgruppe P einer endlichen Gruppe G mit $N_G(P) = C_G(P)$ besitzt ein normales Komplement in G.*

Bemerkung. Aus der Voraussetzung folgt, daß P abelsch ist.

Beweis. Sind je zwei Elemente $x, y \in P$ in G konjugiert, so auch in $N_G(P)$ nach 9.6. Wegen $N_G(P) = C_G(P)$ ist also $x = y$, und die Behauptung folgt aus 18.5. □

18.7. Satz. *Sei G eine endliche Gruppe, p der kleinste Primteiler von $|G|$ und P eine p-Sylowgruppe von G. Ist P zyklisch, so besitzt P ein normales Komplement in G.*

Beweis. Ist P zyklisch der Ordnung p^n, so ist $|\operatorname{Aut}(P)| = p^{n-1}(p-1)$. Da $N_G(P)/C_G(P)$ zu einer Untergruppe von $\operatorname{Aut}(P)$ isomorph ist, folgt $|N_G(P)/C_G(P)| \mid p-1$. Nach Wahl von p folgt $N_G(P) = C_G(P)$, und man kann 18.6 anwenden. □

Bemerkung. Besitzt G eine zyklische 2-Sylowgruppe P, so besitzt also P ein normales Komplement K in G. Da $|K|$ ungerade ist, ist K nach Feit-Thompson auflösbar. Damit ist auch G auflösbar. In der Darstellungstheorie werden wir zeigen, daß Gruppen mit einer Quaternionengruppe als 2-Sylowgruppe nicht einfach sind.

Beispiel. Aus dem Satz folgt insbesondere, daß für ungerades $n \in \mathbb{N}$ Gruppen der Ordnung $2n$ einen Normalteiler der Ordnung n enthalten.

18.8. Satz. *Sind alle Sylowgruppen einer endlichen Gruppe G zyklisch, so ist G auflösbar.*

Beweis. (Induktion nach $|G|$) O.B.d.A. sei $G \neq 1$. Sei p der kleinste Primteiler von $|G|$ und P eine p-Sylowgruppe von G. Nach 18.7 besitzt P ein normales Komplement K in G. Da alle Sylowgruppen von K zyklisch sind, ist K nach Induktion auflösbar. Wegen $G/K = PK/K \cong P/P \cap K = P/1 \cong P$ ist auch G auflösbar. □

Bemerkung. Speziell sind also Gruppen quadratfreier Ordnung (d.h. $|G| = p_1 \dots p_r$ mit paarweise verschiedenen Primzahlen $p_1, \dots, p_r$) auflösbar.

18.9. Satz. *Die Ordnung einer nichtabelschen endlichen einfachen Gruppe G ist durch 12 oder die dritte Potenz ihres kleinsten Primteilers p teilbar.*

Beweis. Sei P eine p-Sylowgruppe von G. Nach 18.7 ist P nichtzyklisch, also $|P| \geq p^2$, o.B.d.A. $|P| = p^2$. Dann ist $P \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z},\ \operatorname{Aut}(P) \cong \mathrm{GL}(2, \mathbb{Z}/p\mathbb{Z})$ und $|N_G(P)/C_G(P)| \mid |\operatorname{Aut}(P)| = |\mathrm{GL}(2, \mathbb{Z}/p\mathbb{Z})| = (p^2-1)(p^2-p) = p(p-1)^2(p+1)$. Nach Burnside ist $1 \neq |N_G(P)/C_G(P)| \mid (p-1)^2(p+1)$. Nach Wahl von p folgt daraus: $|N_G(P)/C_G(P)| = p+1$ ist eine Primzahl. Also ist $p = 2$ und $p+1 = 3$. □

Beispiel. Sei G eine nichtabelsche einfache Gruppe und $|G| = pqrs$ mit Primzahlen p, q, r, s, wobei $p \leq q \leq r \leq s$. Da Gruppen der Ordnung p^3q auflösbar sind, folgt $12 \mid |G|$, d.h. $p = q = 2,\ r = 3$. Da Gruppen der Ordnung p^2q^2 auflösbar sind, folgt $s \geq 5$. Sei S eine s-Sylowgruppe von G, also $1 \neq |G : N_G(S)| \mid 12$ und $|G : N_G(S)| \equiv 1 \pmod{s}$; insbesondere ist $|G : N_G(S)| \geq s+1 \geq 6$, also $|G : N_G(S)| \in \{6, 12\}$.

Im Fall $|G : N_G(S)| = 12$ wäre $s = 11$ und $|N_G(S)| = 11 = |S|$, also $S = N_G(S)$. Insbesondere wäre $N_G(S) = C_G(S)$ im Widerspruch zum Satz von Burnside. Also ist $|G : N_G(S)| = 6$, d.h. $s = 5$, $|G| = 60$ und $G \cong \mathrm{Alt}(5)$ nach Aufgabe 2 von Blatt 6.

18.10. Satz. *Jede auflösbare Untergruppe H einer endlichen Gruppe G mit $H \cap gHg^{-1} = 1$ für alle $g \in G \setminus H$ besitzt ein normales Komplement.*

Beweis. (Induktion nach $|G|$) Sei $h \in H$ und $V^G_{H/H'}(h) = \prod_{i=1}^s r_i^{-1} h^{d_i} r_i H'$ wie in Bemerkung 18.2. Wir können $r_1 = 1$ annehmen. Wegen $hr_1H = hH = H = r_1H$ ist dann $d_1 = 1$ und $r_1^{-1}h^{d_1}r_1 = h$. Für $i = 2, \ldots, s$ ist $r_i \notin H$, also $r_i^{-1}h^{d_i}r_i \in H \cap r_i^{-1}Hr_i = 1$. Folglich ist $V^G_{H/H'}(h) = hH'$ für alle $h \in H$; insbesondere ist $V^G_{H/H'}(H) = H/H'$. Für $g \in G$ existiert also ein Element $h \in H$ mit $V^G_{H/H'}(g) = V^G_{H/H'}(h)$. Folglich ist $h^{-1}g \in \mathrm{Ker}(V^G_{H/H'}) =: N$ und $g = h \cdot h^{-1}g \in HN$. Dies zeigt: $G = HN$. Offenbar ist $H \cap N = H'$, und für $k \in N \setminus H' = N \setminus H$ ist $H' \cap kH'k^{-1} \subseteq H \cap kHk^{-1} = 1$. Nach Induktion besitzt also H' ein normales Komplement F in N. Nach Aufgabe 5 von Blatt 6 ist H' Hallgruppe von N. Daher ist auch F eine Hallgruppe von N; insbesondere ist F charakteristisch in N und damit normal in G. Ferner ist $F \cap H = F \cap N \cap H = F \cap H' = 1$ und $G = HN = HH'F = HF$. □

Bemerkung. In der Darstellungstheorie werden wir zeigen, daß die Auflösbarkeitsbedingung in 18.10 überflüssig ist.

18.11. Satz. *Jede endliche Gruppe G mit einer abelschen maximalen Untergruppe A ist auflösbar.*

Beweis. Sei G ein minimales Gegenbeispiel. Offenbar ist $A \not\trianglelefteq G$, also $A = N_G(A)$. Für $g \in G \setminus A$ ist daher $gAg^{-1} \neq A$, d.h. $\langle A, gAg^{-1}\rangle = G$. Folglich ist $N := A \cap gAg^{-1} \trianglelefteq G$. Ferner ist A/N eine abelsche maximale Untergruppe von G/N. Im Fall $N \neq 1$ wäre G/N auflösbar nach Wahl von G, also auch G. Daher ist $A \cap gAg^{-1} = 1$ für alle $g \in G \setminus A$. Nach 18.10 besitzt A ein normales Komplement K in G. Sei p ein Primteiler von $|K|$ und P eine p-Sylowgruppe von K. Nach Frattini ist $G = KN_G(P)$. Nach Aufgabe 5 von Blatt 6 sind A und K Hallgruppen von G. Daher ist $K \cap N_G(P)$ eine normale Hallgruppe von $N_G(P)$, besitzt also nach Schur-Zassenhaus ein Komplement C in $N_G(P)$. Dann ist $G = KN_G(P) = K(K \cap N_G(P))C = KC$ und $K \cap C = K \cap N_G(P) \cap C = 1$. Nach Schur-Zassenhaus sind A und C in G konjugiert. Insbesondere ist auch C eine maximale Untergruppe von G. Wegen $C < Z(P)C$ folgt also $G = Z(P)C$, d.h. $K = Z(P)$ ist abelsch mit $G/K \cong A$. □

KAPITEL 19

Endliche p-nilpotente Gruppen

Sei p Primzahl und $p' := \{q : q \text{ Primzahl}, \ q \neq p\}$.

19.1. Satz. *Für eine endliche Gruppe G sind äquivalent:*

(1) *Jede p-Sylowgruppe von G besitzt ein normales Komplement in G.*
(2) *Eine p-Sylowgruppe von G besitzt ein normales Komplement in G.*
(3) *$G/O_{p'}(G)$ ist eine p-Gruppe.*
(4) *G besitzt einen p'-Normalteiler K, so daß G/K eine p-Gruppe ist.*

Beweis.

(1)⇒(2): Trivial.
(2)⇒(3): Sei P eine p-Sylowgruppe und $K \trianglelefteq G$ mit $G = PK$ und $P \cap K = 1$. Dann ist $|G| = |P| \cdot |K|$, d.h. $p \nmid |K|$ und $K \subseteq O_{p'}(G)$. Wegen $|O_{p'}(G)| \mid |G : P| = |K|$ folgt daraus: $K = O_{p'}(G)$.
(3)⇒(4): Setze $K := O_{p'}(G)$.
(4)⇒(1): Sei (4) erfüllt und P eine p-Sylowgruppe von G. Dann ist PK/K eine p-Sylowgruppe von G/K, also $PK/K = G/K$ und $PK = G$. Die Behauptung folgt wegen $P \cap K = 1$.

□

Definition. Sind (1)–(4) erfüllt, so nennt man G *p-nilpotent*.

Bemerkung. In diesem Fall ist $O_{p'}(G)$ das einzige (normale) Komplement jeder p-Sylowgruppe.

Beispiel. Jede endliche nilpotente Gruppe ist p-nilpotent für jede Primzahl p. Ist umgekehrt G p-nilpotent für jeden Primteiler p von $|G|$, so ist G nilpotent; denn wegen $\bigcap_{p||G|} O_{p'}(G) = 1$ ist dann die Abbildung $G \to \bigtimes_{p||G|} G/O_{p'}(G)$ ein Monomorphismus in das direkte Produkt der p-Gruppen $G/O_{p'}(G)$.

19.2. Satz. *Mit G ist auch jede Untergruppe und jede Faktorgruppe von G p-nilpotent.*

Beweis. Sei G p-nilpotent und $U \leq G$. Dann ist $U \cap O_{p'}(G)$ ein p'-Normalteiler von U und $U/U \cap O_{p'}(G) \cong UO_{p'}(G)/O_{p'}(G) \leq G/O_{p'}(G)$ eine p-Gruppe. Folglich ist U p-nilpotent.
Für jeden Normalteiler N von G ist $O_{p'}(G)N/N$ ein p'-Normalteiler von G/N und $(G/N)/(O_{p'}(G)N/N) \cong G/O_{p'}(G)N \cong (G/O_{p'}(G))/(O_{p'}(G)N/O_{p'}(G))$ eine p-Gruppe. Folglich ist G/N p-nilpotent. □

19.3. Satz (Frobenius)**.** *Für eine endliche Gruppe G und jede p-Sylowgruppe P von G sind äquivalent:*

(1) *G ist p-nilpotent.*
(2) *Für jede p-Untergruppe $Q \neq 1$ von G ist $N_G(Q)$ p-nilpotent.*
(3) *Für jede p-Untergruppe $Q \neq 1$ von G ist $N_G(Q)/C_G(Q)$ eine p-Gruppe.*
(4) *Für jede p-Untergruppe $Q \neq 1$ von G und jede p-Sylowgruppe R von $N_G(Q)$ ist $N_G(Q) = RC_G(Q)$.*
(5) *Zu jeder Untergruppe Q von P und jedem Element $g \in G$ mit $Q \subseteq gPg^{-1}$ existieren Elemente $z \in C_G(Q)$, $u \in P$ mit $g = zu$.*
(6) *Zu je zwei Elementen $x, y \in P$ und jedem Element $g \in G$ mit $y = gxg^{-1}$ existiert ein Element $u \in P$ mit $y = uxu^{-1}$.*

Beweis.

(1)⇒(2): 19.2.
(2)⇒(3): Sei (2) erfüllt, $Q \neq 1$ eine p-Untergruppe von G und $K := O_{p'}(N_G(Q))$. Wegen $Q \cap K = 1$ ist dann $K \subseteq C_G(Q)$. Wegen (2) ist $N_G(Q)/K$ eine p-Gruppe, also auch $N_G(Q)/C_G(Q)$.

(3)⇒(4): Sei (3) erfüllt, $Q \neq 1$ eine p-Untergruppe von G und R eine p-Sylowgruppe von $N_G(Q)$. Dann ist $RC_G(Q)/C_G(Q)$ eine p-Sylowgruppe von $N_G(Q)/C_G(Q)$, also $N_G(Q)/C_G(Q) = RC_G(Q)/C_G(Q)$ wegen (3) und damit $N_G(Q) = RC_G(Q)$.

(4)⇒(5): Sei (4) erfüllt, $Q \leq P$ und $g \in G$ mit $Q \subseteq gPg^{-1}$. Wir argumentieren durch Induktion nach $|P : Q|$. Im Fall $|P : Q| = 1$ ist $Q = P,\ g \in N_G(P) = PC_G(P) = C_G(P)P$, und wir sind fertig. Sei also $|P : Q| > 1$, d.h. $Q < P$. Dann ist $Q < R_1 := N_P(Q) \leq P$ und $Q < R_2 := N_{gPg^{-1}}(Q) \leq gPg^{-1}$. Wir wählen eine p-Sylowgruppe R von $N_G(Q)$ mit $R_1 \subseteq R$ und ein Element $n \in N_G(Q)$ mit $R_2 \subseteq nRn^{-1}$. Wegen $N_G(Q) = RC_G(Q) = C_G(Q)R$ können wir $n \in C_G(Q)$ annehmen. Ferner wählen wir ein Element $y \in G$ mit $R \subseteq yPy^{-1}$. Wegen $Q < R_1 \leq P$ und $R_1 \subseteq R \subseteq yPy^{-1}$ existieren nach Induktion Elemente $z_1 \in C_G(R_1),\ u_1 \in P$ mit $y = z_1u_1$. Wegen $g^{-1}Qg < g^{-1}R_2g \subseteq P$ und $g^{-1}R_2g \subseteq g^{-1}nRn^{-1}g \subseteq g^{-1}nyPy^{-1}n^{-1}g$ existieren analog Elemente $z_2 \in C_G(R_2),\ u_2 \in P$ mit $g^{-1}ny = g^{-1}z_2g \cdot u_2$. Dann ist aber $g = z_2^{-1}nyu_2^{-1} = z_2^{-1}nz_1u_1u_2^{-1}$ mit $z_2^{-1}nz_1 \in C_G(Q)$ und $u_1u_2^{-1} \in P$.

(5)⇒(6): Sei (5) erfüllt, und seien $x, y \in P,\ g \in G$ mit $y = gxg^{-1}$. Dann ist $\langle y\rangle \subseteq P$ und $\langle y\rangle = \langle gxg^{-1}\rangle = g\langle x\rangle g^{-1} \subseteq gPg^{-1}$. Nach (5) existieren also $z \in C_G(\langle y\rangle),\ u \in P$ mit $g = zu$. Daher ist $y = z^{-1}yz = z^{-1}gxg^{-1}z = uxu^{-1}$.

(6)⇒(1): 18.5.

□

19.4. Satz. *Gegeben sei eine endliche nicht p-nilpotente Gruppe G, in der jede echte Untergruppe p-nilpotent ist. Dann besitzt G eine normale p-Sylowgruppe, und jede echte Untergruppe von G ist sogar nilpotent.*

Bemerkung. Daher ist 10.6 anwendbar.

Beweis. Nach Frobenius existiert eine p-Untergruppe P von G, so daß $N_G(P)/C_G(P)$ keine p-Gruppe ist. Sei $q \neq p$ ein Primteiler von $|N_G(P)/C_G(P)|$ und Q eine q-Sylowgruppe von $N_G(P)$. Dann ist $QC_G(P)/C_G(P)$ eine q-Sylowgruppe von $N_G(P)/C_G(P)$. Sei $g \in Q$ mit $gC_G(P) \neq 1$, und sei $U := \langle P, g\rangle = P\langle g\rangle$. Dann ist $g \in N_U(P) \setminus C_U(P)$, d.h. $N_U(P)/C_U(P)$ ist keine p-Gruppe. Nach Frobenius ist U nicht p-nilpotent. Nach Wahl von G folgt daraus $G = U$; insbesondere ist $P \trianglelefteq G$ und $G/P \cong \langle g\rangle$ eine q-Gruppe.
Jede echte Untergruppe H von G ist p-nilpotent, d.h. $H/O_{p'}(H)$ ist eine p-Gruppe. Andrerseits ist $P \cap H$ wegen $|H : P \cap H| = |PH : P| \mid |G : P|$ eine normale p-Sylowgruppe in H und $H/P \cap H$ ist eine q-Gruppe. Wegen $P \cap H \cap O_{p'}(H) = 1$ ist H zu einer Untergruppe von $H/P \cap H \times H/O_{p'}(H)$ isomorph, also nilpotent. □

19.5. Definition. Für eine endliche abelsche p-Gruppe A bezeichnet man die minimale Erzeugendenzahl als *Rang* von A. Für eine beliebige endliche p-Gruppe P bezeichnet man den maximalen Rang einer abelschen Untergruppe von P als *Rang* von P und $J(P) := \langle A \mid A$ abelsche Untergruppe maximalen Rangs von $P\rangle$ als *Thompsongruppe* von P.

Bemerkung.

(i) Für jede endliche abelsche p-Gruppe A vom Rang r ist $|A/\Phi(A)| = p^r$ nach Burnsides Basissatz. Nach 5.6 ist also $A \cong \mathbb{Z}/p^{a_1}\mathbb{Z} \times \ldots \times \mathbb{Z}/p^{a_r}\mathbb{Z}$ mit $a_1, \ldots, a_r \in \mathbb{N}$.

(ii) Offenbar ist $J(P)$ charakteristisch in P und $J(Q) = J(P)$ für jede Untergruppe Q von P mit $J(P) \subseteq Q$.

(iii) J. Thompson hat bewiesen, daß im Fall $p \neq 2$ eine endliche Gruppe G mit p-Sylowgruppe P bereits dann p-nilpotent ist, wenn $N_G(J(P))$ und $C_G(Z(P))$ p-nilpotent sind. Darauf werden wir im nächsten Semester zurückkommen.

Beispiel. Für $p = 2$ und $G = \mathrm{Sym}(4)$ ist $J(P) = P,\ N_G(J(P)) = N_G(P) = P = C_G(Z(P))$. Daher sind $N_G(J(P))$ und $C_G(Z(P))$ 2-nilpotent, G selbst aber nicht.

19.6. Satz. *Für jede abelsche Hallgruppe H einer endlichen Gruppe G und $N := N_G(H)$ gilt:*

(i) $H = (H \cap Z(N)) \oplus [H, N]$.

(ii) $[H,N] = \mathrm{Foc}_G(H) = H \cap \mathrm{Ker}(V_{H/1}^G)$.
(iii) $(H \cap Z(N))/1 = V_{H/1}^G(H)$.

Beweis. Wir fassen $V_{H/1}^G$ als Abbildung von G in H auf und schreiben statt dessen V_H^G. Sei $x \in H$ und $V_H^G(x) = \prod_{i=1}^s r_i^{-1} x^{d_i} r_i$ wie in 18.2. Für $i = 1, \ldots, s$ sind dann $x^{d_i}, r_i^{-1} x^{d_i} r_i \in H$. Da H abelsch ist, folgt $\langle H, r_i H r_i^{-1} \rangle \subseteq C_G(x^{d_i})$. Als abelsche Hallgruppen von $C_G(x^{d_i})$ sind H und $r_i H r_i^{-1}$ nach Wielandt in $C_G(x^{d_i})$ konjugiert, etwa $c_i r_i H r_i^{-1} c_i^{-1} = H$ mit $c_i \in C_G(x^{d_i})$. Dann ist $c_i r_i \in N$ und $r_i^{-1} x^{d_i} r_i = r_i^{-1} c_i^{-1} x^{d_i} c_i r_i = x^{d_i}[x^{-d_i}, r_i^{-1} c_i^{-1}]$. Folglich ist $V_H^G(x) = x^{|G:H|} d$ mit $d := \prod_{i=1}^s [x^{-d_i}, r_i^{-1} c_i^{-1}] \in [H,N]$. Daher ist $x^{|G:H|} \in V_H^G(H)[H,N]$ und $H = \{x^{|G:H|} : x \in H\} = V_H^G(H)[H,N]$.
Offenbar ist $[H,N] = \langle [g,h] : g \in N,\ h \in H \rangle \subseteq \langle [g,h] : g \in G,\ h \in H,\ [g,h] \in H \rangle = \mathrm{Foc}_G(H) \subseteq H \cap G' \subseteq H \cap \mathrm{Ker}(V_H^G)$. Daher ist auch $H = V_H^G(H)(H \cap \mathrm{Ker}(V_H^G))$. Wegen $[H,N] \subseteq \mathrm{Ker}(V_H^G)$ zeigt die obige Rechnung $V_H^G(V_H^G(x)) = V_H^G(x)^{|G:H|}$ für $x \in H$; insbesondere ist die Einschränkung von V_H^G eine Bijektion auf $V_H^G(H)$. Daher ist $V_H^G(H) \cap \mathrm{Ker}(V_H^G) = 1$, d.h. $H = V_H^G(H) \oplus (H \cap \mathrm{Ker}(V_H^G)) = V_G^H(H) \oplus [H,N]$ und $H \cap \mathrm{Ker}(V_H^G) = [H,N]$.
Für $y, z \in G$ ist $y V_H^G(z) y^{-1} = V_{yHy^{-1}}^G(yzy^{-1})$; für jedes Repräsentantensystem R für G/H ist nämlich yRy^{-1} ein Repräsentantensystem für G/yHy^{-1}. Ist ferner $r \in R$ und $zrH = \rho_z(r)H$ mit $\rho_z(r) \in R$, so ist $yzy^{-1} \cdot yry^{-1} \cdot yHy^{-1} = yzrHy^{-1} = y\rho_z(r)Hy^{-1} = y\rho_z(r)y^{-1} \cdot yHy^{-1}$ mit $y\rho_z(r)y^{-1} \in yRy^{-1}$. Daher ist

$$V_{yHy^{-1}}^G(yzy^{-1}) = \prod_{r \in R} y\rho_z(r)^{-1} y^{-1} \cdot yzy^{-1} \cdot yry^{-1} = y\Big(\prod_{r \in R} \rho_z(r)^{-1} zr\Big) y^{-1} = y V_H^G(z) y^{-1}.$$

Für $y \in N$ und $z \in H$ ist also $y V_H^G(z) y^{-1} = V_H^G(yzy^{-1}) \in V_H^G(H)$, d.h. $V_H^G(H) \trianglelefteq N$. Für $x \in V_H^G(H)$ und $y \in N$ ist $[x,y] \in V_H^G(H) \cap [H,N] = 1$. Folglich ist $V_H^G(H) \subseteq H \cap Z(N)$.
Für $x \in H \cap Z(N)$ ist nach obiger Rechnung $V_H^G(x) = x^{|G:H|}$. Daher ist $H \cap Z(N) = \{x^{|G:H|} : x \in H \cap Z(N)\} \subseteq V_H^G(H)$, und wir sind fertig. □

Bemerkung. Mit $F := \mathrm{Foc}_G(H)$ gilt also nach 18.3: $G/\mathrm{Ker}(V_{H/F}^G) \cong H/F \cong H \cap Z(N)$. Auf diese Weise kann man häufig Normalteiler konstruieren.

19.7. Satz. *Gebenen sei ein minimaler Normalteiler A einer endlichen Gruppe G mit $A = C_G(A)$ und* $\mathrm{ggT}(|A|, |G/A|) = 1$. *Dann ist $Z(G/A)$ zyklisch.*

Beweis. Nach Schur-Zassenhaus besitzt A ein Komplement K in G. Wegen $K \cong G/A$ genügt es zu zeigen, daß $Z(K)$ zyklisch ist. Ist dies nicht der Fall, so enthält $Z(K)$ eine elementarabelsche p-Untergruppe H der Ordnung p^2 für eine Primzahl p. Wir bezeichnen mit $H_0, H_1, \ldots, H_p$ die $p+1$ verschiedenen Untergruppen der Ordnung p von H. Dann ist $H = \{1\} \dot\cup \bigdot_{i=0}^p (H_i \setminus \{1\})$. Für $a \in A$ ist also $\prod_{h \in H} hah^{-1} = a^{-p} \prod_{i=0}^p \prod_{h_i \in H_i} h_i a h_i^{-1}$. Offenbar ist $B := \{\prod_{h \in H} hah^{-1} : a \in A\} \trianglelefteq AK = G$ und $B \subseteq C_A(H) \subseteq A$, also $B \in \{1, A\}$. Im Fall $B = A$ wäre $C_A(H) = A$, also $H \subseteq C_G(A) = A$. Daher ist $B = 1$. Analog ist $B_i := \{\prod_{h_i \in H_i} h_i a h_i^{-1} : a \in A\} = 1$ für $i = 0, \ldots, p$. Dann ist aber $a^{-p} = 1$ für $a \in A$ im Widerspruch zu $p \nmid |A|$. □

19.8. Bemerkung. Nach Aufgabe 3 von Blatt 6 ist $N_{G/H}(PH/H) = N_G(PH)/H = N_G(P)H/H$ für jede p-Untergruppe P und jeden p'-Normalteiler H einer endlichen Gruppe G.

Satz. *Für jede p-Untergruppe P und jeden p'-Normalteiler H einer endlichen Gruppe G ist* $C_{G/H}(PH/H) = C_G(P)H/H$.

Beweis. Offenbar ist $C_G(P)H/H \subseteq C_{G/H}(PH/H) \subseteq N_{G/H}(PH/H) = N_G(P)H/H$. Schreibt man $C_{G/H}(PH/H) = U/H$, so ist also $H \subseteq U \subseteq N_G(P)H$. Nach Dedekind folgt daraus $U = U \cap N_G(P)H = (U \cap N_G(P))H$. Für $u \in U \cap N_G(P)$ und $x \in P$ ist aber $[u,x]H = [uH, xH] = 1$, also $[u,x] \in H \cap P = 1$. Daher ist $U \cap N_G(P) \subseteq C_G(P)$ und $U \subseteq C_G(P)H$, d.h. $C_{G/H}(PH/H) = U/H \subseteq C_G(P)H/H$. □

Index