Charakterisierung des direkten Produkts zweier Gruppen. Erinnerung: Sind A, B Gruppen, so bezeichnet $A \times B$ das *direkte Produkt* von A und B; also die Menge der Paare (a, b) mit $a \in A$ und $b \in B$, mit komponentenweiser Multiplikation. Allgemeiner: Sind $A_1, \ldots, A_t$ Gruppen, so bezeichnet man mit $A_t \times \cdots \times A_t$ das direkte Produkt dieser Gruppen: also die Menge der Folgen $(a_1, \ldots, a_t)$ mit $a_i \in A_i$, und zwar mit komponentenweiser Multiplikation. Ist $A = A_1, \ldots, A_t$ eine Gruppe, so schreibt man A^t statt $A_1 \times \cdots \times A_t$.

Die Gruppen der Form C_p^t mit p Primzahl heißen *elementar abelsche* Gruppen. *Ist G eine abelsche Gruppe und ist p eine Primzahl, so bilden die Elemente der Ordnung p zusammen mit dem 1-Element eine Untergruppe,* und diese Untergruppe ist elementar abelsch.

Ist U eine Untergruppe der Gruppe A und V eine Untergruppe der Gruppe B, so ist $U \times V$ eine Untergruppe von $A \times B$. Sind U, V beides Normalteiler, so ist auch $U \times V$ ein Normalteiler von $A \times B$. Insbesondere sind $A \times \{1\}$ und $\{1\} \times B$ Normalteiler von $A \times B$, die zusammen $A \times B$ erzeugen und deren Durchschnitt die triviale Untergruppe $\{1\} \times \{1\} = \{1_{A \times B}\}$ ist. Durch diese Eigenschaften ist das direkte Produkt zweier Gruppen charakterisiert, denn es gilt:

Lemma. *Sind U, V Normalteiler einer Gruppe G mit $U \cap V = \{1\}$, so gilt $uv = vu$ für alle $u \in U, v \in V$; daher ist UV isomorph zu $U \times V$.* Man schreibt in diesem Fall einfach $UV = U \times V$.

Beweis: Es ist $uvu^{-1}v^{-1} = (uvu^{-1}) \cdot v^{-1}$ in V, aber auch $uvu^{-1}v^{-1} = u \cdot (vu^{-1}v^{-1})$ in U, also $uvu^{-1}v^{-1} = 1$. Dies zeigt, daß $uv = vu$ für alle $u \in U, v \in V$ gilt. Definiere einen Gruppen-Homomorphismus ϕ: $U \times V \to G$ durch $\phi((u, v)) = uv$ (um zu sehen, daß dies wirklich ein Homomorphismus ist, braucht man gerade die Bedingung $uv = vu$ für alle $u \in U, v \in V$.) Das Bild ist UV, und man verifiziert leicht, daß diese Abbildung injektiv ist.

Minimale Normalteiler. Sei G eine Gruppe. Ein Normalteiler N von G heißt *minimal,* wenn gilt: es ist $N \neq \{1\}$, und ist N' ein Normalteiler von G mit $N' \neq \{1\}$ und $N' \subseteq N$, so ist $N' = N$.

Konjugierte Untergruppen. Sei U eine Untergruppe der Gruppe G. Ist $g \in G$, so ist gUg^{-1} wieder eine Untergruppe (sieht man unmittelbar), man nennt dies eine zu U *konjugierte* Untergruppe. *Jede zu U konjugierte Untergruppe ist zu U isomorph,* denn die Abbildung $u \mapsto gug^{-1}$ liefert einen Isomorphismus $U \to gUg^{-1}$.

Satz (Struktur minimaler Normalteiler). *Ist G endliche Gruppe, N ein minimaler Normalteiler von G, so ist N Produkt von Kopien einer einfachen Gruppe.* Genauer gilt: *Es gibt eine einfache Untergruppe E von G und Elemente $g_1 = 1, g_2, \ldots, g_t$, so daß die Abbildung*

$$E^t \longrightarrow N \quad mit \quad (e_1, \ldots, e_t) \mapsto (g_1 e_1 g_1^{-1}, \ldots, g_t e_1 g_t^{-1})$$

ein Gruppen-Isomorphismus ist. Es läßt sich also N als Produkt von zu E konjugierten Untergruppen schreiben.

Beweis: Sei E ein Normalteiler von N (es ist also $E \trianglelefteq N$, aber nicht notwendigerweise $E \trianglelefteq G$; letzteres gilt nur falls N eine einfache Gruppe ist, in diesem Fall ist $t = 1$).

(1) *Für jedes $g \in G$ ist gEg^{-1} ein Normalteiler von N.* Da N normal in G ist, ist gEg^{-1} in N enthalten. Sei nun $x \in N$. Da N normal in G ist, gibt es

$y \in N$ mit $xg = gy$ (und daraus folgt $g^{-1}x^{-1} = y^{-1}g^{-1}$). Also ist $x(gEg^{-1})x^{-1} = xgEg^{-1}x^{-1} = gyEy^{-1}g^{-1} = gEg^{-1}$, denn da E normal in N ist, gilt $yEy^{-1} = E$.

Sei nun E ein minimaler Normalteiler von N.

(2) *Für jedes $g \in G$ ist gEg^{-1} ein minimaler Normalteiler von N.* Denn ist H ein Normalteiler von N der in gEg^{-1} enthalten ist, so ist $g^{-1}Hg$ ein Normalteiler von N, der in E enthalten ist.

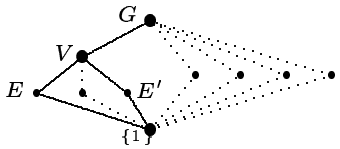
(3) *Ist V ein echter Normalteiler von N, so gibt es $g \in G$ mit $V \cap gEg^{-1} = \{1\}$.* Beweis: Die Untergruppen gEg^{-1} mit $g \in G$ erzeugen einen Normalteiler N_1 von G, der in N enthalten ist. Die Minimalität von N liefert $N_1 = N$. Ist also V eine echte Untergruppe von N, so gibt es $g \in G$ mit $gEg^{-1} \not\subseteq V$, also $V \cap gEg^{-1} \subset gEg^{-1}$. Ist V Normalteiler von N, so ist $V \cap gEg^{-1}$ als Durchschnitt zweier Normalteiler von N selbst ein Normalteiler von N, also wegen der Minimalität von gEg^{-1} folgt $V \cap gEg^{-1} = \{1\}$.

(4) *Ist V ein echter Normalteiler von N, so gibt es $g \in G$ mit $V \cdot gEg^{-1} = V \times gEg^{-1}$, und dies ist wieder ein Normalteiler von N.*

(5) Wir verwenden nun Induktion. Wir beginnen mit $V_1 := E$ und können annehmen, daß dies ein echter Normalteiler von N ist, also finden wir $g_2 \in G$ mit $V_1 \cap g_2Eg_2^{-1} = \{1\}$ und demnach $V_2 := V_1 \cdot g_2Eg_2^{-1} = V_1 \times g_2Eg_2^{-1} = E \times g_2Eg_2^{-1}$. Dies ist wieder ein Normalteiler von N. Ist dies ein echter Normalteiler, so erhalten wir $g_3 \in G$ mit $V_2 \cap g_3Eg_3^{-1} = 1$, also ist $V_3 := V_2 \cdot g_3Eg_3^{-1} = E \times g_2Eg_2^{-1} \times g_3Eg_3^{-1}$, und so weiter.

(6) Es bleibt zu zeigen, daß E eine einfache Gruppe ist. Ist aber H ein Normalteiler von E, so ist H sogar ein Normalteiler von N, denn $N = E \times F$ mit $F = g_2Eg_2^{-1} \times \cdots \times g_tEg_t^{-1}$ (jedes Element von E vertauscht mit allen Elementen von F).

Das einfachste derartige Beispiel ist die A_4, sie besitzt einen einzigen minimalen Normalteiler, nämlich V und $V = C_2 \times C_2$, oder, genauer, $V = E \times E'$ mit $E = \langle(12)(34)\rangle$, und $E' = gEg^{-1}$, wobei $g = (123)$.



Normalreihen versus Ketten von Normalteilern. Ist G eine endliche Gruppe, so ist die Existenz einer Kompositionreihe offensichtlich: Man beginnt "von oben", man wählt also einen maximalen Normalteiler G_1 von $G = G_0$, dann einen maximalen Normalteiler G_2 von G_1 und so weiter; man erhält also eine Kette

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_t = \{1\},$$

und die jeweiligen Faktoren G_{i-1}/G_i sind einfach (aus dem Bijektionssatz folgt nämlich: *Ist H ein Normalteiler von G, so ist genau dann H maximal in G, wenn G/H einfach ist.*) Zu betonen ist hier allerdings, daß die Untergruppen G_i in G zwar "subnormal", aber meist nicht normal sind. Will man eine entsprechende Kette mit Normalteilern von G haben, so muß man auf die Bedingung dr Einfachheit der Faktoren verzichten. Was man verlangen kann, ist, daß jeder Faktor das Produkt von Kopien einer einfachen Gruppe ist:

Korollar. *Ist G eine endliche Gruppe, so gibt es eine Kette von Normalteilern N_i von G*

$$G = N_0 \supset N_1 \supset \cdots \supset N_t = \{1\},$$

wobei jeder Faktor das Produkt von Kopien einer einfachen Gruppe ist.

Beweis: Hier beginnen wir "unten": Wir wählen einen minimalen Normalteiler N von G. Nach Induktion können wir annehmen, daß G/N eine gewünschte Kette von Normalteilern besitzt; die entsprechenden Untergruppen können wir in der Form

$$G/N = N_0/N \supset N_2/N \supset \cdots \supset N_{t-1}/N = \{1\},$$

schreiben, dabei ist N_i ein Normalteiler von G mit $N \subseteq N_i \subseteq G$ und $N_{i-1}/N_i \simeq (N_{i-1}/N)/(N_i/N)$ ist Produkt von Kopien einer einfachen Gruppe, für $1 \leq i \leq t-1$. Und, wie wir wissen, ist auch $N = N_{t-1}$ Produkt von Kopien einer einfachen Gruppe.

3. Auflösbarkeit von Gruppen.

Die Kommutatorgruppe einer Gruppe. Ist G eine Gruppe, so bezeichnet man ein Element der Form $aba^{-1}b^{-1}$ mit $a, b \in G$ als einen *Kommutator.* Mit G' wird die von den Kommutatoren erzeugte Untergruppe von G bezeichnet, man nennt sie die *Kommutatorgruppe* von G. Die Kommutatorgruppe G' von G hat folgende Eigenschaften: *G' ist ein Normalteiler von G und G/G' ist abelsch.* Umgekehrt gilt: *Ist N ein Normalteiler von G und ist G/N abelsch, so ist $N \subseteq G'$.* Beweis: Seien $a, b \in G$. Sei π: $G \to G/N$ die kanonische Projektion. Es ist $\pi(aba^{-1}b^{-1}) = \pi(a)\pi(b)\pi(a)^{-1}\pi(b)^{-1} = 1$, also liegt $aba^{-1}b^{-1}$ im Kern von π, also in N. Insgesamt sieht man also: *Die Kommutatorgruppe G' ist der kleinste Normalteiler in G mit abelscher Faktorgruppe.*

Die folgende ganz offensichtliche Eigenschaft der Bildung der Kommutatorgruppe wird im Folgenden eine wichtige Rolle spielen: $(*)$ *Ist H eine Untergruppe von G, so ist $H' \subseteq G'$.*

Wir können die Bildung der Kommutatorgruppe iterieren. Sei $G^{(0)} = G$ und $G^{(i+1)} = (G^{(i)})'$ für $i \geq 0$. Alle diese Untergruppen sind Normalteiler von G, denn man zeigt mühelos: *Ist N ein Normalteiler von G, so ist auch N' ein Normalteiler von G* (denn N' wird von den Elementen der Form $aba^{-1}b^{-1}$ mit $a, b \in N$ erzeugt; konjugieren wir dieses Element mit $g \in G$ so erhalten wir ein Element, das wieder die Form $cdc^{-1}d^{-1}$ mit $c, d \in N$ hat, dabei ist $c = gag^{-1}$ und $d = gbg^{-1}$).

Satz. *Sei G eine endliche Gruppe. Die folgenden Eigenschaften sind äquivalent:*

(i) *Es gibt eine Kette von Untergruppen*

$$\{1\} = G_0 \subset G_1 \subset \cdots \subset G_n = G,$$

so daß G_{i-1} Normalteiler von G_i ist, und G_i/G_{i-1} Primzahlordnung besitzt.

(ii) *Es gibt Untergruppen G_i von G, die eine Kette*

$$\{1\} = G_0 \subset G_1 \subset \cdots \subset G_n = G$$

bilden, so daß G_{i-1} ein Normalteiler von G_i ist und alle Faktoren N_i/N_{i-1} abelsch sind $(1 \leq i \leq n)$.

(iii) *Es gibt eine natürliche Zahl n mit $G^{(n)} = \{1\}$.*
(iv) *Für jede Untergruppe $U \neq \{1\}$ gilt: $U' \neq U$.*
(v) *Es gibt Normalteiler N_i von G, die eine Kette*

$$\{1\} = N_0 \subset N_1 \subset \cdots \subset N_n = G$$

bilden, so daß alle Faktoren N_i/N_{i-1} abelsch sind $(1 \leq i \leq n)$.
(vi) *Es gibt Normalteiler N_i von G, die eine Kette*

$$\{1\} = N_0 \subset N_1 \subset \cdots \subset N_n = G$$

bilden, so daß alle Faktoren N_i/N_{i-1} elementar abelsch sind $(1 \leq i \leq n)$.

Endliche Gruppen mit diesen Eigenschaften nennt man *auflösbar*. Die Aussage (i) läßt sich auch anders formulieren: *Alle Kompositionsfaktoren sind abelsch* (denn eine Kette mit den genannten Eigenschaften ist gerade eine Kompositionsreihe mit abelschen Faktoren).

Beispiele: (1) *Jede endliche abelsche Gruppe ist auflösbar.* Denn die Eigenschaft (v) ist offensichtlich erfüllt. **(2)** Jede Diedergruppe D_n ist auflösbar: Sie hat die C_n als Untergruppe, und der Index von C_n in D_n ist 2, also ist C_n ein Normalteiler von D_n (sieht man natürlich auch unmittelbar, wenn man D_n als Symmetriegruppe und C_n als Drehgruppe des regelmäßigen n-Ecks interpretiert). Die Gruppe C_n ist auflösbar und $D_n/C_n \simeq C_2$. **(3)** Die Gruppe A_4 ist auflösbar. Dieses Beispiel zeigt, daß man nicht erwarten kann, in einer auflösbaren Gruppe eine Kompositionsreihe aus Normalteilern zu finden.

Beweis des Satzes: (i) $\Longrightarrow$ (ii): trivial

(ii) $\Longrightarrow$ (iii): Mit Induktion zeigen wir $G^{(i)} \subseteq G_{n-i}$. Für $i = 0$ ist nichts zu zeigen. Hat man diese Inklusion für ein i, so folgt aus $(*)$ daß gilt $G^{(i+1)} \subseteq G'_{n-i}$. Da G_{n-i-1} ein Normalteiler von G_{n-i} mit abelscher Faktorgruppe ist, ist $G'_{n-i} \subseteq G_{n-i-1}$.

(iii) $\Longrightarrow$ (iv): Sei U eine Untergruppe von G. Wegen $(*)$ ist $U^{(i)} \subseteq G^{(i)}$ für alle i, insbesondere für $i = n$, also ist $U^{(n)} = \{1\}$. Ist nun $U' = U$, so ist auch $U^{(n)} = U$, also $U = \{1\}$.

(iv) $\Longrightarrow$ (iii): Betrachte die Untergruppen der Form $G^{(i)}$. Ist $G^{(i)} \neq \{1\}$, so ist $G^{(i+1)}$ wegen (ii) eine echte Untergruppe von $G^{(i)}$, also erhalten wir eine echte absteigende Kette

$$G = G^{(0)} \supseteq G^{(1)} \supseteq \cdots \supseteq G^{(t)}$$

die nach endlich vielen Schritten abbrechen muß: dies passiert aber nur, wenn es eine natürliche Zahl n mit $G^{(n)} = 0$ gibt.

(iii) $\Longrightarrow$ (v): Nimm die Kette

$$G = G^{(0)} \supseteq G^{(1)} \supseteq \cdots \supseteq G^{(t)},$$

alle diese Untergruppen sind Normalteiler von G und alle Faktoren sind abelsch.

(v) $\Longleftrightarrow$ (vi): Zu zeigen ist nur, daß (v) aus (vi) folgt. Sei also eine Kette von Normalteilern N_i gegeben mit abelschen Faktoren N_i/N_{i-1}. Es ist N_1 eine abelsche Gruppe, seo p ein Teiler von $|N_1|$. Die Menge U der Elemente mit Ordnung 1 oder p in N_1 ist eine Untergruppe von N_1 und sogar ein Normalteiler von G: denn für

$g \in G$ ist $gUg^{-1} \subseteq N_1$ (da N_1 ein Normalteiler von G ist) und besteht wieder aus Elementen der Ordnung 1 und p, also $gUg^{-1} \subseteq U$. Wir können also durch U die Kette verfeinern, das heißt: wie können annehmen, daß N_1 schon elementar abelsch ist. Betrachte nun G/N_1. Mit Induktion sehen wir, daß G/N_1 eine Normalteilerkette der gewünschten Form hat; verwende nun den Bijektionssatz.

(vi) $\Longrightarrow$ (i): trivial.

Bemerkung: Daß (vi) aus (i) folgt, sieht man auch mit Hilfe des Struktursatzes für minimale Normalteiler.

Vererbungs-Eigenschaften.

(a) *Untergruppen und Faktorgruppen auflösbarer Gruppen sind auflösbar.* Beweis: Sei G eine endliche Gruppe, die auflösbar ist. Sei U eine Untergruppe. Da G auflösbar ist, ist $G^{(n)} = \{1\}$ für eine natürliche Zahl n. Wegen $(*)$ ist auch $U^{(n)} = \{1\}$, also ist auch U auflösbar.

Sei nun N ein Normalteiler von G. Die Eigenschaft $(*)$ läßt sich folgendermaßen verallgemeinern: Ist $f\colon G \to H$ ein Gruppenhomomorphismus, so ist $f(G') \subseteq H'$, denn ein Kommutator wird unter f auf einen Kommutator abgebildet. Ist f surjektiv, so gilt sogar $f(G') = H'$, denn jeder Kommutator in H ist Bild eines Kommutators in G. Allgemeiner gilt $f(G^{(i)}) = H^{(i)}$ für jeden surjektiven Gruppenhomomorphismus $f\colon G \to H$ und jedes i. Ist also N ein Normalteiler und $\pi\colon G \to G/N$ der kanonische Gruppen-Homomorphismus, so ist $\pi(G^{(i)}) = (G/N)^{(i)}$ für jedes i. Aus $G^{(n)} = \{1\}$ folgt $(G/N)^{(n)} = \{1\}$. (Man kann natürlich auch (i) zusammen mit dem Satz von Jordan-Hölder verwenden: Die Kompositionsfaktoren von G/N sind Kompositionsfaktoren von G.)

(b) *Sei G eine endliche Gruppen, N ein Normalteiler von G. Sind die Gruppen G/N und N auflösbar, so ist auch G auflösbar.*

Zum Beweis verwendet man den Bijektionssatz (für Untergrupppen, die N enthalten) und den dritten Isomorphiesatz.

4. Gruppen-Operationen

Sei G eine Gruppe, M eine nicht-leere Menge. Einen Homomorphismus $\phi\colon G \to S_M$ nennt man eine *Operation der Gruppe G auf der Menge M*. Man schreibt für $g \in G$ und $x \in M$ oft $g \cdot m$ oder gm statt $\phi(g)(m)$; man bildet also die Abbildung $G \times M \to M$ mit $(g, m) \mapsto gm = \phi(g)(m)$, sie erfüllt die folgende Bedingung:

(O1) Für $g_1, g_2 \in G$ und $x \in M$ gilt $(g_1 g_2)x = g_1(g_2 x)$.

Ist umgekehrt eine Abbildung $G \times M \to M$ mit der Bedingung (O1) gegeben, und definiert man $\phi\colon G \to S_M$ durch $\phi(g)(x) = gx$ für $g \in G$ und $x \in M$, so ist ϕ ein Gruppen-Homomorphismus. (Häufig wird neben (O1) noch die Bedingung

(O2) $1 \cdot x = x$ für alle $x \in M$

notiert, diese Bedingung folgt aber aus (O1), denn jeder Gruppen-Homomorphismus bildet das Einselement auf das Einselement ab.)

Die Gruppe G operiere auf der Menge M und es sei x ein Element von M. Man nennt die Teilmenge $Gx = \{gx \mid g \in G\} \subseteq M$ die *Bahn* von x unter G. Wir definieren eine Relation $\sim$ auf der Menge M auf folgende Weise: für $x, y \in M$ sei $x \sim y$ genau dann, wenn $g \in G$ mit $gx = y$ existiert; diese Relation $\sim$ ist eine Äquivalenzrelation

(nachrechnen!) und die Äquivalenzklassen sind gerade die Bahnen. Ist $X \subseteq M$ eine Bahn, so nennt man $|X|$ die Länge der Bahn X. Eine Gruppen-Operation heißt *transitiv*, wenn es nur eine Bahn gibt. Man nennt $G_x = \{g \in G \mid gx = x\}$ den *Stabilisator* von x bezüglich der gegebenen Gruppen-Operation. Der Stabilisator von x ist eine Untergruppe von G (nachrechnen!).

Fundamental-Lemma. *Sei G eine endliche Gruppe, G operiere auf der Menge M, sei $x \in M$. Dann gilt*

$$|G| = |G_x| \cdot |Gx|.$$

(Gruppen-Ordnung = Bahnenlänge mal Stabilisator-Ordnung).

Beweis: Definiere eine Abbildung β: $G \to Gx$ durch $\beta(g) = gx$. Diese Abbildung ist surjektiv. Wir werden zeigen, daß für jedes $y \in Gx$ die Kardinalität von $\beta^{-1}(y)$ gerade $|G_x|$ ist.

Sei etwa $y = hx$ mit $h \in G$. Wir behaupten, daß gilt:

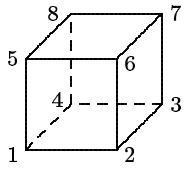
$$\beta^{-1}(hx) = hG_x.$$

Einerseits: Ist $g \in G_x$, so ist $\beta(hg) = (hg)x = h(gx) = hx$, also $hg \in \beta^{-1}(hx)$. Dies zeigt die Inklusion $hG_x \subseteq \beta^{-1}(hx)$. Umgekehrt sei $g \in \beta^{-1}(hx)$, also $gx = \beta(g) = hx$. Aus $gx = hx$ folgt $h^{-1}gx = x$, daher ist $h^{-1}g \in G_x$, und demnach $g \in hG_x$.

Nun ist aber $|hG_x| = |G_x|$, für jedes $h \in G$. Wir sehen: Die Urbilder unter β der einzelnen Elemente $y \in Gx$ haben die gleiche Kardinalität, nämlich $|G_x|$. Die Kardinalität von G ist demnach gegeben durch

$$|G| = \sum_{y \in Gx} \beta^{-1}(y) = \sum_{y \in Gx} |G_x| = |Gx| \cdot |G_x|.$$

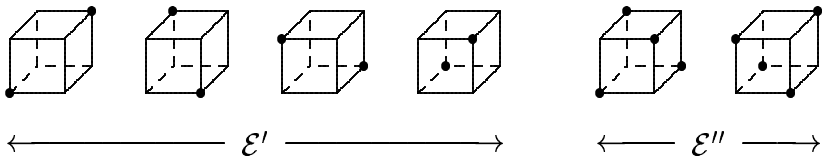
Beispiel. Sei G die Symmetriegruppe des Würfels, sei $H \subset G$ die Drehgruppe des Würfels. *Die Drehgruppe H des Würfels hat die Ordnung 24, die volle Symmetriegruppe G des Würfels hat die Ordnung 48.*



Denn G und H operieren transitiv auf den Ecken des Würfels, die Bahn einer Ecke besteht also aus 8 Elementen. Der Stabilisator in H einer Ecke x besteht aus genau drei Drehungen, also hat die Gruppe die Ordnung $8 \cdot 3 = 24$, der Stabilisator von x in H enthält zusätzlich noch drei Spiegelungen (etwa für die Ecke $x = 1$ die Spiegelungen mit den Spiegelungsebenen, die durch die drei Kanten $\overline{12}, \overline{14}, \overline{15}$ gehen).

Schauen wir uns einen Würfel genauer an. Er hat 6 Flächen, 8 Ecken, 12 Kanten. Zu jeder Fläche, zu jeder Ecke, zu jeder Kante gibt es genau eine gegenüberliegende. Wir bezeichnen mit $\mathcal{F}$ die Menge der Flächen, mit $\mathcal{E}$ die der Ecken, mit $\mathcal{K}$ die der Kanten. Sei $\mathcal{F}'$ die Menge der (ungeordneten) Paare gegenüberliegender Flächen, sei $\mathcal{E}'$ bzw. $\mathcal{K}'$ die der (ungeordneten) Paare gegenüberliegender Ecken bzw. Kanten. Es ist $|\mathcal{F}'| = 3, |\mathcal{E}'| = 4, |\mathcal{K}'| = 6$. Man kann sich $\mathcal{E}'$ auch als die Menge der vier Würfeldiagonalen vorstellen, denn je zwei gegenüberliegender Ecken liefern eine

Würfeldiagonale. Schließlich betrachten wir die beiden Eckenquadrupel, die aus jeweils 4 paarweise nicht-benachbarter Ecken bestehen, und nennen die Menge dieser beiden Eckenquadrupel $\mathcal{E}''$. Bei unserer Nummerierung der Ecken besteht $\mathcal{E}'$ aus den vier Mengen $\{1,7\}$, $\{2,8\}$, $\{3,5\}$ und $\{4,6\}$, und $\mathcal{E}''$ aus den beiden Mengen $\{1,3,6,8\}$ und $\{2,4,5,7\}$.



Offensichtlich operiert G auf allen diesen Mengen (in kanonischer Weise), wir erhalten demnach eine Fülle von Gruppen-Homomorphismen

$$G \to S_{\mathcal{F}} = S_6 \qquad G \to S_{\mathcal{E}} = S_8 \qquad G \to S_{\mathcal{K}} = S_{12}$$
$$G \to S_{\mathcal{F}'} = S_3 \qquad G \to S_{\mathcal{E}'} = S_4 \qquad G \to S_{\mathcal{K}'} = S_6 \qquad G \to S_{\mathcal{E}''} = S_2$$

Weitere Beispiele typischer Gruppen-Operationen:

(a) Linksmultiplikation auf der Menge der Linksnebenklassen. Sei U eine Untergruppe der Gruppe G. Die Gruppe G operiert auf der Menge $\mathcal{U}$ der Linksnebenklassen gU durch Linksmultiplikation (daß es sich hier um eine Gruppen-Operation handelt, ist einfach zu verifizieren). Der Stabilisator von U ist nichts anderes als die Untergruppe U selbst. Die Operation von G auf der Menge $\mathcal{U}$ der Linksnebenklassen ist offensichtlich transitiv, also ist $\mathcal{U}$ die Bahn von U und die Bahnenlänge ist der Index $[G : U]$. Insgesamt sehen wir, daß die Gleichung $|G| = |U| \cdot [G : U]$ ein Spezialfall des Fundamental-Lemmas ist.

(b) Konjugation: G operiert auf G vermöge $g * x = gxg^{-1}$ (für $g, x \in G$). Die Bahn von $x \in G$ unter dieser Operation nennt man die *Konjugiertenklasse* von x, den Stabilisator von x nennt man den *Zentralisator* von x. Das Fundamentallemma besagt insbesondere: Die Anzahl der Elemente in einer Konjugiertenklasse von G ist ein Teiler von $|G|$.

5. p-Untergruppen: Die Sylow-Sätze

Sei G eine Gruppe. Man nennt ein Element $g \in G$ ein *p-Element,* falls die Ordnung von g eine Potenz von p ist. Man nennt eine endliche Gruppe G eine *p-Gruppe,* falls die Ordnung von G eine Potenz von p ist.

Satz. *Sei G eine endliche p-Gruppe.*
(a) *Ist $G \neq \{1\}$, so besitzt G ein zentrales Element der Ordnung p.*
(b) *Es gibt Normalteiler N_i von G, die eine Kette*

$$\{1\} = N_0 \subset N_1 \subset \cdots \subset N_n = G$$

bilden, so daß alle Faktoren N_i/N_{i-1} die Ordnung p haben $(1 \leq i \leq n)$. Insbesondere gibt es also zu jedem Teiler der Gruppenordnung eine Untergruppe mit dieser Ordnung.

Beweis: (a) Betrachte das Konjugieren von G auf G als Gruppen-Operation. Alle Bahnenlängen sind p-Potenzen. Es gibt eine Bahn der Länge 1, nämlich die des Einselements. Die Anzahl der Bahnen der Länge 1 muß durch p teilbar sein,

es gibt also mindestens ein Element $1 \neq h \in G$, das zum Zentrum von G gehört. Die Ordnung von h ist eine p-Potenz, etwa p^s. Dann ist $g = h^{p^{s-1}}$ ein Element der Ordnung p. Mit h ist auch g zentral.

(b): Beweis mit Induktion nach $|G|$. Sei $G \neq \{1\}$. Wegen (b) gibt es ein zentrales Element g der Ordnung der Ordnung p, sei also $N = \langle g \rangle$, dies ist ein Normalteiler. Nach Induktion besitzt G/N eine Kette von Normalteilern, deren Faktoren Ordnung p haben. Nach dem Bijektionssatz können wir diese Normalteiler in der Form N_i/N_1 schreiben, dabei ist $N_1 \subseteq N_i \trianglelefteq G$.

Folgerung. *Endliche p-Gruppen sind auflösbar.*

Nun wenden wir uns beliebigen endlichen Gruppen zu und suchen nach Untergruppen, die p-Gruppen sind (man nennt sie p-Untergruppen). Nicht-triviale p-Untergruppen kann eine Gruppe G natürlich nur besitzen, wenn g die Gruppenordnung $|G|$ teilt (nach dem Satz von Lagrange). Ist G eine Gruppe der Ordnung $p^t m$ mit $(p, m) = 1$, und U eine Untergruppe der Ordnung p^t, so nennt man U eine *p-Sylow-Untergruppe.*

Beispiel: Eine p-Sylow-Untergruppe von $\mathrm{GL}_n(k)$, wobei k ein Körper der Charakteristik p ist.

Ist $|k| = q$, so ist $|G| = (q^n - 1) \cdots (q^n - q^{n-1}) = q^{\binom{n}{2}} \prod_{i=1}^{n} (q^i - 1)$, dabei ist $q^{\binom{n}{2}}$ eine Potenz von q, während keiner der übrigen Faktoren durch p teilbar ist. Und es gilt: $q^{\binom{n}{2}}$ ist gerade die Ordnung der "Borel-Untergruppe" B aller unipotenten oberen Dreiecksmatrizen. Da die Ordnung von B eine Potenz von p ist, ist B eine p-Gruppe.

Um genauer das Potenzieren mit p zu überblicken, bezeichnen wir mit B_t die Menge der Matrizen $(b_{ij})_{ij}$ in B mit $b_{ij} = 0$ falls $j - i < t$. Im Fall $n = 5$ erhalten wir folgende Untergruppen B_1, B_2, B_3, B_4, B_5:

$$\begin{bmatrix} 1 & * & * & * & * \\ & 1 & * & * & * \\ & & 1 & * & * \\ & & & 1 & * \\ & & & & 1 \end{bmatrix} \supset \begin{bmatrix} 1 & 0 & * & * & * \\ & 1 & 0 & * & * \\ & & 1 & 0 & * \\ & & & 1 & 0 \\ & & & & 1 \end{bmatrix} \supset \begin{bmatrix} 1 & 0 & 0 & * & * \\ & 1 & 0 & 0 & * \\ & & 1 & 0 & 0 \\ & & & 1 & 0 \\ & & & & 1 \end{bmatrix} \supset \begin{bmatrix} 1 & 0 & 0 & 0 & * \\ & 1 & 0 & 0 & 0 \\ & & 1 & 0 & 0 \\ & & & 1 & 0 \\ & & & & 1 \end{bmatrix} \supset \{I_5\}$$

Wichtig nun ist, daß gilt: $B_t^p \subseteq B_{t+1}$ (dies läßt sich mühelos nachrechnen und beruht darauf, daß p die Charakteristik von k ist). Insbesondere zeigt dies: Die Ordnung eines Elements in B_t ist ein Teiler von p^{n-t}, die Ordnung eines Elements in B ist also ein Teiler von p^{n-1}.

Satz (Sylow). *Sei G endliche Gruppe, sei p eine Primzahl.*

(a) *Es gibt p-Sylow-Untergruppen. Die Anzahl dier p-Sylow-Untergruppen von G ist kongruent 1 modulo p, und ein Teiler von $|G|$.*

(b) *Alle p-Sylow-Untergruppen von G sind konjugiert.*

(c) *Jede p-Untergruppe von G ist in einer p-Sylow-Untergruppe enthalten.*

Schreiben wir $|G| = p^t m$ mit $(p, m) = 1$, so haben die p-Sylow-Untergruppen die Ordnung p^t. Da die Anzahl a_p der p-Sylow-Untergruppen von G ein Teiler von $|G$ ist, ist a_p sogar ein Teiler von m (denn a_p ist auch kongruent 1 modulo p).

Eine typische Anwendung von Teil (b): *Ist 1 der einzige Teiler von n, der kongruent 1 modulo p ist, so besitzt jede Gruppe der Ordnung n eine einzige p-Sylow-Untergruppe.* Diese Untergruppe muß ein Normalteiler sein!

Betrachten wir zum Beispiel eine Gruppe G der Ordnung 15. Die Teiler von 15 sind 1,3,5,15. Außer 1 ist keine dieser Zahlen kongruent 1 modulo 3, also gibt es genau eine 3-Sylow-Untergruppe

P_3; außer 1 ist keine dieser Zahlen kongruent 1 modulo 5, also gibt es genau eine 5-Sylow-Untergruppe P_5. Die Untergruppe P_3 hat Ordnung 3, also ist sie zyklisch; die Untergruppe P_5 hat Ordnung 5, also ist sie ebenfalls zyklisch. Andererseits ist die Gruppe G isomorph zum Produkt $P_3 \times P_5 \simeq C_3 \times C_5$, und $C_3 \times C_5 \simeq C_{15}$. Wir sehen also: *Bis auf Isomorphie gibt es nur eine Gruppe der Ordnung 15.*

Zum Beweis werden wir gewisse Gruppen-Operationen betrachten. Ist G eine Gruppe, so kann man mit Hilfe der Gundmenge von G einige Mengen definieren, auf denen G operiert: zum Beispiel werden wir alle Teilmengen von G mit Kardinalität p^t betrachten: G operiert auf der Menge $\mathcal{M}$ dieser Teilmengen durch Linksmultiplikation. Auch operiert G vermöge Konjugation auf der Menge $\mathcal{Y}$ aller Untergruppen der Ordnung p^t. Bevor wir mit dem eigentlichen Beweis beginnen, brauchen wir folgenden Hilfssatz.

Hilfssatz. *Sei p eine Primzahl, sei m eine natürliche Zahl, mit $(p,m)=1$. Sei $t \in \mathbb{N}_0$. Dann ist $\binom{p^t m}{p^t}$ nicht durch p teilbar.*

Beweis: Es ist

$$\binom{p^t m}{p^t} = \frac{p^t m \cdot (p^t m - 1) \cdot (p^t m - 2) \quad \cdots \quad (p^t m - (p^t - 1))}{p^t \quad \cdot \quad 1 \quad \cdot \quad 2 \quad \cdots \quad (p^t - 1)}$$

dabei haben wir im Nenner den üblicherweise ganz rechts stehenden Faktor p^t nach links verschoben. Auf diese Weise stehen übereinander zuerst die Zahlen $p^t m$ und p^t und danach jeweils die Zahlen $(p^t m - i)$ und i, mit $1 \leq i \leq p^t - 1$. Auf diese Weise kürzen sich alle Faktoren der Form p: Dies ist richtig für das erste Paar $p^t m$ und p^t, hier verwenden wir, daß $(p,m) = 1$ gilt. Für die weiteren Paare schreiben wir $p^i = p^s n$ mit $(p,n) = 1$. Wegen $1 \leq i < p^t$ gilt $p^s < p^t$, also $s < t$. Schreiben wir jetzt $p^t m - i = p^t m - p^s n = p^s(p^{t-s} m - n)$, so sehen wir, daß diese Zahl durch p^s teilbar ist. Sie ist aber nicht durch p^{s+1} teilbar, denn sonst wäre p ein Teiler von $p^{t-s} m - n$, also, wegen $t - s \geq 1$ auch von n, aber wir haben $(p,n) = 1$ vorausgesetzt.

Beweis von (a). Sei also $|G| = p^t m$ mit $(p,m) = 1$. Sei $\mathcal{M}$ die Menge der Teilmengen von $|G|$, die genau p^t Elemente enthalten. G operiert auf $\mathcal{M}$ durch Linksmultiplikation. Für $M \in \mathcal{M}$ ist der Stabilisator G_M die Untergruppe $G_M = \{g \in G \mid gM = M\}$.

Wir zeigen: Es gibt ein $M \in \mathcal{M}$ mit p^t teilt die Ordnung $|G_M|$. Seien B_i $(i \in I)$ die Bahnen der Gruppen-Operation von G auf $\mathcal{M}$. Sei jeweils G_i der Stabilisator eines Elements M_i in B_i, also gilt

$$\binom{p^t m}{p^t} = |\mathcal{X}| = \sum_{i \in I} |B_i| = \sum_{i \in I} [G : G_i].$$

Da die Zahl p die linke Seite nicht teilt, gibt es mindestens einen Summanden, so daß diese Zahl auch $[G : G_i]$ nicht teilt. Nun teilt aber p^t die Gruppenordnung $|G| = |G_i|[G : G_i]$, also gilt: p^t teilt $|G_i|$. Ist also B_i die Bahn von $M = M_i$, so ist $G_i = G_M$.

Wir haben einen Stabilisator gefunden, dessen Ordnung durch p^t teilbar ist, der also mindestens p^t Elemente enthält. Andererseits gilt für jede Teilmenge M mit p^t Elementen: der Stabilisator dieser Teilmenge kann höchstens p^t Elemente enthalten: denn fixieren wir ein Element $x_0 \in M$, so ist $gx \in M$ für jedes $g \in G_M$; wir erhalten

also durch $g \mapsto gx_0$ eine Abbildung $G_M \to M$ und diese Abbildung ist injektiv. Dies zeigt: $|G_M| = p^t$. Damit haben wir eine Untergruppe mit Ordnung p^t gefunden.

Wir zeigen: *Sei U eine p-Untergruppe, sei P eine p-Sylow-Untergruppe, dann gibt es $g \in G$ mit $U \subseteq gPg^{-1}$.* Daraus folgt sowohl (b) als auch (c). Wir können annehmen: p teilt $|G|$.

Sei $\mathcal{Y}$ die Menge der Untergruppen der Ordnung p^t. Es ist also $P \in \mathcal{Y}$. Die Gruppe G operiert auf dieser Menge per Konjugation. Sei $G * P$ die Bahn von P, und G_P der Stabilisator. Es ist $P \subseteq G_P$, also ist p kein Teiler von $|G * P|$ (denn p ist kein Teiler von $[G : P]$ und $[G : P] = [G : G_P] \cdot [G_P : P]$). Sei nun U eine p-Untergruppe. Betrachte die Bahnen von U auf $G * P$. Alle Bahnenlängen sind p-Potenzen p^i (denn Teiler von $|U|$). Da die Summe dieser Zahlen nicht durch p teilbar ist, gibt es eine Bahn der Länge 1, also ein $P' = g * P$ mit $u * P' = P'$ für alle $u \in U$. Da P und P' die gleiche Ordnung haben, ist auch P' eine p-Sylowgruppe, und es ist $uP'u^{-1} = u * P' = P'$ für alle $u \in U$. Es genügt also, folgenden Hilfssatz zu zeigen:

Hilfsatz: *Sei P eine p-Sylow-Untergruppe und sei U eine p-Untergruppe. Gilt $uPu^{-1} = P$ für alle $u \in U$, so ist $U \subseteq P$.*

Aus $uPu^{-1} = P$ für alle $u \in U$ folgt $uP = Pu$ für alle $u \in U$. Der zweite Isomorphiesatz besagt: Es ist UP eine Untergruppe von G; es ist P ein Normalteiler von UP und es gilt $UP/P \simeq U/(U \cap P)$. Also ist $|UP/P| = |U/(U \cap P)|$ und dies ist ein Teiler von $|U|$ (denn $U/(U \cap P)$ ist eine Faktorgruppe von U), also eine Potenz der Primzahl p. Andererseits ist die Ordnung von UP/P gar nicht durch p teilbar (denn $|UP/P| = [UP : P]$ und dies ist wegen $P \subseteq UP \subseteq G$ ein Teiler von $[G : P]$). Wir sehen: es ist $|UP/P| = 1$, also gilt $P = UP$, also $U \subseteq P$.

Beweis von (a), zweiter Teil. Sei wieder $\mathcal{Y}$ die Menge der p-Sylow-Untergruppen und G operiere auf $\mathcal{Y}$ durch Konjugation. Nach (b) ist dies eine Bahn, und Bahnenlängen sind Teiler der Gruppenordnung. Also ist die Anzahl der p-Sylow-Untergruppen ein Teiler von $|G|$.

Nun lassen wir P auf $\mathcal{Y}$ durch Konjugation operieren. Alle Bahnen haben p-Potenz-Ordnung. Es ist $\{P\}$ eine Bahn, die übrigen Bahnen sind nicht Fixpunkte. (Denn ist P' eine p-Sylow-Untergruppe und wird P' von P normalisiert, so gilt $P \subseteq P'$, siehe den letzten Hilfssatz, also $P = P'$). Es folgt, daß die Anzahl der p-Sylow-Untergruppen kongruent 1 modulo p ist.

Folgerung. *Sei G eine endliche Gruppe und p eine Primzahl. Ist p^s ein Teiler von $|G|$, so gibt es eine Untergruppe von G der Ordnung p^s.* (Diese Untergruppen sind üblicherweise nicht konjugiert).

Dies folgt aus den beiden vorangehenden Sätzen. Für den Nachsatz betrachte die Gruppe A_4 und $p = 2$, $s = 1$: es gibt drei Untergruppen der Ordnung 2, und diese sind nicht konjugiert.

Insbesondere sehen wir **(Satz von Cauchy)**: *Ist G eine endliche Gruppe und ist p ein Teiler von $|G|$, so besitzt G ein Element der Ordnung p.*