1. Gruppen

Als bekannt vorausgesetzt werden

- Gruppen, Untergruppen, Homomorphismen
- Normalteiler, Faktorgruppen, Homomorphiesatz
- symmetrische Gruppe
- zyklische Gruppen
- Ordnungen und der Satz von Lagrange

1.1 Operationen

1.1.1 Def Sei $(G, *)$ eine Gruppe, M eine Menge. Eine <u>Operation</u> von G auf M ist eine Abbildung

$$\bullet : G \times M \longrightarrow M :$$
$$(g, m) \longmapsto g \circ m$$

die folgende Eigenschaften erfüllt:

1) $e \circ m = m \quad \forall\, m \in M$
2) $(a * b) \bullet m = a \bullet (b \bullet m)$
$\forall\, a, b \in G, \quad m \in M$

1.1.2 Bemerkung: Man kann eine Operation als einen Gruppenhomomorphismus

$$\varphi : G \longrightarrow S(M) = \{ f : M \longrightarrow M, f \text{ bijektiv} \}$$
$$g \longmapsto \varphi(g) : M \longrightarrow M$$
$$m \longmapsto g \circ m$$

auffassen:

– φ ist wohldefiniert:

$\varphi(g)$ ist injektiv, denn aus

$g \cdot m_1 = g \cdot m_2$ folgt

$g^{-1} \cdot (g \cdot m_1) = g^{-1} \cdot (g \cdot m_2) \Rightarrow$

$(g^{-1} * g) \cdot m_1 = (g^{-1} * g) \cdot m_2 \Rightarrow$

$e \cdot m_1 = e \cdot m_2 \Rightarrow$

$m_1 = m_2$

$\varphi(g)$ ist surjektiv, denn für

$m \in M$ ist $g^{-1} \cdot m \in M$ und

$\varphi(g)(g^{-1} \cdot m) = g \cdot (g^{-1} \cdot m) =$

$(g * g^{-1}) \cdot m = e \cdot m = m$

$\Rightarrow \varphi(g) \in S(M)$

– φ ist Gruppenhomomorphismus:

$\varphi(g * h) : M \longrightarrow M : m \longmapsto (g * h) \cdot m$
$= g \cdot (h \cdot m)$

$=$

$\varphi(g) \circ \varphi(h) : M \longrightarrow M : m \longmapsto \varphi(g)(\varphi(h)(m))$
$= g \cdot (h \cdot m)$

Umgekehrt liefert ein Gruppenhomomorphismus
$\varphi: G \longrightarrow S(M)$ durch
$g \cdot m := \varphi(g)(m)$ eine Operation,
denn $e \cdot m = \varphi(e)(m) = id(m) = m$
und $(g * h) \cdot m = \varphi(g * h)(m) = \varphi(g) \circ \varphi(h)(m)$
$= g \cdot (h \cdot m)$

1.1.3 Beispiele

1) $Gl_n(K)$ (= invertierbare $n \times n$-Matrizen über einem Körper K)

operiert auf K^n durch
$A \cdot x := A \cdot x$ (Matrixmultiplikation),
denn $\mathbb{1}_n \cdot x = x$ und
$(A \cdot B) \cdot x = A \cdot (B \cdot x)$.

2) S_n ($= S(\{1, \dots, n\})$) operiert
auf $\{1, \dots, n\}$ durch
$\sigma \cdot i := \sigma(i)$, denn
$id \cdot i = id(i) = i$ und
$(\sigma \circ \sigma') \cdot i = \sigma(\sigma'(i)) = \sigma \cdot (\sigma' \cdot i)$.

3) S_n operiert auf $\mathbb{R}^n$, indem
wir für $\sigma \in S_n$ die Permutation
der Einheitsvektoren $e_i \mapsto e_{\sigma(i)}$

linear fortsetzen, zu einer Permutationsmatrix A_σ (in jeder Zeile und Spalte eine 1 und sonst nur Nullen).

Bsp: $n = 3$, $A_{(12)} = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$

Für $x \in K^n$ gilt

$$\mathrm{id} \cdot x = A_{\mathrm{id}} \cdot x = \mathbb{1}_n \cdot x = x$$

und

$$(\sigma \circ \sigma') \cdot x = (A_\sigma \cdot A_{\sigma'}) \cdot x = A_\sigma \cdot (A_{\sigma'} \cdot x)$$
$$= \sigma \cdot (\sigma' \cdot x).$$

4) Eine Gruppe operiert durch die Gruppenoperation auf sich selbst:

$$G \times G \to G : (g, h) \mapsto g \cdot h$$

denn $e \cdot h = h$, $(g_1 \cdot g_2) \cdot h = g_1 \cdot (g_2 \cdot h)$.

5) Sei $U \subset G$ eine Untergruppe, dann operiert U auf G durch die Gruppenoperation:

$$U \times G \to G : (u, g) \mapsto u \cdot g$$

denn $e \cdot g = g$, $(u_1 \cdot u_2) \cdot g = u_1 \cdot (u_2 \cdot g)$.

1.1.4 Def Eine Operation von G auf M heißt <u>treu</u>, wenn der zugehörige Gruppenhomomorphismus φ injektiv ist, i.e. $\mathrm{Ker}(\varphi) = \{e\}$, i.e. nur e wird auf id_M abgebildet durch φ, i.e. $\forall g \neq e \ \exists m : \ g \cdot m \neq m$.

1.1.5 Bsp Wir betrachten die Bsp von eben:

1) Damit $A \cdot x = x \ \forall x \in K^n$ gilt, muß $A = \mathbb{1}_n \Rightarrow$ treu

2) Damit $\sigma \cdot i = i \ \forall i \in \{1, \dots, n\} \Rightarrow$
$\sigma(i) = i \Rightarrow \sigma = id \Rightarrow$ treu

3) wie 1)

4) $g \cdot h = h \ \forall h \in G \Rightarrow g = e$
$\Rightarrow$ treu

5) genauso

6) Sei

$$G = \{\text{obere Dreiecksmatrizen}, \begin{pmatrix} * & * \\ 0 & * \end{pmatrix}\} \underset{\substack{\uparrow \\ \text{Untergruppe}}}{\subset} GL_2(K)$$

$$U = \langle e_1 \rangle \subset K^2.$$

$G \times U \to U : (A, x) \longmapsto A \cdot x$

ist eine Operation, denn

für $x \in U$ ist $A \cdot x \in U$

$$\left(\begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} * \\ 0 \end{pmatrix} \in U \right)$$

$\mathbb{1}_2 \cdot x = x \quad \forall x \in U$ und

$(A \cdot B) \cdot x = A \cdot (B \cdot x)$.

Als Gruppenhomomorphismus betrachtet:

$\varphi : G \longrightarrow S(U) : A \longmapsto f_A$

mit $f_A : U \to U : x \mapsto A \cdot x$

$\mathrm{Ker}(\varphi) = \{ A \mid f_A = \mathrm{id}|_U \} =$

$$\left\{ \begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix} \right\} \supsetneqq \{ \mathbb{1}_2 \}$$

Die Operation ist also nicht treu.

Anders gesagt: $\exists \; A \neq \mathbb{1}_2$ mit

$A \cdot x = x \quad \forall x \in U$, z. B.

$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, denn

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} a \\ 0 \end{pmatrix} = \begin{pmatrix} a \\ 0 \end{pmatrix}.$$

Erinnerung: $\mathbb{R}^n$ ist ein euklidischer Vektorraum.

Die orthogonale Gruppe ist

$O(n) = \{$orthogonale Matrizen$\}$

(Spalten sind Orthonormalbasis, $A \cdot A^T = \mathbb{1}_n$).

A orthogonal $\Leftrightarrow$ f_A orthogonal $\Leftrightarrow$

$\langle x, x \rangle = \langle f_A(x), f_A(x) \rangle \quad \forall x \in \mathbb{R}^n$

$\Leftrightarrow$ f_A ist längen- und winkelerhaltend.

1.1.6 Def: Die Menge der affinen Isometrien auf $\mathbb{R}^n$ ist

$E(n) := \{x \mapsto Ax + b, \ A \in O(n), b \in \mathbb{R}^n\}$

Durch Hintereinanderausführung ist $E(n)$ eine Gruppe.

Für $M \subset \mathbb{R}^n$ definieren wir eine Untergruppe von $E(n)$, die auf M operiert:

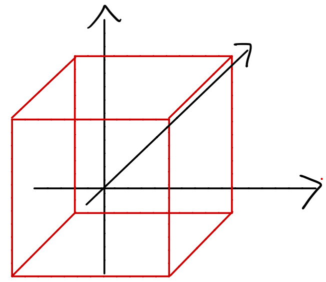
1.1.7 Def: Sei $M \subset \mathbb{R}^n$ eine Teilmenge.

$\mathrm{Sym}(M) = \{f \in E(n) \mid f(M) = M\}$

heißt die Symmetriegruppe von M, ihre Elemente Symmetrien.

<u>Bsp</u>:

$Q = \{ x \in \mathbb{R}^3 \mid |x_i| \leq 1 \ \forall i \} =$ Würfel



Da Symmetrien abstandserhaltend sind, muß die Teilmenge der Punkte größten Abstands zu 0 (= Eckpunkte) auf sich selbst überführt werden. Damit ist

$$\mathrm{Sym}(Q) \subset \left\{ \begin{pmatrix} \pm 1 & & \\ & \pm 1 & \\ & & \pm 1 \end{pmatrix} \cdot A_\sigma \;\middle|\; \sigma \in S_3 \right\}$$

und da jede solche Abb in $\mathrm{Sym}(Q)$ ist gilt Gleichheit.

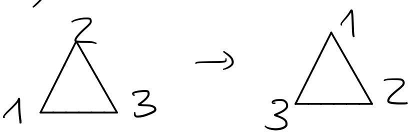
<u>Bsp</u>: Die Symmetriegruppe eines gleichseitigen Dreiecks $\triangle \subset \mathbb{R}^2$ ist

$$S_3 = \{ \mathrm{id}, (123), (132), (12), (13), (23) \}$$

und besteht aus Drehungen

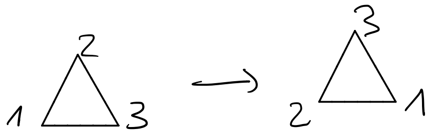
id (um $0°$),

(123):



(um $120°$)

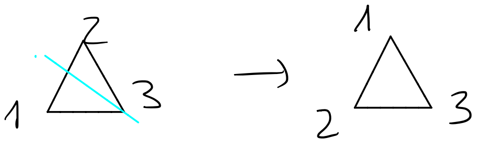
(132):

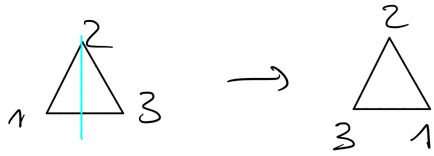


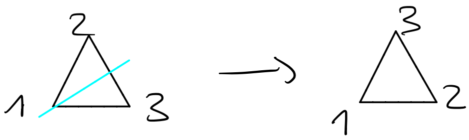
(um $240°$)

sowie

Spiegelungen

(12): 

(13): 

(23): 

<u>1.1.8 Bem</u> Für $M \subset \mathbb{R}^n$ definiert

$$\begin{aligned} \mathrm{Sym}(M) \times M &\longrightarrow M: \\ (f, \; m) &\longmapsto f \cdot m := f(m) \end{aligned}$$

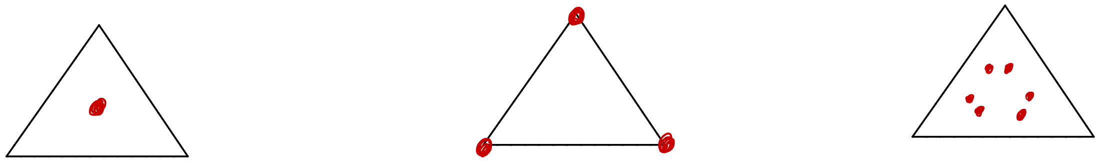
eine Operation, denn $\mathrm{id} \cdot m = m$ und $(f \circ g) \cdot m = f(g(m)) = f \cdot (g \cdot m)$.

<u>1.1.9 Def</u> Sei $G \times M \to M$ eine Operation.

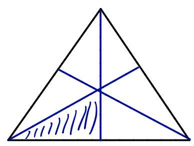
$Gm := \{ g \cdot m \mid g \in G \} \subset M$ heißt die <u>Bahn</u> von m.

<u>1.1.10 Bsp</u>: Sei $\triangle$ ein gleichseitiges Dreieck in $\mathbb{R}^2$, wir betrachten

die Operation $\mathrm{Sym}(\triangle) \times \triangle \to \triangle$ und Bahnen für verschiedene Punkte:



Man kann die Operation auf die Potenzmenge von $\triangle$ fortsetzen und hier Bahnen betrachten: die Bahn des kleinen Dreiecks ist $\triangle$ z. B.



1.1.11 <u>Bsp</u> $m\mathbb{Z} \subset \mathbb{Z}$ ist Untergruppe bezüglich $+$.
Betrachte die dadurch induzierte Operation
$m\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} : (mz, a) \mapsto mz + a$.
Die Bahnen dieser Operation sind die Restklassen mod m.

1.1.12 <u>Bemerkung</u>: Man kann eine Untergruppe $U \subset G$ auch von rechts operieren lassen durch $U \times G \to G : (u,g) \mapsto gu$.

Die Bahnen dieser Operation sind $gU = \{gu \mid u \in U\}$, die Linksnebenklassen.

Für die übliche Operation von links sind die Bahnen die $Ug = \{ug \mid u \in U\}$, die Rechtsnebenklassen.

Normalteiler sind also Untergruppen, für die die Bahnen unter Operation von links und rechts gleich sind.

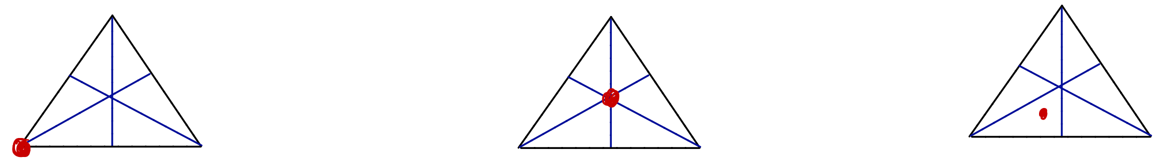
1.1.13 Def Sei $G \times M \to M$ eine Operation.

Für $N \subset M$ ist

$$\mathrm{Stab}(N) := \{g \in G \mid \{gn \mid n \in N\} =: gN = N\}$$

der <u>Stabilisator</u> von N.

1.1.14 Bsp: (siehe Bsp 1.1.10):



1

$\mathrm{Stab}(1) = \{id, (23)\}$ $\mathrm{Stab} = S_3$ $\mathrm{Stab} = \{id\}$

1.1.15 Bem $\bigcap_{n \in M} \mathrm{Stab}(\{n\})$ ist die Untergruppe von $\mathrm{Sym}(M)$, die M punktweise festhält.

1.1.16 Lemma: Sei $G \times M \to M$ eine Operation, $N \subset M$. $\mathrm{Stab}(N)$ ist eine Untergruppe.

Beweis: Seien $a, b \in \mathrm{Stab}(N) \Rightarrow$
$aN = N$, $bN = N \Rightarrow (ab)N = a(bN) = aN = N \Rightarrow ab \in \mathrm{Stab}(N)$ und
$a^{-1}(aN) = a^{-1}N = (a^{-1}a)N = eN = N$
$\Rightarrow a^{-1} \in \mathrm{Stab}(N)$.
$\mathrm{Stab}(N) \neq \emptyset$, denn $id \in \mathrm{Stab}(N)$. $\square$

1.1.17 Lemma Sei $G \times M \to M$ eine Operation, $m_1, m_2 \in M$. Die Bahnen von m_1 und m_2 sind entweder gleich oder disjunkt, i.e.
$Gm_1 = Gm_2$ oder $Gm_1 \cap Gm_2 = \emptyset$.

Beweis: Angenommen, $Gm_1 \cap Gm_2 \neq \emptyset$
$\Rightarrow \exists\, m_3 \in Gm_1 \cap Gm_2 \Rightarrow$
$\exists\, g_1, g_2 \in G : \quad m_3 = g_1 m_1 = g_2 m_2$

$\Rightarrow \quad m_2 = g_2^{-1} g_1 m_1 \in G m_1$

$\Rightarrow \quad G m_2 \subset G m_1$ und analog

$G m_1 \subset G m_2$, also Gleichheit. $\square$

1.1.18 Bsp S_n operiert auf $\{1, \dots, n\}$.

Sei $n = 4$, $\sigma = (1 2 3)$, dann zerlegt σ

$\{1, \dots, n\}$ in die disjunkten Bahnen

$\{1, 2, 3\} \,\dot\cup\, \{4\}$.

Sei $n = 5$, $\sigma = (1 2 3)(4 5)$, dann zerlegt σ

$\{1, \dots, n\}$ in die disjunkten Bahnen

$\{1, 2, 3\} \,\dot\cup\, \{4, 5\}$.

Allgemeiner entspricht die Zerlegung in Bahnen der Zerlegung in Zykel.

1.1.19 Satz (Satz von Cayley)

Sei G eine Gruppe. Dann existiert eine Menge M und ein injektiver Gruppenhomomorphismus $f : G \to S(M)$.

Ist G endlich, so kann man M auch endlich wählen.

Insbesondere kann man jede Gruppe als Untergruppe der Permutationsgruppe einer Menge auffassen.

Beweis: Wir lassen G durch Gruppenoperation auf sich selbst operieren und erhalten dadurch den Gruppenhomomorphismus

$$\varphi: G \longrightarrow S(G) : g \longmapsto \tau_g$$

mit $\tau_g : G \longrightarrow G : h \longmapsto gh$

Da die Gruppenoperation treu ist, ist φ injektiv. $\square$

Bemerkung: Man betrachtet oft Monomorphismen $\varphi: G \longrightarrow Gl_n(K)$

So erhält man Darstellungen von G durch Matrizen, diese heißen lineare Darstellungen von G.

1.1.20 Satz Sei $G \times M \to M$ eine Operation, $m \in M$, $U = \mathrm{Stab}(m)$.

$$G/U \longrightarrow Gm : gU \mapsto gm$$

ist bijektiv.

Beweis: Wohldefiniert:
Sei $g \sim h$, also $gU = hU \Rightarrow$
$\exists u \in U: gu = h \Rightarrow$
$hm = (gu)m = g(um) = gm$,
da m von U stabilisiert wird.

Injektiv: $gm = hm \Rightarrow h^{-1}gm = m$
$\Rightarrow h^{-1}g$ stabilisiert $m \Rightarrow$
$h^{-1}g \in U \Rightarrow g \sim h \Rightarrow gU = hU$.

Surjektiv klar. $\square$

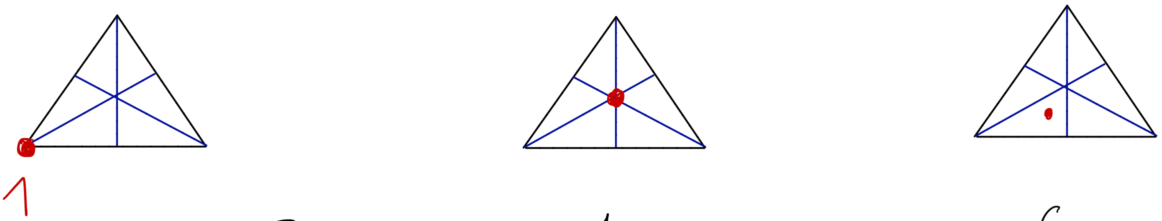
1.1.21 Korollar: Sei $G \times M \to M$ eine Operation, $m \in M$, dann gilt

$$|Gm| \cdot |\mathrm{Stab}(m)| = |G|.$$

Beweis: Sei $U = \mathrm{Stab}(m)$.

$$|G m| \cdot |U| \overset{1.1.20}{=} |G/U| \cdot |U|$$
$$= |G| \quad \text{wegen Satz von Lagrange.}$$
□

1.1.22 Bsp Im gleichseitigen Dreieck $\Delta \subset \mathbb{R}^2$ mit der Operation von $\mathrm{Sym}(\Delta)$ gilt:
(siehe 1.1.10 und 1.1.14)



Bahnlänge = 3	1	6
$\lvert\mathrm{Stab}\rvert = 2$	6	1

1.1.23 Satz (Bahnengleichung)

Sei M endlich, $G \times M \to M$ eine Operation, $R \subset M$ eine Teilmenge, die aus jeder Bahn genau ein Element enthält. Dann gilt

$$|M| = \sum_{r \in R} |G| / |\mathrm{Stab}(r)|$$

Beweis: M ist die disjunkte Vereinigung seiner Bahnen. Für $r \in R$ hat die Bahn Gr $|G|/|\mathrm{Stab}(r)|$ Elemente wegen Satz 1.1.20. $\square$

Anwendung der Bahnengleichung: Klassifikation von Graphen bis auf Isomorphie:

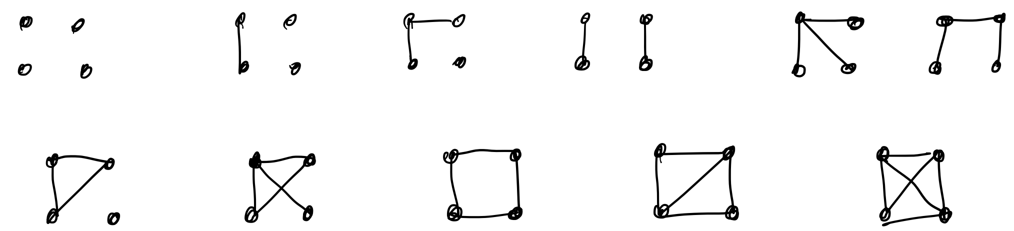
<u>1.1.24 Def</u> Ein Graph ist ein Paar $G = (V, E)$ aus einer Menge V von Ecken und E von Kanten, $E \subset V \times V$. Wir betrachten ungerichtete Graphen, d.h. wir fordern, daß E symmetrisch ist, also aus $(i,j) \in E$ folgt $(j,i) \in E$ – dies steht dann für die Kante zwischen i und j. Wir erlauben keine mehrfachen Kanten und keine Schleifen – $(i,i) \notin E \ \forall i$.

Ein Isomorphismus von Graphen (V,E), (V',E') ist eine Bijektion $\varphi: V \to V'$, die eine Bijektion

$E \longrightarrow E'$ induziert.

<u>1.1.25 Satz</u> Es gibt 11 Isomorphieklassen von Graphen mit 4 Ecken.

<u>Beweis</u>:



sind paarweise nicht isomorph.

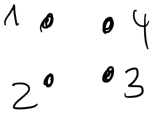
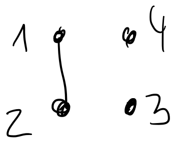
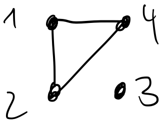
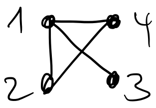
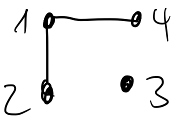
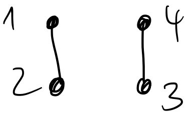
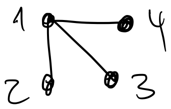
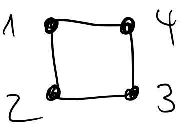
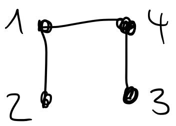
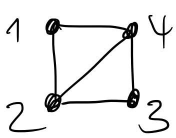
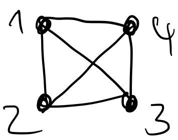
Sei $V = \{1,2,3,4\}$, $M = \{(V,E) \text{ Graph}\}$

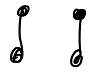
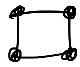
$\# M = 2^6 = 64$, da jede der Kanten

12, 13, 14, 23, 24, 34 dabei sein kann

oder nicht.

S_4 operiert auf M durch Permutation der Ecken. Wir geben für jeden der 11 Typen den Stabilisator und dann mit Hilfe von Satz 1.1.20 die Länge der Bahn an:

Graph	Stabilisator	$\lvert Stab \rvert$	Bahnlänge
	S_4	24	1
	$\{id, (12), (34), (12)(34)\}$	4	6
	$S_3 = S(1,2,4)$	6	4
	$\{id, (24)\}$	2	12
	$\{id, (24)\}$	2	12
	$\{id, (1324), (13)(24), (1423), (12), (34), (12)(34), (14)(23)\}$	8	3
	$S(2,3,4)$	6	4
	$\{id, (1234), (13)(24), (1432), (13), (24), (12)(34), (14)(23)\}$	8	3
	$\{id, (14)(23)\}$	2	12
	$\{id, (24), (13), (13)(24)\}$	4	6
	S_4	24	1

(Beachte,  und  liefern die Symmetriegruppe des Quadrats.)

Wir addieren die Bahnenlängen:

$$1+6+4+12+12+3+4+12+3+6+1$$
$$= 64 = |M|$$

Damit haben wir alle Isomorphieklassen gefunden. $\square$

1.2. Konjugation

1.2.1 Def Sei G eine Gruppe. Die Operation

$$G \times G \to G : (g,h) \mapsto ghg^{-1}$$

von G auf sich selbst heißt <u>Konjugation</u>.

Die Bahnen $h^G = \{ghg^{-1} \mid g \in G\}$ heißen <u>Konjugationsklassen</u>.

Wohldefiniert:

$$(e,g) \longmapsto ege^{-1} = g$$

$$(g_1 g_2, h) \longmapsto g_1 g_2 h (g_1 g_2)^{-1} =$$

$$g_1 g_2 h g_2^{-1} g_1^{-1} = g_1 (g_2 h g_2^{-1}) g_1^{-1}.$$

1.2.2 Bsp:

Konjugationsklassen der S_n:

Sei $n=3$.

$\{id\}$ ist eine Klasse.

Klasse von (12):
$$(12)(12)(12)^{-1} = (12)$$
$$(13)(12)(13)^{-1} = (23)$$
$$(23)(12)(23)^{-1} = (13)$$
$$(123)(12)(123)^{-1} =$$
$$(123)(12)(132) = (23)$$
$$(132)(12)(132)^{-1} = (13)$$

$\Rightarrow$ Wir erhalten alle Transpositionen,
$\{(12), (13), (23)\}$

Klasse von (123):
$$(12)(123)(12) = (132)$$
$$(13)(123)(13) = (132)$$
$$(23)(123)(23) = (132)$$
$$(123)(123)(132) = (123)$$
$$(132)(123)(123) = (123)$$

$\Rightarrow$ Wir erhalten alle 3-Zykel,

$\{(123), (132)\}$

Allgemein gilt:
Die Zerlegung in Konjugationsklassen ist die Zerlegung in Zykeltypen:

Für $\sigma = c_1 \cdots c_s$ Zerlegung in disjunkte Zykel der Länge $\ell(c_i) = l_i$ setzen wir $p(\sigma) = (l_1, \ldots, l_s)$, dies ist eine Partition von n.

z.B. für $n=4$:

$p((123)) = (3,1)$

$p((12)(34)) = (2,2)$.

$p(\sigma)$ heißt der <u>Zykeltyp</u> von σ.

<u>1.2.3 Satz:</u>

$$\left\{\begin{array}{c}\text{Konjugationsklassen} \\ \text{der } S_n\end{array}\right\} \xleftrightarrow{1:1} \left\{\begin{array}{c}\text{Partitionen} \\ \text{von } n\end{array}\right\}$$

durch den Zykeltyp.

<u>1.2.4 Def</u>

Sei G eine Gruppe, $g \in G$.

$i_g : G \to G : h \mapsto ghg^{-1}$

bezeichnet den inneren Automorphismus zu g.

Wohldefiniert:

Homomorphismus: $i_g(h_1 \cdot h_2) = g h_1 h_2 g^{-1} =$

$g h_1 g^{-1} g h_2 g^{-1} = i_g(h_1) \cdot i_g(h_2)$

Injektiv: $gh_1g^{-1} = gh_2g^{-1} \Rightarrow h_1 = h_2$

Surjektiv: $h = i_g(g^{-1}hg) = gg^{-1}hgg^{-1}$

1.2.5 Def Sei $U \subset G$ eine Untergruppe, $g \in G$, dann ist die Konjugation von U mittels g,

$$gUg^{-1} = \{gug^{-1} \mid u \in U\}.$$

1.2.6 Lemma: $gUg^{-1} \cong U$

Beweis: Da $gUg^{-1} = i_g(U)$ das Bild unter dem inneren Automorphismus zu g.

1.2.7 Def Sei

$$S = \{U \mid U \text{ in } G \text{ Untergruppe}\}.$$

G operiert auf S durch Konjugation

$$G \times S \to S: \quad (g, U) \mapsto gUg^{-1}$$

Die Bahnen U^G dieser Operation heißen die Konjugationsklassen von Untergruppen.

Wohldefiniert: $(e, U) \mapsto eUe^{-1} = U$

$$(gh, U) \mapsto ghU(gh)^{-1} = ghUh^{-1}g^{-1}$$

Bem Ein Normalteiler ist eine Untergruppe, die invariant unter Konjugation ist, d.h. deren Konjugationsklasse $U^G = \{U\}$ nur aus einem Element besteht.

1.2.8 Satz Sei $G \times M \to M$ eine Operation, $n, m \in Gm$ in derselben Bahn mit $n = gm$. Dann sind die Stabilisatoren konjugiert,

$$\mathrm{Stab}(n) = g\,\mathrm{Stab}(m)\,g^{-1}.$$

Beweis: „$\supset$" Sei $u \in \mathrm{Stab}(m)$, $u' = gug^{-1}$. Dann gilt $u' \cdot n =$

$$gug^{-1} \cdot n = gum \underset{\text{da } u \in \mathrm{Stab}(m)}{=} gm = n$$

$\Rightarrow u' \in \mathrm{Stab}(n)$.

„$\subset$" Analog mit $m = g^{-1}n$ zeigen wir $g^{-1}\,\mathrm{Stab}(n)\,g \subset \mathrm{Stab}(m)$, daraus folgt „$\subset$" nach Multiplikation von rechts mit g^{-1} und von links mit g. $\square$

Bsp S_3 hat 4 Konjugationsklassen von Untergruppen, $\{ id \}$,

$\{ \langle (12) \rangle, \langle (13) \rangle, \langle (23) \rangle \}$

$\{ \langle (123) \rangle \}$, $\{ S_3 \}$.

Damit besitzt S_3 Untergruppen jeder Größe, die nach Lagrange theoretisch möglich, i.e. für jeden Teiler von 6.

1.2.9 Def Sei G eine Gruppe.

Das Zentrum $Z(G)$ ist

$$Z(G) = \{ g \mid hg = gh \quad \forall h \in G \}$$
$$= \{ g \mid h = ghg^{-1} \quad \forall h \in G \}$$

1.2.10 Lemma Sei G eine Gruppe

Sei $\varphi : G \longrightarrow Aut(G) : g \mapsto i_g$.

Dann ist φ ein Homomorphismus mit $Ker(\varphi) = Z(G)$.

Insbesondere ist $Z(G)$ ein Normalteiler.

Beweis: Homomorphismus:

$\varphi(g_1) \circ \varphi(g_2)\ (h) = i_{g_1} \circ i_{g_2}\ (h) = i_{g_1}\ (i_{g_2}(h)) =$
$g_1 (g_2 h g_2^{-1}) g_1^{-1} = g_1 g_2\ h (g_1 g_2)^{-1} = i_{g_1 g_2}\ (h)$
$= \varphi(g_1 g_2)(h)$

$\mathrm{Ker}(\varphi) = Z(G)$:

$g \in \mathrm{Ker}(\varphi) \iff i_g = \mathrm{id} \iff$
$\forall\, h \in G: ghg^{-1} = h \iff g \in Z(G)$

□

1.2.11 Def

Der Stabilisator der Konjugationsoperation heißt Zentralisator:

$Z_G(h) = \{ g \mid ghg^{-1} = h \}$

Auch für Teilmengen $M \subset G$:

$Z_G(M) = \{ g \mid ghg^{-1} = h \ \forall\, h \in M \}$

der Zentralisator von M.

Der Zentralisator von $M = G$ ist das Zentrum.

1.2.12 Satz (Klassengleichung)

Sei G eine Gruppe, $R \subset G$ eine Teilmenge, die aus jeder Konjugationsklasse genau ein Element enthält.

Dann gilt die Klassengleichung:

$$|G| = |Z(G)| + \sum_{r \in R \setminus Z(G)} |G| / |Z_G(r)|$$

<u>Beweis:</u> Aus der Bahnengleichung 1.1.23 folgt

$$|G| = \sum_{r \in R} |G| / |\mathrm{Stab}(r)| = \sum_{r \in R} |G| / |Z_G(r)| .$$

Die Konjugationsklassen von Elementen im Zentrum sind einelementig, denn aus $gh = hg \ \forall h$ folgt $g = hgh^{-1} \ \forall h$

$\Rightarrow g^G = \{g\} \quad \Rightarrow Z(G) \subset R$

Falls r invariant unter Konjugation folgt $Z_G(r) = G$ und

$|G| / |Z_G(r)| = |G| / |G| = 1 .$

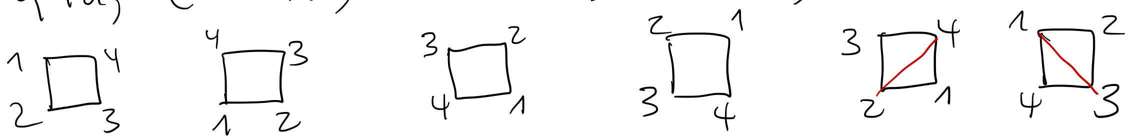
$$\Rightarrow |G| = \sum_{r \in Z(G)} 1 + \sum_{r \in R \setminus Z(G)} |G| / |Z_G(r)|$$

$$= |Z(G)| + \sum_{r \in R \setminus Z(G)} |G| / |Z_G(r)|$$

$\square$

<u>Bsp</u> Sei G die Symmetriegruppe eines Quadrats.

$G = \{ id, (1234), (13)(24), (1432), (13), (24),$



$(12)(34), (14)(23) \}$

Betrachte die Konjugation von G.

r	Konj. klasse r^G	Zentralisator $Z_G(r)$
id	$\{id\}$	G
$(13)(24)$	$\{(13)(24)\}$	G
(13)	$\{(13), (24)\}$	$\{id, (13), (24), (13)(24)\}$
$(12)(34)$	$\{(12)(34), (14)(23)\}$	$\{id, (12)(34), (13)(24), (14)(23)\}$
(1234)	$\{(1234), (1432)\}$	$\{id, (1234), (13)(24), (1432)\}$

$Z(G)$

Bahnengleichung: $8 = 1 + 1 + 2 + 2 + 2$

Klassengleichung: $8 = 2 + 2 + 2 + 2$

1.2.13 Korollar

Sei G eine Gruppe der Ordnung p^k, p Primzahl, $k>0$, dann wird $|Z(G)|$ von p geteilt.

<u>Beweis</u>: $r \notin Z(G) \iff \exists g$ mit $r \neq grg^{-1} \iff g \notin Z_G(r) \iff$
$Z_G(r) \subsetneqq G \iff |G|/|Z_G(r)| > 1$

Da $|G|/|Z_G(r)|$ wie $|Z_G(r)|$ ein Teiler von $|G| = p^k$ ist, folgt $p \,/\, |G|/|Z_G(r)|$

Damit wird auch

$$|Z(G)| = |G| - \sum_{r \in R\setminus Z(G)} |G|/|Z_G(r)|$$

(Klassengleichung 1.2.12, R ist eine Menge, die aus jeder Konjugationsklasse genau ein Element enthält)

$= p^k -$ durch p teilbare Zahlen

von p geteilt. $\square$

Bemerkung:

Daraus folgt, daß die Symmetriegruppe des Quadrats der Ordnung $8 = 2^3$ mindestens ein weiteres Element neben id im Zentrum besitzt.
Wir haben im Bsp gesehen, daß dies die Drehung um 180° ist.

1.2.14 Korollar

Sei G eine Gruppe der Ordnung p^2, p prim. Dann ist G abelsch.

Beweis: Wegen 1.2.13 wird $|Z(G)|$ von p geteilt, ist also p oder p^2.

Falls $|Z(G)| = p^2 \Rightarrow G = Z(G)$ und G ist abelsch.

Falls $|Z(G)| = p \Rightarrow \frac{|G|}{|Z(G)|} = p$

$\Rightarrow \left| G/Z(G) \right| = p$. Da $Z(G)$ Normalteiler, ist $G/Z(G)$ eine Gruppe.
Eine Gruppe von Primzahlordnung ist zyklisch.

$\Longrightarrow \exists g: \quad G/_{Z(G)} = \langle g Z(G) \rangle.$

Seien $g_1, g_2 \in G$, schreibe

$g_i = g^{k_i} \cdot z_i$ mit $z_i \in Z(G)$.

Dann ist $g_1 g_2 = g^{k_1} z_1 g^{k_2} z_2$

$= g^{k_1+k_2} z_1 z_2 = g^{k_1+k_2} z_2 z_1$

$= g^{k_2} z_2 g^{k_1} z_1 = g_2 g_1$, da die

z_i mit jedem Element vertauschen.

Damit ist G abelsch und

$G = Z(G)$, $|Z(G)| = p^2$. $\square$

1.3. Isomorphiesätze

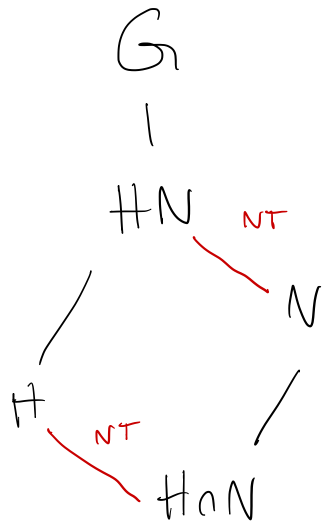
1.3.1 Def Sei G eine Gruppe, H, N Untergruppen.
Wenn $\forall h \in H \quad hNh^{-1} \subset N$
so wird <u>N von H normalisiert</u>.

Bsp Falls N Normalteiler so wird N von jeder Untergruppe normalisiert.

1.3.2 Lemma G Gruppe, H, N Untergruppen
N werde von H normalisiert. Dann:

1) $H \cap N$ ist Normalteiler in H
2) $HN = \{hn \mid h \in H, n \in N\}$ ist Untergruppe von G, N ist Normalteiler von HN.

Ein Teil des Untergruppenverbands ist also:



Beweis:

1) Sei $h \in H$, $n \in H \cap N$, dann gilt $hnh^{-1} \in N$ da H N normalisiert und $hnh^{-1} \in H$, da alle in H sind.

$\Rightarrow hnh^{-1} \in H \cap N$

Also ist $H \cap N$ Normalteiler in H.

2) $HN \neq \emptyset$. Sei $hn \in HN$, dann ist $(hn)^{-1} = n^{-1}h^{-1} = h^{-1}\underbrace{hn^{-1}h^{-1}}_{\in N,\text{ da } N \text{ von } H \text{ normalisiert wird}} \in HN$

Seien $h_1 n_1, h_2 n_2 \in HN$. Dann ist

$$h_1 n_1 h_2 n_2 = h_1 h_2 \underbrace{h_2^{-1} n_1 h_2}_{\in N} n_2 \in HN$$

$\overset{\text{Untergruppen-kriterium}}{\Longrightarrow}$ HN ist Untergruppe.

Sei $hn_1 \in HN$, $n_2 \in N$, dann gilt

$$hn_1 n_2 (hn_1)^{-1} = \underbrace{h \underbrace{n_1 n_2 n_1^{-1}}_{\in N} h^{-1}}_{\in N} \in N$$

$\Rightarrow N$ ist Normalteiler. $\square$

Bsp

1) $G = S_3$, $H = \{id, (12)\}$, $N = \{id, (123), (132)\}$
$= A_3$. Dann ist $G = HN$, da (12) und (123) G erzeugen. N ist Normalteiler in $HN = G$.

2) $G = S_4$, $H = \{id, (14)\}$, $N = \{id, (123), (132)\}$
Dann wird N nicht von H normalisiert, denn z.B. ist
$(14)(123)(14)^{-1} = (14)(123)(14) = (234) \notin N$.
Die Menge $HN = N \cup \{(14), (1234), (1324)\}$ ist keine Untergruppe, da z.B.
$(1234)^2 = ((14)(123))^2 = (13)(24) \notin HN$.

1.3.3 Satz (1. Isomorphiesatz):

Sei G eine Gruppe, H, N Untergruppen, so daß N von H normalisiert wird.
Dann gilt $\quad HN/N \cong H/H\cap N$

$$\begin{tikzcd}[column sep=small]
 & G \arrow[d, dash] & \\
 & HN \arrow[dl, dash] \arrow[dr, dash] & \\
H \arrow[dr, dash] & & N \arrow[dl, dash] \\
 & H\cap N &
\end{tikzcd}$$

Beweis:

Wegen 1.3.2 ist N in HN und $H\cap N$ in H Normalteiler.

Setze

$\varphi: H \hookrightarrow HN \longrightarrow HN/N$

φ ist surjektiv, denn für $[hn] = hnN \in HN/N$ ist $hnN = hN = \varphi(h)$.

$$\operatorname{Ker}(\varphi) = \{h \in H \mid [h] = hN = [e] = N\}$$
$$= \{h \in H \mid h \in N\} = H \cap N.$$

Aus dem Homomorphiesatz folgt

$$H/\operatorname{Ker}\varphi = H/H\cap N \cong \operatorname{Im}(\varphi) = HN/N.$$

$\square$

<u>Bsp</u> $G = \mathbb{Z}$, $H = a\mathbb{Z}$, $N = b\mathbb{Z}$

$H + N = d\mathbb{Z}$ mit $d = ggT(a,b)$

$H \cap N = m\mathbb{Z}$ mit $m = kgV(a,b)$

$$H+N/N = d\mathbb{Z}/b\mathbb{Z} \cong \mathbb{Z}/\tfrac{b}{d}\mathbb{Z}$$

$$H/H\cap N = a\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/\tfrac{m}{a}\mathbb{Z}$$

Der 1. Isomorphiesatz 1.3.3 besagt hier

$$b/d = m/a \iff \frac{ab}{d} = m.$$

1.3.4 Lemma

Seien $H_2 \subset H_1$ Untergruppen von G. Dann gilt $|G/H_2| = |G/H_1| \cdot |H_1/H_2|$.

Beweis:

Wähle einen Vertreter x_i für jede Äquivalenzklasse $[x_i] = x_i H_1$ in G/H_1 und einen Vertreter y_j für jede Äquivalenzklasse $[y_j] = y_j H_2$ in H_1/H_2.

Beh $[x_i y_j] \neq [x_k y_l]$ in G/H_2 $\forall (i,j) \neq (k,l)$.

Angenommen $[x_i y_j] = [x_k y_l] \Rightarrow$

$x_i y_j H_2 = x_k y_l H_2 \Rightarrow x_k^{-1} x_i y_j H_2 = y_l H_2$.

Da $y_l \in H_1$ und $H_2 \subset H_1$ folgt

$x_k^{-1} x_i y_j \in H_1$ und da $y_j \in H_1$

$x_k^{-1} x_i \in H_1 \Rightarrow [x_i] = x_i H_1 = [x_k] = x_k H_1$

$\Rightarrow x_i = x_k$ nach Wahl der x_m

Aus $[x_i y_j] = x_i y_j H_2 = [x_k y_l] = x_k y_l H_2$

folgt dann durch Kürzen $y_j H_2 = y_l H_2$

und nach Wahl der y_n damit $y_j = y_l$.

Beh Für $g \in G$ $\exists (i,j)$: $[g] = gH_2 = x_i y_j H_2 = [x_i y_j]$.

$\exists x_i$: $[g] = gH_1 = x_i H_1 \Rightarrow$
$x_i^{-1} g \in H_1$.

Für $x_i^{-1} g$ $\exists y_j$: $x_i^{-1} g H_2 = y_j H_2$

$\Rightarrow gH_2 = x_i y_j H_2$.

Aus den beiden Behauptungen folgt

$$|G/H_2| = |\{(i,j)\}| = |\{i\}| \cdot |\{j\}| = |G/H_1| \cdot |H_1/H_2|. \qquad \square$$

1.3.5 Satz (2. Isomorphiesatz)

Seien H_1, H_2 Normalteiler von G, $H_2 \subset H_1$. Dann ist H_1/H_2 Normalteiler in G/H_2 und

$$(G/H_2) \big/ (H_1/H_2) \cong G/H_1.$$

<u>Beweis:</u> $\varphi: G/H_2 \longrightarrow G/H_1 : aH_2 \mapsto aH_1$

φ ist wohldefiniert: falls $aH_2 = bH_2$

$\Rightarrow b^{-1}a \in H_2 \subset H_1 \Rightarrow bH_1 = aH_1$

φ ist ein surjektiver Gruppenhomomorphismus.

$\mathrm{Ker}(\varphi) = \{ aH_2 \in G/H_2 \mid aH_1 = [a] = [e] = H_1 \}$

$= \{ aH_2 \in G/H_2 \mid a \in H_1 \} = H_1/H_2$

Aus dem Homomorphiesatz folgt

$$ {}^{G/H_2}\!/_{\mathrm{Ker}\,\varphi} = {}^{G/H_2}\!/_{H_1/H_2} \cong \mathrm{Im}(\varphi) = G/H_1 $$

$\square$

<u>Bsp</u> $G = \mathbb{Z}$, $H_2 = ab\mathbb{Z}$, $H_1 = a\mathbb{Z}$

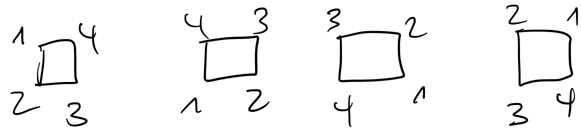
$\Rightarrow G/H_2 = \mathbb{Z}/ab\mathbb{Z}$, $H_1/H_2 = a\mathbb{Z}/ab\mathbb{Z} \cong \mathbb{Z}/b\mathbb{Z}$,

$$ {}^{\mathbb{Z}/ab\mathbb{Z}}\!/_{\mathbb{Z}/b\mathbb{Z}} \cong \mathbb{Z}/a\mathbb{Z} = G/H_1 . $$

1.3.6 Bsp

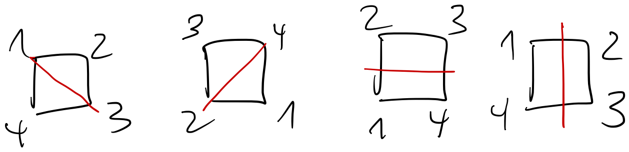
Sei G = Symmetriegruppe des Quadrats $\subset S_4$

Drehungen



$$G = \{ id, (1234), (13)(24), (1432),$$

Spiegelungen



$$(24), (13), (12)(34), (14)(23) \}$$

Sei H_1 die Untergruppe der Drehungen.

Da $|G/H_1| = 2$ ist H_1 Normalteiler.

Sei $H_2 = \{ id, (13)(24) \}$.

$H_2 = Z(G)$, also ist auch H_2 Normalteiler.

G/H_2 hat 4 Elemente:

$e := H_2 = \{ id, (13)(24) \}$ Drehung um 0°, 180°

$a := (1234) H_2 = \{ (1234), (1432) \}$ " 90°, 270°

$b := (13) H_2 = \{ (13), (24) \}$ Diagonalenspiegelungen

$c := (12)(34) H_2 = \{ (12)(34), (14)(23) \}$ Seitenmitten-spiegelungen

Wir analysieren die Gruppenstruktur von G/H_2. Die möglichen Ordnungen der Elemente sind 1, 2, 4. Falls ein Element der Ordnung 4 existierte, würde folgen G/H_2 zyklisch, also $\mathbb{Z}/4\mathbb{Z}$.

Aber a, b, c haben Ordnung 2.

Wir erstellen die Gruppenverknüpfungstabelle:

	e	a	b	c
e	e	a	b	c
a	a	e		
b	b		e	
c	c			e

Es gilt

$ab \neq a$, denn

$b \neq e$ und

$ab \neq b$, denn

$a \neq e \Rightarrow ab = c$

Genauso $ac = b$, $ba = c$, $ca = b$, $bc = a$, $cb = a$.

Also:

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Vergleiche dazu die Verknüpfungstabelle der zyklischen Gruppe der Ordnung 4 mit dem Erzeuger a, $b = a^2$, $c = a^3$:

	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

An der Verknüpfungstabelle erkennen wir: $G/H_2 \cong$

$\{ id, (12), (34), (12)(34) \} \subset S_4$

<u>Kleinsche Vierergruppe</u> K_4.

Oder: $\mathbb{Z}_2 \times \mathbb{Z}_2 = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

$= \{ (0,0), (1,0), (0,1), (1,1) \}$

$$\left. G/H_2 \middle/ H_1/H_2 \right. = \{e,a,b,c\} / \{e,a\}$$

$$= \{ \{e,a\}, b \cdot \{e,a\} \} \cong \mathbb{Z}_2 \times \mathbb{Z}_2 / \mathbb{Z}_2$$

$$\cong \mathbb{Z}_2 \cong G/H_1 .$$

Hierbei ist ein direktes Produkt von Gruppen aufgetaucht, dies wollen wir im folgenden weiter untersuchen.

1.4 Direktes und Semidirektes Produkt von Gruppen

1.4.1 Def Seien $(H_1, \cdot)$, $(H_2, *)$ Gruppen. Das <u>direkte Produkt</u> $H_1 \times H_2$ ist eine Gruppe mit

$$(h_1, h_2) \circ (g_1, g_2) = (h_1 g_1 , h_2 * g_2).$$

1.4.2 Lemma Seien H_1, H_2 Gruppen.

1) $\tilde{H}_1 := \{(h_1, e_2) \mid h_1 \in H_1\}$ und
$\tilde{H}_2 := \{(e_1, h_2) \mid h_2 \in H_2\}$
sind Normalteiler in $H_1 \times H_2$
mit $\tilde{H}_1 \cap \tilde{H}_2 = \{(e_1, e_2)\}$. Je zwei Elemente von $\tilde{H}_1$ und $\tilde{H}_2$ vertauschen:
$\tilde{h}_1 \tilde{h}_2 = \tilde{h}_2 \tilde{h}_1 \quad \forall \; \tilde{h}_1 \in \tilde{H}_1 , \tilde{h}_2 \in \tilde{H}_2 .$

2) $H_1 \times H_2 = \tilde{H}_1 \tilde{H}_2$

3) $H_1 \times H_2 / \tilde{H}_1 \cong \tilde{H}_2$,

$H_1 \times H_2 / \tilde{H}_2 \cong \tilde{H}_1 .$

Beweis:

1) Sei $(g_1, g_2) \in H_1 \times H_2$ und $(h_1, e_2) \in \tilde{H}_1$, dann gilt

$$(g_1, g_2) \cdot (h_1, e_2) \circ (g_1, g_2)^{-1} =$$

$$(g_1, g_2) \cdot (h_1, e_2) \circ (g_1^{-1}, g_2^{-1}) =$$

$$(g_1 h_1 g_1^{-1}, \quad g_2 e_2 g_2^{-1}) =$$

$$(g_1 h_1 g_1^{-1}, \quad e_2) \in \tilde{H}_1$$

$\Rightarrow \tilde{H}_1$ ist Normalteiler.

$\tilde{H}_2$ ebenso.

Sei $\tilde{h}_1 = (h_1, e_2)$, $\tilde{h}_2 = (e_1, h_2)$

$$\Rightarrow \tilde{h}_1 \tilde{h}_2 = (h_1, e_2)(e_1, h_2) = (h_1, h_2)$$
$$= (e_1, h_2)(h_1, e_2) = \tilde{h}_2 \tilde{h}_1.$$

2) „$\supset$" klar

„$\subset$" Sei $(h_1, h_2) \in H_1 \times H_2$

$$\Rightarrow (h_1, h_2) = (h_1, e_2) \circ (e_1, h_2) \in \tilde{H}_1 \circ \tilde{H}_2.$$

3) Aus dem 1. Isomorphiesatz 1.3.3 folgt $H_1 \times H_2 / \tilde{H}_1 = \tilde{H}_1 \tilde{H}_2 / \tilde{H}_1 \cong \tilde{H}_2 / \tilde{H}_1 \cap \tilde{H}_2$

$$= \tilde{H}_2 / \{e\} = \tilde{H}_2.$$

$\square$

Diese Eigenschaften sind charakteristisch für das direkte Produkt:

1.4.3 Proposition

Sei G eine Gruppe mit Untergruppen H_1, H_2. Es gelte

1) $H_1 \cap H_2 = \{e\}$
2) je zwei Elemente von H_1, H_2 vertauschen
3) $H_1 H_2 = G$

Dann ist
$$\varphi: H_1 \times H_2 \xrightarrow{\cong} G$$
$$(h_1, h_2) \longmapsto h_1 h_2$$

und H_1, H_2 sind Normalteiler mit $G/H_1 \cong H_2$ und $G/H_2 \cong H_1$.

Beweis:

φ ist Homomorphismus, denn

$\varphi((h_1,h_2)\cdot(g_1,g_2)) = \varphi((h_1g_1, h_2g_2)) =$

$h_1g_1h_2g_2 \overset{2)}{=} h_1h_2g_1g_2 = \varphi((h_1,h_2))\cdot\varphi((g_1,g_2)).$

Wegen 3) ist φ surjektiv.

Sei $(h_1,h_2) \in \mathrm{Ker}(\varphi) \Rightarrow h_1h_2 = e$

$\Rightarrow h_1 = h_2^{-1}$ mit $h_1 \in H_1$, $h_2^{-1} \in H_2$

$\Rightarrow h_1, h_2 \in H_1 \cap H_2 \overset{1)}{=} \{e\}$

$\Rightarrow \mathrm{Ker}(\varphi) = \{(e,e)\}$.

$\Rightarrow \varphi$ ist Isomorphismus

Unter φ gehen $\tilde{H}_1$, $\tilde{H}_2$ aus 1.4.2 auf H_1, H_2, daher folgt der Rest aus 1.4.2. $\square$

Wir betrachten jetzt eine allgemeinere Konstruktion, bei der 2) weggelassen wird.

1.4.4 Bsp

Sei $G = S_n$, $N = A_n$.

N ist Normalteiler in G, da $|G/N| = 2$, bzw. da $N = \mathrm{Ker}(\mathrm{sgn})$.

$H = \langle (12) \rangle \cong \mathbb{Z}_2$.

Es gilt $S_n = NH$, denn jede Permutation σ ist entweder gerade (und damit in $A_n = N = Ne$) oder ungerade, aber dann ist $\sigma \circ (12)$ gerade und in Ne, und damit
$\sigma = \sigma \circ id = (\sigma \circ (12)) \circ (12) \in N(12)$.

Aber es gilt nicht $S_n \cong N \times H$, denn die Tupel vertauschen nicht: Im direkten Produkt $NH \cong N \times H$ würde gelten
$n_1 h_1 \cdot n_2 h_2 \mathrel{\hat{=}} (n_1, h_1)(n_2, h_2) = (n_1 n_2, h_1 h_2)$
$\mathrel{\hat{=}} n_1 n_2 h_1 h_2$, aber hier gilt

z. B. für $h_1 = h_2 = (12)$, $n_1 = n_2 = (123)$:

$(123)(12)(123)(12) = (13)(13) = id$ aber
$(12)(12)(123)(123) = (132) \neq id$

Wir versuchen, $n_1 h_1 \circ n_2 h_2$ anders umzuformen:

$$n_1 h_1 n_2 h_2 = n_1 \underbrace{h_1 n_2 h_1^{-1}}_{\in N,\ \text{da } N \text{ Normalteiler}} h_1 h_2$$

$$= n_1\, i_{h_1}(n_2)\, h_1 h_2$$

Dies motiviert die folgende Def.

1.4.5 Def und Satz

Seien H, N Gruppen, $\varphi: H \longrightarrow \mathrm{Aut}(N)$ ein Homomorphismus.
Dann ist die Menge $N \times H$ mit der Verknüpfung

$$(n_1, h_1) \cdot (n_2, h_2) := (n_1 \varphi(h_1)(n_2), h_1 h_2)$$

eine Gruppe, das <u>semidirekte Produkt</u> $N \rtimes_\varphi H$ von N und H bez. φ.
Man schreibt oft $N \rtimes H$.
$N \cong N \times \{e_H\} \subset N \rtimes H$ ist Normalteiler in $N \rtimes H$ und
$N \rtimes H / N \cong H$.

<u>Beweis:</u>

Assoziativität:

$$((n_1, h_1) \cdot (n_2, h_2)) \cdot (n_3, h_3) =$$
$$(n_1 \cdot \varphi(h_1)(n_2), h_1 h_2) \cdot (n_3, h_3) =$$
$$(n_1 \varphi(h_1)(n_2) \cdot \varphi(h_1 h_2)(n_3), h_1 h_2 h_3) =$$
$$(n_1 \cdot \varphi(h_1)(n_2) \cdot \varphi(h_1) \circ \varphi(h_2)(n_3), h_1 h_2 h_3) =$$

$(n_1 \cdot \varphi(h_1)(n_2) \cdot \varphi(h_1)(\varphi(h_2)(n_3)), h_1 h_2 h_3)$

$= (n_1 \cdot \varphi(h_1)(n_2 \varphi(h_2)(n_3)), h_1 h_2 h_3)$

$= (n_1, h_1)(n_2 \varphi(h_2)(n_3), h_2 h_3)$

$= (n_1, h_1)((n_2, h_2) \cdot (n_3, h_3))$

Neutrales:

$(e_N, e_H) \cdot (n, h) =$

$(e_N \cdot \varphi(e_H)(n), e_H \cdot h) = (e_N \cdot id(n), h)$

$= (n, h)$

Inverse:

$\varphi(h) \in Aut(N)$, $\varphi(h)^{-1}$ bezeichne sein Inverses.

Damit gilt:

$((\varphi(h)^{-1}(n))^{-1}, h^{-1}) \cdot (n, h) =$

$((\varphi(h)^{-1}(n))^{-1} \cdot \varphi(h^{-1})(n), h^{-1}h) \overset{\text{da } \varphi \text{ Homomorphismus}}{=}$

$((\varphi(h)^{-1}(n))^{-1} \cdot \varphi(h)^{-1}(n), e_H) =$

(e_N, e_H).

Damit ist $N \rtimes H$ eine Gruppe.

N ist Normalteiler:

Für $(n,h) \in N \rtimes H$ und $(m, e_H) \in N$

gilt:

$(n,h)(m,e_H) \cdot (n,h)^{-1} =$

$(n,h)(m,e_H) \cdot ((\varphi(h)^{-1}(n))^{-1}, h^{-1}) =$

$(\ldots, h e_H h^{-1}) = (\ldots, e_H) \in N$.

$\Psi : \{e_N\} \times H \hookrightarrow N \rtimes H \longrightarrow N \rtimes H / N$

ist surjektiv, denn jede Klasse

$(n,h) \cdot N \times \{e_H\}$ kann man schreiben

als $(e_N, h) \cdot N \times \{e_H\}$, indem man

den Vertreter mit

$(\varphi(h)^{-1}(n^{-1}), e_H) \in N \times \{e_H\}$

multipliziert:

$(n,h) \cdot (\varphi(h)^{-1}(n^{-1}), e_H) =$

$(n \cdot \varphi(h)(\varphi(h)^{-1}(n^{-1})), h e_H) =$

$(n \cdot \varphi(h) \circ \varphi(h)^{-1}(n^{-1}), h) =$

$(n \cdot id(n^{-1}), h) = (n n^{-1}, h) =$

(e_N, h)

$\operatorname{Ker}(\Psi) =$

$\{(e_N, h) \mid [(e_N, h)] = (e_N, h) \cdot N \times \{e_H\}$
$= (e_N, e_H) \cdot N \times \{e_H\} = [(e_N, e_H)]\}$

$= \{(e_N, h) \mid (e_N, h) \in N \times \{e_H\}\}$

$= \{(e_N, e_H)\}$

Aus dem Homomorphiesatz folgt

$H \cong \{e_N\} \times H = \{e_N\} \times H / \operatorname{Ker} \Psi$

$\cong \operatorname{Im} \Psi = N \rtimes H / N$ $\square$

1.4.6 Bsp

1) Für $\varphi: H \longrightarrow \operatorname{Aut}(N)$
$h \longmapsto \mathrm{id}_N$

ist das semidirekte Produkt gleich dem direkten Produkt

2) Bsp. 1.4.4 zeigt
$S_n = A_n \rtimes_\varphi \mathbb{Z}_2$

mit $\varphi: \mathbb{Z}_2 \longrightarrow \mathrm{Aut}(A_n)$:

$$0 \longmapsto \mathrm{id}$$

$$1 \longmapsto i_{(12)},$$ Konjugation mit (12)

denn $\langle (12) \rangle \cong \mathbb{Z}_2$

3) Sei $N = \mathbb{Z}_3$, $H = \mathbb{Z}_2$,

$\varphi: H \longrightarrow \mathrm{Aut}(N)$:

$$0 \longmapsto \mathrm{id}$$

$$1 \longmapsto \begin{pmatrix} N \longrightarrow N: \\ x \longmapsto -x \end{pmatrix}$$

Setze $\Psi: \mathbb{Z}_3 \rtimes_\varphi \mathbb{Z}_2 \xrightarrow{\Psi} S_3$

$$(a, 0) \longmapsto (123)^a$$

$$(a, 1) \longmapsto (123)^a (12)$$

<u>Beh</u>: Ψ ist Isomorphismus.

Homomorphismus:

Fallunterscheidung nach dem 2. Eintrag:

1) $\Psi((a,0) + (b,0)) = \Psi(a+b, 0) =$

$(123)^{a+b} = (123)^a \circ (123)^b = \Psi(a,0) \circ \Psi(b,0)$

2) $\Psi((a,0)+(b,1)) =$

$\Psi((a+b,1)) = (123)^{a+b}(12) =$

$(123)^a \circ (123)^b (12) =$

$\Psi(a,0) \circ \Psi(b,1)$

3) $\Psi((a,1)+(b,0)) =$

$\Psi(a+\varphi(1)(b), 1) =$

$\Psi(a-b, 1) = (123)^{a-b} (12)$

$\Psi(a,1) \circ \Psi(b,0) = (123)^a (12) (123)^b$

$= (123)^a (12) \left((123)(12)(12)\right)^b$

$= (123)^a \left[(12)(123)(12)\right]\left[(12)(123)(12)\right]\left[(12)\dots\right.$

$\left.(123)(12)\right](12)$

$= (123)^a (132)^b (12)$

$= (123)^a \left((123)^{-1}\right)^b (12)$

$= (123)^a (123)^{-b} (12)$

$= (123)^{a-b} (12)$

4) $\Psi((a,1)+(b,1)) =$

$\Psi(a-b,0) = (123)^{a-b}$

$\Psi(a,1) \circ \Psi(b,1) =$

$(123)^a (12) (123)^b (12) \overset{\text{wie in 3)}}{=}$

$(123)^{a-b} (12)(12) = (123)^{a-b}$

Ψ ist surjektiv, denn

$(123) = \Psi(1,0)$, $(12) = \Psi(0,1)$

sind im Bild und diese

erzeugen S_3.

Ψ ist injektiv:

$\Psi(a,0) = \Psi(a',0) \Rightarrow$

$(123)^a = (123)^{a'} \Rightarrow a \equiv a' \bmod 3$

$\Rightarrow a = a'$ in $\mathbb{Z}/3\mathbb{Z} = \mathbb{Z}_3$

$\Psi(a,1) = \Psi(a',1)$ genauso

$\Psi(a,0) = \Psi(a',1) \Rightarrow$

$(123)^a = (123)^{a'}(12)$ $\lightning$

denn links ist eine grade Permutation, rechts eine ungerade.

1.5 Sylowsätze

Die Ordnung eines Untergruppe teilt die Gruppenordnung.
Gibt es für jeden Teiler der Gruppenordnung eine Untergruppe?
I.A. unklar, Ergebnisse für Primzahlpotenzen.

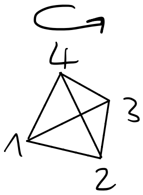
1.5.1 Bsp

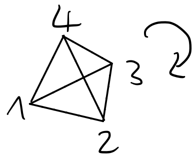
S_4 = Symmetriegruppe des Tetraeders

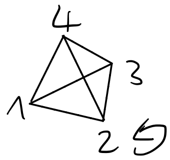
Ordnung $24 = 2^3 \cdot 3$

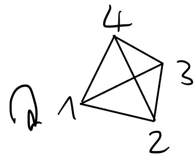
Untergruppen der Ordnung 3 sind zyklisch, erzeugt von einem 3-Zykel.
Es gibt $8 = \frac{4 \cdot 3 \cdot 2}{3}$ 3-Zykel, jeweils zwei sind zueinander invers, damit gibt es 4 Untergruppen der Ordnung 3:

$\{id, (123), (132)\}$

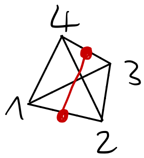


$\{id, (124), (142)\}$ 

$\{id, (134), (143)\}$ 

$\{id, (234), (243)\}$ 

jeweils erzeugt von einer Drehung um eine Ecke um 120°.

Kantenmittendiagonalen: 

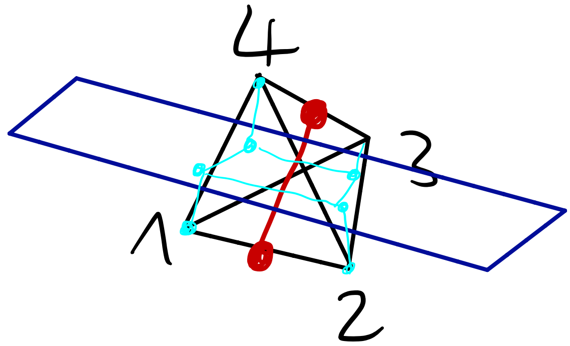
z.B. 12 nach 34.

Betrachte den Stabilisator der Kantenmittendiagonale. Die Kante 12 muß festgehalten werden (1, 2 fest oder 1, 2 vertauscht), 34 genauso, oder 12 geht auf 34:

$\{id, (12), (34), (12)(34), (1324), (1423), (13)(24), (14)(23)\}$

= Symmetriegruppe des Quadrats.

Geometrisch sieht man das, indem man den Tetraeder auf die Ebene senkrecht zur Kantenmittendiagonalen durch den Mittelpunkt der Kantenmittendiagonalen projeziert: der gesuchte Stabilisator hält die Kantenmittendiagonale fest und wirkt nur auf der Projektion des Tetraeders auf die senkrechte Ebene, dies ist ein Quadrat:



Es gibt 3 Kantenmittendiagonalen und 3 zugehörige Stabilisatoren, damit 3 Untergruppen der Ordnung 8:

{id, (12), (34), (12)(34), (1324), (1423), (13)(24), (14)(23)}

{id, (13), (24), (13)(24), (1234), (1432), (12)(34), (14)(23)}

{id, (14), (23), (14)(23), (1342), (1243), (13)(24), (12)(34)}

Untergruppen der Ordnung 4:

Drei erzeugt von Drehspiegelungen:

{id, (1234), (13)(24), (1432)}

$\{id, (1243), (14)(23), (1342)\}$

$\{id, (1324), (12)(34), (1423)\}$

Vier Kleinsche Vierergruppen:

$\{id, (12), (34), (12)(34)\}$

$\{id, (13), (24), (13)(24)\}$

$\{id, (14), (23), (14)(23)\}$

$\{id, (12)(34), (13)(24), (14)(23)\}$

6 Untergruppen der Ordnung 2 erzeugt von Spiegelungen:

$\langle(12)\rangle, \langle(13)\rangle, \langle(14)\rangle, \langle(23)\rangle, \langle(24)\rangle, \langle(34)\rangle$

4 Untergruppen der Ordnung 6 = Stabilisatoren von Ecken $\cong S_3$:

$S(1,2,3), S(1,3,4), S(1,2,4), S(2,3,4)$

1 Untergruppe der Ordnung 12: A_4.

24 hat die Teiler

24, 12, 8, 6, 4, 3, 2, 1

Zu jedem Teiler haben wir Untergruppen gefunden.

1.5.2 Bsp

$|A_4| = 12$

$6 | 12$ aber A_4 hat keine Untergruppe der Ordnung 6.

Angenommen, sie hätte, N, N ist Normalteiler, denn $|A_4/N| = 2$.

Sei H eine Untergruppe der Ordnung 3, erzeugt von einer Drehung, z. B. $\langle (123) \rangle = H$.

Mit dem 1. Isomorphiesatz 1.3.3 folgt

$$HN/N \cong H/H\cap N \Rightarrow$$

$$|HN/N| = |H/H\cap N| \Rightarrow$$

$$|HN| / |N| = |H| / |H\cap N| \Rightarrow$$

$$12 = |A_4| \geq |HN| = |H| \cdot |N| / |H\cap N| = \frac{3 \cdot 6}{|H\cap N|}$$

$$= \frac{18}{|H\cap N|}$$

$\Rightarrow H\cap N \supsetneqq \{id\}$, damit existiert ein 3-Zykel in $H\cap N$. Da $H\cap N$ eine Untergruppe ist, liegt auch sein Inverses in $H\cap N \Rightarrow |H\cap N| = 3$

$\Rightarrow H \subset H \cap N \Rightarrow H \subset N$

Da dieses Argument für jede Wahl von H greift, folgt

$\{3\text{-Zykel}\} \subset N$.

Es gibt 8 3-Zykel $\lightning$.

<u>1.5.3 Def</u> Sei G eine endliche Gruppe, p eine Primzahl.

1) G heißt p-Gruppe, falls $|G| = p^r$ für ein $r \in \mathbb{N}$.

2) Ist $|G| = p^k \cdot m$ mit $p \nmid m$, so heißt eine Untergruppe $H \subset G$ mit $|H| = p^k$ eine p-Sylow-(Unter-)Gruppe von G.

<u>Bsp</u>: Stab(Kantenmittendiagonalen) = Sym(Quadrat) sind 2-Sylowgruppen der S_4, denn $|S_4| = 24 = 2^3 \cdot 3$

Erzeugnisse von Drehungen (z.B. $\langle (123) \rangle$) sind 3-Sylowgruppen der S_4.

1.5.4 Satz

Sei G endlich, p eine Primzahl mit $p \mid |G|$, $|G| = p^k \cdot m$, $p \nmid m$.

Dann gibt es zu jedem r mit $1 \leq r \leq k$ eine Untergruppe H von G mit $|H| = p^r$.

Insbesondere hat G für jedes p eine p-Sylowuntergruppe.

1.5.5 Def

Sei G eine Gruppe, der Exponent von G ist $\min\{k \in \mathbb{N}_{>0} \mid g^k = e \ \forall g \in G\}$

Bsp $\mathrm{Exp}(\mathbb{Z}_2 \times \mathbb{Z}_2) = 2$, $\mathrm{Exp}(\mathbb{Z}_4) = 4$, $\mathrm{Exp}(S_3) = 6$, $\mathrm{Exp}(\mathrm{Sym}(\square)) = 4$

1.5.6 Lemma

Sei $|G| = n$.

1) Der Exponent m von G ist das kgV der Ordnungen der Elemente von G.
2) Falls $g^k = e \ \forall g \in G \Rightarrow m \mid k$.
3) $m \mid n$.

Beweis:

1) $g^k = e \iff \mathrm{ord}(g) \mid k$

m wird also von allen $\mathrm{ord}(g)$ geteilt und das es nach Def das kleinste ist, folgt $m = \mathrm{kgV}(\mathrm{ord}(g) \mid g \in G)$.

2) folgt aus 1).

3) folgt, da n ein Vielfaches von $\mathrm{ord}(g)$ ist $\forall g \in G$. $\square$

1.5.7 Lemma Sei G endlich und abelsch, $m = \mathrm{Exp}(G)$. Dann $\exists$ $k \in \mathbb{N}_{>0}$: $|G| \mid m^k$.

Beweis: Induktion nach $|G|$.

Induktionsanfang: $|G| = 1$ klar.

Induktionsvoraussetzung: Die Behauptung gelte $\forall$ abelschen G' mit $|G'| < |G|$.

Induktionsschluß:

Sei $e \neq g \in G$, $H = \langle g \rangle$, $|H| = \mathrm{ord}(g) \mid m$.

Da G abelsch, ist H Normalteiler und G/H eine Gruppe.

Sei $g'H \in G/H$, dann ist

$(g'H)^m = g'^m H = eH = H$

also teilt der Exponent von G/H m nach Lemma 1.5.6 2).

Da $|G/H| < |G|$ greift die Induktionsvoraussetzung und wir erhalten k' mit $|G/H| \mid \operatorname{Exp}(G/H)^{k'}$ $\Longrightarrow$

$$|G/H| \mid m^{k'}$$

Setze $k = k'+1$, dann gilt

$$|G| = |H| \cdot |G/H| = \operatorname{ord}(g) \cdot |G/H| \;\Big|\; m \cdot m^{k'} = m^{k'+1} = m^k$$

$\square$

<u>1.5.8 Lemma</u> Sei G endlich und abelsch, p Primzahl, $p \mid |G|$, dann hat G eine Untergruppe der Ordnung p.

<u>Beweis</u>: $p \mid |G|$ und $|G| \mid m^k$, wobei $m = \operatorname{Exp}(G)$ $\Longrightarrow$ $p \mid m^k$

$\Longrightarrow$ $p \mid m$ da p prim

Da $m = \operatorname{kgV}(\operatorname{ord}(g) \mid g \in G)$ $\exists\, g$: $p \mid \operatorname{ord}(g)$. Sei $\operatorname{ord}(g) = r \cdot p$.

Dann hat g^r Ordnung p und $\langle g^r \rangle$ ist eine (notwendigerweise zyklische) Untergruppe der Ordnung p. $\square$

<u>Beweis von Satz 1.5.4</u>:

Induktion nach $n = |G|$.

Induktionsanfang: $n=1$, $n=2$ klar.

Induktionsvoraussetzung: Die Behauptung gelte für alle G' mit $|G'| < n$.

Induktionsschluß:

Hat G eine echte Untergruppe U mit $p^k \mid |U|$, so wenden wir die Induktionsvoraussetzung auf U an und die Behauptung folgt, da Untergruppen von U auch Untergruppen von G sind.

Hat G keine solche Untergruppe, so folgt aus $|G| = |U| \cdot |G/U|$

$p \mid |G/U|$ $\forall$ echten Untergruppen U.

Betrachte die Konjugation von G,

Sei $R \subset G$ eine Teilmenge, die aus jeder Konjugationsklasse genau ein Element enthält. Nach der Klassengleichung 1.2.12 gilt

$$|G| = |Z(G)| + \sum_{r \in R \setminus Z(G)} |G/Z_G(r)|$$

wobei für $r \in R \setminus Z(G)$ der Zentralisator $Z_G(r)$ eine echte Untergruppe ist, daher gilt $p \mid |G/Z_G(r)|$

$\Rightarrow \quad p \mid |Z(G)|$.

Da $Z(G)$ abelsch ist, folgt mit Lemma 1.5.8, daß $Z(G)$ eine Untergruppe N der Ordnung p hat.

Als Untergruppe des Zentrums, das Normalteiler in G und abelsch ist, ist N Normalteiler in G und wir können G/N betrachten.

Es gilt $|G/N| = \frac{|G|}{|N|} = \frac{p^k m}{p} = p^{k-1} \cdot m$.

Nach Induktionsvoraussetzung hat G/N für jedes r' mit $1 \leq r' \leq k-1$ eine Untergruppe H' der Ordnung $p^{r'}$.
G/N hat auch die Untergruppe $\{e\}$ der Ordnung $1 = p^0$.
Sei $\pi : G \longrightarrow G/N$, setze

$$H = \pi^{-1}(H').$$

Dann ist H eine Untergruppe von G der Ordnung $p^{r'+1}$, und mit $r = r'+1$ haben wir solche $\forall \; 1 \leq r \leq k$. $\square$

1.5.9 Korollar

Für jede Primzahl $p \mid |G|$ $\exists$ ein Element der Ordnung p.

Beweis: Aus Satz 1.5.4 folgt, daß es für jedes $p \mid |G|$ eine Untergruppe der Ordnung p gibt, diese ist notwendigerweise zyklisch und daher erzeugt von einem Element der Ordnung p. $\square$

1.5.10 Satz (Sylowsche Sätze)

Sei G endlich, $p \mid |G|$, p prim.

1) Jede p-Untergruppe H ist in einer p-Sylowgruppe enthalten.
2) Alle p-Sylowgruppen sind zueinander konjugiert
3) Die Anzahl n_p der p-Sylowgruppen von G ist ein Teiler von $|G|$ mit $n_p \equiv 1 \mod p$.

Bsp $G = S_4$, $|G| = 24 = 2^3 \cdot 3$

Die 2-Sylowgruppen haben Ordnung 8.

$n_2 \mid 24$ und $n_2 \equiv 1 \mod 2$

$\Rightarrow n_2 \mid 3$

Wir kennen 3 2-Sylowgruppen (Bsp. 1.5.1), die drei $\mathrm{Sym}(\square)$, also $n_2 = 3$.

Die 3-Sylowgruppen haben Ordnung 3.

$n_3 \mid 24$, $n_3 \equiv 1 \mod 3$

$\Rightarrow n_3 \in \{1, 4\}$

Wir kennen schon 4 Untergruppen der Ordnung 3 – die 4 Sym(Δ) der Seiten, erzeugt von einer Drehung,

$\langle(123)\rangle$, $\langle(124)\rangle$, $\langle(134)\rangle$, $\langle(234)\rangle$

$\Rightarrow$ $n_3 = 4$.

1.5.11 Korollar

Sei $|G| = p^k \cdot m$, $p \nmid m$,

so gilt $n_p \mid m$.

Beweis: $n_p \equiv 1 \mod p$ $\Rightarrow$

$p \nmid n_p$, aber $n_p \mid |G| = p^k \cdot m$ $\square$

1.5.12 Def

Sei G eine Gruppe, S eine Untergruppe.

Der Normalisator von S,

$$N_G(S) = \{g \in G \mid gSg^{-1} = S\}.$$

1.5.13 Lemma

Sei $H \subset G$ eine p-Gruppe,

S eine p-Sylowgruppe von G.

Ist H im Normalisator $N_G(S)$ enthalten, so gilt schon $H \subset S$.

<u>Beweis:</u> Sei $|G| = p^k \cdot m$, $p \nmid m$.

Da $H \subset N_G(S)$ wird S von H normalisiert.

Mit dem 1. Isomorphiesatz 1.3.3 erhalten wir

$$HS/S \cong H/H \cap S$$

Damit ist $|HS/S|$ ein Teiler von $|H|$ und daher eine p-Potenz.

Also ist auch $|HS| = |HS/S| \cdot |S|$ eine p-Potenz, größer gleich $|S| = p^k$.

Wegen 1.3.2 2) (Vorbereitung zum 1. Isomorphiesatz) ist HS eine Untergruppe von G $\Rightarrow |HS| \mid |G|$

$\Rightarrow |HS| \mid p^k \cdot m \Rightarrow |HS| = p^k$

$\Rightarrow |HS/S| = 1 \Rightarrow HS = S$

$\Rightarrow \quad hs \in S \quad \forall h \in H, \; s \in S \quad \Rightarrow$

$$h = \underbrace{(hs)}_{\in S} \underbrace{s^{-1}}_{\in S} \in S \quad \forall h \in H$$

$\Rightarrow \quad H \subset S.$ $\square$

<u>1.5.14 Def</u> Eine Gruppenoperation mit nur einer Bahn heißt <u>transitiv</u>.

<u>1.5.15 Prop</u> Sei $U \subset G$ eine p-Sylowgruppe, $H \subset G$ eine p-Gruppe, dann $\exists\, g \in G : H \subset gUg^{-1}$ und gUg^{-1} ist auch p-Sylowgruppe.

<u>Beweis</u>:

Sei U^G = Menge der Konjugationsklassen von U
$$= \{ gUg^{-1} \mid g \in G \}$$

Betrachte die Konjugationsoperation von G auf U^G:

$$G \times U^G \longrightarrow U^G : (g, S) \mapsto gSg^{-1}$$

Sie ist per Def transitiv.

Aus Korollar 1.1.21 folgt

$|G| = \text{Bahnlänge} \cdot |\text{Stab}| =$

$|U^G| \cdot |\text{Stab}(U)| =$

$|U^G| \cdot |N_G(U)|$, da der Normalisator $N_G(U)$ per Def der Stabilisator dieser Operation ist.

Sei $|G| = p^k \cdot m$, $p \nmid m$, dann ist $|U| = p^k$. Da $U < N_G(U)$ Untergruppe gilt $p^k \mid |N_G(U)|$

$\Rightarrow \quad p \nmid |U^G|$

Wir schränken die Operation jetzt auf H ein:

$H \times U^G \longrightarrow U^G, \quad (h, S) \mapsto hSh^{-1}$

Dann zerfällt U^G in eine disjunkte Vereinigung von Bahnen.

Sei $R \subset U^G$ eine Menge, die aus jeder Bahn genau ein Element enthält. Dann gilt mit der

Bahnengleichung 1.1.23

$$|U^G| = \sum_{S \in R} |H| / |Stab_H(S)| = \sum_{S \in R} p^{j_S}$$

für geeignete $j_S \geq 0$, da H eine p-Gruppe ist und daher die Ordnungen von Untergruppen und Faktorgruppen auch p-Potenzen sind.

Da $p \nmid |U^G|$ $\exists S : j_S = 0$

Wir schreiben dieses $S \in R \subset U^G$ als gUg^{-1} für ein $g \in G$.

Für dieses S gilt:

$$\Rightarrow |H| / |Stab_H(S)| = 1$$

$$\Rightarrow H = Stab_H(S) = \{h \in H \mid hSh^{-1} = S\} \subset Stab_G(S) = N_G(S)$$

$$\overset{1.5.13}{\Longrightarrow} H \subset S = gUg^{-1}$$

S ist das Bild von U unter

einer Konjugation und damit isomorph zu U, insbesondere ist S eine p-Sylowgruppe. $\square$

Beweis der Sylowschen Sätze 1.5.10:

1) Wegen Satz 1.5.4 $\exists$ eine p-Sylowgruppe $U \subset G$. Wegen Prop 1.5.15 $\exists$ g mit $H \subset gUg^{-1}$ und dies ist eine p-Sylowgruppe.

2) Sei H eine (weitere) p-Sylowgruppe, dann ist H eine p-Gruppe und wir können Prop 1.5.15 auf H anwenden. Wir erhalten g mit $H \subset gUg^{-1}$, und

$$p^k = |H| = |gUg^{-1}| \Rightarrow H = gUg^{-1}$$

Damit ist H zu U konjugiert.

3) Sei U p-Sylowgruppe, jede zu U konjugierte Untergruppe ist auch p-Sylowgruppe, aus 2) folgt

$U^G = \{$ p-Sylowgruppen von $G\}$

$\Rightarrow n_p = |U^G|$.

Wie in 1.5.15 sehen wir

$|G| = |U^G| \cdot |Stab(U)| = n_p \cdot |Stab(U)|$

$\Rightarrow n_p \mid |G|$.

Wir schränken die Konjugation auf U ein:

$U \times U^G \longrightarrow U^G : (u, S) \mapsto uSu^{-1}$

Sei $R \subset U^G$ eine Teilmenge, die aus jeder Bahn genau ein Element enthält.

Die Bahn von U ist

$\{uUu^{-1} \mid u \in U\} = \{U\}$.

Angenommen, es gäbe eine weitere Bahn mit nur einem Element, also $S \in U^G$ mit

$uSu^{-1} = S \ \forall u \in U$.

Dann wäre $U \subset N_G(S)$ und

mit 1.5.13 folgte $U \subset S$

$\Longrightarrow$ $U = S$ da beides p-Sylowgruppen

sind.

Mit der Bahnengleichung 1.1.23

gilt also

$$n_p = |U^G| = \sum_{S \in R} {|U|}/{|Stab_U(S)|} =$$

$$\sum_{S \in R} p^{j_S}$$ mit geeigneten $j_S \geq 0$,

da U p-Gruppe.

Weiter gilt $U \in R$ und $j_U = 0$

sowie $j_S > 0 \;\forall\; S \neq U$,

denn ${|U|}/{|Stab_U(S)|}$ = Bahnlänge (S)

nach 1.1.21 und damit

$$n_p = 1 + \sum_{S \in R \setminus \{U\}} p^{j_S} \equiv 1 \mod p \quad \square$$

Die Sylowsätze sind wichtig bei der Klassifikation der endlichen Gruppen.
Eine Anwendung:

<u>1.5.16 Satz</u> Seien p, q prim, $p<q$, $p \nmid q-1$. Dann ist jede Gruppe G der Ordnung pq zyklisch,

$$G \cong \mathbb{Z}_{pq}.$$

<u>Beweis</u> $n_p = 1 + k \cdot p$ wegen der Sylowsätze 1.5.10 3) und $n_p \mid q$ wegen Korollar 1.5.11.

$\Rightarrow n_p \in \{1, q\}$

Wäre $n_p = q \Rightarrow q = 1 + kp$

$\Rightarrow q-1 = kp \Rightarrow p \mid q-1$ ↯.

$\Rightarrow n_p = 1$.

Sei P die einzige p-Sylowgruppe.

$n_q = 1 + lq$, $n_q \mid p$ $\Rightarrow$ $n_q \in \{1, p\}$

Wäre $n_q = p \Rightarrow p = 1 + lq$ ↯ zu $p < q$

$\Rightarrow$ $n_q = 1$.

Sei Q die einzige q-Sylowgruppe.

P und Q haben Primzahlordnung p bzw. q, sind also zyklisch:

$P \cong \mathbb{Z}_p$, $Q \cong \mathbb{Z}_q$.

Betrachte die Bahnen von P und Q unter Konjugation.

Nach 1.5.10 2) sind es jeweils alle p- bzw. q-Sylowgruppen, also einelementig.

$\Rightarrow$ $gPg^{-1} = P$, $gQg^{-1} = Q$ $\forall g \in G$

$\Rightarrow$ P, Q Normalteiler

Da P und Q teilerfremde Ordnungen

haben, gilt $P \cap Q = \{e\}$.
Mit 1.3.2 2) und dem 1. Isomorphiesatz folgt PQ ist Untergruppe von G

und $PQ/P \cong Q/P \cap Q \cong Q$

$$\Rightarrow \quad |PQ|/|P| = |Q| \quad \Rightarrow \quad |PQ| = p \cdot q$$

$$\Rightarrow \quad PQ = G.$$

Sei $g \in P$, $h \in Q \Rightarrow$
$ghg^{-1} \in Q$, da Q Normalteiler
$\Rightarrow ghg^{-1}h^{-1} \in Q$
Andererseits ist
$hg^{-1}h^{-1} \in P$, da P Normalteiler
$\Rightarrow ghg^{-1}h^{-1} \in P$

$$\Rightarrow \quad ghg^{-1}h^{-1} \in P \cap Q = \{e\}$$

$\Rightarrow \quad gh = hg \quad \Rightarrow$ g und h vertauschen

1.4.3, Charakterisierung des direkten Produkts

$$\Rightarrow \quad G = P \times Q \cong \mathbb{Z}_p \times \mathbb{Z}_q.$$

Beh $\mathbb{Z}_{pq} \cong \mathbb{Z}_p \times \mathbb{Z}_q$

Dies folgt aus dem chinesischen Restsatz:

Betrachte
$$\varphi: \mathbb{Z} \longrightarrow \mathbb{Z}_p \times \mathbb{Z}_q$$
$$a \longmapsto (a+p\mathbb{Z}, a+q\mathbb{Z})$$

φ ist Homomorphismus.

φ ist surjektiv wegen des chinesischen Restsatzes: Für $(a_1, a_2) \in \mathbb{Z}_p \times \mathbb{Z}_q$ suchen wir a mit $a \equiv a_1 \mod p$, $a \equiv a_2 \mod q$, dies existiert nach dem chinesischen Restsatz und ist eindeutig mod pq.

$\operatorname{Ker} \varphi = pq\mathbb{Z}$

$$\overset{\text{Homomorphiesatz}}{\Longrightarrow} \mathbb{Z}_{pq} = \mathbb{Z}/pq\mathbb{Z} = \mathbb{Z}/\operatorname{Ker}\varphi \cong \operatorname{Im}\varphi = \mathbb{Z}_p \times \mathbb{Z}_q.$$

$\Longrightarrow G \cong \mathbb{Z}_{pq}$ ist zyklisch. $\square$

<u>1.5.17 Korollar</u> Jede Gruppe der Ordnung 15 ist zyklisch.

Anders gesagt: Bis auf Isomorphie $\exists!$ Gruppe der Ordnung 15, $\mathbb{Z}_{15}$.

1.6 Auflösbare Gruppen

1.6.1 Def

Eine Gruppe G heißt <u>einfach</u>, wenn sie nur die Normalteiler $\{e\}$ und G besitzt.

1.6.2 Lemma

Eine abelsche Gruppe $G \supsetneqq \{e\}$ ist einfach $\Longleftrightarrow$ G zyklisch von Primzahl-ordnung

<u>Beweis:</u>

„$\Longleftarrow$" Eine zyklische Gruppe von Primzahl-ordnung hat nur $\{e\}$ und G als Untergruppen

„$\Longrightarrow$" Ist $|G|$ keine Primzahl, so existiert eine Primzahl p mit $p \mid |G|$.
Nach Satz 1.5.4 $\exists$ Untergruppe U mit $|U| = p$, da G abelsch, ist U Normalteiler. $\square$

1.6.3 Prop

Die alternierende Gruppe A_5 ist einfach.

Beweis:

A_5 hat $\frac{5!}{5} = 24$ 5-Zykel und

$\frac{5 \cdot 4 \cdot 3}{3} = 20$ 3-Zykel.

$|A_5| = 60 = 2^2 \cdot 3 \cdot 5$

$\Rightarrow$ Die 5-Sylowgruppen haben Ordnung 5, sind zyklisch von einem 5-Zykel erzeugt und enthalten je 4 5-Zykel.

$\Rightarrow \exists$ 6 5-Sylowgruppen.

Genauso: die 3-Sylowgruppen haben Ordnung 3, sind zyklisch und enthalten je 2 3-Zykel

$\Rightarrow \exists$ 10 3-Sylowgruppen.

Sei $\{e\} \subsetneq N \subsetneq A_5$ ein Normalteiler.

Angenommen, $5 \mid |N|$. Dann enthält N eine 5-Sylowuntergruppe, die auch 5-Sylowgruppe von A_5 ist.

Da alle 5-Sylowgruppen konjugiert sind, und $gNg^{-1} \subset N$, da N Normalteiler folgt, alle 5-Sylowgruppen der A_5 sind in N $\Rightarrow$ $|N| \geq 1 + 24 = 25$

$\Rightarrow$ $|N| \in \{30, 60\}$. $\Rightarrow$ $3 \mid |N|$.

Damit enthält N auch eine (und damit alle) 3-Sylowgruppen, also folgt

$|N| \geq 1 + 24 + 20 = 45$ $\Rightarrow$ $|N| = 60$

$\Rightarrow$ $N = A_5$. $\lightning$

Angenommen, $3 \mid |N|$.

$\Rightarrow$ N enthält eine (und damit alle) 3-Sylowgruppen $\Rightarrow$ $|N| \geq 1 + 20 = 21$

$\Rightarrow$ $|N| \in \{30, 60\}$ $\Rightarrow$ $5 \mid |N|$

Dann folgt wieder $N = A_5$. $\lightning$

Angenommen, $|N| = 4$.

Dann ist N 2-Sylowgruppe. Da die 2-Sylowgruppen konjugiert sind, und N Normalteiler ist, ist N die einzige 2-Sylowgruppe.

Aber alle (2,2)-Zykel haben Ordnung 2, also $\frac{5 \cdot 4}{2} \cdot \frac{3 \cdot 2}{2} \cdot \frac{1}{2} = 15$ Elemente, und jeweils 3 davon

liegen in einer Kleinschen Vierergruppe
$\Rightarrow$ $\exists$ 5 4-Sylowgruppen $\lightning$.

Angenommen, $|N| = 2$.
Dann ist $N = \langle n \rangle$ für ein Element n der Ordnung 2, also einen (2,2)-Zykel.
Da N Normalteiler gilt $gng^{-1} = n$
$\forall g \in A_5$, aber für $n = (ab)(cd)$
und $g = (abe)$ gilt
$$gng^{-1} = (abe)(ab)(cd)(aeb) = (be)(cd) \neq n$$
$\lightning$
Also gibt es keinen solchen Normalteiler und A_5 ist einfach. $\square$

1.6.4 Def

Eine Gruppe G heißt <u>auflösbar</u>, wenn es eine Kette
$$\{e\} = G_k \subset G_{k-1} \subset \cdots \subset G_0 = G$$
gibt, so daß $G_i \subset G_{i-1}$ Normalteiler und G_{i-1}/G_i abelsch $\forall i = 1, \ldots, k$.

Eine solche Kette heißt Subnormalteiler-kette mit abelschen Faktoren.

<u>Bsp</u>

1) Abelsche Gruppen G sind auflösbar mit $\{e\} \subset G$.

2) S_4 ist auflösbar mit Subnormalteilerkette
$\{id\} \subset K_4 \subset A_4 \subset S_4$,
wobei K_4 die kleinsche Vierergruppe
$\{id, (12)(34), (13)(24), (14)(23)\}$ ist.
Da $|S_4/A_4| = 2$, ist A_4 in S_4 Normalteiler. Daß K_4 in A_4 Normalteiler ist, läßt sich nachrechnen.
(Es gilt sogar $K_4 \subset S_4$ ist Normalteiler, man kann dies geometrisch begründen, da $S_4 = \mathrm{Sym}$ (Tetraeder), und $K_4 = \ker(\varphi)$ für $\varphi : S_4 \to S_3 = S$ (Kantenmittendiagonalen).)

$S_4/A_4 \cong \mathbb{Z}_2$ ist abelsch,

$A_4/K_4 \cong \mathbb{Z}_3$ " ,

K_4 ist auch abelsch.

3) A_5 ist einfach, nicht abelsch, also auch nicht auflösbar.

1.6.5 Prop

Sei G endlich, $U \subset G$ Untergruppe, N Normalteiler.

1) G auflösbar $\Rightarrow$ U auflösbar
2) G auflösbar $\Leftrightarrow$ N, G/N auflösbar.

Beweis:

1) Sei G auflösbar mit Subnormalteiler-kette

$$\{e\} = G_k \subset G_{k-1} \subset \dots \subset G_0 = G.$$

Setze $U_i := G_i \cap U$.

Dann ist

$$\{e\} \subset U_k \subset U_{k-1} \subset \dots \subset U_0 = U$$

eine Kette von Untergruppen in U.

Dabei gilt

$$U_i = G_i \cap U = G_i \cap G_{i-1} \cap U = G_i \cap U_{i-1}$$

Wegen 1.3.2 1) ($H \cap N$ Normalteiler in H) folgt $U_i = G_i \cap U_{i-1}$ ist Normalteiler in U_{i-1} (denn G_i ist Normalteiler in G_{i-1}).

$$\begin{tikzcd}[column sep=small] & HN \arrow[dl, dash] \arrow[dr, dash] & \\ H \arrow[dr, dash] & & N \arrow[dl, dash] \\ & H \cap N & \end{tikzcd}$$

Außerdem gilt

$$U_{i-1}/U_i = U_{i-1}/G_i \cap U_{i-1} \overset{\substack{\text{1. Isom. satz} \\ 1.3.3}}{\cong} G_i U_{i-1}/G_i$$

$\subset G_{i-1}/G_i$ ist Untergruppe, denn

$G_i U_{i-1} \subset G_{i-1}$ ist Untergruppe wegen

1.3.2. G_{i-1}/G_i ist abelsch, damit

Aber

auch U_{i-1}/U_i.

2) „$\Rightarrow$" N ist auflösbar wegen 1).

Sei $\{e\} = G_k \subset G_{k-1} \subset \dots \subset G_0 = G$

Subnormalteilerkette von G

Durch Multiplikation mit N erhalten wir

wegen 1.3.2 eine Kette von Untergruppen

$N = G_k N \subset G_{k-1} N \subset \dots \subset G_0 N = G$.

<u>Bew</u>: $G_i N \subset G_{i-1} N$ ist Normalteiler.

Sei $g_1 n_1 \in G_i N$ und $g_2 n_2 \in G_{i-1} N$

Dann gilt

$$g_2 n_2 (g_1 n_1)(g_2 n_2)^{-1} = g_2 n_2 g_1 n_1 n_2^{-1} g_2^{-1}$$

Da N Normalteiler in G gilt

$g_1 n_1 g_1^{-1} \in N \Rightarrow \exists\, n_3 \in N:$

$g_1 n_1 g_1^{-1} = n_3 \Rightarrow g_1 n_1 = n_3 g_1$

$\Rightarrow g_2 n_2 g_1 n_1 n_2^{-1} g_2^{-1} = g_2 n_2 n_3 g_1 n_2^{-1} g_2^{-1}$

Genauso $\exists\, n_4 \in N:$

$g_2 (n_2 n_3) g_2^{-1} = n_4 \Rightarrow g_2 n_2 n_3 = n_4 g_2$

$\Rightarrow g_2 n_2 n_3 g_1 n_2^{-1} g_2^{-1} = n_4 g_2 g_1 n_2^{-1} g_2^{-1}$

Da $G_i \subset G_{i-1}$ Normalteiler, $g_1 \in G_i$,

$g_2 \in G_{i-1}$, $\exists\, g_3 \in G_i:$

$g_2 g_1 g_2^{-1} = g_3 \Rightarrow g_2 g_1 = g_3 g_2$

$\Rightarrow n_4 g_2 g_1 n_2^{-1} g_2^{-1} = n_4 g_3 g_2 n_2^{-1} g_2^{-1}$

Weiterhin $\exists\, n_5 \in N: g_3^{-1} n_4 g_3 = n_5$

$\Rightarrow n_4 g_3 = g_3 n_5$

$\Rightarrow n_4 g_3 g_2 n_2^{-1} g_2^{-1} = g_3 n_5 \underbrace{g_2 n_2^{-1} g_2^{-1}}_{\in N, \text{ da } N \text{ Normalteiler}}$

$\in G_i N.$

Mit dem 1. und 2. Isomorphiesatz (1.3.3, 1.3.5) folgt

$$G_{i-1}N / G_i N = G_{i-1} G_i N / G_i N \overset{1.}{\cong} G_{i-1} / G_{i-1} \cap G_i N$$

$$\overset{2.}{\cong} \left(G_{i-1}/G_i \right) \Big/ \left(G_{i-1} \cap G_i N / G_i \right)$$

$\Rightarrow$ $G_{i-1}N / G_i N$ ist isomorph zu einer Faktorgruppe der abelschen Gruppe G_{i-1}/G_i und damit selbst abelsch.

$\Rightarrow$ $N = G_k N \subset G_{k-1} N \subset \dots \subset G_0 N = G$ ist Subnormalteilerreihe

$\Rightarrow$ $\{e_{G/N}\} = N/N = G_k N / N \subset \dots \subset G_0 N / N = G/N$ ist Subnormalteilerreihe mit abelschen Faktoren $\left(G_{i-1} N/N \right) \Big/ \left(G_i N/N \right) \overset{2.}{\cong} G_{i-1} N / G_i N$.

$\Rightarrow$ G/N ist auflösbar.

„$\Leftarrow$" Seien N und G/N auflösbar mit

$\{e\} = N_k \subset N_{k-1} \subset \cdots \subset N_0 = N$ und

$\{e_{G/N}\} = G_l/N \subset G_{l-1}/N \subset \cdots \subset G_0/N = G/N$.

Dann ist

$\{e\} = N_k \subset \cdots \subset N_0 = N = G_l \subset G_{l-1} \subset \cdots \subset G_0 = G$

eine Subnormalteilerkette mit abelschen Faktoren, denn $G_{i-1}/G_i \overset{2.}{\cong} G_{i-1}/N \big/ G_i/N$ $\square$

1.6.6 Korollar

Für $n \geq 5$ sind S_n, A_n nicht auflösbar.

Beweis: Da $A_5 \subset A_n \subset S_n$ Untergruppe ist und A_5 nicht auflösbar ist. $\square$

1.6.7 Korollar

Sei G eine p-Gruppe, dann ist G auflösbar.

Beweis: Sei $|G| = p^n$, p Primzahl.

Induktion nach n.

$n = 0$: nichts zu zeigen.

$n = 1$: G ist zyklisch und auflösbar.

Sei $n > 0$. Nach 1.2.13 gilt $p \mid |Z(G)|$

$\Rightarrow \{e\} \subsetneqq Z(G) \subset G$.

Falls $Z(G) = G \Rightarrow G$ ist abelsch $\Rightarrow G$ auflösbar.

Falls $Z(G) \subsetneqq G$, so sind $Z(G)$ und $G/Z(G)$ selbst p-Gruppen, die nach Induktionsvoraussetzung auflösbar sind $\overset{1.6.5\,2)}{\Longrightarrow}$ G ist auflösbar. $\square$

<u>1.6.8 Def</u>

Sei G eine endliche Gruppe. Eine Kette $\{e\} \subset G_k \subset G_{k-1} \subset \dots \subset G_0 = G$ eine von Untergruppen, so daß $G_i \subset G_{i-1}$ Normalteiler ist und G_{i-1}/G_i zyklisch von Primzahlordnung, heißt <u>Kompositionsreihe</u>.

<u>1.6.9 Satz</u> Sei G endliche Gruppe.

G auflösbar $\Leftrightarrow$ G besitzt eine Kompositionsreihe

<u>Beweis</u>: „$\Leftarrow$“ klar.

„$\Rightarrow$" Wir müssen eine Subnormalteilerkette zu einer Kompositionsreihe verfeinern. Falls G_{i-1}/G_i nicht Primzahlordnung hat, so ist G_{i-1}/G_i nach Lemma 1.6.2 nicht einfach, besitzt also einen echten Normalteiler, mit dem wir verfeinern können. Die Ordnungen der Faktorgruppen werden dabei echt kleiner, nach endlich vielen Schritten erhalten wir also Faktorgruppen von Primzahlordnung. $\square$

<u>Bsp</u> 1) S_4 hat die Kompositionsreihe
$\{id\} \subset \langle (12)(34) \rangle \subset K_4 \subset A_4 \subset S_4$.

2) Gruppen der Ordnung pq mit p, q prim sind auflösbar:
Wie in Satz 1.5.16 folgt für $q < p$, daß es nur eine q-Sylowgruppe gibt, und diese ist somit Normalteiler, und
$\{e\} \subset Q \subset G$ ist Kompositionsreihe,
da $|Q| = q$ und $|G/Q| = \frac{pq}{q} = p$.