## I. Nilpotente und auflösbare Gruppen

### §0 Notationen, Definitionen[1)]

**a. Gruppen.** Wir beginnen der Vollständigkeit halber mit der

**(0.1) 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), die folgenden Axiomen genügt:

(1) $\cdot$ ist assoziativ.

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

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

(I) $\bigwedge_{a\in G} \bigvee_{a^{-1}\in G} a^{-1} \cdot a = e = a \cdot a^{-1}$.

('Existenz von neutralem Element und Inversem'.)

**(0.2) 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 $\Omega$. Es ist $S_n = S(\{1, \ldots, n\})$ die symmetrische Gruppe vom Grade $n$. Es gilt $\#S(\Omega) = (\#\Omega)!$ für endliche Mengen $\Omega$.

(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

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

**b. Untergruppen, Nebenklassen.**

**(0.3) Definition:** a) Ist $H$ eine *Untergruppe* einer Gruppe $G$ (d. h. $1_G \in H$ und $a, b \in H \implies ab^{-1} \in H$), 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 nach $H$,
$H\backslash G = \{Ha \mid a \in G\}$ 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:

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

[1)] Nicht vorgetragen.

Aufgrund der Gruppeneigenschaft bilden die Nebenklassen eine Klasseneinteilung: $Ha \cup Hb = \emptyset$ 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

**(0.4) 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.

**(0.5) 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.**

**(0.6) 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 $G/\operatorname{Ke} f$ in natürlicher Weise mit einer Gruppenverknüpfung versieht: $a \operatorname{Ke} f \cdot b \operatorname{Ke} f = ab \operatorname{Ke} f$. Aber nicht für jede Untergruppe $H \leq G$ erhält man auf diese Weise eine Gruppenstruktur auf $G/H$! Vielmehr gilt:

**(0.7) 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)* $H = \operatorname{Ke} \nu$ *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

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

Damit ist i) $\Rightarrow$ iii) bewiesen. Wir zeigen nun iii) $\Rightarrow$ ii): Sei $H = \operatorname{Ke}\nu$ 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. $a^{-1}ha \in \operatorname{Ke}\nu = H$, 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. □

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

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

*ein Gruppenisomorphismus.*

## §1 Nilpotente Gruppen

1/9.4.2008

### a. Konjugation, innere Automorphismen, das Zentrum.

**(1.1) 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) Wir betrachten die Automorphismengruppe* $\operatorname{Aut}(G)$ *mit der Verknüpfung $\varphi \cdot \psi = \psi \circ \varphi$. Dann wird durch $x^\varphi = \varphi(x)$ für $x \in G$, $\varphi \in \operatorname{Aut}(G)$ eine Operation der Gruppe $(\operatorname{Aut}(G), \cdot)$ von rechts auf $G$ definiert, d. h. es gilt $x^{\varphi\psi} = (x^\varphi)^\psi$.*
*c) 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 $G$.*
*d) Die Abbildung $\iota : G \to \operatorname{Aut}(G)\,,\ a \mapsto (x \mapsto a^{-1}xa = x^a)$ ist ein Gruppenhomomorphismus von $G$ in die Gruppe $(\operatorname{Aut}(G), \cdot)$, 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 $G$:*

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

*e) $\operatorname{Inn}(G)$ 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 d), kann aber auch direkt nachgerechnet werden. b) ist klar.
c) 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.
d) 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. Wegen $x^{\iota(a)} = x^a$ zeigt sie zugleich die Homomorphie von $\iota$. Der Kern ist

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

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

$$x^{\varphi^{-1}\iota(a)\varphi} = \left(a^{-1} \cdot x^{\varphi^{-1}} \cdot a\right)^{\varphi} = (a^{-1})^{\varphi} \cdot x \cdot a^{\varphi} = x^b$$

mit $b = a^{\varphi}$. Damit ist das Konjugierte eines inneren Automorphismus $\iota(a)^{\varphi}$ in $\mathrm{Aut}(G)$ wieder ein innerer Automorphismus, nämlich $\iota(a^{\varphi})$. Gemäß (0.7) ist damit $\mathrm{Inn}(G)$ Normalteiler in $\mathrm{Aut}(G)$. □

**b. $p$-Gruppen.**

**(1.2) Proposition:** *Die Gruppe $G$ operiere (von links) auf der nicht-leeren endlichen Menge $\Omega$: $a \mapsto \sigma a$ ($\sigma \in G$). Es sei $Ga$ die Bahn von $a \in \Omega$ unter $G$ und $G_a = \{\sigma \in G \mid \sigma a = a\}$ die Fixgruppe. Dann gilt:*

*a) $G_{\sigma a} = \sigma G_a \sigma^{-1}$ für $a \in \Omega$, $\sigma \in G$: Die Fixgruppen der Elemente einer Bahn sind konjugierte Untergruppen.*

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

*c) Die Bahnen bilden eine Klasseneinteilung von $\Omega$:*

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

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

*d) (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 $\geq 2$ und Teiler von $\#G$.*

*Beweis:* a) rechne man nach. b) 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.
c) 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 $\Omega$ überdecken, folgt c).
d) 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 $2 \leq \#Ga = (G : G_a)$. □

**Zusatz:** Dieselben Aussagen gelten auch für eine Operation von rechts: $a \mapsto a^{\sigma}$ ($a \in \Omega$, $\sigma \in G$). Regel b) lautet dann recht suggestiv: $G_{a^{\sigma}} = \sigma^{-1}G_a\sigma = G_a^{\sigma}$.

**(1.3) Korollar:** *Operiert eine p-Gruppe G (eine Gruppe von Primzahlpotenzordnung $p^n$) auf einer Menge $\Omega$, so gilt:*

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

*Beweis:* In einer $p$-Gruppe sind alle Gruppenindizes $(G : G_a)$, die $\geq 2$ 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

**(1.4) Satz:** *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: $a \mapsto a^\sigma = \sigma^{-1}a\sigma$. Es liegt ein Operation von rechts vor, denn $a^{\sigma\tau} = (a^\sigma)^\tau$. Die *Bahn* von $a$ ist die Konjugationsklasse $C(a) = [a] = \{a^\sigma \mid \sigma \in G\}$ von $a$ in $G$. Die *Fixgruppe* $\{\sigma \in G \mid a^\sigma = a\} = \{\sigma \in G \mid a\sigma = \sigma a\} = \mathrm{Zentr}_G(a)$ ist der *Zentralisator* von $a$ in $G$. Die Länge der Bahn ist also die Mächtigkeit der Konjugationsklasse $\#C(a) = (G : \mathrm{Zentr}_G(a))$ und somit der Index des Zentralisators von $a$ in $G$.

Schließlich ist die Fixpunktmenge $\{a \in G \mid \bigwedge_{\sigma\in G} a^\sigma = a\} = Zentr(G)$ das Zentrum von $G$. Gemäß (1.3) gilt also in $p$-Gruppen $G$:

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

Ist $G$ nicht trivial, so ist mit $\#G$ auch $\#\mathrm{Zentr}(G)$ durch $p$ teilbar, also $\#\mathrm{Zentr}(G)$ nicht trivial. Damit ist (1.4) bewiesen. □

**b. Sylowsätze** 2/16.4.2008

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.

**(1.5) Proposition:** *In endlichen zyklischen Gruppen gibt es zu jedem Teiler d der Gruppenordnung genau 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 $\mathrm{ord}(a) = n$, 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 $d = \mathrm{ord}(a^k)$, 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 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 $\#H \leq p^s$

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

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 $T \subset G$

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

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

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

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. $\Omega'$ 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

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

($h_G(p^s)$ 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 $\Omega'$ 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

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

Da $p$ kein Teiler von $m$ ist, gilt nun

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

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 (1.5) 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:

**(1.6) 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:

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

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.

**(1.7) 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:*
*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:*

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

*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 (1.3)

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

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 $\Omega$ 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 $P^\sigma$ 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 $P^\sigma$ 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 (1.7) c)

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

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 (1.4) wissen wir, dass nicht-triviale $p$-Gruppen ein nicht-triviales Zentrum haben:

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

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

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

**(1.8) 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 und entsprechende Faktorgruppen sind isomorph:*

$$(G' : H') = (G : f^{-1}(H')) , \quad f^{-1}(H')^\sigma = f^{-1}(H'^{f(\sigma)}) ,$$
$$H' \lhd G' \Leftrightarrow f^{-1}(H') \lhd G , \quad H' \lhd G' \implies G/f^{-1}(H') \xrightarrow{\sim} G'/H' .$$

*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 $f$. Die Isomorphie der Faktorgruppen ergibt sich aus dem Isomorphiesatz. □

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 (1.8) (angewendet auf $\nu_i : G \twoheadrightarrow G/Z_i$) ergibt sich:

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

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

$$\{1\} \underset{\neq}{\subset} Z_1(G) \underset{\neq}{\subset} Z_2(G) \underset{\neq}{\subset} \ldots \underset{\neq}{\subset} Z_k(G) = G$$

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.

**(1.9) Satz:** *Nilpotente Gruppen sind charakterisiert durch die folgenden äquivalenten Bedingungen:* 3/30.4.2008

*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*

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

*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.*

*vii) Alle Elemente $x, y \in G$ mit teilerfremden Ordnungen sind vertauschbar.*

*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.

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 $G_k \subset N_k = \{1\}$, womit iii) bewiesen ist.

ad $(*)$: Seien $\sigma \in G$, $\tau \in N_i$ und damit $[\sigma, \tau] = \sigma^{-1}\tau^{-1}\sigma\tau$ 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 $(**)$:

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

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:

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

(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 allgemein für jede endliche Gruppe $G$:

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

Ist dies gezeigt, so folgt unter der Voraussetzung iv) daraus $H \not< G$, $H = G$, insbesondere $\mathcal{N}_G(P) = G$: $P$ ist Normalteiler in $G$.
Beweis der obigen Behauptung:

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

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 $\varphi_s$. 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 $\varphi_s$ 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.

vi) $\Longrightarrow$ vii) und vii) $\Longrightarrow$ v) als Übung. □

**Anmerkung:** a) Nilpotenz vererbt sich auf Unter- und Faktorgruppen.
Nilpotenz impliziert Auflösbarkeit, aber nicht umgekehrt.
Anders als bei der Auflösbarkeit, folgt aus der Nilpotenz von Normalteiler $N$ und Faktorgruppe $G/N$ nicht die Nilpotenz der Gruppe $G$.

**(1.10) 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 (1.9), 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 (1.9), vi), da abelsche Gruppen nilpotent sind (gemäß Charakterisierung i)).

### c. Frattinigruppe, Burnsidescher Basissatz.

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

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

**(1.12) Proposition:** *Sei $G$ eine endliche Gruppe.*

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

*b)* $\Phi(G)$ *besteht genau aus den Elementen von* $G$*, die in allen Erzeugendensystemen überflüssig sind:*

$$x \in \Phi(G) \iff \Big( \bigwedge_{M \subset G} \langle M \rangle = G \implies \langle M \setminus \{x\} \rangle = G \Big) .$$

*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) Es sind äquivalent:*

$$G \text{ nilpotent} \iff G/\Phi(G) \text{ abelsch} \iff G/\Phi(G) \text{ nilpotent.}$$

*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.