Norbert Klingen

Endliche Gruppen I

Universität zu Köln SS 1988

Inhaltsverzeichnis

§1 Notationen, Definitionen

a. Gruppen

Wir beginnen der Vollständigkeit halber mit der

(1.1) Definition: Eine *Gruppe* ist ein Paar $(G, \cdot)$ bestehend aus einer Menge G und einer Abbildung

$$\cdot : G \times G \to G\,,$$

(einer binären Verknüpfung auf G), die folgenden Axiomen genügt:
(G1) Die Verknüpfung ist *assoziativ,* d. h.

$$\bigwedge_{a,b,c\in G} a \cdot (b \cdot c) = (a \cdot b) \cdot c\,.$$

(G2) Es gibt ein Element $e \in G$ mit

(E)
$$\bigwedge_{a\in G} e \cdot a = a = a \cdot e\,.$$

(I)
$$\bigwedge_{a\in G} \bigvee_{a'\in G} a' \cdot a = e = a \cdot a'\,.$$

(Existenz von neutralem Element und Inversem)

(1.2) Beispiele:

(1) Die diversen Zahlbereiche, die in der Regel abelsche (=kommutative) Gruppen bilden.

(2) Permutationsgruppen:
Ist $\Omega \neq \emptyset$ eine Menge, so ist

$$S(\Omega) = \{f \mid f : \Omega \xrightarrow{\sim} \Omega \text{ bijektiv}\}$$

mit der Hintereinanderausführung $\circ$ eine Gruppe, die *symmetrische Gruppe* über der Menge Ω. Es ist $S_n = S(\{1, \ldots, n\})$ die symmetrische Gruppe vom Grade n. Es gilt $\#S(\Omega) = (\#\Omega)!$ für endliche Mengen Ω.

(3) Matrixgruppen:
Ist K ein Körper, so bilden die quadratischen $n \times n$-Matrizen über K einen Ring $M_n(K)$. Die invertierbaren Elemente darin bilden bzgl. der Matrixmultiplikation die *allgemeine lineare Gruppe*

$$\mathrm{GL}_n(K) = \{A \in M_n(K) \mid \det A \neq 0\}\,.$$

Dasselbe kann man für einen zugrundeliegenden Ring R statt eines Körpers K bilden. Man beachte dabei aber, daß eine Matrix $A \in M_n(R)$ mit Koeffizienten in einem Ring R invertierbar ist, wenn $\det A$ im Ring R invertierbar ('eine Einheit') ist:

$$\mathrm{GL}_n(R) = \{A \in M_n(R) \mid \det A \text{ invertierbar in } R\}\,.$$

Speziell für $R = \mathbb{Z}$ ergibt sich so

$$\mathrm{GL}_n(\mathbb{Z}) = \{A \in M_n(\mathbb{Z}) \mid \det A = \pm 1\}\,.$$

(4) Endlich präsentierte Gruppen. (Dies wird ein Thema dieser Vorlesung sein.)

b. Untergruppen, Nebenklassen

(1.3) Definition: a) Ist H eine *Untergruppe* einer Gruppe G (d. h. $1_G \in H$ und $a, b \in H \Longrightarrow ab^{-1} \in H$), so schreiben wir kurz $H \leq G$.
b) Wir bezeichnen die *Nebenklassen* nach einer Untergruppe wie folgt:
$G/H = \{aH \mid a \in G\}$ Menge der *Links*nebenklassen von H,
$H\backslash G = \{Ha \mid a \in G\}$ Menge der *Rechts*nebenklassen nach H.
c) Der *Index* $(G : H)$ einer Untergruppe in einer Obergruppe ist die Anzahl der Nebenklassen:

$$(G : H) = \#(G/H) = \#(H\backslash G)\,.$$

Die Anzahl der Rechts- und die der Linksnebenklassen stimmt überein, da die Inversenabbildung eine Bijektion erzeugt:

$$G/H \xrightarrow{\sim} H\backslash G\,, \quad T = aH \mapsto T^{-1} = Ha^{-1}\,.$$

Aufgrund der Gruppeneigenschaft bilden die Nebenklassen eine Klasseneinteilung: $Ha \cap Hb = \emptyset$ oder $Ha = Hb$, und man erhält daher eine disjunkte Zerlegung

$$G = \dot{\bigcup_{aH \in G/H}} aH\,.$$

Da in einer Gruppe die Multiplikation mit einem Element eine bijektive Selbstabbildung ist, haben alle Nebenklassen die gleiche Elementanzahl: $\#(aH) = \#H = \#(Ha)$. Daher ergibt die obige Klasseneinteilung durch Abzählen den

(1.4) Satz: (Satz von Lagrange) *Ist G eine endliche Gruppe und $H \leq G$, so gilt:*

$$\#G = \#(G/H) \cdot \#H = (G : H) \cdot \#H\,.$$

Insbesondere ist die Ordnung jeder Untergruppe ein Teiler der Gruppenordnung.

Ist zum Beispiel G eine Gruppe von Primzahlordnung, so hat G nur die offensichtlichen Untergruppen $\{1\}$ und G selbst.

(1.5) Definition: Für eine Teilmenge $S \subseteq G$ einer Gruppe G definieren wir die von S *erzeugte Untergruppe*

$$\langle S\rangle = \bigcap_{\substack{H \leq G \\ S \subset H}} H = \{s_1^{\varepsilon_1} \cdot s_2^{\varepsilon_2} \cdot \ldots \cdot s_r^{\varepsilon_r} \mid r \in \mathbb{N}\,,\ s_i \in S\,,\ \varepsilon_i = \pm 1\ (i = 1, \ldots, r)\}\,.$$

$\langle S\rangle$ ist die kleinste Untergruppe von G, die S enthält (siehe die erste Gleichung, Beschreibung 'von oben'); sie wird gebildet von den Produkten von Elementen aus S und deren Inversen (siehe die zweite Gleichung, Beschreibung 'von unten'). Es gilt $\langle\emptyset\rangle = \{1_G\}$.

Ist zum Beispiel G eine Gruppe von Primzahlordnung p und $a \in G$, $a \neq 1_G$, so ist die von a erzeugte Untergruppe $\langle a\rangle \neq \{1_G\}$, also (siehe oben) notwendig $\langle a\rangle = G$. G wird also von *einem* Element erzeugt. Solche Gruppen nennt man *zyklisch.*

c. Homomorphismen, Normalteiler, Faktorgruppen

(1.6) Definition: Ist $f : G \to G'$ ein Homomorphismus zweier Gruppen (d. h. $f(ab) = f(a)f(b)$), so werden dadurch zwei zugehörige Untergruppen definiert:

$$\begin{aligned} &\operatorname{Ke} f := \{a \in G \mid f(a) = 1_{G'}\} \leq G\,, && \text{der Kern von } f\,,\\ &\operatorname{Im} f := f(G) \leq G'\,, && \text{das Bild von } f\,. \end{aligned}$$

Man erhält eine natürliche Bijektion

$$\tilde{f} : G/\operatorname{Ke} f \xrightarrow{\sim} \operatorname{Im} f\,,\ a \operatorname{Ke} f \mapsto f(a)\,.$$

Diese ist sogar ein Isomorphismus, wenn man $G/\mathrm{Ke}\, f$ in natürlicher Weise mit einer Gruppenverknüpfung versieht: $a\,\mathrm{Ke}\, f \cdot b\,\mathrm{Ke}\, f = ab\,\mathrm{Ke}\, f$. Aber nicht für jede Untergruppe $H \leq G$ erhält man auf diese Weise eine Gruppenstruktur auf G/H! Vielmehr gilt:

(1.7) Proposition: *Sei G eine Gruppe und $H \leq G$ eine Untergruppe. Dann sind äquivalent:*

i) G/H *ist eine Gruppe vermöge* $G/H \times G/H \to G/H\,,\ (aH, bH) \mapsto abH$,
die sog. Faktorgruppe von G modulo H.

ii) $a^{-1}Ha \subset H$ *für alle* $a \in G$;

ii′) $a^{-1}Ha = H$ *für alle* $a \in G$;
man sagt H ist ein Normalteiler von G (in Zeichen: $H \lhd G$).

ii″) $Ha = aH$ *für alle* $a \in G$.

iii) $H = \mathrm{Ke}\,\nu$ *für irgendeinen Gruppenhomomorphismus* $\nu : G \to G'$.

Für abelsche Gruppen G sind diese Eigenschaften für jede Untergruppe H erfüllt.

Beweis: Offensichtlich ist ii′) $\iff$ ii″). Trifft i) zu, so ist

$$\nu : G \to G/H\,,\ a \mapsto aH$$

ein Gruppenhomomorphismus, der sog. *natürliche Homomorphismus* $G \to G/H$. Dessen Kern ist

$$\mathrm{Ke}\,\nu = \{a \in G \mid \nu(a) = 1_{G/H}\} = \{a \in G \mid aH = H\} = H\,.$$

Damit ist i) $\Rightarrow$ iii) bewiesen. Wir zeigen nun iii) $\Rightarrow$ ii): Sei $H = \mathrm{Ke}\,\nu$ und $a^{-1}ha \in a^{-1}Ha$. Dann gilt $\nu(a^{-1}ha) = \nu(a)^{-1}\nu(h)\nu(a) = \nu(a)^{-1} \cdot 1_{G'} \cdot \nu(a) = 1_{G'}$, d. h. $a^{-1}ha \in \mathrm{Ke}\,\nu = H$, also $a^{-1}Ha \subset H$ für alle $a \in G$.
ii) $\Rightarrow$ ii′): Mit $a = b^{-1} \in G$ erhält man aus ii): $bHb^{-1} \subset H$ bzw. $H \subset b^{-1}Hb$ für alle $b \in G$. Insgesamt folgt nun aus ii) die Gleichheit $H = b^{-1}Hb$ für alle $b \in G$, d. h. ii′).
Schließlich zeigen wir ii″) $\Rightarrow$ i): Wir definieren für Teilmengen S, T von G das *Mengenprodukt* $S \cdot T := \{s \cdot t \mid s \in S\,,\ t \in T\}$. Mit dieser Definition gilt gemäß ii″) für die Nebenklassen $S = aH$ und $T = bH$:

$$S \cdot T = aH \cdot bH = aH \cdot Hb = aHb = abH\,.$$

Dies zeigt, daß abH nicht von den Repräsentanten a, b, sondern nur von den Nebenklassen S, T abhängt, also die angegebene Verknüpfung auf G/H wohldefiniert ist. Daß dann die Gruppenaxiome erfüllt sind, ist kein Problem mehr.

(1.8) Satz: (Homomorphiesatz)
Ist $f : G \to G'$ ein Homomorphismus, so ist

$$\tilde{f} : G/\mathrm{Ke}\, f \xrightarrow{\sim} \mathrm{Im}\, f\,,\ a\,\mathrm{Ke}\, f \mapsto f(a)$$

ein Gruppenisomorphismus.

d. Zyklische Gruppen

Als Anwendung des Homomorphiesatzes klassifizieren wir nun die zyklischen Gruppen. Ist G eine Gruppe und $a \in G$ beliebig, so wird durch

$$\varphi : \mathbb{Z} \to G\,,\ i \mapsto a^i$$

ein Gruppenhomomorphismus von der additiven Gruppe $(\mathbb{Z}, +)$ in die Gruppe G definiert mit $\mathrm{Im}\,\varphi = \langle a \rangle = G$. Nach dem Isomorphiesatz also

$$\mathbb{Z}/\mathrm{Ke}\,\varphi \xrightarrow{\sim} \langle a \rangle \subset G\,.$$

Wir bestimmen den Kern von φ. Dazu bestimmen wir alle Untergruppen H von $\mathbb{Z}$. Ist $H \neq \{0\}$ eine Untergruppe, so existiert in H eine positive Zahl h, also ist

$$d := \min\{h \in H \mid h > 0\}$$

wohldefiniert. Da H eine additive Untergruppe ist, ist $\langle d\rangle = d\mathbb{Z} \subset H$. Es gilt sogar die Gleichheit: Sei dazu $h \in H$, ohne Einschränkung $h > 0$. Wir dividieren h durch d mit Rest und erhalten

$$h = qd + r \quad \text{mit } q \in \mathbb{N}\,,\ 0 \leq r < d\,.$$

Wegen $d \in H$ folgt $qd \in H$, also $r = h - qd \in H$. Da d die kleinste positive Zahl in H ist, muß $r = 0$ sein, also $h = qd \in d\mathbb{Z}$. Damit sind die Untergruppen H von $\mathbb{Z}$ bestimmt:

(1.9) Proposition: *a) Ist H Untergruppe von $\mathbb{Z}$, so gilt $H = \{0\}$ oder $H = d\mathbb{Z}$ mit $d = \min\{h \in H \mid h > 0\}$.*
b) Die entsprechenden Faktorgruppen sind $\mathbb{Z}/\{0\} \simeq \mathbb{Z}$ (unendlich) oder $\mathbb{Z}/d\mathbb{Z} \simeq \{\overline{0}, \overline{1}, \ldots, \overline{d-1}\}$ von der Ordnung d.

Angewendet auf den Kern von $\varphi : \mathbb{Z} \to G$ ergeben sich damit für zyklische Gruppen $G = \langle a\rangle$ die folgenden Möglichkeiten:

(1.10) Proposition: *Ist $G = \langle a\rangle$ eine zyklische Gruppe, so liegt eine der folgenden Möglichkeiten vor:*

(1) $G \simeq \mathbb{Z}$ ist unendlich und alle Potenzen von a sind verschieden, oder

(2) $G \simeq \mathbb{Z}/d\mathbb{Z}$ ist endlich von der Ordnung $d = \min\{i > 0 \mid a^i = 1_G\}$ und es gilt $a^i = 1_G \iff d \mid i$ bzw. $a^i = a^j \iff d \mid (i-j)$.

Die Struktur einer zyklischen Gruppe ist also allein durch ihre Mächtigkeit bestimmt; es gibt zu jedem $d \in \mathbb{N}_+ \cup \{\infty\}$, $d \geq 1$, genau eine zyklische Gruppe mit der Ordnung d.
$\#\langle a\rangle$ nennt man auch die *Ordnung* $\operatorname{ord}(a)$ von a. Im zweiten Fall ist sie gegeben durch $\operatorname{ord}(a) = \min\{i > 0 \mid a^i = 1\}$ und es gilt $a^i = 1 \iff \operatorname{ord}(a) \mid i$.

e. Konjugation, innere Automorphismen, das Zentrum

(1.11) Definition/Proposition: Sei G eine Gruppe.

a) Das *Zentrum* $\operatorname{Zentr}(G) := \{a \in G \mid ab = ba \text{ für alle } b \in G\}$ der Gruppe G ist ein Normalteiler in G.

b) Für alle $a \in G$ ist die *Konjugation* mit a definiert durch $x \mapsto a^{-1}xa := x^a$ ein Automorphismus von G. Die Konjugationen nennt man auch *innere Automorphismen* von G.

c) Die Abbildung $\iota : G \to \operatorname{Aut}(G)\,,\ a \mapsto (x \mapsto axa^{-1} = x^{a^{-1}})$ ist ein Gruppenhomomorphismus, dessen Kern das Zentrum von G ist. Es ist $G/\operatorname{Zentr}(G)$ isomorph zur Gruppe $\operatorname{Inn}(G) = \operatorname{Im}\iota$ aller inneren Automorphismen von G:

$$G/\operatorname{Zentr}(G) \xrightarrow{\sim} \operatorname{Inn}(G)\,,\ a \mapsto a(\ldots)a^{-1}\,.$$

d) $\operatorname{Inn}(G)$ ist ein Normalteiler in $\operatorname{Aut}(G)$. Die Faktorgruppe $\operatorname{Out}(G) = \operatorname{Aut}(G)/\operatorname{Inn}(G)$ nennt man die *äußere Automorphismengruppe* von G.

Beweis: a) folgt aus c), kann aber auch direkt nachgerechnet werden.
b) Es gilt

$$x^a y^a = a^{-1}xa \cdot a^{-1}ya = a^{-1}xya = (xy)^a\,,$$

also ist die Konjugation ein Gruppenhomomorphismus. Offenbar ist die Konjugation mit a^{-1} invers zur Konjugation mit a, so daß die Konjugationen Automorphismen von G sind.
c) Es ist

$$x^{ab} = (ab)^{-1} \cdot x \cdot ab = b^{-1}a^{-1} \cdot x \cdot ab = (x^a)^b \,.$$

(Diese Rechenregel rechtfertigt die Exponentenschreibweise für die Konjugation.) Dies ergibt für beliebige $a, b, x \in G$

$$\iota(ab)(x) = x^{b^{-1}a^{-1}} = (x^{b^{-1}})^{a^{-1}} = \iota(a)(\iota(b)(x))\,, \text{ also } \iota(ab) = \iota(a) \circ \iota(b)\,.$$

Damit ist $\iota : G \to \mathrm{Aut}(G)$ ein Gruppenhomomorphismus. Der Kern ist

$$\mathrm{Ke}\,\iota = \{a \in G \mid \bigwedge_{x \in G} axa^{-1} = x\} = \{a \in G \mid \bigwedge_{x \in G} ax = xa\} = \mathrm{Zentr}(G)\,.$$

Als Kern eines Homomorphismus ist das Zentrum somit ein Normalteiler in G und gemäß dem Homomorphiesatz gilt $G/\mathrm{Zentr}(G) \simeq \mathrm{Inn}(G)$.
d) Sei $\varphi \in \mathrm{Aut}(G)$ und $\iota(a) \in \mathrm{Inn}(G)$. Dann gilt für alle $x \in G$

$$(\varphi \circ \iota(a) \circ \varphi^{-1})(x) = \varphi(a \cdot \varphi^{-1}(x) \cdot a^{-1}) = \varphi(a) \cdot x \cdot \varphi(a)^{-1} = \iota(\varphi(a))(x)\,.$$

Damit ist das Konjugierte eines inneren Automorphismus wieder ein innerer Automorphismus, also $\varphi \circ \mathrm{Inn}(G) \circ \varphi^{-1} \subset \mathrm{Inn}(G)$ für alle $\varphi \in \mathrm{Aut}(G)$. Gemäß (1.7) ist damit $\mathrm{Inn}(G)$ Normalteiler in $\mathrm{Aut}(G)$.

§2 p-Gruppen

a. Operation von Gruppen auf Mengen

(2.1) Definition: Sei G ein Gruppe und $\Omega \neq \emptyset$ eine nicht-leere Menge.

a) Eine *Operation* von G auf Ω ist eine Abbildung

$$G \times \Omega \to \Omega\,,\ (\sigma, a) \mapsto \sigma a$$

mit den Eigenschaften:

(1) $1_G a = a$ für alle $a \in \Omega$ und
(2) $(\sigma\tau)a = \sigma(\tau a)$ für alle $\sigma, \tau \in G$, $a \in \Omega$.

b) Unter einer Operation *von rechts* versteht man eine Abbildung $\Omega \times G \to \Omega$ wie oben, bei der jedoch (2) ersetzt wird durch

(2′) $a(\sigma\tau) = (a\sigma)\tau$ für alle $\sigma, \tau \in G$, $a \in \Omega$.

(2.2) Beispiele: Sei G eine Gruppe.

a) Die Gruppe G operiert auf sich selbst durch Linksmultiplikation: $(\sigma, a) \mapsto \sigma \cdot a$ (Multiplikation in G).

b) Die Gruppe G operiert auf sich selbst von rechts durch Konjugation: $(a, \sigma) \mapsto a^\sigma = \sigma^{-1}a\sigma$.

c) Die allgemeine lineare Gruppe $\mathrm{GL}_n(K)$ operiert durch Matrixmultiplikation von links und auch von rechts auf dem Vektorraum K^n.

(2.3) Bemerkung:

a) Ist $G \times \Omega \to \Omega$ eine Operation von G auf Ω, so ist durch

$$P : G \to S(\Omega)\,, P(\sigma) = (a \mapsto \sigma a)$$

ein Gruppenhomomorphismus von G in die symmetrische Gruppe von Ω definiert;
und umgekehrt:
Ein Homomorphismus $P : G \to S(\Omega)$ definiert eine Operation von G auf Ω vermöge $\sigma a = P(\sigma)(a)$.
Eine Operation von G auf Ω ist also nichts anderes als ein Gruppenhomomorphismus $P : G \to S(\Omega)$.

b) Ist $\Omega \times G \to G, (a, \sigma) \mapsto a\sigma$ eine Rechts-Operation von G auf Ω, so wird durch $(\sigma, a) \mapsto a\sigma^{-1}$ eine (Links-)Operation definiert.

c) Rechts-Operationen von G auf Ω sind Gruppenhomomorphismen von G in die Gruppe $(S(\Omega), \cdot)$ mit der 'verdrehten' Operation $\sigma \cdot \tau = \tau \circ \sigma$.

d) Alle nachfolgenden Begriffsbildungen werden nur für (Links-)Operationen eingeführt und studiert, gelten aber genauso für Operationen von rechts.

(2.4) Definition: Es operiere G auf Ω. Dann definieren wir:

a) die *Bahn* oder den *Orbit* von a unter G:

$$G \cdot a = Ga = \{\sigma a \mid \sigma \in G\}\,,$$

b) die *Fixgruppe* von a in G

$$G_a = \mathrm{Fix}_G(a) = \{\sigma \in G \mid \sigma a = a\}\,,$$

c) die *Fix(punkt)menge* von G in Ω

$$\Omega^G = \{a \in \Omega \mid \bigwedge_{\sigma \in G} \sigma a = a\}\,.$$

Läßt man die multiplikative Gruppe $\mathbb{C}^\times$ auf $\mathbb{C}$ durch Multiplikation operieren und betrachtet die Untergruppen $G = \mathbb{R}_+$, $\mathbb{R}^\times$, $S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$ sowie ganz $\mathbb{C}^\times$, so erhält man für $\alpha = 0$ immer die Bahn $\{0\}$ (0 ist Fixpunkt). Für $\alpha \neq 0$ erhält man die Bahnen

$$G\alpha = \begin{cases} \text{Strahl von 0 durch } \alpha \text{ (ohne 0)} & G = I\!R_+, \\ \text{Gerade durch 0 und } \alpha \text{ (ohne 0)} & G = I\!R^\times, \\ \text{Kreis um 0 durch } \alpha & G = S^1, \\ \mathbb{C}^\times & G = \mathbb{C}^\times. \end{cases}$$

Für die in (2.2) gegebenen Beispiele erhält man:
a) Linksmultiplikation: Diese Operation hat nur eine Bahn, ganz G. Man sagt, die Operation ist *transitiv.* Die Fixgruppe G_a eines jeden $a \in G$ ist trivial: $G_a = \{1\}$. Der Gruppenhomomorphismus $P : G \to S(G)$, $a \mapsto a \cdot (\ldots)$ ist injektiv. Man sagt, die Operation ist *treu.*
b) Konjugation: Die Bahnen dieser Operation sind die *Konjugationsklassen* von Elementen:

$$C(a) = [a] = \{a^\sigma \mid \sigma \in G\}\,.$$

Die Fixgruppen G_a bzgl. dieser Operation sind die *Zentralisatoren*

$$\mathrm{Zentr}_G(a) = \{\sigma \in G \mid \sigma a = a\sigma\}\,.$$

Die Fixmenge unter der Konjugation ist das Zentrum von G.
c) Matrixmultiplikation: Die Operation von $\mathrm{GL}_n(K)$ auf K^n hat zwei Bahnen: $\{0\}$ und $K^n \setminus \{0\}$. 0 ist der einzige Fixpunkt der Operation. Die Fixgruppe eines $v \in K^n$, $v \neq 0$, ist die Menge der Matrizen A, die den Eigenwert 1 haben und v als einen Eigenvektor zu diesem Eigenwert.
Begründung: Diese Aussagen sind Umformulierungen der Definitionen. Bei a) beachte man die Gruppenaxiome: $b = (ba^{-1}) \cdot a \in Ga$ für alle $b \in G$, also $G \subset Ga$ bzw. $G = Ga$. Und $G_a = \{1\}$ wegen $\sigma \cdot a = a \iff \sigma = 1$.

(2.5) Proposition: *Die Gruppe G operiere auf der nicht-leeren endlichen Menge Ω. Dann gilt:*

a) $G_a \leq G$ *für alle* $a \in \Omega$.

b) $G_{\sigma a} = \sigma G_a \sigma^{-1}$ *für* $a \in \Omega$, $\sigma \in G$.

c) $(G : G_a) = \#Ga$ *für* $a \in \Omega$*; Bahnlängen sind Gruppenindizes.*

d) Die Bahnen bilden eine Klasseneinteilung von Ω*:*

$$\Omega = \dot{\bigcup_{a \in \mathcal{R}}} Ga\,,$$

wobei $\mathcal{R}$ *ein Repräsentantensystem der Bahnen unter* G *ist.*

e) (Bahnengleichung)

$$\#\Omega = \#\Omega^G + \sum_{a \in \mathcal{R}'} (G : G_a)$$

wobei $\mathcal{R}'$ *ein Repäsentantensystem der Bahnen* Ga *mit* $\#Ga \geq 2$ *ist. Die Summanden* $(G : G_a)$ *in der Bahnengleichung sind also* ≥ 2 *und Teiler von* $\#G$.

Beweis: a), b) rechne man nach. c) ergibt sich aus der Bijektion

$$G/G_a \xrightarrow{\sim} Ga\,,\ \sigma G_a \mapsto \sigma a\,.$$

Dabei ist die Surjektivität durch die Definition der Bahn Ga gegeben, während sich die Injektivität aus der Definition der Fixgruppe G_a ergibt:

$$\sigma a = \tau a \ \Leftrightarrow\ \tau^{-1}\sigma a = a \ \Leftrightarrow\ \tau^{-1}\sigma \in G_a \ \Leftrightarrow\ \tau^{-1}\sigma G_a = G_a \ \Leftrightarrow\ \sigma G_a = \tau G_a\,.$$

d) Ist $Ga \cap Gb \neq \emptyset$, also $\sigma a = \tau b$ für geeignete $\sigma, \tau \in G$, so folgt $b = \rho a \in Ga$ für $\rho = \tau^{-1}\sigma$. Dann gilt aber $Gb = G\rho a = Ga$. Die Bahnen sind also disjunkt oder gleich. Da sie ganz Ω überdecken, folgt d).
e) erhält man schließlich, indem man die einelementigen Bahnen (in denen gerade die Fixpunkte liegen) von den nicht-einelementigen trennt. Letztere haben gemäß c) die Mächtigkeit $2 \leq \#Ga = (G : G_a)$.

(2.6) Korollar: *Operiert eine p-Gruppe G (eine Gruppe von Primzahlpotenzordnung p^n) auf einer Menge Ω, so gilt:*

$$\#\Omega \equiv \#\Omega^G \bmod p\,.$$

Beweis: In einer p-Gruppe sind alle Gruppenindizes $(G : G_a)$, die ≥ 2 sind, notwendig durch p teilbar, also ist in der obigen Bahnengleichung die gesamte Summe durch p teilbar, also $\#\Omega - \#\Omega^G$ ein Vielfaches von p, wie behauptet. □

Als Beispiel für eine gruppentheoretische Anwendung zeigen wir

(2.7) Korollar: *Eine Gruppe G von Primzahlpotenzordnung $p^n > 1$ hat ein nicht-triviales Zentrum.*

Zum *Beweis* betrachten wir die Operation von G auf sich selbst ($\Omega = G$) durch Konjugation. Dann ist $\Omega^G = \mathrm{Zentr}(G)$ und gemäß (2.6) gilt

$$\#G \equiv \#\mathrm{Zentr}(G) \bmod p\,.$$

Mit $\#G$ ist also auch $\#\mathrm{Zentr}(G)$ durch p teilbar, also $\#\mathrm{Zentr}(G) \geq p$. Damit ist (2.7) bewiesen.

b. Sylowsätze

Wir untersuchen die Umkehrung des Satzes von Lagrange: Gibt es zu einem Teiler d der Ordnung einer endlichen Gruppe G eine Untergruppe H von G mit $\#H = d$? Betrachtet man *spezielle* Gruppen, so kann man positive Antworten finden; z. B.

(2.8) Proposition: *In endlichen zyklischen Gruppen gibt es zu jedem Teiler d der Gruppenordnung eine Untergruppe der Ordnung d. Genauer: Ist $G = \langle a\rangle$ zyklisch von der Ordnung n und d ein Teiler von n, so ist $\langle a^{n/d}\rangle$ die einzige Untergruppe von G mit der Ordnung d.*

Beweis: Sei $k = n/d$. Es ist $\operatorname{ord} a = n$, also $a^i = 1 \iff n \mid i$. Daraus folgt

$$(a^k)^i = 1 \iff n \mid k\cdot i \iff k\cdot d \mid k\cdot i \iff d \mid i\,.$$

Damit ist $d = \operatorname{ord} a^k$, also $\langle a^k\rangle$ eine (zyklische) Untergruppe der Ordnung d.

Nun zur Eindeutigkeit. Sei H eine Untergruppe von G mit der Ordnung d. Da G zyklisch, insbesondere also abelsch ist, ist H ein Normalteiler und wir können die Faktor*gruppe* G/H betrachten. Diese hat die Ordnung $(G:H) = \#G/\#H = n/d = k$. Also gilt nach dem Satz von Lagrange $\bar a^k = \bar 1$ für $\bar a = aH \in G/H$. Dies bedeutet

$$\bar a^k = a^k H = H\,,\ \text{bzw. } a^k \in H\,.$$

Damit liegt a^k in H, also $\langle a^k\rangle \subset H$. Wegen gleicher Ordnung stimmen die beiden Gruppen überein, womit die Eindeutigkeit gezeigt ist. □

Diese Proposition gibt für *spezielle* Gruppen eine positive Antwort auf die Frage nach der Umkehrung des Satzes von Lagrange. Die Sylowsätze hingegen geben eine positive Antwort für spezielle Teiler d, nämlich für *Primzahlpotenzen* $d = p^s$. Die fundamentale Bedeutung der Sylowsätze liegt nun darin, daß sie für *beliebige* Gruppen gelten. Sie spielen daher eine nicht zu überschätzende Rolle bei der Strukturaufklärung beliebiger Gruppen.

Sei nun G eine Gruppe der Ordnung n, p eine Primzahl und es gelte $p^s \mid n$. Dann ist $\#G = n = p^r \cdot m$ mit $p \nmid m$ und $r \geq s$. Um eine Untergruppe H von G mit der gewünschten Ordnung p^s zu finden, betrachten wir zunächst sämtliche Teilmengen von G mit der Mächtigkeit p^s:

$$\Omega = \binom{G}{p^s} = \{T \subset G \mid \#T = p^s\}\,.$$

Darauf operiert G durch Linksmultiplikation. Für ein $T \in \Omega$ ist dann die Fixgruppe $G_T = \{\sigma \in G \mid \sigma T = T\}$ eine Untergruppe von G. Diese operiert nun ihrerseits auf den *Elementen* von T durch Linksmultiplikation und man erhält so (bei Wahl eines beliebigen $a \in T$) eine injektive Abbildung

$$\varphi_a : G_T \hookrightarrow T\,,\ \sigma \mapsto \sigma a\,.$$

Insbesondere folgt also für jedes $T \in \Omega$: $\#G_T \leq \#T = p^s$.

Wir suchen nun unter diesen Fixgruppen $H = G_T$ eine mit der maximalen Ordnung p^s. Nun gilt für $H = G_T$:

$$\#H = p^s \iff \varphi_a : H \xrightarrow{\sim} T \iff T = Ha\,.$$

Andererseits gilt wegen $\#H \leq p^s$

$$\begin{aligned} \#H = p^s &\iff p^s \mid \#H = \tfrac{\#G}{(G:H)} = \tfrac{p^r m}{(G:H)} \iff (G:H) \mid p^{r-s} m \\ &\iff p^{r-s+1} \nmid (G:H) = (G:G_T) = \#GT\,. \end{aligned}$$

Dabei ist $GT = \{\sigma T \mid \sigma \in G\} \subset \Omega$ die Bahn von $T \in \Omega$. Faßt man beide Aussagen zusammen, so erhält man für $T \subset G$

$$T \in \Omega \wedge p^{r-s+1} \nmid \#(GT) \iff T \in \Omega \wedge \bigvee_{a \in G} T = G_T a \iff \bigvee_{a \in G} \bigvee_{\substack{H \leq G \\ \#H = p^s}} T = Ha\,. \tag{1}$$

Bei der zweiten Äquivalenz gilt '$\Leftarrow$', weil aus $T = Ha$ folgt: $\#T = \#H = p^s$ und $G_T = H$. Insbesondere erhalten wir aus (1)

$$\bigvee_{H \leq G} \#H = p^s \iff \bigvee_{T \in \Omega} p^{r-s+1} \nmid \#(GT)\,. \tag{2}$$

Wir wollen nun zeigen, daß es derartige $T \in \Omega$ und folglich Untergruppen der gesuchten Art gibt. Dazu betrachten wir die Menge

$$\Omega' = \{T \in \Omega \mid p^{r-s+1} \nmid \#(GT)\} \underset{(1)}{=} \{Ha \mid H \leq G\,,\ \#H = p^s\,,\ a \in G\}$$

und müssen zeigen, daß sie nicht leer ist. Ω' besteht aus allen Nebenklassen aller Untergruppen der Ordnung p^s. Nun sind Nebenklassen von verschiedenen Untergruppen notwendig verschieden (siehe oben: $T = Ha \Rightarrow H = G_T$), also gilt

$$\Omega' = \dot{\bigcup_{\substack{H \leq G \\ \#H = p^s}}} \{Ha \mid a \in G\} = \dot{\bigcup_{\substack{H \leq G \\ \#H = p^s}}} H\backslash G\,.$$

Da alle $H\backslash G$ dieselbe Mächtigkeit

$$(G:H) = \frac{\#G}{\#H} = \frac{n}{p^s} = p^{r-s} m$$

haben, folgt

$$\#\Omega' = p^{r-s} m \cdot \#\{H \leq G \mid \#H = p^s\} =: p^{r-s} m \cdot h_G(p^s)\,. \tag{3}$$

($h_G(p^s)$ bezeichnet also die Anzahl der Untergruppen H von G mit $\#H = p^s$, die wir ja studieren wollen.) Weiter gilt bekanntlich

$$\#\Omega = \binom{n}{p^s} = \frac{n}{p^s} \cdot \binom{n-1}{p^s - 1} = p^{r-s} m \cdot \binom{n-1}{p^s - 1}\,. \tag{4}$$

Andererseits besteht $\Omega \setminus \Omega'$ nach Definition von Ω' gerade aus allen $T \in \Omega$ mit $p^{r-s+1} \mid \#GT$, also zerfällt $\Omega \setminus \Omega'$ in lauter Bahnen, deren Mächtigkeit durch p^{r-s+1} teilbar ist. Das bedeutet

$$p^{r-s+1} \mid \#(\Omega \setminus \Omega') = \#\Omega - \#\Omega'\,, \quad \text{bzw.} \quad \#\Omega \equiv \Omega' \mod p^{r-s+1}\,. \tag{5}$$

Aus (3) – (5) folgt

$$\begin{aligned} p^{r-s} m \cdot \tbinom{n-1}{p^s-1} &\equiv p^{r-s} m \cdot h_G(p^s) \mod p^{r-s+1}\,, \quad \text{bzw.} \\ m \cdot \tbinom{n-1}{p^s-1} &\equiv m \cdot h_G(p^s) \mod p\,. \end{aligned}$$

Da p kein Teiler von m ist, gilt nun

$$p \mid m \cdot \Big(\binom{n-1}{p^s-1} - h_G(p^s) \Big) \implies p \mid \binom{n-1}{p^s-1} - h_G(p^s)\,,$$

und daher

$$h_G(p^s) \equiv \binom{n-1}{p^s-1} \mod p\,. \tag{6}$$

Wir zeigen nun

$$\binom{n-1}{p^s-1} \equiv 1 \bmod p\,. \tag{7}$$

Dies kann man rein zahlentheoretisch für $p^s \mid n$ beweisen. Man kann es aber auch gruppentheoretisch aus (6) folgern. Dazu benutzt man, daß in (6) die rechte Seite nicht von G, sondern nur von $\#G = n$ abhängig ist! Und für $G = C_n$ zyklisch von der Ordnung n ist die linke Seite von (6) gemäß (2.8) gleich 1. Also

$$1 = h_{C_n}(p^s) \equiv \binom{n-1}{p^s-1} \bmod p\,,$$

womit (7) bewiesen ist. (6) und (7) zusammen ergeben für jede Gruppe G der Ordnung n und Primzahlpotenzen $p^s \mid n$:

$$h_G(p^s) \equiv 1 \bmod p\,. \tag{8}$$

Insbesondere kann die Zahl der Untergruppen der Ordnung p^s nicht 0 sein! Damit ist der folgende Satz bewiesen:

(2.9) Satz: (Erster Sylowsatz) *Sei G eine endliche Gruppe.*
a) Dann gibt es zu jeder Primzahlpotenz p^s, die die Gruppenordnung $\#G$ teilt, eine Untergruppe H von G mit $\#H = p^s$.
b) Für die Anzahl $h_G(p^s)$ solcher Untergruppen gilt genauer:

$$h_G(p^s) \equiv 1 \bmod p\,.$$

Unter den p-Untergruppen von G spielen die von größtmöglicher Ordnung eine besondere Rolle. Dies sind die sog. p-Sylow(unter)gruppen von G. Ist $\#G = p^r m$ mit einer Primzahl p, $p \nmid m$, so definiert man:

$$\begin{aligned} P \text{ } p\text{-Sylowuntergruppe von } G \;&:\Longleftrightarrow\; P \le G \text{ und } \#P = p^r \\ &\Longleftrightarrow\; P \text{ } p\text{-Gruppe und } p \nmid (G:P)\,. \end{aligned}$$

Nach dem vorangehenden Satz besitzt *jede* Gruppe für *jede* Primzahl eine p-Sylowuntergruppe. Eine Übersicht über alle p-Sylowuntergruppen gibt unter anderem der folgende Satz.

(2.10) Satz: (Zweiter Sylowsatz) *Sei G eine endliche Gruppe, p eine Primzahl, P eine p-Sylowuntergruppe und H eine beliebige p-Untergruppe von G. Dann existiert ein $\sigma \in G$ mit*

$$H \subset \sigma^{-1} P \sigma = P^\sigma\,.$$

Folglich gilt:

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

b) *p-Sylowgruppen von G sind genau die (bzgl. Inklusion) maximalen p-Untergruppen von G.*

c) Sämtliche p-Sylowuntergruppen von G sind in G untereinander konjugiert:

$$P, P' \text{ p-Sylowuntergruppen von } G \Longrightarrow \bigvee_{\sigma \in G} P' = P^\sigma \,.$$

d) Ist s_p die Anzahl der p-Sylowgruppen von G und $\#G = p^r m$ mit $p \nmid m$, so gilt:

$$s_p \mid m \quad \textit{und} \quad s_p \equiv 1 \bmod p \,.$$

Beweis: Die p-Untergruppe $H \subset G$ operiert durch Linksmultiplikation auf den Linksnebenklassen $\Omega = G/P = \{aP \mid a \in G\}$ von P. Dann gilt nach (2.6)

$$\#\Omega \equiv \#\Omega^H \bmod p \,.$$

Ist $G = p^r m$ mit $p \nmid m$, so ist $\#\Omega = (G : P) = m$ nicht durch p teilbar, also

$$\#\Omega^H \equiv \#\Omega \not\equiv 0 \bmod p \,.$$

Insbesondere ist $\#\Omega^H \neq 0$, also existiert in Ω ein Fixelement aP unter der Operation von H:

$$\bigwedge_{h \in H} haP = aP \,, \text{ bzw. } a^{-1}ha \in P \,.$$

Damit gilt $a^{-1}Ha \subset P$ bzw. $H \subset aPa^{-1}$, womit die Behauptung bewiesen ist.

Nun zu den Folgerungen. a) Mit P ist auch P^σ eine p-Sylowuntergruppe.
b) p-Sylowuntergruppen sind natürlich maximale p-Untergruppen, da größere p-Potenzen nicht mehr $\#G$ teilen. Sei nun umgekehrt H eine (bzgl. Inklusion) maximale p-Untergruppe. Wie gezeigt, liegt H in einer p-Sylowuntergruppe, muß also wegen der Maximalität mit dieser übereinstimmen. Also ist H selbst p-Sylowuntergruppe.
c) Sind P, P' p-Sylowuntergruppen, so existiert ein $\sigma \in G$ mit $P' \subset P^\sigma$. Da P' und P^σ als p-Sylowuntergruppen gleichmächtig sind, folgt $P' = P^\sigma$.
d) Die Gruppe G operiert durch Konjugation auf den Untergruppen. Ist P eine p-Sylowuntergruppe, so ist die Bahn von P unter dieser Operation (nach c)) gerade die Menge aller p-Sylowuntergruppen. Nun sind Bahnlängen aber Indizes von Fixgruppen. In diesem Falle ist diese Fixgruppe gerade

$$\mathrm{Fix}_G(P) = \{\sigma \in G \mid P^\sigma = P\} =: \mathcal{N}_G(P) \,,$$

der sog. Normalisator von P in G. Also gilt nach (2.5) c)

$$s_p = \#\{P \mid P \text{ p-Sylowuntergruppe von } G\} = \#\{P^\sigma \mid \sigma \in G\} = (G : \mathcal{N}_G(P)) \,.$$

Diese Überlegungen zeigen allgemein: *Die Anzahl der Konjugierten einer Untergruppe ist der Index des Normalisators in der Gruppe.*

Nun ist der Normalisator nach Definition die größte Untergruppe von G, in der P ein Normalteiler ist:

$$\mathcal{N}_G(P) = \{\sigma \in G \mid \sigma^{-1} P \sigma = P\} \,,$$

also $\mathcal{N}_G(P) \supset P$ und daher gilt $s_p = (G : \mathcal{N}_G(P)) \mid (G : P) = m$. Damit ist auch d) bewiesen, denn die Kongruenz modulo p wurde bereits im ersten Sylowsatz gezeigt.

c. Nilpotente Gruppen

Alle Gruppen seien im Folgenden endlich!
Nach (2.7) wissen wir, daß nicht-triviale p-Gruppen ein nicht-triviales Zentrum haben:

$$G \neq \{1\} \; p\text{-Gruppe} \implies \{1\} \neq Z_1(G) := \mathrm{Zentr}(G) \,.$$

$Z_1(G)$ ist ein Normalteiler von G und wir definieren induktiv eine aufsteigende Kette von Normalteilern durch

$$\nu_i : G \twoheadrightarrow G/Z_i(G) \text{ natürlicher Epimorphismus}\,,$$
$$Z_{i+1}(G) := \nu_i^{-1}(\mathrm{Zentr}(G/Z_i(G)))\,.$$

(2.11) Bemerkung: Ist $f : G \twoheadrightarrow G'$ ein Gruppenepimorphismus, so erhält man durch die Zuordnung $H' \mapsto f^{-1}(H')$ eine Bijektion zwischen den Untergruppen von G' und den Untergruppen von G, die $\mathrm{Ke}\, f$ umfassen:

$$\{H' \mid H' \leq G'\} \xrightarrow{\sim} \{H \mid \mathrm{Ke}\, f \leq H \leq G\}\,,\ H' \mapsto f^{-1}(H')\,.$$

Dabei bleiben Inklusionen, Gruppenindizes, Konjugiertheit und Normalteilereigenschaft erhalten:

$$(G' : H') = (G : f^{-1}(H'))\,,\ f^{-1}(H')^{\sigma} = f^{-1}(H'^{f(\sigma)}) \text{ und } H' \lhd G' \Leftrightarrow f^{-1}(H') \lhd G\,.$$

Beweis: Es ist $f(f^{-1}(H')) = H'$ und für $\mathrm{Ke}\, f \leq H \leq G$ gilt $f^{-1}(f(H)) = H$, so daß (auf der angegebenen Menge) die Umkehrabbildung durch Anwendung von f gegeben ist.
Ist $G = \dot{\bigcup}_{i\in I} a_i f^{-1}(H')$ die Nebenklassenzerlegung von G modulo $f^{-1}(H')$, so erhält man durch Anwendung von f eine Nebenklassenzerlegung von G' modulo H':

$$G' = f(G) = \dot{\bigcup_{i\in I}} f(a_i)H'\,.$$

Dabei überträgt sich die Disjunktheit, denn es gilt $f^{-1}(f(a_i)H') = a_i f^{-1}(H')$. Damit sind die Anzahlen der Nebenklassen, d. h. die jeweiligen Gruppenindizes identisch.

Die Konjugiertheitsaussage rechnet man unmittelbar nach und die Normalteilereigenschaft ergibt sich daraus unter Beachtung der Surjektivität von f. □

(Übung: Für $H' \lhd G'$ sind auch die Faktorgruppen $G/f^{-1}(H') \xrightarrow{\sim} G'/H'$ isomorph.)

Sind G und damit auch alle Faktorgruppen G/Z_i p-Gruppen, so haben diese alle ein nichttriviales Zentrum $\mathrm{Zentr}(G/Z_i) \neq \{1\}$, sofern sie selbst nichttrival sind, d. h. $G \neq Z_i$ ist. Aus (2.11) (angewendet auf $\nu_i : G \twoheadrightarrow G/Z_i$) ergibt sich:

$$Z_i = \mathrm{Ke}\, \nu_i = \nu_i^{-1}(\{1\}) \subsetneq \nu_i^{-1}(\mathrm{Zentr}(G/Z_i)) = Z_{i+1} \quad \text{falls } Z_i \neq G\,.$$

Für endliche p-Gruppen G folgt so die Existenz eines k mit $Z_k(G) = G$:

$$\{1\} \subsetneq Z_1(G) \subsetneq Z_2(G) \subsetneq \ldots \subsetneq Z_k(G) = G$$

Diese *aufsteigende Zentralreihe* $Z_i(G)$ wird erst bei G stationär. Diese Eigenschaft charakterisiert die sog. *nilpotenten* Gruppen. Die obigen Überlegungen besagen daher, daß p-Gruppen nilpotent sind.

(2.12) Satz: *Nilpotente Gruppen sind charakterisiert durch die folgenden äquivalenten Bedingungen:*

i) Die aufsteigende Zentralreihe $Z_i(G)$ definiert durch

$$Z_0(G) = \{1\}\,,\ Z_{i+1}(G) = \nu_i^{-1}(\mathrm{Zentr}(G/Z_i(G)))$$

bricht erst bei G ab: $Z_k(G) = G$ für ein k.

ii) Es gibt eine Kette von Normalteilern

$$G \rhd N_1 \rhd \ldots \rhd N_r = \{1\}$$

mit $N_i \lhd G$ und $N_i/N_{i+1} \subset \mathrm{Zentr}(G/N_{i+1})$ (eine Zentralreihe bis hinunter zu $\{1\}$).

iii) Die absteigende Zentralreihe definiert durch

$$G_0 = G\,,\ G_{i+1} = [G, G_i] := \langle \sigma^{-1}\tau^{-1}\sigma\tau \mid \sigma \in G\,,\ \tau \in G_i \rangle$$

bricht erst bei $\{1\}$ *ab:* $G_k = \{1\}$ *für ein* k*.*

iv) Jede echte Untergruppe $H < G$ *ist auch echte Untergruppe in ihrem Normalisator:*

$$H < G \ \Rightarrow\ H < \mathcal{N}_G(H) = \{\sigma \in G \mid H^\sigma = H\}\,.$$

v) Alle Sylowuntergruppen von G *sind Normalteiler in* G*.*

vi) G *ist direktes Produkt von Gruppen von Primzahlpotenzordnung.*

Beweis: Daß durch i) eine aufsteigende Kette von Normalteilern definiert ist, haben wir bereits oben gesehen. Überprüfen Sie selbst zur Übung, daß durch iii) eine absteigende Kette von Normalteilern $G_i \lhd G$ definiert ist.
vi) $\Rightarrow$ i): Man zeige als Übung, daß sich Eigenschaft i) auf direkte Produkte von Gruppen vererbt. (Tip: Man berechne das Zentrum in einem direkten Produkt von Gruppen.).
i) $\Rightarrow$ ii) ist eine logische Abschwächung.
ii) $\Rightarrow$ iii): Wir zeigen

$$[G, N_i] \subset N_{i+1}\,, \qquad (***)$$

woraus wegen $G_0 \subseteq N_0 = G$ dann induktiv $G_{i+1} = [G, G_i] \subset [G, N_i] \subset N_{i+1}$ folgt. Insbesondere erhält man $G = G_r \subset N_r = \{1\}$, womit iii) bewiesen ist.
ad $(***)$: Seien $\sigma \in G$, $\tau \in N_i$ und damit $[\sigma, \tau]$ ein typisches Erzeugendes von $[G, N_i]$. Es bezeichne $\bar\sigma$ und $\bar\tau$ die Restklassen in G/N_{i+1}. Wegen $\bar\tau \in N_i/N_{i+1} \subset \mathrm{Zentr}(G/N_i)$ sind die Elemente $\bar\sigma$ und $\bar\tau$ vertauschbar, also $[\sigma, \tau]N_{i+1} = [\bar\sigma, \bar\tau] = \bar 1$. Damit folgt

$$[\sigma, \tau] \in N_{i+1} \text{ für } \sigma \in G\,,\ \tau \in N_i\,,$$

also wie behauptet $[G, N_i] \subset N_{i+1}$.
iii) $\Rightarrow$ i): Man zeigt für beliebige i, j

$$G_i \subseteq Z_j \iff G_{i-1} \subseteq Z_{j+1} \qquad (*)$$

und erhält dann induktiv

$$G_k \subset Z_0(G) = \{1\} \iff G = G_0 \subset Z_k(G)\,.$$

Damit sind i) und iii) äquivalent, und zwar sogar mit demselben Index k.
Beweis von $(*)$:

$$\begin{aligned}
&G_{i-1} \subset Z_{j+1} = \nu_j^{-1}(\mathrm{Zentr}(G/Z_j)) \\
&\iff \nu_j(G_{i-1}) \subset \mathrm{Zentr}(G/Z_j) \\
&\iff \textstyle\bigwedge_{\sigma\in G} \bigwedge_{\tau\in G_{i-1}} \nu_j([\tau, \sigma]) = [\nu_j(\tau), \nu_j(\sigma)] = 1 \\
&\iff G_i = [G, G_{i-1}] \subset \mathrm{Ke}\,\nu_j = Z_j
\end{aligned}$$

i) $\Rightarrow$ iv): Wir setzen $H_0 := H$, $H_{i+1} := \mathcal{N}_G(H_i)$ und zeigen induktiv $Z_i(G) \subset H_i$. Gelte dies also für i. Dann folgt:

$$\begin{aligned}
&z \in Z_{i+1} = \nu_i^{-1}(\mathrm{Zentr}(G/Z_i)) \\
&\iff \textstyle\bigwedge_{\sigma\in G} \nu_i(\sigma)\nu_i(z) = \nu_i(z)\nu_i(\sigma) \\
&\iff \textstyle\bigwedge_{\sigma\in G} \sigma^{-1}z^{-1}\sigma z \in \mathrm{Ke}\,\nu_i = Z_i \subset H_i \\
&\Longrightarrow \textstyle\bigwedge_{\sigma\in H_i} z^{-1}\sigma z \in H_i \\
&\iff z^{-1}H_i z \subset H_i \iff z^{-1}H_i z = H_i \iff z \in H_{i+1}
\end{aligned}$$

(Man beachte bei der vorletzten Äquivalenz die Endlichkeit von H_i!)

Ist nun H eine Untergruppe von G mit $H = \mathcal{N}_G(H)$, so folgt $H = H_i$ für alle i, insbesondere also $G = Z_k(G) \subset H_k = H$, mithin ist H keine echte Untergruppe von G.

iv) $\Rightarrow$ v): Wir zeigen:

$$P \text{ } p\text{-Sylowgruppe } \wedge \ \mathcal{N}_G(P) \subseteq H \subseteq G \implies H = \mathcal{N}_G(H)\,. \qquad (**)$$

Ist dies gezeigt, so folgt unter der Voraussetzung iv) daraus für $H = \mathcal{N}_G(P)$: $H = G$, also $P \triangleleft \mathcal{N}_G(P) = G$: P ist Normalteiler in G.
Nun zum Beweis von $(**)$:

$$\begin{aligned}
&\sigma \in \mathcal{N}_G(H) \implies H = H^\sigma \supset P^\sigma \\
&\implies P \text{ und } P^\sigma \text{ sind } p\text{-Sylowgruppen in } H \text{ (!)} \\
&\implies \bigvee_{h\in H} P^\sigma = P^h \implies \bigvee_{h\in H} P^{\sigma h^{-1}} = P \\
&\implies \bigvee_{h\in H} \sigma h^{-1} \in \mathcal{N}_G(P) \subset H \\
&\implies \sigma \in H
\end{aligned}$$

v) $\Rightarrow$ vi): Seien $p_1, \ldots, p_r$ die Primteiler der Ordnung von G und $P_1, \ldots, P_r$ die zugehörigen Sylowgruppen. Diese sind nach Voraussetzung Normalteiler in G (und daher eindeutig). Wegen der Normalteilereigenschaft der P_i gilt für $\sigma_i \in P_i\,,\ \sigma_j \in P_j$

$$[\sigma_i, \sigma_j] = \begin{cases} (\sigma_i^{-1}\sigma_j^{-1}\sigma_i) \cdot \sigma_j \in P_j^{\sigma_i} P_j = P_j\,, \\ \sigma_i^{-1} \cdot (\sigma_j^{-1}\sigma_i\sigma_j) \in P_i P_i^{\sigma_j} = P_i\,. \end{cases}$$

Da die Sylowgruppen teilerfremde Ordnungen haben, haben sie paarweise trivialen Schnitt: $P_i \cap P_j = \{1\}$ für $i \neq j$, also

$$[P_i, P_j] \subset P_i \cap P_j = \{1\} \text{ für } i \neq j\,.$$

Damit sind die Elemente aus *verschiedenen* P_i miteinander vertauschbar. Wir setzen $G_s := \langle P_1, \ldots, P_s\rangle \subset G$. Wegen der Vertauschbarkeit der P_i erhalten wir Gruppenepimorphismen

$$\varphi_s : P_1 \times \ldots \times P_s \twoheadrightarrow G_s\,,\ (\sigma_1, \ldots, \sigma_s) \mapsto \sigma_1 \cdot \ldots \cdot \sigma_s\,.$$

Wir zeigen nun per Induktion über $s \leq r$, daß diese injektiv sind. Im Falle $s = 1$ ist nichts zu zeigen. Sei $s \geq 2$ und $(\sigma_1, \ldots, \sigma_s)$ im Kern von φ_s. Dann gilt

$$\sigma_s^{-1} = \sigma_1 \cdot \ldots \cdot \sigma_{s-1} \in G_{s-1}$$

Nach Induktionsvoraussetzung ist $G_{s-1} \simeq P_1 \times \ldots \times P_{s-1}$, also $\#G_{s-1} = \prod_{i=1}^{s-1} \#P_i$ teilerfremd zu $\#P_s$. Daraus folgt

$$\sigma_s^{-1} = \sigma_1 \cdot \ldots \cdot \sigma_{s-1} \in P_s \cap G_{s-1} = \{1\}\,.$$

Damit ist $\sigma_s = 1$ und $\sigma_1 \cdot \ldots \cdot \sigma_{s-1} = 1$, woraus nach Induktionsvoraussetzung $\sigma_1 = \ldots = \sigma_{s-1} = 1$ folgt. Insgesamt ist damit die Injektivität von φ_s gezeigt.

Wir erhalten schließlich

$$P_1 \times \ldots \times P_r \xrightarrow{\sim} G_r \subset G\,.$$

Nun gilt nach Definition der p-Sylowgruppen

$$\#G = \prod_{i=1}^{r} \#P_i = \#G_r\,,$$

so daß $G = G_r$ ist und dadurch vi) bewiesen ist.

(2.13) Folgerungen: *Für endliche Gruppen gilt:*

a) *Maximale Untergruppen in nilpotenten Gruppen sind Normalteiler; die zugehörigen Faktorgruppen sind zyklisch von Primzahlordnung.*

b) *Wir bezeichnen für eine Teilmenge M einer Gruppe G mit $\langle\langle M\rangle\rangle$ den kleinsten Normalteiler von G, der M enthält, das sog. Normalteilererzeugnis von M. Mit dieser Bezeichnung gilt in nilpotenten Gruppen:*

$$\langle\langle M\rangle\rangle = G \implies \langle M\rangle = G\,.$$

c) *Endliche abelsche Gruppen sind direktes Produkt abelscher Gruppen von Primzahlpotenzordnung:*

$$A = \bigoplus_p A(p)\,,\ A(p) \text{ abelsche } p\text{-Gruppen der Ordnung } p^r \mid\mid \#A\,.$$

(Dabei bedeutet $p^r \mid\mid m$, daß p^r die höchste p-Potenz ist, die m teilt.)

Beweis: ad a): Aus (2.12), iv) folgt zunächst, daß für eine maximale Untergruppe H von G der Normalisator $\mathcal{N}_G(H) = G$ sein muß, also H Normalteiler ist. In der Faktorgruppe G/H gibt es dann keine echten Untergruppen, da zwischen H und G keine Zwischengruppen existieren. Eine Gruppe $\neq 1$ ohne Untergruppen muß aber Primzahlordnung haben, denn ist p ein Primteiler der Gruppenordnung, so gibt es eine zyklische Untergruppe der Ordnung p, die dann die volle Gruppe sein muß.
b) Ist $\langle M\rangle \neq G$, so liegt M in einer maximalen Untergruppe U von G. Diese ist nach a) Normalteiler in G, also $\langle\langle M\rangle\rangle \subseteq U \neq G$, im Widerspruch zur Voraussetzung.
c) folgt aus (2.12) v), da abelsche Gruppen nilpotent sind (gemäß Charakterisierung i)).

d. Frattinigruppe, Burnsidescher Basissatz

(2.14) Definition: Sei G eine beliebige Gruppe. Die *Frattinigruppe* $\Phi(G)$ von G ist definiert als der Durchschnitt aller maximalen Untergruppen von G:

$$\Phi(G) = \bigcap_{U<G \text{ maximal}} U\,.$$

(2.15) Proposition: *Sei G eine endliche Gruppe.*

a) *$\Phi(G)$ ist eine charakteristische Untergruppe von G, d. h. invariant unter allen Automorphismen von G; insbesondere: $\Phi(G) \lhd G$.*

b) *In jedem Erzeugendensystem von G sind Elemente aus $\Phi(G)$ überflüssig:*

$$\langle M\rangle = G \implies \langle M \setminus \Phi(G)\rangle = G\,.$$

c) *Für $x_1, \ldots, x_d \in G$ gilt:*

$$x_1, \ldots, x_d \text{ erzeugen } G \iff \bar{x}_1, \ldots, \bar{x}_d \text{ erzeugen } \bar{G} = G/\Phi(G)\,.$$

d) *Ist G nilpotent, so ist $G/\Phi(G)$ abelsch. (Es gilt sogar die Umkehrung.)*

e) *Ist G eine p-Gruppe (p eine Primzahl), so ist $G/\Phi(G)$ eine elementar-abelsche p-Gruppe, also eine $\mathbb{F}_p$-Vektorraum.*

Beweis: ad a): Ein Automorphismus von G bildet die Menge aller maximalen Untergruppe in sich ab, läßt also deren Durchschnitt invariant.
ad b): Sei $\langle M\rangle = G$. Ist $\langle M \setminus \Phi(G)\rangle \neq G$, so gibt es eine maximale Untergruppe U von G mit $M \setminus \Phi(G) \subset U$. Wegen $\Phi(G) \subset U$ folgt dann aber $M \subset U$, im Widerspruch zu $\langle M\rangle = G$.
ad c): '$\Rightarrow$' ist klar. Ist umgekehrt $\bar{x}_1, \ldots, \bar{x}_d$ ein Erzeugendensystem für $\bar{G} = G/\Phi(G)$, so wird G von $\Phi(G) \cup \{x_1, \ldots, x_d\}$ erzeugt. Gemäß b) ist $\Phi(G)$ dabei überflüssig und daher $x_1, \ldots, x_d$ ein Erzeugendensystem von G.
ad d): Gemäß (2.13) a) sind maximale Untergruppen U von G Normalteiler und die Faktorgruppen G/U primzyklisch, insbesondere also abelsch. Letzteres bedeutet, daß alle Kommutatoren $[\sigma, \tau] = \sigma^{-1}\tau^{-1}\sigma\tau$ im Kern von $\nu : G \twoheadrightarrow G/U$, also in U liegen. Da dies für alle maximalen Untergruppen gilt, folgt $[G, G] \subset \Phi(G)$, insbesondere ist $G/\Phi(G)$ abelsch.
(Übung: $[G, G]$ ist der kleinste Normalteiler von G mit abelschem Quotienten; $G^{\mathrm{ab}} := G/[G, G]$ ist die größte abelsche Faktorgruppe von G.)
ad e): Hier argumentiert man genauso wie bei d), benutzt nur zusätzlich, daß G/U nach (2.13) a) Primzahlordnung hat. Also gilt in G/U stets $\bar{\sigma}^p = \bar{1}$ und folglich $[G, G]G^p \subset U$. Wieder vererbt sich dies auf den Durchschnitt $\Phi(G)$, so daß auch in $G/\Phi(G)$ alle nichttrivialen Elemente die Ordnung p haben. Dies charakterisiert unter den abelschen Gruppen die p-elementar-abelschen. Diese sind dann nicht nur $\mathbb{Z}$-Moduln (wie alle abelschen Gruppen), sondern sogar $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$-Vektorräume.

(2.16) Satz: (Burnside'scher Basissatz) *Sei p eine Primzahl und G eine p-Gruppe. Dann gilt:*

a) $\Phi(G) = [G, G]G^p$.
$\Phi(G)$ ist der kleinste Normalteiler mit p-elementar-abelschem Quotienten;
$\bar{G} = G/\Phi(G)$ ist der größte p-elementar-abelsche Quotient von G.

b) *$x_1, \ldots, x_d$ minimales Erzeugendensystem von G*
$\iff$ *$\bar{x}_1, \ldots, \bar{x}_d$ $\mathbb{F}_p$-Basis von $G/\Phi(G) = G/[G, G]G^p = G^{\mathrm{ab}}/(G^{\mathrm{ab}})^p$.*

c) *Alle minimalen Erzeugendensysteme von G haben dieselbe Länge d,*
und zwar $d = \dim_{\mathbb{F}_p}(G/\Phi(G))$. d ist charakterisiert durch $p^d = \#(G/\Phi(G))$.

d) *Jedes $x \in G$, $x \notin \Phi(G)$, ist zu einem minimalen Erzeugendensystem von G ergänzbar.*

Beweis: ad a): Nach (2.15) e) ist $G/\Phi(G)$ p-elementar-abelsch. Daher werden alle Elemente aus $[G, G]G^p$ unter $\nu : G \twoheadrightarrow G/\Phi(G)$ auf 1 abgebildet, liegen also im Kern: $[G, G]G^p \subseteq \Phi(G)$.
(Übung: $[G, G]G^p$ ist der kleinste Normalteiler von G mit p-elementar-abelscher Faktorgruppe.)
Wir zeigen nun die umgekehrte Inklusion: Ist $N \triangleleft G$ und G/N p-elementar-abelsch (etwa $N = [G, G]G^p$), so folgt $\Phi(G) \subseteq N$. Angenommen, es gibt ein $x \in \Phi(G)$, $x \notin N$. Dann ist $\bar{x} \in \bar{G} = G/N$ in dem $\mathbb{F}_p$-Vektorraum G/N nicht-trivial und kann daher zu einer $\mathbb{F}_p$-Basis $\bar{x}, \bar{x}_2, \ldots, \bar{x}_d$ von G/N ergänzt werden. Also gilt

$$G = \langle x, x_2, \ldots, x_d, N\rangle .$$

Nach (2.15) b) ist $x \in \Phi(G)$ in dieser Erzeugung überflüssig, also folgt

$$G = \langle x_2, \ldots, x_d, N\rangle .$$

Damit wäre $\bar{x}_2, \ldots, \bar{x}_d$ ein $\mathbb{F}_p$-Erzeugendensystem von G/N, im Widerspruch zur Basiseigenschaft von $\bar{x}, \bar{x}_2, \ldots, \bar{x}_d$.
b) folgt unmittelbar aus (2.15) c). c) und d) sind dann klar, wegen der entsprechenden Eigenschaften in Vektorräumen. □

Anmerkung: Für beliebige nilpotente Gruppen ist die Aussage c) des vorangehenden Satzes falsch. So ist z. B. $\mathbb{Z}/6\mathbb{Z} = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$ nilpotent und hat das minimale Erzeugendensystem $\{\bar{1}\}$ ($\mathbb{Z}/6\mathbb{Z}$ ist zyklisch); aber auch $\{\bar{2}, \bar{3}\}$ ist ein minimales Erzeugendensystem!

Wir wollen zum Abschluß dieses Paragraphen noch die abelschen Gruppen etwas genauer betrachten. Gemäß (2.13) c) ist jede endliche abelsche Gruppe A direkte Summe abelscher p-Gruppen $A(p)$. Für letztere gilt nach dem Burnside'schen Basissatz: $a_1, \ldots, a_d$ minimales Erzeugendensystem von $A(p) \iff \bar{a}_1, \ldots, \bar{a}_d$ $\mathbb{F}_p$-Basis von $A(p)/A(p)^p$.
(Übung: $p \neq q \Rightarrow A(q)^p = A(q)$, $A/A^p \simeq A(p)/A(p)^p$)

Unter diesen minimalen Erzeugendensystemen von $A(p)$ gibt es spezielle, nämlich solche, die eine Zerlegung von $A(p)$ in direkte zyklische Summanden bewirken.

(2.17) Satz: *Jede endliche abelsche Gruppe ist direkte Summe zyklischer Gruppen.*

Dieser Satz ist Teil des Hauptsatzes über endlich erzeugte abelsche Gruppen, der üblicherweise im Rahmen der Algebra-Vorlesung bewiesen wird, und zwar in der Form:

> *Ist R ein Hauptidealring, so gilt:*
> *a) Untermoduln von freien R-Moduln endlichen Ranges sind selbst frei; die Übergangsmatrix zwischen den Basen kann als Diagonalmatrix gewählt werden.*
> *b) Endlich erzeugte Moduln über Hauptidealringen sind direkte Summen zyklischer Moduln.*

Direkter *Beweis* von (2.17): Wegen (2.13) c) genügt es, Satz (2.17) für abelsche p-Gruppen zu beweisen. Wir notieren die Gruppen additiv. Wir schließen induktiv über die Ordnung von A. Sei $a \in A$ von maximaler Ordnung $\operatorname{ord}(a) = p^m$. Da alle Elementordnungen in A p-Potenzen sind, teilen sie p^m, und es gilt für alle $x \in A$ $p^m.x = 0$. Da $A/\langle a\rangle$ kleinere Ordnung als A hat, gilt nach Induktionsvoraussetzung

$$A/\langle a\rangle = \bigoplus_{i=1}^{n} \langle \bar{b}_i\rangle$$

Seien p^{e_i} die Ordnungen der $\bar{b}_i \in A/\langle a\rangle$. Dann gilt

$$p^{e_i} b_i \in \langle a\rangle\,, \text{ also } p^{e_i} b_i = s_i a \text{ mit } s_i \in \mathbb{N}\,.$$

Wegen der Maximalität der Ordnung von a gilt $p^{e_i} = \operatorname{ord}(\bar{b}_i) \leq \operatorname{ord}(b_i) \leq p^m$. Wir bilden nun in obiger Gleichung das p^{m-e_i}-fache und erhalten

$$0 = p^m b_i = s_i p^{m-e_i} a \Longrightarrow \operatorname{ord}(a) = p^m \mid s_i p^{m-e_i} \Longrightarrow p^{e_i} \mid s_i\,.$$

Wir setzen nun

$$t_i = \frac{s_i}{p^{e_i}} \text{ und } a_i = b_i - t_i a\,.$$

Dann ist $\bar{a}_i = \bar{b}_i$ und daher $\operatorname{ord}(a_i) \geq \operatorname{ord}(\bar{a}_i) = p^{e_i}$. Es gilt nun sogar die Gleichheit, denn

$$p^{e_i} a_i = p^{e_i} b_i - t_i p^{e_i} a = s_i a - s_i a = 0\,.$$

Damit folgt $\operatorname{ord}(a_i) = \operatorname{ord}(\bar{a}_i) = p^{e_i}$ und wir zeigen

$$A = \bigoplus_{i=1}^{n} \langle a_i\rangle \oplus \langle a\rangle$$

Ist $x \in A$, so folgt aufgrund der Induktionsvoraussetzung für $A/\langle a\rangle$:

$$\bar{x} = \sum_i \lambda_i \bar{b}_i = \sum_i \lambda_i \bar{a}_i \text{ mit eindeutig bestimmten } 0 \leq \lambda_i < \operatorname{ord}(\bar{a}_i) = \operatorname{ord}(a_i)\,.$$

Daraus folgt dann

$$x - \sum_i \lambda_i a_i = \mu a \text{ mit eindeutig bestimmtem } 0 \leq \mu < p^m = \operatorname{ord}(a)\,.$$

Damit erhält man insgesamt

$$x = \sum_i \lambda_i a_i + \mu a \text{ mit eindeutig bestimmten } 0 \le \lambda_i < \operatorname{ord}(a_i)\,,\ 0 \le \mu < \operatorname{ord}(a)\,.$$

und Satz (2.17) ist bewiesen.

§3 Gruppenerweiterungen

Ein wichtiger Schritt zur Konstruktion von Gruppen ist ihr Aufbau aus einer Untergruppe H und der zugehörigen Faktorgruppe $\mathfrak{g}$. Dabei genügt aber die Kenntnis beider Bestandteile noch nicht, um die Gruppe eindeutig festzulegen: Die Gruppen $C_4 = \mathbb{Z}/4\mathbb{Z}$ und $V_4 = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ haben beide eine zyklische Untergruppe H der Ordnung 2 mit einer zyklischen Faktorgruppe $\mathfrak{g}$ der Ordnung 2, sind aber nicht isomorph. Neben der Struktur von H und $\mathfrak{g}$ muß man die Frage klären, wie sich die Gesamtgruppe G aus den beiden Teilen zusammensetzt. Dies ist Gegenstand dieses Paragraphen.

a. Gruppenerweiterungen, Faktorensysteme

Wir analysieren zunächst die Situation und gehen von einer Gruppe G aus mit einem Normalteiler $H \lhd G$ und der Faktorgruppe $\mathfrak{g} = G/H$. Es sei $\nu : G \twoheadrightarrow \mathfrak{g} = G/H$ der natürliche Epimorphismus. Zu jeder Nebenklasse $\sigma \in \mathfrak{g} = G/H$ wählen wir einen Repräsentanten $u_\sigma \in G$: $\nu(u_\sigma) = \sigma$. Ohne Einschränkung wählen wir das Repräsentantensystem *normiert*, d. h. $u_1 = 1$. Wir erhalten so die Zerlegung

$$G = \dot{\bigcup_{\sigma \in \mathfrak{g}}} u_\sigma H$$

von G in Linksnebenklassen von H. Damit lassen sich alle Elemente von G eindeutig darstellen als $u_\sigma a$ mit $\sigma \in \mathfrak{g}$ und $a \in H$. Um die Struktur von G zu erfassen, muß man die Multiplikation solcher Elemente beschreiben. Dies bedeutet, man muß das Produkt $u_\sigma a \cdot u_\tau b$ in der Form $u_\rho c$ mit $\rho \in \mathfrak{g}$ und $c \in H$ darstellen. Dies leistet die folgende Umformung:

$$u_\sigma a \cdot u_\tau b = u_\sigma u_\tau \cdot u_\tau^{-1} a u_\tau \cdot b =: u_{\sigma\tau} \cdot f(\sigma,\tau) \cdot a^{u_\tau} \cdot b$$

Hierin sind $f(\sigma,\tau) \in H$ und $a^{u_\tau} \in H$, denn: Da ν ein Homomorphismus ist, gilt $\nu(u_\sigma u_\tau) = \sigma\tau = \nu(u_{\sigma\tau})$, also $u_{\sigma\tau}^{-1} u_\sigma u_\tau =: f(\sigma,\tau) \in \operatorname{Ke}\nu = H$. Und wegen $H \lhd G$ gilt $a^{u_\tau} \in H$. Damit hat die rechte Seite der obigen Formel die gewünschte Gestalt der Form $u_\rho \cdot c$ mit $\rho = \sigma\tau \in \mathfrak{g}$ und $c = f(\sigma,\tau) a^{u_\tau} b \in H$.

Wir haben durch diese Überlegungen bei gegebenem Repräsentantensystem u_σ ($\sigma \in \mathfrak{g}$) durch die Multiplikation auf G die folgenden Objekte konstruiert:

1) Faktorensystem: $f : \mathfrak{g} \times \mathfrak{g} \to H$, $(\sigma,\tau) \mapsto f(\sigma,\tau) := u_{\sigma\tau}^{-1} u_\sigma u_\tau$,
2) Automorphismensystem: $\alpha : \mathfrak{g} \to \operatorname{Aut}(H)$, $\sigma \mapsto \alpha_\sigma = u_\sigma^{-1}(\ldots)u_\sigma\,|_H$.

Umgekehrt legen Faktoren- und Automorphismensystem (wieder bei gegebenem Repräsentantensystem) die Multiplikation in G, und damit die Struktur von G, eindeutig fest gemäß der

(M) Multiplikationsformel: $u_\sigma a \cdot u_\tau b = u_{\sigma\tau} \cdot f(\sigma,\tau) a^{\alpha_\tau} b$.

Hier wie im folgenden werden die Automorphismen von G als Exponenten geschrieben. Dadurch operiert die Automorphismengruppe von rechts, wenn man für $\varphi, \psi \in \operatorname{Aut}(G)$ definiert $\varphi\psi = \psi \circ \varphi$. Es gilt dann

$$a^{\alpha_\tau} = \alpha_\tau(a) = u_\tau^{-1} a u_\tau = a^{u_\tau} \text{ für } a \in H\,,\ \tau \in \mathfrak{g}\,.$$

Die Multiplikationsformel ist äquivalent zu den folgenden zwei Formeln:

(R) Repräsentantenmultiplikation: $u_\sigma u_\tau = u_{\sigma\tau} f(\sigma,\tau)$,
(V) Vertauschungsregel: $a \cdot u_\tau = u_\tau a^{\alpha_\tau}$.

Wir wollen nun untersuchen, welche Eigenschaften f und α haben müssen, damit sie auf diese Weise zur Multiplikation in einer Erweiterungsgruppe G von H mit $\mathfrak{g}$ als Faktorgruppe

gehören. Zunächst einmal erhalten wir aus der Normiertheit des Repräsentantensystems die folgende Normiertheitsbedingung für f und α:

(N) $\quad f(\sigma,1)=f(1,\sigma)=1\,,\ \alpha_1=\mathrm{id}_H$

Sodann analysieren wir die Assoziativität der Multiplikation in G. Es gilt:
Die durch (M) gegebene Multiplikation ist genau dann assoziativ, wenn die folgenden beiden Eigenschaften gelten:

$$(F)\quad f(\sigma\tau,\rho)f(\sigma,\tau)^{\alpha_\rho}=f(\sigma,\tau\rho)f(\tau,\rho)\quad \textit{für alle } \sigma,\tau,\rho\in\mathfrak{g}\,,$$
$$(A)\quad \alpha_\sigma\alpha_\tau=\alpha_{\sigma\tau}(\ldots)^{f(\sigma,\tau)}=\alpha_{\sigma\tau}f(\sigma,\tau)\quad \textit{für alle } \sigma,\tau\in\mathfrak{g}\,.$$

[Anmerkung: Bei der exponentiellen Schreibweise von Automorphismen legen wir die Multiplikation $\varphi\psi=\psi\circ\varphi$ in $\mathrm{Aut}(H)$ zugrunde. Diese ist dann auch mit der exponentiellen Schreibweise für die Konjugation $x^h=h^{-1}xh$ verträglich. Auf diese Weise kann jedes Element $h\in H$ auch als innerer Automorphismus von H verstanden werden vermöge $H\to\mathrm{Aut}(H)$, $h\mapsto(\ldots)^h$. Davon wurde in der letzten Gleichung von (A) Gebrauch gemacht.]
Es gilt:

$$\begin{aligned}&(u_\sigma a\cdot u_\tau b)\cdot u_\rho c\\ &=(u_{\sigma\tau}\cdot f(\sigma,\tau)a^{\alpha_\tau}b)\cdot u_\rho c\\ &=u_{\sigma\tau\rho}\cdot f(\sigma\tau,\rho)(f(\sigma,\tau)a^{\alpha_\tau}b)^{\alpha_\rho}c\\ &=u_{\sigma\tau\rho}\cdot f(\sigma\tau,\rho)f(\sigma,\tau)^{\alpha_\rho}a^{\alpha_\tau\alpha_\rho}b^{\alpha_\rho}c\end{aligned}\qquad\qquad\begin{aligned}&u_\sigma a\cdot(u_\tau b\cdot u_\rho c)\\ &=u_\sigma a\cdot(u_{\tau\rho}\cdot f(\tau,\rho)b^{\alpha_\rho}c)\\ &=u_{\sigma\tau\rho}\cdot f(\sigma,\tau\rho)a^{\alpha_{\tau\rho}}f(\tau,\rho)b^{\alpha_\rho}c\\ &=u_{\sigma\tau\rho}\cdot f(\sigma,\tau\rho)f(\tau,\rho)a^{\alpha_{\tau\rho}f(\tau,\rho)}b^{\alpha_\rho}c\end{aligned}$$

Sind (F) und (A) erfüllt, so stimmen beide Seiten der Assoziativitätsgleichung überein. Und umgekehrt ergibt der Vergleich beider Seiten für $a=b=c=1$ zunächst die Eigenschaft (F). Mit $\sigma=1$, $b=c=1$ ergibt sich (unter Beachtung von (N)) für beliebige $a\in H$ die Gleichung $a^{\alpha_\tau\alpha_\rho}=a^{\alpha_{\tau\rho}f(\tau,\rho)}$, also die Gleichheit (A) in der Automorphismengruppe $\mathrm{Aut}(H)$.

Die so gefundenen Eigenschaften (N), (F), (A) sind nicht nur notwendig, sondern auch hinreichend dafür, daß f und α zu einer Erweiterungsgruppe G gehören:

(3.1) Satz: *Seien H, $\mathfrak{g}$ Gruppen und $f:\mathfrak{g}\times\mathfrak{g}\to H$, $\alpha:\mathfrak{g}\to\mathrm{Aut}(H)$ zwei Abbildungen. Dann sind äquivalent:*

i) f und α erfüllen die obigen Eigenschaften (N), (F) und (A).

ii) Es gibt eine Erweiterungsgruppe G von H mit Faktorgruppe $\mathfrak{g}$ und ein normiertes Repräsentantensystem u_σ von $G/H\simeq\mathfrak{g}$, so daß f das zugehörige Faktoren- und α das zugehörige Automorphismensystem ist.

Beweis: Die Implikation 'ii) ⇒ i)' ist oben gezeigt worden. Für 'i) ⇒ ii)' muß man zu f und α eine geeignete Gruppe $G_{\alpha,f}$ konstruieren. Wir setzen als Menge $G=\mathfrak{g}\times H$. Die Multiplikation auf G definieren wir gemäß (M), wobei $u_\sigma=(\sigma,1)$ ist und $a\in H$ mit $(1,a)$ identifiziert wird:

$$(\sigma,a)\cdot(\tau,b):=(\sigma\tau,f(\sigma,\tau)a^{\alpha_\tau}b)\,.$$

Bei dieser Definition ist (wegen (N)) in der Tat $(\sigma,a)=(\sigma,1)\cdot(1,a)=u_\sigma a$. Wie oben gezeigt, folgt aus (F) und (A) die Assoziativität der so definierten Multiplikation. Weiter ist $(1,1)$ Einselement dieser Multiplikation und

$$(\sigma^{-1},(f(\sigma^{-1},\sigma)a^{\alpha_{\sigma^{-1}}})^{-1})\text{ invers zu }(\sigma,a)\,.$$

Damit ist eine Gruppe $G_{\alpha,f}$ definiert und die $u_\sigma=(\sigma,1)$ bilden ein normiertes Repräsentantensystem. Bzgl. dieses Repräsentantensystems ist f das Faktoren- und α das Automorphismensystem von G. □

Durch diesen Satz haben wir die Möglichkeit aus zwei Gruppen H und $\mathfrak{g}$ alle Erweiterungsgruppen G zu konstruieren. Wir müssen nun untersuchen, inwieweit wir dabei verschiedene, d. h. nicht-isomorphe Gruppenerweiterungen erhalten. Dafür müssen wir nun den Begriff der Gruppenerweiterung und ihrer Isomorphien präzisieren.

(3.2) Definition: Seien H und $\mathfrak{g}$ endliche Gruppen.
a) Eine *Gruppenerweiterung* von H durch $\mathfrak{g}$ ist eine Gruppe G mit einem Epimorphismus $\nu : G \twoheadrightarrow \mathfrak{g}$ und einem Isomorphismus $i : H \xrightarrow{\sim} \mathrm{Ke}\,\nu$.
(Die beiden Isomorphismen gehören mit zum Begriff der Gruppenerweiterung! Identifiziert man H vermöge i mit $\mathrm{Ke}\,\nu$, so wird $H = \mathrm{Ke}\,\nu$ Normalteiler in G und vermöge ν die Faktorgruppe $G/H = G/\mathrm{Ke}\,\nu$ isomorph zu $\mathfrak{g}$.)
Man stellt solche Gruppenerweiterungen meist durch kurze exakte Sequenzen dar:

$$(E) \qquad H \overset{i}{\hookrightarrow} G \overset{\nu}{\twoheadrightarrow} \mathfrak{g}$$

Dabei ist die Exaktheit einer solchen Sequenz definiert durch $\mathrm{Im}\, i = \mathrm{Ke}\,\nu$.
b) Ein *Isomorphismus* zweier Gruppenerweiterungen (i, G, ν) und (i', G', ν') ist ein Gruppenisomorphismus $\varphi : G \xrightarrow{\sim} G'$ mit den zusätzlichen Eigenschaften

$$\varphi \circ i = i' \quad \text{und} \quad \nu' \circ \varphi = \nu\,.$$

Diese Bedingung veranschaulicht man vorteilhaft durch kommutative Diagramme exakter Sequenzen:

$$\begin{array}{ccccc} H & \overset{i}{\hookrightarrow} & G & \overset{\nu}{\twoheadrightarrow} & \mathfrak{g} \\ \| & /\!/\!/ & \downarrow \varphi & /\!/\!/ & \| \\ H & \overset{i'}{\hookrightarrow} & G' & \overset{\nu'}{\twoheadrightarrow} & \mathfrak{g} \end{array}$$

Die obigen Bedingungen besagen gerade, daß die beiden Teilquadrate des Diagramms kommutativ sind (gekennzeichnet durch das Zeichen $/\!/\!/$); das bedeutet: Verfolgt man Abbildungen längs verschiedener 'Wege', so erhält man doch immer dasselbe Ergebnis.

Wir analysieren nun für zwei isomorphe Gruppenerweiterungen (i, G, ν) und (i', G', ν') von H durch $\mathfrak{g}$ die Automorphismen- und Faktorensysteme. Seien u_σ und u'_σ Repräsentantensysteme in G bzw. G', d. h. $\nu(u_\sigma) = \sigma = \nu'(u'_\sigma)$ für alle $\sigma \in \mathfrak{g}$ und (α, f) bzw. (α', f') die dadurch festgelegten Automorphismen- und Faktorensysteme (siehe 1) und 2)). Ist nun $\varphi : G' \xrightarrow{\sim} G$ ein Isomorphismus *der Gruppenerweiterungen*, so gilt $\nu\varphi(u'_\sigma) = \nu'(u'_\sigma) = \sigma$. Damit ist $\varphi(u'_\sigma)$ $(\sigma \in \mathfrak{g})$ neben u_σ ein zweites Repräsentantensystem derselben Gruppenerweiterung (i, G, ν). Und das dazu gehörende Automorphismen- und Faktorensystem ist (α', f'). Damit ist das Isomorphieproblem auf die Frage zurückgeführt: Wie ändern sich Automorphismensystem α und Faktorensystem f bei Änderung des Repräsentantensystems?

Sei also u_σ ein Repräsentantensystem von G/H und $u'_\sigma = u_\sigma h_\sigma$ ein zweites ($h_\sigma \in H$ normiert, d. h. $h_1 = 1$). Dann gilt:

$$\begin{aligned} f'(\sigma,\tau) &= (u_{\sigma\tau}h_{\sigma\tau})^{-1}u_\sigma h_\sigma u_\tau h_\tau = h_{\sigma\tau}^{-1}u_{\sigma\tau}^{-1}u_\sigma u_\tau u_\tau^{-1}h_\sigma u_\tau h_\tau \\ &= h_{\sigma\tau}^{-1} f(\sigma,\tau) h_\sigma^{\alpha_\tau} h_\tau\,, \\ \alpha'_\sigma &= (\ldots)^{u_\sigma h_\sigma}\,|_H = (\ldots)^{u_\sigma}\,|_H (\ldots)^{h_\sigma}\,|_H \\ &= \alpha_\sigma h_\sigma \in \mathrm{Aut}(H)\,. \end{aligned}$$

Anmerkung: Die letzte Beziehung zwischen α_σ, α'_σ und h_σ ist eine Gleichung *in* $\mathrm{Aut}(H)$. Sie besagt, daß sich α_σ und α'_σ um einen *inneren* Automorphismus von H unterscheiden, und daß h_σ diesen inneren Automorphismus liefert.

(3.3) Satz: *Seien $\mathfrak{g}$ und H zwei endliche Gruppen. Dann gibt es eine Bijektion zwischen:*

A) Isomorphieklassen von Gruppenerweiterungen $H \overset{i}{\hookrightarrow} G \overset{\nu}{\twoheadrightarrow} \mathfrak{g}$ und

B) Äquivalenzklassen von Funktionen $\alpha : \mathfrak{g} \to \mathrm{Aut}(H)$, $f : \mathfrak{g} \times \mathfrak{g} \to H$ mit den Eigenschaften (N), (F), (A) bzgl. der Äquivalenzrelation

$$(\alpha, f) \sim (\alpha', f') \iff \bigvee_{\substack{h:\mathfrak{g}\to H \\ h \text{ normiert}}} \begin{cases} f'(\sigma,\tau) = h_{\sigma\tau}^{-1} f(\sigma,\tau) h_\sigma^{\alpha_\tau} h_\tau \,, \\ \alpha'_\sigma = \alpha_\sigma h_\sigma \in \mathrm{Aut}(H) \,. \end{cases}$$

Die Bijektion ist folgendermaßen definiert: Bei gegebener Gruppenerweiterung wähle man ein beliebiges normiertes Repräsentantensystem von $\mathfrak{g}$ und definiere damit α und f gemäß 1), 2). Umgekehrt ordne man irgendeinem Paar (α, f) die im Beweis von (3.1) konstruierte Gruppenerweiterung $G_{\alpha,f}$ zu.

Beweis: Wie oben gezeigt, führen isomorphe Gruppenerweiterungen zu äquivalenten Paaren (α, f). Die Abbildung in der einen Richtung ist wohldefiniert. Für die Umkehrabbildung muß man zeigen, daß äquivalente Paare zu isomorphen Gruppenerweiterungen $(i, G_{\alpha,f}, \nu) \simeq (i', G_{\alpha',f'}, \nu')$ führen. Sei $h : \mathfrak{g} \to H$ die die Äquivalenz herstellende Abbildung. Dann definieren wir (geleitet durch $\varphi(u'_\sigma a) = u_\sigma h_\sigma a$):

$$\varphi : G_{\alpha',f'} \to G_{\alpha,f} \,,\ (\sigma, a)' \mapsto (\sigma, h_\sigma a) \,.$$

Zunächst gilt $\varphi i'(a) = \varphi((1,a)') = (1,a) = i(a)$ und $\nu\varphi((\sigma,a)') = \nu((\sigma, h_\sigma a)) = \sigma = \nu'((\sigma,a)')$. Die Umkehrabbildung zu φ definiert man analog mittels a_σ^{-1}. Es bleibt zu zeigen, daß φ ein Gruppenhomorphismus ist:

$$\begin{aligned} \varphi((\sigma,a)'(\tau,b)') &= \varphi((\sigma\tau, f'(\sigma,\tau) a^{\alpha'_\tau} b)') = (\sigma\tau, h_{\sigma\tau}\, f'(\sigma,\tau) a^{\alpha'_\tau} b) \\ &= (\sigma\tau, f(\sigma,\tau) h_\sigma^{\alpha_\tau} h_\tau\, a^{\alpha_\tau h_\tau} b) = (\sigma\tau, f(\sigma,\tau) h_\sigma^{\alpha_\tau}\, a^{\alpha_\tau} h_\tau\, b) \\ &= (\sigma\tau, f(\sigma,\tau)(h_\sigma a)^{\alpha_\tau} h_\tau b) = (\sigma, h_\sigma a)(\tau, h_\tau b) \\ &= \varphi((\sigma,a)')\, \varphi((\tau,b)') \,. \end{aligned}$$

Damit ist Satz (3.3) bewiesen. (Da Isomorphie eine Äquivalenzrelation ist, zeigt der Beweis auch, daß die Relation $\sim$ eine Äquivalenzrelation ist. Eine Tatsache, die man natürlich auch direkt nachrechnen kann.)

b. Semidirekte Produkte, Komplemente

In diesem Abschnitt studieren wir den Spezialfall $f = 1$, d. h. Gruppenerweiterungen mit trivialem Faktorensystem. Dies bedeutet für die Multiplikation der Repräsentanten: $u_\sigma u_\tau = u_{\sigma\tau}$. Die Repräsentanten bilden also eine zu $\mathfrak{g}$ isomorphe Untergruppe von G. Für Gruppenerweiterungen (i, G, ν) von H durch $\mathfrak{g}$ gilt daher:

$$f = 1 \iff \bigvee_{U \le G} \nu : U \xrightarrow{\sim} \mathfrak{g} \,.$$

Identifiziert man H vermöge i mit dem Kern von ν, so erhält man:

$$U \cap H = \{1\} \,, \quad G = U \cdot H \,,$$

bzw. äquivalent dazu: Jedes $g \in G$ ist eindeutig darstellbar als $g = ua$ mit $u \in U$, $a \in H$. Die Gruppenstruktur von G ist durch die Vertauschungsregel festgelegt: Für $U \ni u \mapsto \sigma \in \mathfrak{g}$ gilt $au = ua^{\alpha_\sigma}$ bzw. $au = ua^{\alpha_{\nu(u)}}$. Nun ergibt sich gemäß (A) aus $f = 1$, daß α ein Gruppenhomomorphismus ist:

$$\alpha : \mathfrak{g} \to \mathrm{Aut}(H) \,.$$

α beschreibt also eine Operation von $\mathfrak{g}$ auf der *Gruppe* H (durch Gruppenautomorphismen). Diese legt die Vertauschungsregel in der Gruppenerweiterung fest.

Diesen speziellen Typ von Gruppenerweiterungen nennen wir *semidirektes Produkt* von $\mathfrak{g}$ mit H zur Operation α von $\mathfrak{g}$ auf H. Für die triviale Operation ($\alpha = 1$) erhält man das *direkte Produkt* von Gruppen.

(3.4) Definition: a) Seien $\mathfrak{g}$ und H endliche Gruppen und $\alpha : \mathfrak{g} \to \mathrm{Aut}(H)$ ein Gruppenhomomorphismus.
Das *semidirekte Produkt* $H \rtimes \mathfrak{g}$ von H mit $\mathfrak{g}$ zur Operation α ist (bis auf Isomorphie) die Gruppenerweiterung $G := G_{\alpha,1}$. Explizit (mit den obigen Bezeichnungen):

$$H \rtimes \mathfrak{g} = \{(\sigma, a) \mid \sigma \in \mathfrak{g},\ a \in H\}, \quad (\sigma, a) \cdot (\tau, b) = (\sigma\tau, a^{\alpha_\tau} b)\,.$$

bzw. äquivalent dazu: $H \rtimes \mathfrak{g} = G$ mit

$$H \lhd G, \quad \mathfrak{g} \simeq U \leq G, \quad U \cap H = 1 \quad \text{und} \quad au = ua^{\alpha_{\nu(u)}} \text{ für alle } u \in U,\ a \in H\,.$$

b) Sei G eine Gruppe und $H \lhd G$. Ein *Komplement* zu H in G ist eine Untergruppe $U \leq G$ mit den äquivalenten Eigenschaften:

i) Jedes $g \in G$ ist eindeutig darstellbar als $g = ua$ mit $u \in U$, $a \in H$.

ii) Der natürliche Epimorphismus $\nu : G \twoheadrightarrow G/H$ induziert einen Isomorphismus $\nu : U \xrightarrow{\sim} G/H$.

iii) $U \cap H = 1$ und $G = U \cdot H$.

(3.5) Proposition: *a) Ist G semidirektes Produkt von H und $\mathfrak{g}$, so besitzt $H \lhd G$ ein Komplement.*
b) Besitzt $H \lhd G$ ein Komplement, so ist G semidirektes Produkt von H und $\mathfrak{g} := G/H$ bzgl. der folgenden Operation von $\mathfrak{g}$ auf H:
Man wähle ein Komplement U und dann zu jedem $\sigma \in \mathfrak{g}$ ein Urbild $u_\sigma \in U$. α_σ ist dann die Konjugation mit u_σ auf H.
c) Eine Gruppenerweiterung $G_{\alpha,f}$ von H durch $\mathfrak{g}$ ist semidirektes Produkt von H und $\mathfrak{g}$ (man sagt: sie zerfällt) genau dann, wenn ein normiertes $h : \mathfrak{g} \to H$ existiert mit

$$f(\sigma, \tau) = h_{\sigma\tau} h_\tau^{-1} h_\sigma^{-\alpha_\tau}\,.$$

Beweis: a) ist klar. b): Sei U ein Komplement. Wir zeigen zuerst, daß α ein Homomorphismus ist: Zu $\sigma, \tau \in \mathfrak{g}$ seien u_σ, u_τ die Repräsentanten in U. Da U Untergruppe ist, ist $u_\sigma u_\tau \in U$ der Repräsentant von $\sigma\tau$ in U. Daraus folgt dann $\alpha_\sigma \alpha_\tau = \alpha_{\sigma\tau}$.
Nach Voraussetzung ist jedes Element von G eindeutig darstellbar als $u_\sigma a$ und es gilt $au_\sigma = u_\sigma u_\sigma^{-1} a u_\sigma = u_\sigma a^{u_\sigma} = u_\sigma a^{\alpha_\sigma}$. Damit erhält man den Isomorphismus

$$G \xrightarrow{\sim} H \rtimes \mathfrak{g}, \quad u_\sigma a \mapsto (\sigma, a)\,.$$

c) Nach Satz (3.3) ist $G_{\alpha,f}$ isomorph zum semidirekten Produkt $H \rtimes \mathfrak{g} = G_{\alpha',1}$ bzgl. einer gewissen Operation α', wenn (α, f) äquivalent ist zu $(\alpha', 1)$, d. h. wenn ein normiertes $h : \mathfrak{g} \to H$ existiert mit $\alpha'_\sigma = \alpha_\sigma h_\sigma$ und $1 = h_{\sigma\tau}^{-1} f(\sigma, \tau) h_\sigma^{\alpha_\tau} h_\tau$. Die erste Eigenschaft definiert α', während die zweite äquivalent ist zur Aussage in c). □

Mit den semidirekten Produkten eng verbunden sind die sog. *Kranzprodukte*

(3.6) Definition: Seien $H, \mathfrak{g}$ Gruppen.

a) Ist für ein $k \in \mathbb{N}_+$ zusätzlich eine Operation $\mathfrak{g} \to \mathcal{S}_k$ von $\mathfrak{g}$ auf $\Omega = \{1, \ldots, k\}$ gegeben, so definiert man das *Kranzprodukt* $H \wr \mathfrak{g}$ (bzgl. dieser Operation) als das semidirekte Produkt

$$H \wr \mathfrak{g} = H^k \rtimes \mathfrak{g} = \underbrace{H \times \ldots \times H}_{k-\text{mal}} \rtimes \mathfrak{g}$$

wobei die Operation von $\mathfrak{g}$ auf H^k durch Permutation der k Faktoren erfolgt:

$$\sigma \in \mathfrak{g}\,,\ a = (a_1, \ldots, a_k) \in H^k \implies \sigma a = (a_{\sigma 1}, \ldots a_{\sigma k})\,.$$

[Die Abhängigkeit des Kranzprodukts von der Operation von $\mathfrak{g}$ wird im Symbol nicht ausgedrückt.]

b) Das *reguläre Kranzprodukt* $H \wr \mathfrak{g}$ ist definiert als Kranzprodukt von H mit $\mathfrak{g}$ bzgl. der regulären Operation von $\mathfrak{g}$ auf sich selbst:

$$H \wr \mathfrak{g} = H^{\mathfrak{g}} \rtimes \mathfrak{g} \quad \text{mit der Operation von } \ \sigma \in \mathfrak{g} \ \text{ auf } \ H^{\mathfrak{g}}: \quad ((g_\tau)_{\tau\in\mathfrak{g}})^\sigma = (g_{\sigma\tau})_{\tau\in\mathfrak{g}})\,.$$

[Das reguläre Kranzprodukt ist nur von den beiden Gruppen abhängig.]

(3.7) Proposition: *Jede Gruppenerweiterung $H \hookrightarrow G \twoheadrightarrow \mathfrak{g}$ ist Untergruppe des regulären Kranzproduktes $H \wr \mathfrak{g}$.*

Beweis: Wir verwenden die Bezeichnungen wie zum Beginn von Abschnitt a.: Sei $G = \dot{\bigcup\limits_{\sigma\in\mathfrak{g}}} u_\sigma H$ eine Nebenklassenzerlegung von G nach H mit $\nu(u_\sigma) = \sigma$. Dann erhält man für jedes $g \in G$ und $\sigma \in \mathfrak{g}$ eine eindeutige Darstellung der Form

$$g u_\sigma = u_\tau \hat{g}_\sigma \quad \text{mit eindeutigen} \quad \hat{g}_\sigma \in H\,,\ \tau \in \mathfrak{g}\,. \tag{$*$}$$

Also bestimmt jedes $g \in G$ ein

$$\hat{g} = (\hat{g}_\tau)_{\tau\in\mathfrak{g}} \in H^{\mathfrak{g}}\,.$$

Unter Anwendung des kanonischen Epimorphismus $\nu : G \twoheadrightarrow \mathfrak{g}$ erhält man die Beziehungen

$$\nu(g u_\sigma) = \nu(g)\sigma\,, \quad \nu(g u_\sigma) = \nu(u_\tau \hat{g}_\sigma) = \tau\,, \quad \tau = \nu(g)\sigma = \bar{g}\sigma$$

und damit

$$g u_\sigma = u_{\bar{g}\sigma} \cdot \hat{g}_\sigma \quad \text{für alle } g \in G\,,\ \sigma \in \mathfrak{g}\,.$$

Wir definieren nun

$$\Phi : G \to H \rtimes \mathfrak{g}\,, \quad g \mapsto (\bar{g}, \hat{g})\,.$$

Nachweis der Homomorphie: Es ist $\Phi(gg') = (\bar{g}\bar{g}', \widehat{gg'})$ und wir berechnen $\widehat{gg'}$:

$$gg' u_\sigma = g \cdot u_{\bar{g}'\sigma} \widehat{g'}_\sigma = u_{\bar{g}\bar{g}'\sigma} \hat{g}_{\bar{g}'\sigma} \widehat{g'}_\sigma\,, \ \text{also} \quad (\widehat{gg'})_\sigma = \hat{g}_{\bar{g}'\sigma}\ g'_\sigma\,.$$

Nun zum Produkt $\Phi(g)\Phi(g') \in H \wr \mathfrak{g} = H^{\mathfrak{g}} \rtimes \mathfrak{g}$:

$$\Phi(g)\cdot\Phi(g) = (\bar{g}, \hat{g}) \cdot (\bar{g'}, \hat{g'}) = \bar{g}\hat{g} \cdot \bar{g'}\hat{g'} = \bar{g}(\hat{g}_\sigma)_{\sigma\in\mathfrak{g}} \cdot \bar{g'}\hat{g'} = \bar{g}\bar{g'} \cdot (\hat{g}_\sigma)^{\bar{g'}}_{\sigma\in\mathfrak{g}} \cdot \hat{g'} = \bar{g}\bar{g'} \cdot (\hat{g}_{\bar{g'}\sigma})_{\sigma\in\mathfrak{g}} \cdot \hat{g'}\,.$$

Damit ist die Homomorphie bewiesen und wir bestimmen nun den Kern:

$$1 = \Phi(g) = (\bar{g}, \hat{g}) = 1 \implies \bar{g} = 1 \ \wedge \bigwedge_{\sigma\in\mathfrak{g}} \hat{g}_\sigma = 1 \implies g \in H \ \wedge \ g = g \cdot u_1 = u_{\bar{g}\cdot 1} \cdot \hat{g}_1 = \hat{g}_1 = 1\,.$$

Also ist $\operatorname{Ke}\Phi = \{1\}$ und Proposition (3.7) bewiesen. □

Wir wollen nun speziell sog. *teilerfremde Gruppenerweiterungen* studieren. Darunter verstehen wir Gruppenerweiterungen $H \hookrightarrow G \twoheadrightarrow \mathfrak{g}$, bei denen $\#H$ und $\#\mathfrak{g}$ teilerfremd sind. Dies hat zur Folge, daß jede Untergruppe $U \le G$ mit $\#U = \#\mathfrak{g}$ ein Komplement zu H ist: Da $U \cap H$ eine Ordnung hat, die $\#\mathfrak{g}$ *und* $\#H$ teilt, muß diese gleich 1 sein, d. h. $U \cap H = \{1\}$. Damit ist die natürliche Abbildung $\nu : G \twoheadrightarrow G/H = \mathfrak{g}$ eingeschränkt auf U injektiv: $\nu|_U : U \hookrightarrow \mathfrak{g}$. Wegen $\#U = \#\mathfrak{g}$ ist sie dann auch surjektiv: $U \xrightarrow{\sim} \mathfrak{g}$.

(3.8) Satz: (Zassenhaus) *Teilerfremde Gruppenerweiterungen zerfallen, d. h. zu einem Normalteiler $H \lhd G$, dessen Ordnung $\#H$ teilerfremd ist zu seinem Index $(G : H)$, existiert stets ein Komplement.*
Zusatz ohne Beweis: *Alle Komplemente sind in G konjugiert.*

Beweis: Sei G ein Gegenbeispiel kleinster Ordnung. Dann gibt es einen Normalteiler $H \lhd G$ mit $\#H$ teilerfremd zu $(G:H)$, aber es gibt keine Untergruppe $U \leq G$ mit $\#U = (G:H)$. Wir zeigen:
1) *H ist nilpotent:* Ist $P \leq H$ eine Sylowuntergruppe von H, so gilt $\tilde{H} := \mathcal{N}_G(P) \cdot H = G$, denn:

$$\begin{aligned} g \in G &\Longrightarrow P^g \leq H^g = H \text{ Sylowuntergruppe} \\ &\Longrightarrow \bigvee_{h \in H} P^g = P^h \Longrightarrow gh^{-1} \in \mathcal{N}_G(P) \\ &\Longrightarrow g \in \mathcal{N}_G(P) \cdot H\,. \end{aligned}$$

Schränkt man die natürliche Abbildung $\nu : G \to G/H$ ein auf $\mathcal{N}_G(P)$, so ist diese wegen $\mathcal{N}_G(P)H = G$ immer noch surjektiv: $\nu : \mathcal{N}_G(P) \twoheadrightarrow G/H$, so daß aus dem Homomorphiesatz folgt

$$\mathcal{N}_G(P)/\mathcal{N}_G(P) \cap H \xrightarrow{\sim} G/H\,.$$

Damit enthält $G' = \mathcal{N}_G(P)$ einen Normalteiler $H' = \mathcal{N}_G(P) \cap H = \mathcal{N}_H(P)$, dessen Ordnung (die $\#H$ teilt) prim ist zum Index $(G':H') = (G:H)$. Da G keine Untergruppe der Ordnung $(G:H)$ enthält, gilt dies erst recht für die Untergruppe G'. Aufgrund der Minimalität von G folgt $G = G' = \mathcal{N}_G(P)$, $P \lhd G$. Insbesondere $P \lhd H$ für alle Sylowuntergruppen von H. Damit ist H nilpotent (siehe Satz (2.12) v)).
2) *H ist abelsch:* Angenommen $H' = [H,H] \neq 1$. Dann ist H' als charakteristische Untergruppe von $H \lhd G$ ein Normalteiler in G und die Gruppe $\bar{G} = G/H'$ hat kleinere Ordnung als G. In dieser Gruppe gibt es einen Normalteiler $\bar{H} = H/H'$, dessen Ordnung (die $\#H$ teilt) prim ist zu $(\bar{G}:\bar{H}) = (G:H)$ (H ist das volle Urbild von $\bar{H}$ unter $G \twoheadrightarrow \bar{G}$, Bemerkung (2.11)). Wegen der Minimalität von G muß also in $\bar{G}$ ein Komplement für $\bar{H}$ existieren.
Sei $\bar{U} = U/H'$, $H' \leq U \leq G$, ein solches Komplement, also $\#\bar{U} = (\bar{G}:\bar{H}) = (G:H)$. Damit enthält U einen Normalteiler H', dessen Ordnung $\#H'$ ($\mid \#H$) teilerfremd ist zu $(U:H') = \#\bar{U} = (G:H)$. Nun existiert in G, also erst recht in U, keine Untergruppe der Ordnung $(G:H)$; U ist also ebenfalls ein Gegenbeispiel zu Satz (3.8). Aufgrund der Minimalität von G muß $U = G$ sein. Dann folgt aber $(G:H') = (U:H') = (G:H)$, also $\#H' = \#H$. Dies bedeutet $H = H' = [H,H]$, ein Widerspruch zur Nilpotenz von H (siehe (2.12) iii)). Die Annahme $H' \neq 1$ war also falsch: $H' = 1$, H ist abelsch.

Damit ist Satz (3.8) zurückgeführt auf den nachfolgenden Satz, der abelsche Normalteiler behandelt, für diese aber ein verschärftes Resultat liefert.

(3.9) Satz: *Sei $A \lhd G$ ein abelscher Normalteiler und $\#A$ teilerfremd zum Index $(G:A)$. Dann besitzt A ein Komplement in G und alle Komplemente sind untereinander konjugiert in G.*

Ist dieser Satz bewiesen, so folgt (3.8), denn wie oben gezeigt hat das minimimale Gegenbeispiel einen abelschen Normalteiler; für diesen existiert gemäß (3.9) aber ein Komplement. Folglich gibt es kein Gegenbeispiel zu (3.8).

Das Studium abelscher Normalteiler und der Beweis von (3.9) ist Gegenstand des nächsten Abschnittes.

c. Abelsche Normalteiler, Kohomologiegruppen

Wir betrachten Gruppenerweiterungen $A \hookrightarrow G \twoheadrightarrow \mathfrak{g}$ mit abelschem, additiv geschriebenem Kern A. Aufgrund der Kommutativität sind alle inneren Automorphismen von A trivial. Daraus folgt: Das Automorphismensystem $\alpha : \mathfrak{g} \to \mathrm{Aut}(A)$ ist ein *Gruppenhomomorphismus* und außerdem vom Repräsentantensystem *unabhängig:*

$$\begin{aligned} f(\sigma,\tau) \in A &\Longrightarrow \alpha_\sigma \alpha_\tau = \alpha_{\sigma\tau}(\ldots)^{f(\sigma,\tau)} = \alpha_{\sigma\tau} \\ a_\sigma \in A\,,\ u'_\sigma = u_\sigma a_\sigma &\Longrightarrow \alpha'_\sigma = \alpha_\sigma(\ldots)^{a_\sigma} = \alpha_\sigma\,. \end{aligned}$$

Da α ein Gruppenhomomorphismus ist, erhält man durch die Festetzung $a^\sigma := a^{\alpha_\sigma}$ eine Operation von $\mathfrak{g}$ auf A, denn: $(a^\sigma)^\tau = a^{\alpha_\sigma \alpha_\tau} = a^{\alpha_{\sigma\tau}} = a^{\sigma\tau}$. Wegen $\alpha_\sigma \in \mathrm{Aut}(A)$ gilt weiter $(a+b)^\sigma = a^\sigma + b^\sigma$. Damit wird A zu einem *$\mathfrak{g}$-Modul.* Also:

Gruppenerweiterungen $A \hookrightarrow G \twoheadrightarrow \mathfrak{g}$ mit abelschem Kern bestimmen eine $\mathfrak{g}$-Modulstruktur auf A vermöge

$$a^\sigma = a^{\alpha_\sigma} = u_\sigma^{-1} a u_\sigma \text{ für } a \in A\,,\ \sigma \in \mathfrak{g}\,,\ u_\sigma \in G \text{ mit } \nu(u_\sigma) = \sigma\,.$$

Da die Operation α vom Repräsentantensystem unabhängig ist, definieren isomorphe Gruppenerweiterungen *dieselbe* $\mathfrak{g}$-Modulstruktur auf A. Man unterteilt daher die Gesamtheit aller Gruppenerweiterungen zunächst nach den verschiedenen $\mathfrak{g}$-Modulstrukturen auf A, und untersucht dann die Gruppenerweiterungen $A \hookrightarrow G \twoheadrightarrow \mathfrak{g}$ bei *fester* $\mathfrak{g}$-Modulstruktur auf A. Diese Gruppenerweiterungen werden beschrieben durch die zugehörigen
Faktorensysteme *des $\mathfrak{g}$-Moduls A*:

$$f : \mathfrak{g} \times \mathfrak{g} \to A\,, \quad f(\sigma\tau, \rho) + f(\sigma, \tau)^\rho = f(\sigma, \tau\rho) + f(\tau, \rho)$$

Satz (3.3) ergibt dann für eine endliche Gruppe $\mathfrak{g}$ und einen $\mathfrak{g}$-Modul A:

Die Isomorphieklassen von Gruppenerweiterungen $A \hookrightarrow G \twoheadrightarrow \mathfrak{g}$ mit der vorgegebenen Operation von $\mathfrak{g}$ auf A entsprechen bijektiv den Faktorensystemen $f : \mathfrak{g} \times \mathfrak{g} \to A$ des $\mathfrak{g}$-Moduls A modulo der Äquivalenzrelation:

$$f \sim f' \iff \bigvee_{a:\mathfrak{g}\to A} f'(\sigma, \tau) - f(\sigma, \tau) = a_\sigma^\tau + a_\tau - a_{\sigma\tau}\,.$$

Wir haben dabei die Normiertheitsbedingung sowohl bei f als auch bei a fallen gelassen. Dies ändert nichts an der obigen Formulierung von (3.3), da man ein beliebiges f mittels eines geeigneten a äquivalent normieren kann. (Man wähle a mit $a_1 = -f(1,1)$ und $a_\sigma = 0$ für $\sigma \neq 1$.)

Durch diese Beschreibung erhält man auf der Menge aller Gruppenerweiterungen von A mit $\mathfrak{g}$, die eine feste $\mathfrak{g}$-Modulstruktur auf A bestimmen, die Struktur einer *abelschen Gruppe.* Wir stellen dies hier in den Rahmen der Kohomologie von $\mathfrak{g}$-Moduln.

Definition der Kohomologiegruppen:
Man definiert für $n \geq 0$ die Gruppe der *n-Koketten*

$$C^n(\mathfrak{g}, A) := \{f : \mathfrak{g}^n \to A \mid f \text{ Abbildung}\}$$

und die Korandabbildungen

$$\begin{aligned}
&\partial^n : C^n(\mathfrak{g}, A) \to C^{n+1}(\mathfrak{g}, A)\,,\ f \mapsto \partial^n f \\
&(\partial^n f)(\sigma_1, \ldots, \sigma_{n+1}) = f(\sigma_2, \ldots, \sigma_{n+1}) + \ldots \\
&\qquad \ldots + \textstyle\sum_{i=1}^n (-1)^i f(\sigma_1, \ldots, \sigma_{i-1}, \sigma_i\sigma_{i+1}, \sigma_{i+2}, \ldots, \sigma_{n+1}) + \ldots \\
&\qquad \ldots + (-1)^{n+1} (f(\sigma_1, \ldots, \sigma_n))^{\sigma_{n+1}}
\end{aligned}$$

Dabei ist $\mathfrak{g}^0$ einelementig und daher $C^0(\mathfrak{g}, A) = A$; für $f = a \in C^0(\mathfrak{g}, A)$ ist $\partial^0 f(\sigma) = a - a^\sigma$.

Man erhält so eine Sequenz abelscher Gruppen und Homomorphismen

$$0 \xrightarrow{\partial^{-1}} A \xrightarrow{\partial^0} C^1(\mathfrak{g}, A) \xrightarrow{\partial^1} C^2(\mathfrak{g}, A) \xrightarrow{\partial^2} C^3(\mathfrak{g}, A) \to \cdots\,.$$

Dies ist ein *Komplex* abelscher Gruppen, d. h. es gilt

$$\partial^n \circ \partial^{n-1} = 0\,, \quad \text{bzw.} \quad \operatorname{Im} \partial^{n-1} \subset \operatorname{Ke} \partial^n\,.$$

Man definiert nun die

$$\begin{aligned}
&\text{Gruppe der } n\text{-Kozyklen:} && Z^n(\mathfrak{g}, A) := \operatorname{Ke} \partial^n \leq C^n(\mathfrak{g}, A)\,, \\
&\text{Gruppe der } n\text{-Koränder:} && B^n(\mathfrak{g}, A) := \operatorname{Im} \partial^{n-1} \leq Z^n(\mathfrak{g}, A) \leq C^n(\mathfrak{g}, A)\,, \\
&n\text{-te Kohomologiegruppe:} && H^n(\mathfrak{g}, A) := Z^n(\mathfrak{g}, A)/B^n(\mathfrak{g}, A)\,.
\end{aligned}$$

Die Kohomologiegruppen sind wichtige Invarianten des $\mathfrak{g}$-Moduls A. Eine systematische Untersuchung dieser Gruppen, insbesondere ihres funktoriellen Verhaltens (Änderung von $\mathfrak{g}$, A), führt zu einem Aufbau eines aufwendigen, aber wirkungsvollen Formalismus, der insbesondere die Berechnung solcher Kohomologiegruppen ermöglicht.

Wir wollen hier unser Klassifikationsproblem für Gruppenerweiterungen in Termen von Kohomologiegruppen *formulieren.* Das angestrebte Resultat erweist sich dann als eine Aussage über Kohomologiegruppen. Diese Aussage werden wir aber *direkt* beweisen (ohne Rückgriff auf allgemeine Resultate über Kohomologiegruppen).

Gruppenerweiterungen und Kohomologiegruppen:
Man zeigt zunächst, daß die oben betrachteten Faktorensysteme des $\mathfrak{g}$-Moduls A nichts anderes sind als die 2-Kozyklen. Es gilt nämlich:

$$f : \mathfrak{g} \times \mathfrak{g} \to A \implies \partial^2 f(\sigma, \tau, \rho) = f(\tau, \rho) - f(\sigma\tau, \rho) + f(\sigma, \tau\rho) - f(\sigma, \tau)^\rho \,,$$

und daher

$$f \in Z^2(\mathfrak{g}, A) \iff \partial^2 f = 0 \iff f(\sigma\tau, \rho) + f(\sigma, \tau)^\rho = f(\sigma, \tau\rho) + f(\tau, \rho) \,.$$

Die letzte Bedingung ist gerade die charakterisierende Eigenschaft der Faktorensysteme.

Auch die Äquivalenzrelation $\sim$ ist beschreibbar in kohomologischen Termen.
Für $a \in C^1(\mathfrak{g}, A)$, $\sigma \mapsto a_\sigma$, gilt nämlich

$$\partial^1 a(\sigma, \tau) = a_\tau - a_{\sigma\tau} + a_\sigma^\tau \,,$$

also

$$f \sim f' \iff \bigvee_{a:\mathfrak{g}\to A} f - f' = \partial^1 a \iff f - f' \in \operatorname{Im} \partial^1 = B^2(\mathfrak{g}, A) \,.$$

Die Menge der Äquivalenzklassen modulo $\sim$ ist also gerade die Faktorgruppe

$$Z^2(\mathfrak{g}, A)/B^2(\mathfrak{g}, A) = H^2(\mathfrak{g}, A) \,.$$

Man erhält damit die folgende *abelsche* Version von Satz (3.3):

(3.3$^{\mathbf{ab}}$) Satz: *Sei $\mathfrak{g}$ eine endliche Gruppe und A ein $\mathfrak{g}$-Modul. Ordnet man jeder Isomorphieklasse von Gruppenerweiterungen $A \hookrightarrow G \twoheadrightarrow \mathfrak{g}$, die die vorgegebene $\mathfrak{g}$-Struktur auf A induziert, sein Faktorensystem f modulo $\sim$ zu, so erhält man eine Bijektion auf die zweite Kohomologiegruppe $H^2(\mathfrak{g}, A)$.*

Offenbar gehört zum 0-Element von $H^2(\mathfrak{g}, A)$ das semidirekte Produkt $A \rtimes \mathfrak{g}$ (bzgl. der fixierten Operation). Daraus folgt:

$$H^2(\mathfrak{g}, A) = (0) \iff \left\{\begin{array}{l}\text{Jede Gruppenerweiterung } A \hookrightarrow G \twoheadrightarrow \mathfrak{g} \text{ mit der ge-}\\ \text{gebenen } \mathfrak{g}\text{-Struktur auf } A \text{ zerfällt.}\end{array}\right\}$$

Die Existenzaussage von Satz (3.9) ist damit reduziert auf den Nachweis von $H^2(\mathfrak{g}, A) = 0$ für $\#\mathfrak{g}$ teilerfremd zu $\#A$.

Aber auch die Konjugiertheitsaussage von (3.9) für die Komplemente ist kohomologisch faßbar. Es gilt:

(3.10) Bemerkung: $\mathfrak{g}$ endliche Gruppe, A ein $\mathfrak{g}$-Modul, $G = A \rtimes \mathfrak{g}$ das zugehörige semidirekte Produkt. Dann gilt:
a) Die Gruppe $Z^1(\mathfrak{g}, A)$ operiert treu und transitiv auf der Menge der Komplemente von A in G. Man erhält dadurch eine Bijektion zwischen der Menge der Komplemente und der Gruppe der 1-Kozyklen $Z^1(\mathfrak{g}, A)$.
b) Dabei bildet $a \in Z^1(\mathfrak{g}, A)$ ein Komplement auf ein in G konjugiertes ab, genau dann wenn a ein Korand ist. Die Konjugationsklassen von Komplementen von A in G entsprechen daher bijektiv den Elementen der 1-dimensionalen Kohomologiegruppe $H^1(\mathfrak{g}, A)$.

Beweis: a) Sei $a \in Z^1(\mathfrak{g}, A)$ und $U = \{u_\sigma \mid \sigma \in \mathfrak{g}\}$ ein beliebiges Komplement von A in G. Dann definieren wir

$$U \cdot a := \{u'_\sigma = u_\sigma a_\sigma \mid \sigma \in \mathfrak{g}\}$$

und zeigen, daß dadurch ein weiteres Komplement definiert ist: Wegen $a_\sigma \in A = \operatorname{Ke}\nu$ gilt $\nu(u_\sigma a_\sigma) = \sigma$ und man muß nur zeigen, daß die u'_σ multiplikativ abgeschlossen sind. Da a ein 1-Kozyklus ist, gilt

$$0 = \partial^1 a(\sigma, \tau) = a_\tau - a_{\sigma\tau} + a_\sigma^\tau \iff a_\sigma^\tau + a_\tau = a_{\sigma\tau}\,,$$

oder in multiplikativer Form[1)] $a_\sigma^\tau a_\tau = a_{\sigma\tau}$. Daraus folgt dann

$$u'_\sigma u'_\tau = u_\sigma a_\sigma \cdot u_\tau a_\tau \underset{(V)}{=} u_\sigma \cdot u_\tau a_\sigma^\tau \cdot a_\tau = u_{\sigma\tau} a_{\sigma\tau} = u'_{\sigma\tau}\,.$$

Damit operiert $Z^1(\mathfrak{g}, A)$ auf der Menge der Komplemente. Ist $U \cdot a = U$, so ist jedes $u'_\sigma = u_\sigma a_\sigma$ von der Form $u_\tau \in U$. Wegen $\tau = \nu(u_\tau) = \nu(u_\sigma a_\sigma) = \nu(u_\sigma) = \sigma$ ist τ notwendig σ und es folgt $U \cdot a = U \iff u_\sigma a_\sigma = u_\sigma \iff a_\sigma = 1$ (bzw. in A $a_\sigma = 0$) für alle $\sigma \in \mathfrak{g}$. In Termen der Operation von Z^1 auf den Komplementen bedeutet dies $U \cdot a = U \iff a = 0$; die Operation ist treu. Damit ist bei beliebig gewähltem Komplement U (dessen Existenz in einem semidirekten Produkt ja gegeben ist) die Abbildung

$$a \mapsto U \cdot a$$

injektiv. Wir müssen nun zeigen, daß sie surjektiv ist.
Sei $U' = \{u'_\sigma\}$ ein weiteres Komplement, also existieren $a_\sigma \in A$ mit $u'_\sigma = u_\sigma a_\sigma$. Wir zeigen, daß (a_σ) notwendig ein 1-Kozyklus ist. Seien f und f' die zu U bzw. U' gehörenden Faktorensysteme. Dann gilt

$$f'(\sigma, \tau) - f(\sigma, \tau) = a_\sigma^\tau + a_\tau - a_{\sigma\tau} = \partial^1 a(\sigma, \tau)\,.$$

Da die f und f' bestimmenden Repräsentanten Komplemente von A bilden, gilt $f(\sigma, \tau) = f'(\sigma, \tau) = 0$ und folglich

$$\partial^1 a = 0\,, \quad \text{d. h.} \quad a \in Z^1(\mathfrak{g}, A)\,.$$

b) Sei $U' = U \cdot a$ konjugiert zu U, also $U' = U^g$ für ein $g \in G$. Wir stellen g dar als $g = u_\tau b$ mit $\tau = \nu(g) \in \mathfrak{g}$ und $b \in A$. Wegen $u_\tau \in U$ folgt dann, $U^g = U^b$ für ein $b \in A$. Konjugiertheit kann also stets durch ein Element aus A erreicht werden. $U' = U^b$ bedeutet dann $u'_\sigma = u_\tau^b = b^{-1} u_\tau b$ mit einem geeigneten $\tau \in \mathfrak{g}$. Wegen $b \in A = \operatorname{Ke}\nu$ folgt wie oben $\sigma = \nu(u'_\sigma) = \nu(b)^{-1}\nu(u_\tau)\nu(b) = \tau$. Also:

$$\begin{aligned} U \cdot a = U' = U^b &\iff u_\sigma a_\sigma = u'_\sigma = b^{-1} u_\sigma b \\ &\iff u_\sigma a_\sigma = u_\sigma b^{-u_\sigma} b \iff a_\sigma = b^{-\sigma} b\,. \end{aligned}$$

In additiver Schreibweise lautet die letzte Gleichung:

$$a_\sigma = b - b^\sigma = \partial^0 b(\sigma)\,.$$

Damit folgt für $a \in Z^1(\mathfrak{g}, A)$:

$$U' = U \cdot a \sim_G U \iff \bigvee_{b \in A} a = \partial^0 b \iff a \in B^1(\mathfrak{g}, A)\,.$$

[1)] Die Gruppe A ist additiv notiert, jedoch als Untergruppe der (nicht abelschen) Gruppe G wird sie wie diese multiplikativ notiert. Diese Ambivalenz wird vermieden, wenn man A nicht als Untergruppe von G betrachtet, sondern vermöge des zum Begriff der Gruppenerweiterung gehörenden injektiven Gruppenhomomorphismus $i : A \to G$ in G einbettet. Dabei ist dann i ein Homomorphismus einer additiven in eine multiplikative Gruppe: $i(a + b) = i(a) \cdot i(b)$.

Dies bedeutet:

$$H^1(\mathfrak{g},A)=(0) \iff \left\{\begin{array}{l}\text{Alle Komplemente von } A \text{ im semidirekten Produkt}\\ G=A\rtimes\mathfrak{g} \text{ sind in } G \text{ konjugiert.}\end{array}\right\}$$

Insgesamt ist damit Satz (3.9) reduziert auf den Beweis der

(3.11) Proposition: *Ist $\mathfrak{g}$ eine endliche Gruppe und A ein endlicher $\mathfrak{g}$-Modul, so gilt:*

$$(\#\mathfrak{g},\#A)=1 \implies H^1(\mathfrak{g},A)=0=H^2(\mathfrak{g},A)\,.$$

Beweis: Da der ggT als Vielfachsumme darstellbar ist, gibt es ganze Zahlen x,y mit $1=x\cdot\#\mathfrak{g}+y\cdot\#A$, und daher

$$\bigwedge_{a\in A} x\#\mathfrak{g}\,.\,a=a\,. \tag{1}$$

Nachweis von $H^2=0$: Sei $f\in Z^2(\mathfrak{g},A)$, also

$$f(\sigma\tau,\rho)+f(\sigma,\tau)^\rho=f(\sigma,\tau\rho)+f(\tau,\rho)\,. \tag{2}$$

Wir definieren nun mit dem obigen $x\in\mathbb{Z}$ eine 1-Kokette $f^1\in C^1(\mathfrak{g},A)$ vermöge

$$f^1(\tau):=x\sum_{\sigma\in\mathfrak{g}} f(\sigma,\tau)\in A$$

und berechnen ihren Rand:

$$\begin{aligned}\partial^1 f^1(\tau,\rho)&=f^1(\rho)-f^1(\tau\rho)+f^1(\tau)^\rho\\ &=x\textstyle\sum_{\sigma\in\mathfrak{g}}\left(f(\sigma,\rho)-f(\sigma,\tau\rho)+f(\sigma,\tau)^\rho\right)\\ &\underset{(2)}{=}x\textstyle\sum_{\sigma\in\mathfrak{g}}\left(f(\sigma,\rho)-f(\sigma\tau,\rho)+f(\tau,\rho)\right)\\ &=x\textstyle\sum_{\sigma\in\mathfrak{g}} f(\sigma,\rho)-x\sum_{\sigma\in\mathfrak{g}} f(\sigma\tau,\rho)+x\sum_{\sigma\in\mathfrak{g}} f(\tau,\rho)\\ &=x\textstyle\sum_{\sigma\in\mathfrak{g}} f(\sigma,\rho)-x\sum_{\sigma'\in\mathfrak{g}} f(\sigma',\rho)+x\sum_{\sigma\in\mathfrak{g}} f(\tau,\rho)\\ &=x\#\mathfrak{g}\,.\,f(\tau,\rho)\underset{(1)}{=}f(\tau,\rho)\,.\end{aligned}$$

Damit ist $f=\partial^1 f^1$ ein 2-Korand, also $Z^2(\mathfrak{g},A)\subset B^2(\mathfrak{g},A)$: $H^2(\mathfrak{g},A)=0$.
Nachweis von $H^1=0$: Sei $a\in Z^1(\mathfrak{g},A)$, also

$$a_{\sigma\tau}=a_\sigma^\tau+a_\tau\,. \tag{3}$$

Analog wie oben definieren wir nun eine 0-Kokette, d. h. ein Element in A:

$$b=x\sum_{\sigma\in\mathfrak{g}} a_\sigma\in A$$

und berechnen den Korand

$$\begin{aligned}\partial^0 b(\tau)&=b-b^\tau=x\textstyle\sum_{\sigma\in\mathfrak{g}}(a_\sigma-a_\sigma^\tau)\\ &\underset{(3)}{=}x\textstyle\sum_{\sigma\in\mathfrak{g}}(a_\sigma-a_{\sigma\tau}+a_\tau)\\ &=x\textstyle\sum_{\sigma\in\mathfrak{g}} a_\sigma-x\sum_{\sigma\in\mathfrak{g}} a_{\sigma\tau}+x\sum_{\sigma\in\mathfrak{g}} a_\tau\\ &=x\#\mathfrak{g}\,.\,a_\tau\underset{(1)}{=}a_\tau\,.\end{aligned}$$

Damit ist $a=\partial^0 b\in B^1(\mathfrak{g},A)$ und die Behauptung bewiesen.

d. Gruppen der Ordnung p^3

In diesem Abschnitt wollen wir (als konkrete Anwendung der bisherigen Resultate) alle Gruppen der Ordnung p^3 bestimmen. Wir verwenden dabei zunächst die Erweiterungstheorie zur Bestimmung aller nicht-abelschen Gruppen der Ordnung p^{n+1} (p eine Primzahl), die einen zyklischen Normalteiler der Ordnung p^n enthalten.

(3.12) Satz: *Sei p eine Primzahl, $n \in \mathbb{N}$, $n \geq 2$.*

a) *Für $p \neq 2$ gibt es genau eine nicht-abelsche Gruppe G der Ordnung p^{n+1} mit einem zyklischen Normalteiler A der Ordnung p^n, nämlich das semidirekte Produkt $C_{p^n} \rtimes C_p$ mit der folgenden Operation von $C_p = \langle\sigma\rangle$ auf $C_{p^n} = \langle a\rangle$:*

$$a^\sigma = a^{1+p^{n-1}} .$$

Also gilt

$$G = \langle a, \sigma\rangle \quad mit \quad \#G = p^{n+1} ,\ a^{p^n} = 1 ,\ \sigma^p = 1 ,\ a^\sigma = a^{1+p^{n-1}} .$$

b) *Sei $p = 2$ und $n \geq 3$. Dann gibt es genau 4 nicht-abelsche, nicht-isomorphe Gruppen G der Ordnung 2^{n+1} mit einem zyklischen Normalteiler A der Ordnung 2^n, nämlich:*

(1) Die Diedergruppe $D_{2^{n+1}} = \langle a, \sigma\rangle$ definiert durch

$$\#D_{2^{n+1}} = 2^{n+1} ,\ a^{2^n} = \sigma^2 = 1 ,\ a^\sigma = a^{-1} .$$

(2) Die (verallgemeinerte) Quaternionengruppe $Q_{2^{n+1}} = \langle a, \sigma\rangle$ definiert durch

$$\#Q_{2^{n+1}} = 2^{n+1} ,\ a^{2^n} = 1 ,\ \sigma^2 = a^{2^{n-1}} ,\ a^\sigma = a^{-1} .$$

(3) Die Gruppe $G = \langle a, \sigma\rangle$ (wie für $p \neq 2$) definiert durch

$$\#G = 2^{n+1} ,\ a^{2^n} = \sigma^2 = 1 ,\ a^\sigma = a^{1+2^{n-1}} .$$

(4) Die Quasidiedergruppe $G = \langle a, \sigma\rangle$ definiert durch

$$\#G = 2^{n+1} ,\ a^{2^n} = \sigma^2 = 1 ,\ a^\sigma = a^{-1+2^{n-1}} .$$

c) *$\underline{p = 2 ,\ n = 2}$: Es gibt genau 2 nicht-abelsche nicht-isomorphe Gruppen der Ordnung 8 mit einem zyklischen Normalteiler der Ordnung 4, nämlich die Diedergruppe D_8 (siehe b)(1) mit $n = 2$) und die Quaternionengruppe Q_8 (siehe b)(2) mit $n = 2$).*

d) *Alle genannten Gruppen existieren und sind untereinander nicht isomorph. Sie sind durch die angegebenen Eigenschaften bis auf Isomorphie eindeutig bestimmt.*

Beweis: Sei $\langle a\rangle \hookrightarrow G \twoheadrightarrow \langle\sigma\rangle$ eine Gruppenerweiterung der genannten Art. Da A abelsch ist, ist das Automorphismensystem ein Homomorphismus

$$\alpha : \mathfrak{g} \to \mathrm{Aut}(A) ,\ \text{also } \alpha : C_p \to \mathrm{Aut}(C_{p^n}) .$$

Wir klassifizieren zunächst diese Homomorphismen. Da $\mathfrak{g}$ zyklisch von Primzahlordnung ist, ist α ist entweder injektiv oder trivial.

Zwischenbemerkung: Ist $\alpha = 1$, so ist G abelsch.

Beweis: Wegen $\alpha = 1$ gilt

$$u_\sigma a = a u_\sigma \quad \text{für alle } \sigma \in \mathfrak{g} , a \in A \tag{1}$$

und es bleibt zu zeigen $u_\sigma u_\tau = u_\tau u_\sigma$ für alle $\sigma, \tau \in \mathfrak{g}$. Ist $\sigma = 1$ oder $\tau = 1$, so folgt wegen $u_1 \in A$ die Kommutativität der Repräsentanten bereits aus (1). Da $\mathfrak{g}$ zyklisch ist, etwa $\mathfrak{g} = \langle\sigma\rangle$, ist zu zeigen

$$u_{\sigma^i} u_{\sigma^j} = u_{\sigma^j} u_{\sigma^i} .$$

Der Beweis erfolgt induktiv über i; der Induktionsanfang $i = 0$ ist bereits gezeigt. Sei nun $i = 1$. Hier erfolgt der Beweis induktiv über j. $j = 0$ ist ebenfalls bereits gezeigt. Sei nun $j \geq 1$. Dann gilt gemäß der Repräsentantenmultiplikation (R)

$$u_\sigma u_{\sigma^j} \underset{(R)}{=} u_\sigma \cdot u_\sigma u_{\sigma^{j-1}} f(\sigma, \sigma^{j-1})^{-1} \underset{\text{(Ind.Vor)}}{=} u_\sigma u_{\sigma^{j-1}} u_\sigma f(\sigma, \sigma^{j-1})^{-1}$$
$$\underset{(1)}{=} u_\sigma u_{\sigma^{j-1}} f(\sigma, \sigma^{j-1})^{-1} \cdot u_\sigma \underset{(R)}{=} u_{\sigma^j} u_\sigma \,.$$

Genauso argumentiert man beim Induktionsschritt bzgl. i. Wieder benutzt man die Aufspaltung $u_{\sigma^i} = u_\sigma u_{\sigma^{i-1}} f(\sigma, \sigma^{i-1})^{-1}$, wobei man dann für den Induktionsschritt neben (1) die Induktionsvoraussetzung für $i - 1$ *und* 1 benötigt. (Daher der Induktionsanfang bei $i = 0$ *und* $i = 1$.)

Aufgrund dieser Zwischenbemerkung können wir uns zum Beweis von Satz (3.12) auf *injektive* Gruppenhomomorphismen $\alpha : \mathfrak{g} \hookrightarrow \mathrm{Aut}(A)$ beschränken. Da $\mathfrak{g}$ zyklisch von der Ordnung p ist, erhält man so Isomorphismen $\alpha : C_p \xrightarrow{\sim} \mathcal{A}$ auf zyklische Automorphismengruppen $\mathcal{A} \leq \mathrm{Aut}(A)$ von A mit der Ordnung p. Wir bestimmen daher zunächst für $A \simeq \mathbb{Z}/p^n\mathbb{Z}$ die Automorphismengruppe und ihre Untergruppen $\mathcal{A}$ der Ordnung p.

(3.13) Lemma: (Automorphismen zyklischer Gruppen) *Sei m eine natürliche Zahl.*
a) Ist a ein Element der Ordnung m in einer beliebigen Gruppe, so gilt

$$\mathrm{ord}(a^k) = \frac{m}{\mathrm{ggT}(m,k)} \,.$$

b) Die Automorphismengruppe einer zyklischen Gruppe $A = \langle a \rangle$ der Ordnung m ist die prime Restklassengruppe mod *m:*

$$\mathrm{Aut}(\mathbb{Z}/m\mathbb{Z}) \xrightarrow{\sim} \mathcal{P}(m) := \{\bar{k} \in \mathbb{Z}/m\mathbb{Z} \mid k \in \mathbb{Z}\,,\ \mathrm{ggT}(k,m) = 1\}\,, \quad \varphi \mapsto \varphi(\bar{1})\,.$$

Beweis: a) Sei $d = \mathrm{ggT}(m,k)$ und $dm' = m$, $dk' = k$, also m' und k' teilerfremd. Dann gilt für ein beliebiges l:

$$(a^k)^l = 1 \iff \mathrm{ord}(a) = m \mid kl \iff m' \mid k'l \iff m' \mid l\,.$$

Damit folgt $\mathrm{ord}(a^k) = m'$, wie behauptet.
b) a^k erzeugt $\langle a \rangle$, wenn es dieselbe Ordnung $m' = m$ hat, also nach a), wenn $\mathrm{ggT}(m,k) = 1$ ist. Nun ist $a = \bar{1}$ Erzeugendes von $A = \mathbb{Z}/m\mathbb{Z}$, also auch das Bild $\varphi(\bar{1}) = \bar{k} = k.\bar{1}$ unter einem Automorphismus φ. Daher muß k zu m teilerfremd sein, d. h. es ist $\bar{k} \in \mathcal{P}(m)$. Die angegebene Abbildung ist somit wohldefiniert; sie ist offensichtlich ein Gruppenhomomorphismus (bzgl. der Multiplikation in $\mathcal{P}(m)$); und sie ist injektiv, da φ durch seinen Wert auf dem Erzeugenden $a = \bar{1}$ der zyklischen Gruppe A festgelegt ist. Ist $\varphi(a)$ ein Element, das dieselbe Ordnung m wie a hat, so wird durch $\varphi(a^k) = \varphi(a)^k$ ein Automorphismus wohldefiniert. Dies liefert die Surjektivität der obigen Abbildung.

(3.14) Satz: (Struktur der primen Restklassengruppen)

a) *$\mathcal{P}(m)$ ist die Einheitengruppe $R^\times = \{r \in R \mid \bigvee_{s \in R} rs = 1\}$ des Ringes $R = \mathbb{Z}/m\mathbb{Z}$.*

b) *$\mathcal{P}(mn) \xrightarrow{\sim} \mathcal{P}(m) \times \mathcal{P}(n)$ für teilerfremde m, n.*

c) *Für Primzahlpotenzen $m = p^n$ einer Primzahl $p \neq 2$ und für $p = 2$, $n \leq 2$ ist $\mathcal{P}(p^n)$ zyklisch von der Ordnung $(p-1)p^{n-1}$. Für $n \geq 2$ gibt es in diesen Fällen genau eine Untergruppe der Ordnung p in $\mathcal{P}(p^n)$; sie wird erzeugt von der Restklasse von $1 + p^{n-1}$.*

d) *Für $n \geq 3$ ist $\mathcal{P}(2^n) = \langle -\bar{1} \rangle \times \langle \bar{5} \rangle$ direktes Produkt einer zyklischen Gruppe der Ordnung 2 und einer der Ordnung 2^{n-2}. Es gibt genau drei Untergruppen der Ordnung 2 darin; sie werden erzeugt von den Restklassen von -1 bzw. von $\pm 1 + 2^{n-1}$.*

Beweis: a) Wir benutzen die Darstellbarkeit des größten gemeinsamen Teilers als Vielfachsumme. Diese beweist man mit dem euklidischen Algorithmus. Wendet man diesen auf zwei Zahlen k und m an, so erhält man am Ende nicht nur den ggT d, sondern auch dessen Darstellung als $d = xk + ym$ mit ganzen Zahlen x, y. Für teilerfremde Zahlen k, m ergibt sich

$$1 = xk + ym\,, \quad \text{also} \quad xk \equiv 1 \bmod m\,.$$

Damit hat k modulo m ein Inverses, d. h. $\bar{k} \in (\mathbb{Z}/m\mathbb{Z})^\times$. Umgekehrt folgt aus $xk \equiv 1 \bmod m$, also $1 = xk + ym$, daß $d = \mathrm{ggT}(m,k)$ ein Teiler von $xk + ym = 1$ sein muß, also $d = 1$ ist.
b) folgt aus dem Chinesischen Restsatz für teilerfremde n, m:

$$\mathbb{Z}/mn\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}\,, \quad x + mn\mathbb{Z} \mapsto (x + m\mathbb{Z}, x + n\mathbb{Z})\,.$$

(Wegen der Teilerfremdheit von n, m ist der angegebene Homomorphismus injektiv; da Definitions- und Zielbereich gleichmächtig sind, liegt ein Isomorphismus vor.) Diese Isomorphie überträgt sich auf die Einheitengruppen.

Die Strukturaussagen c), d) werden im Rahmen der Algebra und elementaren Zahlentheorie bewiesen. Wir skizzieren die benötigten Schritte.
1) $\#\mathcal{P}(p^n) = (p-1)p^{n-1}$ für jede Primzahl p und $n \in \mathbb{N}$. Mittels b) erhält man eine allgemeine Formel für $\#\mathcal{P}(m)$.
2) Endliche Untergruppen von Multiplikationsgruppen von Körpern sind zyklisch; $\mathcal{P}(p) = \mathbb{F}_p^\times$ ist zyklisch von der Ordnung $p - 1$.
3) Für $p \neq 2$ hat $1 + p \bmod p^n$ in $\mathcal{P}(p^n)$ die Ordnung p^{n-1}.
4) $\mathcal{P}(p^n)$ enthält ein Element der Ordnung $p-1$. Ist $w \bmod p^n$ ein derartiges Element und $p \neq 2$, so wird $\mathcal{P}(p^n)$ von $w(1+p)$ erzeugt.
5) $5^{2^k} \equiv 1 + 2^{k+2} \bmod 2^{k+3}$ für $k \geq 0$.
Begründungen:
1) Teilerfremd zu p^n zu sein, bedeutet nicht durch p teilbar zu sein, also gilt

$$\mathbb{Z}/p^n\mathbb{Z} \setminus \mathcal{P}(p^n) = \{\bar{a} \in \mathbb{Z}/p^n\mathbb{Z} \mid p \mid a\} = \{\overline{kp} \mid 0 \leq k < p^{n-1}\}\,.$$

Diese Menge enthält p^{n-1} Elemente, also folgt $\#\mathcal{P}(p^n) = p^n - p^{n-1}$, womit 1) gezeigt ist.
2) Sei $A \leq K^\times$ eine endliche Untergruppe und $a \in A$ ein Element maximaler Ordnung m. Da A abelsch ist, gilt dann $\mathrm{ord}(b) \mid m$ bzw. $b^m = 1$ für *jedes* $b \in A$. Zum Beweis nehmen wir an, es gäbe ein $b \in A$ mit $\mathrm{ord}(b) = k \not| \, m$. Dann gibt es eine Primzahlpotenz $p^\nu \mid k$ mit $p^\nu \not| \, m$. Das Element $\tilde{a} = a^{p^\nu}$ hat dann die Ordnung $\tilde{m} = m/\mathrm{ggT}(m, p^\nu)$, während $\tilde{b} = b^{k/p^\nu}$ die Ordnung $\tilde{k} = p^\nu$ hat. Wegen $p^\nu \not| \, m$ ist $\mathrm{ggT}(m, p^\nu)$ die größte p-Potenz, die m teilt, also p kein Teiler mehr von $\tilde{m}$. Damit haben $\tilde{a}$ und $\tilde{b}$ *teilerfremde* Ordnungen $\tilde{m}$ und $\tilde{k}$. Nun gilt in beliebigen *abelschen* Gruppen

$$\mathrm{ggT}(\mathrm{ord}(x), \mathrm{ord}(y)) = 1 \implies \mathrm{ord}(xy) = \mathrm{ord}(x)\,\mathrm{ord}(y)\,.$$

Zur Begründung setzen wir $m = \mathrm{ord}(x)$, $n = \mathrm{ord}(y)$. Dann gilt für beliebige $l \in \mathbb{Z}$

$$1 = (xy)^l \implies 1 = x^{ln} \wedge 1 = y^{lm} \implies m \mid ln \wedge n \mid lm \implies m \mid l \wedge n \mid l \implies mn \mid l\,.$$

Also hat das Produkt $\tilde{a}\tilde{b}$ die Ordnung $\mathrm{ord}(\tilde{a}\tilde{b}) = \tilde{m}\tilde{k} = p^\nu \cdot m/\mathrm{ggT}(m, p^\nu) > m$. Dies widerspricht der Maximalität von m.
Damit ist $x^m = 1$ für alle $x \in A$. Da A in einem Körper liegt, bedeutet dies: Alle Elemente von A sind Wurzeln des Polynoms $X^m - 1$. Dieses hat in einem Körper höchstens m Wurzeln, also $\#A \leq m$. Da andererseits in A ein Element a mit der Ordnung m existiert, folgt $A = \langle a \rangle$.
3) Wir zeigen induktiv für $p \neq 2$:

$$(1+p)^{p^k} \equiv 1 + p^{k+1} \bmod p^{k+2} \quad \text{für } k \geq 0\,.$$

$k = 0$ ist klar. Sei $k \geq 0$ und $(1+p)^{p^k} = 1 + p^{k+1} + ap^{k+2}$ für ein $a \in \mathbb{Z}$. Dann folgt

$$\begin{aligned}(1+p)^{p^{k+1}} &= (1 + p^{k+1}(1+ap))^p \\ &= 1 + p \cdot p^{k+1}(1+ap) + \tbinom{p}{2} p^{2k+2}(1+ap)^2 + \ldots \\ &\equiv 1 + p^{k+2} \bmod p^{k+3}\,,\end{aligned}$$

denn für $p \neq 2$ ist p ein Teiler von $\binom{p}{2}$. Aus der bewiesenen Kongruenz folgt zunächst (mit $k = n-1$) $(1+p)^{p^{n-1}} \equiv 1 \bmod p^n$; die Ordnung von $1+p \bmod p^n$ ist also ein Teiler von p^{n-1}. Die Ordnung kann aber kein echter Teiler sein, da für $k < n-1$, also $k+2 \leq n$ folgt

$$(1+p)^{p^k} \equiv 1 + p^{k+1} \pmod{p^{k+2}} \not\equiv 1 \pmod{p^{k+2}} \not\equiv 1 \pmod{p^n}\,.$$

4) Sei $u \bmod p$ ein Element der Ordnung $p-1$ in $\mathcal{P}(p)$ (siehe 2)). Dann gehört $\bar{u} = u \bmod p^n$ zu $\mathcal{P}(p^n)$ und hat mindestens die Ordnung $p-1$. Wegen $\#\mathcal{P}(p^n) = (p-1)p^{n-1}$ hat $u \bmod p^n$ daher die Ordnung $(p-1)p^k$ mit $0 \leq k \leq n-1$. Dann ist $w = u^{p^k} \bmod p^n$ ein Element der angestrebten Ordnung $p-1$.
Damit haben die Elemente w und $1+p$ in $\mathcal{P}(p^n)$ die teilerfremden Ordnungen $p-1$ und p^{n-1}, ihr Produkt $w(1+p)$ also (siehe Beweis von 2)) die Ordnung $(p-1)p^{n-1} = \#\mathcal{P}(p^n)$. $w(1+p)$ ist folglich ein Erzeugendes von $\mathcal{P}(p^n)$. In dieser zyklischen Gruppe gibt es dann für $n \geq 2$, also $p \mid \#\mathcal{P}(p^n)$, genau eine Untergruppe der Ordnung p. Ein Element der Ordnung p ist gegeben durch $(1+p)^{p^{n-2}} \equiv 1 + p^{n-1} \bmod p^n$ (siehe die Kongruenz im Beweis von 3)). Satz (3.14), c) ist daher für die Fälle $p \neq 2$ bewiesen. Nun ist $\mathcal{P}(2)$ trivial und $\mathcal{P}(4) = \{\pm\bar{1}\}$ zyklisch von der Ordnung 2, so daß man die restlichen Behauptungen von c) unmittelbar überprüfen kann.
5) $k = 0$ ist wieder klar. Sei $k \geq 0$ und $5^{2^k} = 1 + 2^{k+2} + 2^{k+3}a$ mit $a \in \mathbb{Z}$. Dann folgt

$$5^{2^{k+1}} = (1 + 2^{k+2}(1+2a))^2 = 1 + 2^{k+3}(1+2a) + 2^{2k+4}(1+2a)^2 \equiv 1 + 2^{k+3} \bmod 2^{k+4}\,.$$

Daraus folgt wie unter 3), daß für $n \geq 2$ $5 \bmod 2^n$ die Ordnung 2^{n-2} hat.

Wir kommen nun zum Beweis von Satz (3.14),d). Läge $-1 \bmod 2^n$ in der von $5 \bmod 2^n$ erzeugten Untergruppe, so existierte ein k, $0 < k < 2^{n-2}$, mit

$$\begin{aligned}&-1 \equiv 5^k \bmod 2^n \implies 5^{2k} \equiv 1 \bmod 2^n \\ &\implies \operatorname{ord}(\bar{5}) = 2^{n-2} \mid 2k \implies 2^{n-3} \mid k \implies 2^{n-3} = k \\ &\implies -1 \equiv 5^{2^{n-3}} \equiv 1 + 2^{n-1} \bmod 2^n \implies -1 \equiv 1 \bmod 2^{n-1}\,.\end{aligned}$$

Dies ist wegen $n-1 \geq 2$ falsch. $\mathcal{P}(2^n)$ hat also die behauptete Struktur als direktes Produkt einer zyklischen Gruppe der Ordnung 2 und einer der Ordnung 2^{n-2} (mit den explizit angegebenen Erzeugenden).

Offenbar ist $-1 \bmod 2^n$ ein Element der Ordnung 2. Sei nun $\pm 5^k$ $(0 < k < 2^{n-2})$ ein anderes Element der Ordnung 2 in $\mathcal{P}(2^n)$. Dann folgt wie oben

$$1 \equiv 5^{2k} \bmod 2^n \iff 2^{n-2} \mid 2k \iff 2^{n-3} \mid k \iff k = 2^{n-3}\,.$$

Damit gibt es genau drei Elemente der Ordnung 2 in $\mathcal{P}(2^n)$. Nun gilt nach 5)

$$5^{2^{n-3}} \equiv 1 + 2^{n-1} \bmod 2^n\,,$$

so daß zusammen mit $\pm(1 + 2^{n-1}) \equiv \pm 1 + 2^{n-1} \bmod 2^n$ Satz (3.14),d) folgt. □

Wir führen nun den Beweis von Satz (3.12) fort. Es ist $\alpha : \mathfrak{g} \xrightarrow{\sim} \mathcal{A}$ ein Isomorphismus auf eine zyklische Untergruppe $\mathcal{A} = \langle \bar{k} \rangle$ der Ordnung p in $\mathcal{P}(p^n)$, und diese sind gemäß (3.13) bekannt. Wir müssen folgende Möglichkeiten für k untersuchen:

$$k = \begin{cases} 1 + p^{n-1} & \text{für } p \neq 2,\ n \geq 2 \text{ oder } p = 2,\ n \geq 3, \\ -1 + 2^{n-1} & \text{für } p = 2,\ n \geq 3, \\ -1 & \text{für } p = 2,\ n \geq 2. \end{cases}$$

Man wählt nun in $\mathfrak{g}$ das Erzeugende σ so, daß $\alpha_\sigma = \bar{k}$ ist. Es gilt dann

$$a^\sigma = a^k \quad \text{für alle } a \in A\,.$$

Wir wollen nun untersuchen, in welchen Fällen ein Komplement zu A existiert, d. h. ob ein semidirektes Produkt vorliegt. Wir gehen dazu von einem beliebigen Repräsentanten u_σ von σ aus und suchen ein anderes Urbild $u'_\sigma = u_\sigma b$ ($b \in A$) mit der Eigenschaft $(u_\sigma b)^p = 1$. Existiert ein solches b, so erhält man durch $u'_{\sigma^i} := (u_\sigma b)^i$ eine zu $\mathfrak{g} = \langle\sigma\rangle$ isomorphe Untergruppe von G. Um ein solches b zu konstruieren, berechnet man induktiv aufgrund der Vertauschungsregel $a^\sigma = a^k$

$$(u_\sigma b)^p = u_\sigma^p b^{k^{p-1}+k^{p-2}+\ldots+k+1} =: u_\sigma^p b^K\,.$$

Gesucht ist also ein $b \in A$ mit $b^{-K} = u_\sigma^p =: d$. Wegen $\nu(u_\sigma^p) = \sigma^p = 1$ liegt d in A und es gilt

$$d^k = d^\sigma = u_\sigma^{-1} d u_\sigma = u_\sigma^{-1} u_\sigma^p u_\sigma = u_\sigma^p = d\,.$$

Wir lösen nun die Gleichung $b^{-K} = d$ in A. Dabei unterscheiden wir wieder die drei Fälle für k.

1. $k = 1 + p^{n-1}$: Dann ist

$$\begin{aligned} K &= k^{p-1} + k^{p-2} + \ldots + k + 1 = \textstyle\sum_{i=0}^{p-1}(1+p^{n-1})^i \equiv \sum_{i=0}^{p-1} 1 + \sum_{i=0}^{p-1} i p^{n-1} \bmod p^n \\ &\equiv p + \tfrac{p(p-1)}{2} p^{n-1} \bmod p^n \equiv \begin{cases} p \pmod{p^n} & \text{für } p \neq 2 \\ 2 + 2^{n-1} \pmod{2^n} & \text{für } p = 2. \end{cases} \\ &\equiv p \cdot l \bmod p^n \quad \text{mit } p \nmid l\,. \end{aligned}$$

(Man beachte, daß im Falle $p = 2$ $n \geq 3$ ist.) Wegen $b \in A$ und $p^n = \#A$ folgt daraus $b^K = b^{pl}$ und die zu lösende Gleichung lautet dann

$$b^{-pl} = d = u_\sigma^p\,.$$

Da l teilerfremd zu p ist, ist in der p-Gruppe A jedes Element eine l-te Potenz ($1 = xl + yp^n \implies 1 \equiv xl \bmod \#A \implies a = a^{xl} \in A^l$). Es genügt also letztendlich ein $c \in A$ zu finden mit $c^p = u_\sigma^p$, d. h. zu zeigen:

$$d = u_\sigma^p \text{ ist } p\text{-te Potenz eines Elementes } \underline{\text{aus } A}.$$

Nun gilt $d = d^k = d^{1+p^{n-1}}$, also $1 = d^{p^{n-1}}$. Dies bedeutet in der zyklischen Gruppe A der Ordnung p^n, daß d eine p-te Potenz ist. ($d = a^j$ und $1 = d^{p^{n-1}} = a^{jp^{n-1}}$ implizieren $p^n \mid jp^{n-1}$ bzw. $p \mid j$.)

2. $k = -1 + 2^{n-1}$: Wegen $p = 2$ ist dann $K = 1 + k = 2^{n-1}$ und die Gleichung lautet $b^{-2^{n-1}} = d$, d. h. es gilt zu zeigen:

$$d = u_\sigma^2 \text{ ist } 2^{n-1}\text{-te Potenz eines Elementes } \underline{\text{aus } A}.$$

Da A zyklisch von der Ordnung 2^n ist, muß man beweisen, daß $d := u_\sigma^2$ höchstens die Ordnung 2 hat (siehe analogen Schluß unter 1.). Nun gilt wieder

$$d = d^k = d^{-1+2^{n-1}}\,,\ \text{also } 1 = d^{-2+2^{n-1}} = d^{2(-1+2^{n-2})}\,.$$

Nun ist $-1 + 2^{n-2}$ für $n \geq 3$ ungerade und damit prim zu 2^n, so daß man durch Potenzierung der letzten Gleichung mit dem Inversen modulo 2^n $d^2 = 1$ erhält.

3. $k = -1$. Dann ist $K = 1 + k = 0$ und die zu untersuchende Gleichung lautet nun $d = b^0 = 1$. Diese ist unabhängig von b. Es gilt also nur zu entscheiden, ob $d = 1$ ist oder nicht. Wegen $d = d^k = d^{-1}$ gilt $d^2 = 1$, so daß es in der zyklischen Gruppe $A = \langle a\rangle$ der Ordnung 2^n nur zwei Möglichkeiten für dieses Element d gibt:

$$d = 1 \quad \text{oder} \quad d = a^{2^{n-1}}\,.$$

Im Falle $u_\sigma^2 = d = 1$ erhält man wieder ein semidirektes Produkt, die Diedergruppe (1), während im Falle $u_\sigma^2 = d = a^{2^{n-1}}$ sich die angegebene (verallgemeinerte) Quaternionengruppe (2) ergibt. Diese kann kein semidirektes Produkt sein, da $u_\sigma^2 = d \neq 1$ für *jeden* Repräsentanten von σ gilt.

Dieses letzte Resultat deckt in Satz (3.12) Teil c) und von b) die Fälle (1), (2) ab. Dagegen war in den beiden erstgenannten Fällen für k die Gruppenerweiterung G notwendig das semidirekte Produkt mit der angegebenen Operation von $\mathfrak{g}$ auf A. Dies ergibt in Satz (3.12) Teil a) und die Fälle (3), (4) von b).

d) Die verschiedenen Gruppen für $p = 2$ sind nicht isomorph, denn die Fälle 1. – 3. unterscheiden sich bereits in der Operation von $\mathfrak{g} = C_2$ auf A, während die Unterfälle von 3. sich in der Existenz eines Komplementes unterscheiden.

Alle genannten Gruppen existieren. Dies ist klar für die semidirekten Produkte mit den angegebenen Operationen. (Man hat lediglich zu überprüfen, daß durch die angegebenen Gleichungen $a^\sigma = a^k$ *Operationen* von $C_p = \langle\sigma\rangle$ auf $C_{p^n} = \langle a\rangle$ gegeben sind. Das bedeutet, für die angegebenen Werte von k gilt $a^{k^p} = a^{\sigma^p} = a^1 = a$ bzw. $k^p \equiv 1 \bmod p^n$.) Aber nicht nur die semidirekten Produkte, sondern auch die verallgemeinerte Quaternionengruppe ist wohldefiniert. Letztere konstruiert man mit der angegebenen Operation $a^\sigma = a^{-1}$ und dem folgenden (normierten) Faktorensystem

$$f(1,\sigma) = f(\sigma,1) = f(1,1) = 1 \quad \text{und} \quad f(\sigma,\sigma) = a^{2^{n-1}}\,.$$

Man rechnet dazu nach, daß f ein Kozyklus ist: Ist in der Kozyklenbedingung

$$f(\alpha\beta,\gamma) + f(\alpha,\beta)^\gamma = f(\alpha,\beta\gamma) + f(\beta,\gamma)$$

ein Gruppenelement trivial, so gilt die Gleichung aufgrund der Normiertheit. Sind nun alle drei Elemente α,β,γ gleich dem einzigen nicht-trivialen Element σ von $\mathfrak{g}$, so gilt mit $d = f(\sigma,\sigma)$

$$f(1,\sigma) + f(\sigma,\sigma)^\sigma = f(\sigma,1) + f(\sigma,\sigma) \iff d^\sigma = d \iff d^{-1} = d \iff d^2 = 1\,.$$

Für $d = a^{2^{n-1}}$ ist die letzte Gleichung wahr, die Kozyklenbedingung also erfüllt.

Wir kommen nun zu der angestrebten vollständigen Bestimmung aller Gruppen der Ordnung p^3, p eine Primzahl. Die Gruppen der Ordnung p und p^2 sind bekannt, da sie notwendig abelsch sind. (Im Falle $\#G = p^2$ betrachtet man das nicht-triviale (siehe (2.7)) Zentrum Z. Wäre G nicht abelsch, also $Z \neq G$, so wäre G/Z zyklisch von der Ordnung p und daher jedes Element von G darstellbar als $a^i z$ mit $z \in Z$. Daraus folgert man, daß G dennoch abelsch ist.)

(3.15) Satz: *Sei p eine Primzahl. Die Gruppen der Ordnung p^3 sind die folgenden:*

a) *abelsch:* $C_p \times C_p \times C_p$, $C_{p^2} \times C_p$, C_{p^3}.

b) *nicht-abelsch, $p = 2$:*

$$\begin{array}{lll} \textit{Diedergruppe} & D_8 = \langle a,b\rangle & \textit{mit} \quad a^4 = 1\,,\ b^2 = 1\,,\ a^b = a^{-1}\,, \\ \textit{Quaternionengruppe} & Q_8 = \langle a,b\rangle & \textit{mit} \quad a^4 = 1\,,\ b^2 = a^2\,,\ a^b = a^{-1}\,, \end{array}$$

c) *nicht-abelsch, $p \neq 2$:*

$$\begin{aligned} &G = \langle a,b\rangle \quad \textit{mit} \quad a^{p^2} = 1\,,\ b^p = 1\,,\ a^b = a^{1+p}\,, \\ &G = \langle a,b,c\rangle \quad \textit{mit} \quad a^p = b^p = c^p = 1\,,\ a^b = a^c = a\,,\ b^c = ab\,. \end{aligned}$$

Alle genannten Gruppen der Ordnung p^3 existieren und sind untereinander nicht isomorph: Sie sind durch die genannten Eigenschaften als Gruppen der Ordnung p^3 eindeutig bestimmt.

Beweis: a) folgt unmittelbar aus Satz (2.17).
b) Sei nun G nicht abelsch und $p = 2$. Zunächst gilt

$$\bigwedge_{a\in G} \operatorname{ord}(a) \mid 2 \implies \bigwedge_{a\in G} a = a^{-1} \implies \bigwedge_{a,b\in G} ab = a^{-1}b^{-1} = (ba)^{-1} = ba\,,$$

so daß es in der nicht-abelschen Gruppe G ein Element a der Ordnung 4 geben muß. Dann ist $\langle a\rangle$ eine maximale Untergruppe von G und daher Normalteiler in der 2-Gruppe G (siehe (2.13) a)). Damit ist G eine Gruppe der Ordnung $2^3 = 8$ mit einem zyklischen Normalteiler der Ordnung $2^2 = 4$, so daß b) aus Satz (3.12),c) folgt.

c) Sei nun G nicht abelsch und $p \neq 2$. Wieder können wir Satz (3.12) anwenden, wenn in G ein a existiert mit $\operatorname{ord}(a) = p^2$. G ist dann notwendig die erste der beiden angegebenen Gruppen in c).

Bleibt also der Fall zu untersuchen, daß für alle $a \in G$ gilt $a^p = 1$. (Man sagt, die Gruppe G hat *Exponent p*. Aber anders als im Falle $p = 2$ folgt daraus nicht, daß G abelsch sein muß.)
Da G eine p-Gruppe ist, ist das Zentrum Z von G nicht trivial. Da G nicht abelsch ist, muß Z die Ordnung p haben. (Hätte Z die Ordnung p^2, so wäre es ein Normalteiler mit zyklischer Faktorgruppe G/Z, woraus wieder die Kommutativität folgt, siehe die Bemerkung vor Satz (3.15).) Man wähle nun ein Erzeugendes a von Z und $b \in G \setminus Z$. Dann ist $A = \langle a, b\rangle$ abelsch, vom Exponenten p und von der Ordnung p^2. Als maximale Untergruppe ist A dann Normalteiler in der p-Gruppe G. Man wähle nun $c \in G \setminus A$. Dann wird G von a, b, c erzeugt. Da a im Zentrum liegt, gilt $a^b = a^c = a$. Wir untersuchen b^c:

$$A \lhd G \implies \bigvee_{0\leq\mu,\nu<p} b^c = a^\mu b^\nu\,.$$

Da $G/\langle a\rangle$ als Gruppe der Ordnung p^2 abelsch ist, gilt in $G/\langle a\rangle$:

$$\bar b = \bar b^{\bar c} = \bar a^\mu \bar b^\nu = \bar b^\nu\,.$$

Wegen $\operatorname{ord}(b) = p$ und $b \notin \langle a\rangle$ hat $\bar b$ ebenfalls die Ordnung p und daher gilt:

$$\bar b = \bar b^\nu \implies \nu \equiv 1 \bmod p \implies b^c = a^\mu b\,.$$

Schließlich gilt $\mu \not\equiv 0 \bmod p$, da andernfalls $b^c = b$ folgte und $G = \langle a, b, c\rangle$ abelsch wäre. μ ist also prim zu p, so daß

$$\langle a^\mu\rangle = \langle a\rangle = Z$$

gilt. Ersetzt man also a durch a^μ, so erhält man die angegebene Beschreibung für G:

$$G = \langle a, b, c\rangle \quad \text{mit} \quad a^p = b^p = c^p = 1\,,\ a^b = a^c = a\,,\ b^c = ab\,.$$

Abgesehen von dieser letzten Gruppe ist die Existenz und Nicht-Isomorphie der Gruppen von Satz (3.15) bereits durch Satz (3.12) bewiesen. Aber auch die letztgenannte Gruppe existiert; sie ist ebenfalls ein semidirektes Produkt, und zwar der elementar-abelschen p-Gruppe $A = \langle a, b\rangle \simeq C_p \times C_p = \mathbb{F}_p^2$ mit $C_p = \langle c\rangle$ bzgl. der Operation

$$C_p \to \operatorname{Aut}(F_p^2) = \mathrm{GL}_2(\mathbb{F}_p)\,, \quad c \mapsto \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\,.$$

(Die angegebene Matrix hat die Ordnung p, so daß die Abbildung ein wohldefinierter Homomorphismus ist.) Es bleibt zu zeigen, daß auch die letzte Gruppe nicht zu einer der vorherigen isomorph sein kann. Dazu zeigen wir, daß diese Gruppe den Exponenten p hat, d. h. $x^p = 1$ für alle $x \in G$ gilt. Dies scheint klar, da die Erzeugenden die Ordnung p haben, erfordert aber einen Beweis, da G nicht abelsch ist. (Der Beweis ist auch nur im Falle $p \neq 2$ möglich!) Jedes $x \in G$

ist darstellbar als $x = c^l h$ mit $h \in A = \langle a, b\rangle$, also wegen der Kommutativität von A $h = b^m a^n$. Damit sind alle Elemente von G von der Form $x = c^l b^m a^n$. Wir folgern

$$
\begin{aligned}
&b^c = ab \implies b^{c^2} = (ab)^c = a^c b^c = a \cdot ab = a^2 b \implies \ldots \implies b^{c^l} = a^l b\,,\\
&(b^\mu)^{c^l} = (b^{c^l})^\mu = (a^l b)^\mu = b^\mu a^{l\mu} \implies b^\mu c^l = c^l b^\mu a^{l\mu}\,,\\
&c^\lambda b^\mu a^\nu \cdot c^l b^m a^n = c^\lambda b^\mu c^l b^m a^{\nu+n} = c^{\lambda+l} b^{\mu+m} a^{l\mu} a^{\nu+n} = c^{\lambda+l} b^{\mu+m} a^{\nu+n+l\mu}\,,\\
&(c^l b^m a^n)^3 = c^{2l} b^{2m} a^{2n+lm} \cdot c^l b^m a^n = c^{3l} b^{3m} a^{3n+lm+l\cdot 2m}\,,\\
&(c^l b^m a^n)^p = c^{pl} b^{pm} a^{pn+lm+2lm+3lm+\ldots+(p-1)lm} = a^{lm\frac{p(p-1)}{2}} = (a^p)^{lm(p-1)/2} = 1
\end{aligned}
$$

(Man beachte am Ende $p \neq 2$!)

Anmerkung: Die letztgenannte Gruppe existiert auch für $p = 2$, ist dann aber *nicht* vom Exponenten 2. Für $p = 2$ entnimmt man nämlich aus der letzten Formel

$$(c^l b^m a^n)^2 = c^{2l} b^{2m} a^{2n+lm} = a^{lm}\,,$$

so daß sich für $l = m = 1$ *nicht* $(cb)^2 = 1$ ergibt. Vielmehr gilt $(cb)^2 = a$, also $\mathrm{ord}(cb) = 4$. Damit hat $G = \langle a, b, c\rangle = \langle cb, c\rangle$ einen zyklischen Normalteiler $A = \langle cb\rangle$ der Ordnung 4, auf dem c wie folgt operiert:

$$(cb)^c = c^c b^c = c \cdot ab = c(cb)^2 b = ccbcbb = bc = b^{-1}c^{-1} = (cb)^{-1}\,.$$

Damit ist $G = \langle cb, c\rangle$ die Diedergruppe D_8.

§4 Auflösbare Gruppen

a. Hauptreihen, Satz von Jordan-Hölder

(4.1) Definition: Sei G eine endliche Gruppe, A eine Automorphismengruppe von G, d.h. $A \leq \mathrm{Aut}(G)$. Dann definieren wir:

a) Eine *A-Reihe* von G ist eine Folge

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

von A-invarianten Untergruppen G_i von G mit $G_i \triangleleft G_{i-1}$ für alle i.

Spezialfälle: $A = \{\mathrm{id}_G\}$: Subnormalreihe
$A = \mathrm{Inn}\, G$: Normalreihe
$A = \mathrm{Aut}\, G$: charakteristische Reihe

b) Eine *A-Hauptreihe* von G ist eine maximale A-Reihe von G ohne Wiederholungen, d.h. eine A-Reihe aus lauter verschiedenen Untergruppen, die sich nicht echt erweitern läßt zu einer längeren A-Reihe.

Als *Länge* einer solchen A-Hauptreihe wollen wir die um 1 verringerte Anzahl der Untergruppen in dieser Reihe definieren, also die Zahl r bei der in a) gewählten Indizierung.

Spezialfälle: $A = \{\mathrm{id}_G\}$: Kompositionsreihe
$A = \mathrm{Inn}\, G$: Hauptreihe

c) Die *Faktoren* einer A-Reihe $G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_r = \{1\}$ sind die Faktorgruppen

$$G_{i-1}/G_i \quad (i = 1, \ldots, r).$$

Entsprechend spricht man von *Kompositions-* bzw. *Hauptfaktoren.*

Wir bemerken, daß für endliche Gruppen A-Hauptreihen stets existieren, genauer: Jede A-Reihe läßt sich nach Weglassen der Wiederholungen zu einer A-Hauptreihe verfeinern. Da ein Normalteiler $G_{i+1} \lhd G_i$ genau dann maximal ist, wenn die Faktorgruppe G_i/G_{i+1} einfach ist, kann man Kompositionsreihen charakterisieren als die Subnormalreihen mit einfachen Faktoren. Auf die Struktur der Hauptfaktoren werden wir später (Satz (4.13)) zurückkommen.

Eine endliche Gruppe besitzt im allgemeinen viele A-Hauptreihen, aber der folgende wichtige Satz von Jordan-Hölder zeigt, daß die A-Hauptfaktoren verschiedener A-Hauptreihen übereinstimmen, also *Invarianten* der Gruppe G sind.

(4.2) Satz: (Jordan-Hölder)
Sei G eine endliche Gruppe und A eine Automorphismengruppe von G. Dann gilt:
Je zwei A-Hauptreihen haben die gleiche Länge und nach geeigneter Umnumerierung sind ihre Faktoren isomorph.
Die A-Hauptfaktoren und ihre Vielfachheiten in einer beliebigen A-Hauptreihe sind also Invarianten der Gruppe G.

Dieser Satz ergibt sich unmittelbar aus dem folgenden Verfeinerungssatz von Zassenhaus-Schreier:

(4.3) Proposition: (Zassenhaus-Schreier) *Je zwei A-Reihen von G*

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_r = \{1\}, \quad G = H_0 \rhd H_1 \rhd \cdots \rhd H_s = \{1\}$$

besitzen Verfeinerungen mit gleich viel Gliedern und – nach geeigneter Umnumerierung – isomorphen Faktoren.

Beweis: : Diese Verfeinerungen definieren wir, indem wir in jeden Schritt der einen Reihe die andere Reihe 'hineinzwängen' durch die Definition:

$$G_{ij} := G_{i+1} \cdot (G_i \cap H_j), \quad i = 0, \ldots, r\,;\, j = 0, \ldots, s\,.$$

Dabei haben wir – der leichteren Indizierung wegen – $G_{r+1} = \{1\}$ gesetzt. Wir erhalten so die folgende Reihe von A-invarianten Untergruppen

$$G = G_{00} \rhd G_{01} \rhd \cdots \rhd G_{0s} = G_{10} \rhd G_{11} \rhd \cdots \rhd G_{r-1,s} = G_{r0} = \cdots = G_{rs} = \{1\},$$

die wegen $G_{i0} = G_i$ eine Verfeinerung der Reihe der G_i darstellt.

Genauso verfährt man mit der Reihe der H_i und definiert

$$H_{ji} := H_{j+1} \cdot (H_j \cap G_i), \quad j = 0, \ldots, s\,;\, i = 0, \ldots, r\,.$$

Beide Reihen haben $(r+1)\cdot(s+1)$ Glieder und wegen $G_{i-1,s} = G_{i0}$ für $i = 1, \ldots, r$ bzw. $H_{j-1,r} = H_{j0}$ für $j = 1, \ldots, s$ bleibt zu zeigen:

$$\begin{array}{lll} G_{i,j+1} & \lhd G_{ij} & \text{für } i = 0, \ldots, r\,,\, j = 0, \ldots, s-1\,, \\ H_{j,i+1} & \lhd H_{ji} & \text{für } j = 0, \ldots, s\,,\, i = 0, \ldots, r-1\,, \\ \text{und} & & \\ G_{ij}/G_{i,j+1} & \simeq H_{ji}/H_{j,i+1} & \text{für } i = 0, \ldots, r-1\,, j = 0, \ldots, s-1\,. \end{array}$$

Diese Behauptungen sind Inhalt des folgenden

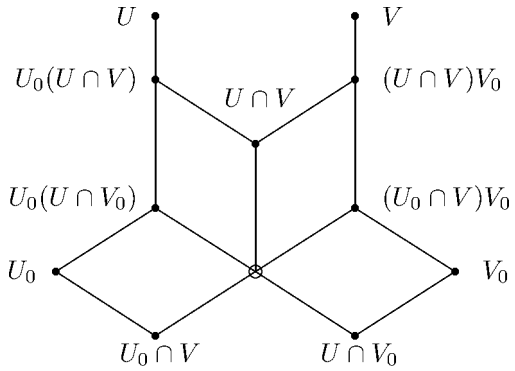
(4.4) Lemma: (Butterfly-Lemma) *Sei G eine Gruppe, U, U_0, V, V_0 Untergruppen von G mit $U_0 \lhd U$ und $V_0 \lhd V$. Dann gilt:*

$$U_0(U \cap V_0) \lhd U_0(U \cap V), \quad (U_0 \cap V)V_0 \lhd (U \cap V)V_0$$

und die Faktorgruppen sind isomorph:

$$U_0(U \cap V)/U_0(U \cap V_0) \simeq (U \cap V)V_0/(U_0 \cap V)V_0\,.$$

Das folgende Diagramm veranschaulicht die in diesem Lemma studierte Situation und auch den Namen 'Butterfly-Lemma':



Beweis von (4.4): Wegen $U_0 \lhd U$ ist $U_0 \cdot (U \cap V)$ Untergruppe von U; da außerdem V_0 Normalteiler in V, also $U \cap V_0$ Normalteiler in $U \cap V$ ist, folgen zunächst einmal die Behauptungen von (4.4) über die Normalteilereigenschaft.

Aufgrund eines der Isomorphiesätze der Gruppentheorie gilt

$$U_0(U \cap V) \,/\, U_0(U \cap V_0) \simeq U \cap V \,/\, (U \cap V) \,\cap\, U_0(U \cap V_0).$$

Wir zeigen nun, daß der 'Nenner' dieser Faktorgruppe $U \cap V \cap U_0(U \cap V_0)$ übereinstimmt mit $(U_0 \cap V)(U \cap V_0)$ (siehe das besonders gekennzeichnete Zentrum des obigen Diagramms):

$$U_0(U \cap V_0) \,\cap\, U \cap V = (U_0 \cap V)(U \cap V_0).$$

Zum Beweis braucht man dabei lediglich die Inklusion '$\subseteq$' zu überprüfen. Für $u_0 \in U_0$ und $w \in U \cap V_0$ gilt nun:

$$u_0 w \in U_0(U \cap V_0) \,\cap\, U \cap V \;\Rightarrow\; u_0 w \in V \;\Rightarrow\; u_0 \in V \;\Rightarrow u_0 w \in (U_0 \cap V)(U \cap V_0).$$

Wir erhalten also die folgende Isomorphie

$$U_0(U \cap V) \,/\, U_0(U \cap V_0) \simeq U \cap V \,/\, (U_0 \cap V)(U \cap V_0)\,,$$

aus der sich aus Symmetriegründen die Behauptung des Butterfly-Lemmas ergibt. □

b. Auflösbare Gruppen

(4.5) Definition: Eine endliche Gruppe heißt *auflösbar,* wenn alle ihre Kompositionsfaktoren abelsch sind.

Da Kompositionsfaktoren einfache Gruppen sind, bedeutet die Forderung in (4.5), daß die Kompositionsfaktoren auflösbarer Gruppen zyklische Gruppen von Primzahlordnung ('primzyklisch') sind. Offenbar sind abelsche Gruppen auflösbar. Aber auch nilpotente Gruppen sind auflösbar, denn (siehe (2.13)) maximale Untergruppen in nilpotenten Gruppen sind Normalteiler und haben Primzahlindex.

(4.6) Proposition: *Für eine endliche Gruppe G sind äquivalent:*

i) G ist auflösbar.

ii) G besitzt eine Subnormalreihe

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

mit abelschen Faktoren.

iii) Definiert man induktiv die absteigende Kommutatorreihe
durch $G^{(0)} := G$ und $G^{(i+1)} := [G^{(i)}, G^{(i)}]$, so existiert ein $k \in \mathbb{N}$ mit $G^{(k)} = \{1\}$.

Wir vermerken als Folgerung das

(4.7) Korollar: *Sei G eine endliche Gruppe. Dann gilt:*
a) Untergruppen auflösbarer Gruppen sind selbst auflösbar.
b) Ist N Normalteiler in G, so gilt sogar:

$$G \text{ auflösbar} \iff N \text{ und } G/N \text{ auflösbar.}$$

Beweis von (4.7) aus (4.6):
a) ergibt sich unmittelbar aus der Charakterisierung (4.6),iii) der Auflösbarkeit.
b)'$\Rightarrow$' ergibt sich aus a) und der Charakterisierung (4.6),ii): Der natürliche Epimorphismus $\nu\colon G \to G/N$ bildet eine Subnormalreihe von G mit abelschen Faktoren auf eine Subnormalreihe von G/N ab, deren Faktoren dann ebenfalls abelsch sind. Für '$\Leftarrow$' setzt man eine Subnormalreihe von N fort zu einer Subnormalreihe von G, indem man die vollen Urbilder einer Subnormalreihe von G/N unter ν bildet.

Beweis von (4.6): i) $\Rightarrow$ ii): Ist G auflösbar, so ist eine Kompositionsreihe von G eine Subnormalreihe mit den in ii) geforderten Eigenschaften.
ii) $\Rightarrow$ i): Verfeinert man ein Subnormalreihe wie in ii) zu einer Kompositionsreihe, so hat diese abelsche Faktoren und G ist auflösbar.
iii) $\Rightarrow$ ii): Die Kommutatorgruppe $G' = [G, G]$ ist charakterisiert als der kleinste Normalteiler in G mit abelscher Faktorgruppe. Daher ist die absteigende Kommutatorreihe $G^{(i)}$, wenn sie bis $\{1\}$ 'hinabsteigt', eine Subnormalreihe mit abelschen Faktoren. ii) $\Rightarrow$ iii): Da G/G_1 abelsch ist, folgt aus der bereits genannten Charakterisierung der Kommutatorgruppe $G^{(1)} = G' \subseteq G_1$, woraus man induktiv $G^{(i)} \subseteq G_i$, und damit iii) folgert. □

Wir wollen nun die Untersuchungen aus §3 über Komplemente in 'teilerfremden Gruppenerweiterungen', insbesondere Satz (3.9), vom abelschen Fall auf die auflösbare Situation ausdehnen und den folgenden Satz von Zassenhaus beweisen:

(4.8) Satz: (Zassenhaus) *Sei G eine endliche Gruppe, H ein Normalteiler, dessen Ordnung $\# H$ zu seinem Index $(G\colon H)$ teilerfremd ist. Dann gilt:*
Sind H oder G/H auflösbar, so sind alle Komplemente zu H in G konjugiert.

Anmerkung: Auf die Auflösbarkeitsforderung kann man verzichten, da sie nach dem Satz von Feit-Thompson stets erfüllt ist: Dieser Satz besagt, daß jede Gruppe ungerader Ordnung auflösbar ist. Da $\# H$ und $(G\colon H) = \# G/H$ teilerfremd sind, hat eine der beiden Gruppen ungerade Ordnung und ist folglich auflösbar.

Beweis: Nach Satz (3.8) wissen wir, daß ein Komplement U zu H in G existiert. Die Voraussetzung von (4.8) besagt dann: Der Normalteiler H oder das Komplement U ist auflösbar. Der Beweis von (4.8) erfolgt induktiv über die Ordnung $\# G$ von G (für beide Fälle getrennt).
1) Der Normalteiler ist auflösbar.
Die Behauptung gelte für alle auflösbaren Normalteiler $\widetilde{H} \lhd \widetilde{G}$ in Gruppen $\widetilde{G}$ mit $\# \widetilde{G} < \# G$, wenn die Teilerfremdheitsbedingung erfüllt ist.

Seien nun U_1 und U_2 zwei Komplemente zu H in G. Da H auflösbar ist, ist $H' = [H, H] \neq H$ und als charakteristische Untergruppe des Normalteilers $H \lhd G$ ist H' auch Normalteiler in G. Offenbar sind die Gruppen $U_i H'/H'$ Komplemente zu H/H' in G/H', denn

$$\# U_i H'/H' = \# U_i/U_i \cap H' = \# U_i = (G\colon H) = (G/H'\colon H/H')$$

und bei teilerfremden Gruppenerweiterungen sind Komplemente bereits als Untergruppen der passenden Ordnung charakterisiert (siehe die Überlegungen unmittelbar vor Satz (3.8)).

Ist nun $\#\,G/H' = \#\,G$, so muß $H' = \{1\}$, also H abelsch sein. In diesem Fall ist aber die Behauptung bereits bewiesen worden (Satz (3.9)).

Also sei $H' \neq \{1\}$ und somit $\#\,G/H' < \#\,G$. Aufgrund der Induktionsvoraussetzung (alle Forderungen sind offenbar erfüllt) folgt die Konjugiertheit der Komplemente U_iH'/H' in G/H': Es existiert also ein $\sigma \in G$ mit

$$U_1H'/H' = (U_2H'/H')^{\sigma H'} = U_2^\sigma H'/H'.$$

Ersetzt man U_2 durch die konjugierte Gruppe U_2^σ, so kann man o.E. annehmen

$$U_1H' = U_2H' =: \widetilde{G}.$$

Damit sind die U_i offenbar Komplemente zum auflösbaren Normalteiler $H' \lhd \widetilde{G}$. Wegen $H' \neq H$ hat $\widetilde{G}$ kleinere Ordnung als G und es folgt wiederum aus der Induktionsvoraussetzung die behauptete Konjugiertheit der U_i.

2) Das Komplement ist auflösbar.

Man wählt zunächst einen Normalteiler $N \lhd G$ minimal mit der Eigenschaft $H \subsetneq N$.

Ist $N = G$, so ist $U \simeq G/H$ einfach und auflösbar, also $U \simeq C_p$ primzyklisch (p eine Primzahl). Wegen der Teilerfremdheitsbedingung ist U, und jedes Komplement zu H in G eine p-Sylowgruppe. Diese sind aber bekanntlich untereinander konjugiert.

Sei nun also $N \neq G$. Wegen $H \subset N$ gilt $N = N \cap G = N \cap U_iH = (N \cap U_i)H$. Die Untergruppen $N \cap U_i$ sind daher Komplemente zu H in N. Mit U_i sind natürlich auch die Untergruppen $N \cap U_i$ auflösbar und ihre Ordnung prim zur Ordnung von H, so daß wieder nach Induktionsvoraussetzung folgt:

$$N \cap U_1 = (N \cap U_2)^\rho = N \cap U_2^\rho\,.$$

O. E. sei $N \cap U_1 = N \cap U_2 =: L$. Wegen $N \lhd G$ ist L Normalteiler in U_i, also $U_i \subset N_G(L)$. Daraus folgt

$$N_G(L) = N_G(L) \cap U_iH = U_i(N_G(L) \cap H).$$

Damit sind die U_i auflösbare Komplemente zu $N_G(L) \cap H$ in $N_G(L)$, und wir erhalten im Falle $N_G(L) \neq G$ per Induktionsvoraussetzung die Behauptung.

Ist $N_G(L) = G$, so betrachte man G/L. Hierin sind dann die U_i/L auflösbare Komplemente zu $HL\,/\,L$. Wäre nun $\#\,G/L = \#G$, so müßte $L = N \cap U_i = \{1\}$ sein. Dann aber erhielte man den Widerspruch

$$\#G \geq \#N \cdot \#U_i > \#H \cdot \#U_i = \#G\,.$$

Also ist G/L von echt kleinerer Ordnung als G und nach Induktionsvoraussetzung sind die U_i/L, und damit die U_i selbst konjugiert.

c. π-Hallgruppen

(4.9) Definition: Sei π eine nicht-leere Menge von Primzahlen. π' bezeichne das Komplement von π in der Menge $\mathcal{P}$ aller Primzahlen. Eine *π-Zahl* ist eine natürliche Zahl, in deren Primzerlegung nur Primfaktoren aus π vorkommen. $\langle\pi\rangle$ bezeichne die Menge aller π-Zahlen.

a) Eine *π-Gruppe* ist eine Gruppe G, deren Ordnung eine π-Zahl ist.

b) Eine π-Halluntergruppe einer Gruppe G ist eine π-Untergruppe $H \subseteq G$, deren Index in G eine π'-Zahl ist.

c) Eine Gruppe G heißt *π-separiert,* wenn alle Hauptfaktoren von G π- oder π'-Gruppen sind.

d) Schließlich heißt G *π-auflösbar,* wenn G π-separiert ist und die π-Hauptfaktoren auflösbar sind.

Offenbar sind Ordnung und Index von π-Halluntergruppen teilerfremd und ihre Ordnung als die größte π-Zahl, die $\#G$ teilt, eindeutig festgelegt. Außerdem sind die Halluntergruppen natürliche Verallgemeinerungen der Sylowuntergruppen, denn für eine Primzahl p sind die $\{p\}$-Halluntergruppen gerade die p-Sylowuntergruppen von G.

(4.10) Bemerkung: Unter- und Faktorgruppen von π-separierten bzw. π-auflösbaren Gruppen sind selbst π-separiert bzw. π-auflösbar.

Beweis: Sei N *Normalteiler* in G und $\nu\colon G \to G/N$ der natürliche Epimorphismus. Dann überführt ν eine Hauptreihe von G in eine Hauptreihe von G/N, deren Faktoren Quotienten der Hauptfaktoren von G sind (Isomorphiesätze anwenden). Damit ist die Behauptung in diesem Falle klar.
Für Untergruppen U in G schneidet man eine Hauptreihe von G mit U und erhält eine Normalreihe von U, deren Faktoren Untergruppen der Hauptfaktoren von G sind. Verfeinert man diese Normalreihe zu einer Hauptreihe, so haben deren Faktoren ebenfalls die behaupteten Eigenschaften. □

(4.11) Satz: *Sei π eine nicht-leere Menge von Primzahlen und G eine endliche, π-separierte Gruppe. Dann gilt:*

a) G besitzt π-Halluntergruppen.

Ist G zusätzlich π- oder π'-auflösbar, so gilt:

b) Je zwei π-Halluntergruppen von G sind konjugiert in G, und

c) jede π-Untergruppe U von G ist in einer π-Halluntergruppe enthalten.

Anmerkung: Wie beim Satz von Zassenhaus (4.8) kann auch hier nach dem Satz von Feit-Thompson auf die Auflösbarkeitsforderung für b),c) verzichtet werden, da sie stets erfüllt ist.

Beweis: Der Beweis dieses Satzes erfolgt per Induktion über die Gruppenordnung. Der Satz gelte für alle Gruppen $\widetilde{G}$ mit einer kleineren Ordnung als G. Um den Induktionsschritt durchzuführen, wählen wir einen minimalen Normalteiler $N \lhd G$. Dieser ist ein Hauptfaktor von G, also eine π- oder π'-Gruppe.

Zum Beweis von a): Wegen $N \neq \{1\}$ hat G/N kleinere Ordnung als G; außerdem ist G/N gemäß Bemerkung (4.10) selbst π-separiert, so daß nach Induktionsvoraussetzung eine π-Halluntergruppe $H/N \subseteq G/N$ existiert. Es gilt also

$$\#\, H/N = (H\colon N) \in \langle\pi\rangle \text{ und } (G\colon H) = (G/N\colon H/N) \in \langle\pi'\rangle.$$

Ist $\#N$ eine π-Zahl, so auch $\#H$, also ist H eine π-Halluntergruppe.

Gilt jedoch $\#N \in \langle\pi'\rangle$, so sind Index und Ordnung des Normalteilers $N \lhd H$ teilerfremd, so daß N nach dem Satz von Zassenhaus (3.8) ein Komplement U in H besitzt. Offenbar gilt dann

$$\#U = (H\colon N) \in \langle\pi\rangle \;\text{ und }\; (G\colon U) = (G\colon H)(H\colon U) = (G\colon H)\#N \in \langle\pi'\rangle,$$

das heißt U ist eine π-Halluntergruppe von G.

ad b): Seien H_1 und H_2 π-Halluntergruppen von G und G π- oder π'-auflösbar. Zunächst einmal sind dann die Gruppen H_iN/N π-Halluntergruppen in G/N, also nach Induktionsvoraussetzung konjugiert in G/N:

$$H_2N = (H_1N)^\sigma \supseteq H_1^\sigma \quad \text{für ein } \sigma \in G.$$

Gilt $\#N \in \langle\pi\rangle$, so ist auch $\#\, H_2N$ als Teiler von $\#H_2\#N$ eine π-Zahl. Daher muß die π-Halluntergruppe H_2 mit H_2N übereinstimmen, also folgt

$$H_2 = H_2N \supseteq H_1^\sigma,$$

und damit aus Ordnungsgründen die Gleichheit $H_2 = H_1^\sigma$.

Es gelte nun $\#N \in \langle\pi'\rangle$. Dann ist $\#H_1^\sigma = \#H_2$ prim zu $\#N$, also sind Ordnung und Index des Normalteilers $N \lhd H_1^\sigma N = H_2 N$ teilerfremd. Nach Satz (4.8) sind dann die Komplemente H_1^σ und H_2 von N in dieser Gruppe konjugiert, wenn N oder H_2 auflösbar sind. Eins von beidem muß aber gelten, denn ist G π-auflösbar, so ist die π-Untergruppe H_2 auflösbar, und ist G π'-auflösbar, so ist die π'-Untergruppe N auflösbar.

ad c): Sei U eine π-Untergruppe von G. Dann ist die π-Untergruppe UN/N in einer π-Halluntergruppe H'/N von G/N enthalten. Ist H eine π-Halluntergruppe von G, so ist HN/N eine π-Halluntergruppe von G/N, also zu H'/N konjugiert, so daß folgt:

$$U \subseteq H' = (HN)^\sigma = H^\sigma N \quad \text{für ein } \sigma \in G.$$

Ist $\#N \in \langle\pi\rangle$, so ist $H^\sigma N$ eine π-Gruppe, also gleich der darin liegenden π-Halluntergruppe H^σ, und c) ist in diesem Fall bewiesen.

Ist $\#N \in \langle\pi'\rangle$, so folgt

$$UN = UN \cap H^\sigma N = (UN \cap H^\sigma)N = VN$$

mit $V := UN \cap H^\sigma \subseteq H^\sigma$. U und V sind π-Gruppen, mithin Komplemente zum π'-Normalteiler N in der Gruppe $UN = VN$. Wiederum ist N oder U auflösbar, so daß wie in b) die Konjugiertheit der Komplemente U und V in $UN = VN$ folgt. Da nach Definition V in einer π-Halluntergruppe H^σ liegt, gilt dies dann auch für die konjugierte Untergruppe U, und c) ist bewiesen. □

Die Aussagen von Satz (4.11) sind offenbar Verallgemeinerungen der p-Sylowsätze, jedoch sind hier die Voraussetzungen an G von der Primzahlmenge π, für die die π-Hallsätze gelten sollen, abhängig. Die Gültigkeit *aller* π-Hallsätze für eine Gruppe G ist gesichert, wenn G auflösbar ist:

(4.12) Satz: (π-Hallsätze)
Ist G eine endliche auflösbare Gruppe, so gilt für jede Primzahlmenge π:

a) Es existieren π-Halluntergruppen in G,

b) sie sind alle untereinander konjugiert und

c) jede π-Untergruppe ist in einer π-Halluntergruppe enthalten.

Beweis: Da G und also alle Hauptfaktoren auflösbar sind, genügt es nach Satz (4.11) zu zeigen, daß G für alle $\pi \subseteq \mathcal{P}$ π-separiert ist. Dies ist genau dann der Fall, wenn alle Hauptfaktoren von G Gruppen von Primzahlpotenzordnung sind, denn enthielte ein Hauptfaktor in seiner Ordnung zwei Primzahlen $p \neq q$, so wäre er weder eine $\{p\}$- noch eine $\{p\}'$-Gruppe. Wir werden nun sogar zeigen, daß die Hauptfaktoren auflösbarer Gruppen abelsche Gruppen von Primzahlexponenten sind.

Um dies nachzuweisen, studieren wir allgemeiner die Struktur von Hauptfaktoren beliebiger endlicher Gruppen. Nun ist jeder Hauptfaktor einer Gruppe G zugleich minimaler Normalteiler einer Faktorgruppe von G, also genügt es, die Struktur minimaler Normalteiler in beliebigen endlichen Gruppen zu untersuchen.

Sei N ein minimaler Normalteiler in G. Dann ist N charakteristisch einfach, das heißt N enthält außer $\{1\}$ und N keine unter allen Automorphismen von N invariante Untergruppe.

Begründung: Ist M eine charakteristische Untergruppe von N, so ist M ein Normalteiler in G, denn die Konjugation mit einem Element aus G ist ein Automorphismus des Normalteilers N, läßt also M invariant. Da N ein minimaler Normalteiler ist, muß $M = N$ oder $M = \{1\}$ sein.

Damit ist gezeigt, daß die Hauptfaktoren endlicher Gruppen charakteristisch einfache Gruppen sind, die natürlich selbst auch auflösbar sind, wenn G auflösbar ist. Die obigen Behauptungen ergeben sich damit aus dem nachfolgenden Struktursatz für charakteristisch einfache Gruppen.

(4.13) Satz: *a) Eine Gruppe G ist genau dann charakteristisch einfach, wenn sie das n-fache direkte Produkt einer einfachen Gruppe E mit sich selbst ist:*

$$G \simeq E^n = E \times \cdots \times E.$$

b) Ist $G = \prod_{i=1}^{n} E_i$ ein solches n-faches direktes Produkt einer einfachen Gruppe $E = E_i$ mit sich, so sind alle minimalen Normalteiler von G isomorph zu E; ist zusätzlich G nicht-abelsch, so sind die Untergruppen $E_J := \prod_{j\in J} E_j$ ($J \subseteq \{1, \ldots, n\}$) die einzigen Normalteiler von G.

Hieraus folgt (4.12): Die Hauptfaktoren *auflösbarer* Gruppen sind *auflösbare* charakteristische einfache Gruppen. Nach (4.13) haben sie die Struktur E^n mit einer einfachen *und auflösbaren* Gruppe E. Also ist E zyklisch von Primzahlordnung und $E^n \simeq \mathbb{F}_p^n$ eine p-elementar-abelsche Gruppe, insbesondere von Primzahlpotenzordnung. Dies genügte zum Beweis von (4.12).

Beweis von (4.13): a) Sei G charakteristisch einfach. Wir wählen einen minimalen Normalteiler E in G. Dann sind auch alle E^α ($\alpha \in \operatorname{Aut} G$) minimale Normalteiler und ihr Erzeugnis $\langle E^\alpha \mid \alpha \in \operatorname{Aut} G\rangle$ stimmt als charakteristische Untergruppe von G mit G überein:

$$G = \langle E^\alpha \mid \alpha \in \operatorname{Aut} G\rangle.$$

Wir zeigen nun, daß G direktes Produkt gewisser E^{α_i} ist. Dazu wählen wir einen Normalteiler $H \lhd G$ maximal mit der Eigenschaft

$$H = E^{\alpha_1} \times \cdots \times E^{\alpha_r}$$

und zeigen, daß H alle E^α umfaßt, also G ist.

Angenommen $E^\alpha \not\subseteq H$ für ein $\alpha \in \operatorname{Aut} G$. Dann ist $E^\alpha \cap H$ ein Normalteiler in G, echt enthalten im minimalen Normalteiler E^α, also $E^\alpha \cap H = \{1\}$. Da sowohl E^α als auch H Normalteiler in G sind, folgt hieraus

$$\langle H, E^\alpha\rangle = H \cdot E^\alpha \simeq H \times E^\alpha,$$

denn die Elemente von H und E^α sind vertauschbar: Ist nämlich $h \in H$ und $e \in E^\alpha$, so gilt für den Kommutator

$$[h,e] = h^{-1}e^{-1}he = \begin{cases} h^{-1}h^e \in H \\ (e^{-1})^h e \in E^\alpha \end{cases}, \text{ also } [h,e] \in H \cap E^\alpha = \{1\}.$$

Damit ist ein größerer Normalteiler $\langle H, E^\alpha\rangle \lhd G$ gefunden, der direktes Produkt gewisser E^{α_i} ist, im Widerspruch zur Maximalität von H. Also ist eine Implikation von a) bewiesen. Die andere folgern wir aus b).

Ad b): Offenbar ist die Reihe

$$G = \prod_{i=1}^{n} E_j \rhd \prod_{i=1}^{n-1} E_j \rhd \cdots \rhd E_1 \rhd \{1\}$$

eine Normalreihe von G, deren sämtlich Faktoren zu E isomorph sind. Da E einfach ist, ist diese Normalreihe eine Hauptreihe. Also ist E einziger Hauptfaktor von G (mit Vielfachheit n), und jeder minimale Normalteiler von G muß nach dem Satz von Jordan-Hölder (4.2) zu E isomorph sein.

Zum Beweis der zweiten Behauptung von b) sei G, also E nicht-abelsch und N ein beliebiger Normalteiler von G. Ist $x \in N$, $x = e_1 \cdot \ldots \cdot e_n$ mit $e_i \in E_i$, so gilt für alle j:

$$(*) \qquad e_j \neq 1 \implies E_j \subseteq N.$$

Ist dies gezeigt, so muß N mit dem direkten Produkt E_J all der E_j übereinstimmen, die in N liegen: Existierte nämlich ein $x \in N \setminus E_J$, so folgte $x = \prod_{i=1}^{n} e_i$ mit $e_i \neq 1$ für ein $i \notin J$. Gemäß $(*)$ läge dann E_i doch in N, im Widerspruch zur Wahl von $J \subseteq \{1, \ldots, n\}$.

Zum Beweis von $(*)$: Da $E_j = E$ nicht abelsch und einfach ist, muß E_j triviales Zentrum haben, also gilt $e_j \notin \mathrm{Zentr}(E_j)$ und es existiert ein $y \in E_j$ mit

$$1 \neq c := [y, e_j] = [y, x].$$

Da N und E_j Normalteiler in G sind, liegt c in $N \cap E_j$. Da E_j einfach ist und $N \cap E_j$ das Element $c \neq 1$ enthält, folgt $E_j = N \cap E_j \subseteq N$.

Wir beweisen nun die Umkehrung von a), indem wir für jeden Normalteiler $N \triangleleft G = \prod_{i=1}^{n} E_i$, $\{1\} \neq N \neq G$ zeigen, daß er nicht charakteristisch ist.

Abelscher Fall: Dann ist $E_i = E = \mathbb{F}_p$ der Primkörper von p Elementen und G ein $\mathbb{F}_p$-Vektorraum. Dessen Normalteiler sind die $\mathbb{F}_p$-Unterräume. Aus der linearen Algebra wissen wir, daß für jeden echten, nichttrivialen Unterraum N von G ein Automorphismus $\alpha \in \mathrm{Aut}\, G = \mathrm{GL}_n(\mathbb{F}_p)$ existiert mit $\alpha N \neq N$. (Zugleich sehen wir, daß Aussage b) im abelschen Fall nicht richtig ist, da es in einem Vektorraum der Dimension $n \geq 2$ wesentlich mehr Unterräume gibt, als die 2^n in b) genannten Unterräume.)

Nicht-abelscher Fall: Dann sind gemäß b) die Normalteiler von G gegeben durch die Untergruppen E_J. Diese sind echte Normalteiler für $\emptyset \neq J \neq \{1, \ldots, n\}$. Nun induziert jede Permutation $\sigma \in S_n$ einen Automorphismus $\widehat{\sigma} \in \mathrm{Aut}\, G$ durch

$$\widehat{\sigma}(e_1, \ldots, e_n) = (e_{\sigma(1)}, \ldots, e_{\sigma(n)}).$$

Offenbar kann man eine Permutation $\sigma \in S_n$ mit $\sigma(J) \neq J$ wählen, also folgt $\widehat{\sigma}(E_J) \neq E_J$. Damit ist E_J nicht $\widehat{\sigma}$-invariant, also nicht charakteristisch. □

Wir wollen nun zum Abschluß dieses Abschnittes zeigen, daß Satz (4.12) scharf ist, d.h. daß eine Gruppe, in der sämtliche π-Hallsätze gelten, notwendig auflösbar sein muß. Als Vorbereitung beweisen wir den folgenden

(4.14) Satz: (Wielandt) *Besitzt eine endliche Gruppe G drei auflösbare echte Untergruppen U_i mit paarweise teilerfremden Indizes in G, so ist G selbst auflösbar.*

Der *Beweis* erfolgt induktiv über die Gruppenordnung. Da die Untergruppen U_i teilerfremde Indizes haben, ergibt sich aus dem nachfolgenden Hilfssatz $(G\colon U_1 \cap U_2) = (G : U_1)(G : U_2)$ und daher $G = U_1 \cdot U_2$.

Hilfssatz: *Für eine endliche Gruppe G und Untergruppen U_i gilt:*

a) $(G : U_1 \cap U_2) \leq (G : U_1)(G : U_2)$

b) $(G : U_1 \cap U_2) = (G : U_1)(G : U_2) \iff G = U_1 \cdot U_2$

c) Haben die Untergruppen teilerfremde Indizes in G, so gelten die äquivalenten Bedingungen von b).

Beweis: Sei $D := U_1 \cap U_2$ der Durchschnitt und

$$U_1 = \dot{\bigcup_{i \in I}} D u_i^1$$

die Nebenklassenzerlegung von U_1 modulo D. Dann sind auch die Nebenklassen $U_2 u_i^1$ disjunkt; genauer:

$$(*) \qquad U_2 \ni u_i^1 (u_j^1)^{-1} \iff D = U_2 \cap U_1 \ni u_i^1 (u_j^1)^{-1} \iff i = j.$$

Damit folgt $(U_1 : D) = \#I \leq (G : U_2)$, wegen der Multiplikativität von Gruppenindizes also a).

Zugleich erkennt man, daß genau dann $\#I = (U_1 : D) = (G : U_2)$ gilt, wenn die Nebenklassen $U_2 u_i^1$ $(i \in I)$ sämtliche Nebenklassen modulo U_2 sind, d.h. wenn $G = \bigcup_{i\in I} U_2 u_i^1$ gilt. Offenbar ist dann $G = U_2U_1$. Aber auch umgekehrt folgt aus $G = U_2U_1$, daß man in U_1 ein Repräsentantensystem der U_2-Nebenklassen von G finden kann, welches dann nach $(*)$ ein Repräsentantensystem der D-Nebenklassen in U_1 ist. Damit ergibt sich die Indexgleichheit $(U_1 : D) = \#I = (G : U_2)$, und die Äquivalenz in b) ist bewiesen.

Wegen der Multiplikativität der Gruppenindizes sind die Indizes $(G : U_i)$ Teiler von $(G : D)$. Sind diese teilerfremd, so muß ihr Produkt $(G : U_1)(G : U_2)$ den Index $(G : D)$ teilen, also gemäß a) mit diesem übereinstimmen. □

Wir kehren zum Beweis von (4.14) zurück und wählen einen minimalen Normalteiler N in U_1. Dieser ist als auflösbare, charakteristisch einfache Gruppe gemäß Satz (4.13) eine p-Gruppe (p eine Primzahl). Nach Voraussetzung ist p entweder kein Teiler von $(G : U_2)$ oder von $(G : U_3)$; o.E. etwa $p \nmid (G : U_2)$. Dann gilt also

$(**)$ $\qquad\qquad \#N$ und $(G : U_2)$ sind teilerfremd.

Da N ein Normalteiler in U_1 ist, ist $N(U_1 \cap U_2)$ Untergruppe in U_1. Wendet man nun Teil b) des Hilfssatzes auf N, $D := U_1 \cap U_2$ und die Obergruppe ND an, so erhält man $(ND : N \cap D) = (ND : D)(ND : N)$, also $(ND : D) = (N : N \cap D)$. Diese Zahl ist offenbar sowohl Teiler von $\#N$ als auch von $(U_1 : D) = (G : U_2)$. Wegen $(**)$ folgt also $(ND : D) = 1$, d.h. $N \subseteq U_1 \cap U_2$.

Hieraus folgern wir, daß dann alle G-Konjugierten von N in U_2 liegen, denn für $\sigma = u_1u_2 \in G = U_1U_2$ gilt

$$N^\sigma = N^{u_1u_2} = N^{u_2} \subseteq D^{u_2} \subseteq U_2.$$

Da U_2 als auflösbar vorausgesetzt ist, ist der darin liegende von N erzeugte Normalteiler $\widehat{N} = \langle N^\sigma \mid \sigma \in G\rangle \lhd G$ ebenfalls auflösbar.

Die Faktorgruppe $G/\widehat{N}$ hat kleinere Ordnung als G und erfüllt wieder die Voraussetzungen des Satzes (mit den Untergruppen $U_i\widehat{N}/\widehat{N}$ (i=1,2,3)), so daß nach Induktionsvoraussetzung die Auflösbarkeit von $G/\widehat{N}$, und damit die von G folgt. □

Wir wollen dieses Auflösbarkeitskriterium von Wielandt benutzen, um die folgende Abgrenzung von Satz (4.12) zu beweisen:

(4.15) Satz: *Sei G eine endliche Gruppe und $\#G = \prod_{i=1}^r p_i^{n_i}$ die Primzerlegung ihrer Ordnung. Besitzt G für alle i Untergruppen U_i vom Index $p_i^{n_i}$, so ist G auflösbar.*

Beweis per Induktion über r: Ist $r = 1$, so ist G eine p-Gruppe, also bekanntermaßen auflösbar.

Im Falle $r = 2$ berufen wir uns auf den Satz von Burnside, demzufolge alle Gruppen mit einer Ordnung p^nq^m (p,q Primzahlen) auflösbar sind. [Dieser Satz ist mit Methoden der Darstellungstheorie beweisbar. Siehe etwa B. Huppert: Endliche Gruppen I, V, §7, (7.3)]

Sei nun $r \geq 3$. Wir setzen $U_{ij} = U_i \cap U_j$. Nach dem Hilfssatz im Beweis von (4.14) gilt dann

$$(U_i : U_{ij}) = p_j^{n_j} \quad \text{für } i \neq j.$$

Damit erfüllen die U_i alle Voraussetzungen von Satz (4.15), sind also gemäß Induktionsannahme auflösbar. Satz (4.14) zeigt dann die Auflösbarkeit von G.