1.17 Satz + Def Sei G eine Gruppe. Dann definiert
$G \times G \to G$ $(g,h) \mapsto ghg^{-1}$ eine Operation
von G auf sich selbst, die Operation durch Konjugation, da
$(g_1 g_2, h) \mapsto g_1 g_2 h (g_1 g_2)^{-1} = g_1 (g_2 h g_2^{-1}) g_1^{-1}$ gilt
Die Bahnen von h unter dieser Operation
$C_h = \{ ghg^{-1} \mid g \in G \}$ heißt Konjugationsklasse von G.

Für $g \in G$ heißt $\varphi_g : G \to G$, $h \mapsto ghg^{-1}$ der Automorphismus von G, der durch Konjugation gegeben ist.
Da $\varphi_g(h_1 h_2) = g h_1 h_2 g^{-1} = (g h_1 g^{-1})(g h_2 g^{-1}) = \varphi_g(h_1) \cdot \varphi_g(h_2)$
ist φ_g in der Tat ein Automorphismus
Die Abb $\varphi : G \to \mathrm{Aut}(G)$ $g \mapsto \varphi_g$ ist ein Gruppenhomomorphismus
$\varphi_{g_1 g_2}(h) = g_1 g_2 h (g_1 g_2)^{-1} = \varphi_{g_1}(\varphi_{g_2}(h)) = (\varphi_{g_1} \circ \varphi_{g_2})(h)$
Der Kern $\ker(\varphi) =: Z(G) = \{ g \in G \mid gh = hg \ \forall h \in G \}$
heißt das Zentrum von G.
Das Bild $\mathrm{Im}(\varphi) = \mathrm{Inn}(G) \subset \mathrm{Aut}(G)$ heißt die Gruppe der inneren Automorphismen von G.
Es ist $\mathrm{Inn}(G) \cong G/Z(G)$ (Homom.satz)
$\mathrm{Inn}(G) \subset \mathrm{Aut}(G)$ ist ein Normalteiler, denn sei $\psi \in \mathrm{Aut}(G)$, $\varphi_g \in \mathrm{Inn}(G)$, dann $(\psi \varphi_g \psi)(h) = \psi(g \psi^{-1}(h) g^{-1})$
$= \psi(g)\, h \cdot \underbrace{(\psi(g))^{-1}}_{= \psi(g^{-1})} = \varphi_{\psi(g)}(h) \Rightarrow \psi \varphi_g \psi^{-1} = \varphi_{\psi(g)} \in \mathrm{Inn}(G)$
Die Quotientengruppe $\mathrm{Out}(G) := \frac{\mathrm{Aut}(G)}{\mathrm{Inn}(G)}$ heißt die Gruppe der äußeren Automorphismen.
Bsp $Z_4 = \mathbb{Z}/4\mathbb{Z}$. Z_4 abelsch $\Rightarrow$ jeder innere Autom. $\varphi_g(h) = ghg^{-1} = h$
ist die Identität $\mathrm{Inn}(G) = \{id\}$
$\Rightarrow$ Alle Automorphismen sind äußere Automorphismen
Da G zyklisch ist ein Automorphismus eind. durch das Bild von $\bar{1}$ festgelegt
$\Rightarrow \mathrm{Out}(Z_4) = \{ id, \psi \}$, $\psi : G \to G$, $\bar{1} \to \bar{3}$
einzige nicht triviale Aut wegen $\mathrm{ord}(\bar{1})$

Beispiel (Konjugationsklassen der S_n)

Sei $\tau = (i_1, i_2, \dots)(\dots) \in S_n$ eine Permutation in Zykelschreibweise und $\sigma \in S_n$ eine weitere Permutation. Dann gilt

$$\sigma((i_1, \dots)(\dots))\sigma^{-1} = (\sigma(i_1), \sigma(i_2) \dots)(\dots)$$

σ^{-1} bildet $\sigma(i_1)$ auf i_1 ab $\rightarrow$ τ bildet i_1 auf i_2 ab und σ bildet i_2 auf $\sigma(i_2)$ ab usw

D.h. Konjugation ändert zwar den Zykel aber nicht den Zykeltyp

Zykeltypen stehen in Bijektion zu Partitionen

Def: Eine Partition von $n \in \mathbb{N}$ ist ein Tupel $(n_1, n_2, \dots, n_r)$ mit $n_1 \geq n_2 \geq \dots \geq n_r$ und $n_1 + n_2 + \dots + n_r = n$

Zykel $\underbrace{(\dots)}_{l_1}\underbrace{(\dots)}_{l_2}\underbrace{(\dots)}_{l_3} \dots \underbrace{(\dots)}_{l_r} \Leftrightarrow$ Partition $(l_1, l_2 \dots l_r)$

Bsp. S_4:

$4 = 4$	$C((1234))$
$4 = 3+1$	$C((123)(4)) = C((123))$
$4 = 2+2$	$C((12)(34))$
$4 = 2+1+1$	$C((12)(3)(4)) = C((12))$
$4 = 1+1+1+1$	$C((1)(2)(3)(4)) = C_e$

Folgerung: Die Konjugationsklassen von S_n stehen in Bijektion zu Partitionen von n.

Bew: bleibt z.z. dass τ_1, τ_2 mit gleichem Zykeltyp auch wirklich konjugiert zueinander sind. Schreibe $\tau_1 = (i_1, \dots i_{n_1})(i_2 \dots i_{n_2})(\dots)$

$\tau_2 = (j_1, \dots j_{n_1})(j_2 \dots j_{n_2})(\dots)$

Dann ist $\sigma = \begin{pmatrix} i_1 & i_2 & \dots \\ j_1 & j_2 & \dots \end{pmatrix} \in S_n$

mit $\tau_2 = \sigma \tau_1 \sigma^{-1}$ per Konstr. $\square$

Satz 1.19 Sei G eine Gruppe, $H \subset G$ UG und $N \subset G$ ein Normalteiler (NT). Dann ist $HN \{hn \mid h \in H$ und $n \in N\} \subset G$ eine Untergruppe mit Normalteiler N, $H \cap N$ ist ein Normalteiler in H und die kanonische Abbildung $H/H\cap N \to HN/N$ ist ein Isomorphismus.

<u>Beweis</u>: HN ist UG, da mit $h_1n_1, h_2n_2 \in HN$ wegen $h_2N = Nh_2$ ($N \subset G$ NT) $\overset{ex}{\text{ein}}$ $n' \in N$ mit $n_1h_1 = h_2n'$, also

$$h_1n_1h_2n_2 = \underbrace{h_1h_2}_{\in H} \underbrace{n'n_2}_{\in N} \in HN$$

$N \subset HN$ Normalteiler ist folgt, da $N \subset G$ Normalteiler ist.

Betrachte nun den kanonischen Homomorphismus

$\varphi: H \to HN/N,\ h \mapsto hN$

φ surjektiv mit Kern $\ker(\varphi) = H \cap N \Rightarrow H \cap N \subset H$ Normalteiler

Mit dem Homomorphiesatz folgt nun, dass $H/\ker(\varphi) = H/H\cap N \simeq HN/N$ $\square$

<u>Satz 1.20</u> (2. Isomomorphiesatz)

Sei G eine Gruppe und $H, N \subset G$ Normalteiler mit $N \subset H \subset G$.

- Dann ist N ein Normalteiler in H.
- Der kanonische Gruppenhom. $G/N \to G/H$, $aN \mapsto aH$ ist surjektiv mit Kern H/N und es gilt $(G/N)/(H/N) \simeq G/H$

<u>Beweis</u>: Da N der Kern der Komposition $H \hookrightarrow G \to G/N$ ist, ist $N \subset H$ ein Normalteiler.

$H/N = \{hN \mid h \in H\} \subset \{gN \mid g \in G\} = G/N$ ist auf natürliche Weise eine Untergruppe.

Der kan. Gruppenhomomorphismus $\varphi: G/N \to G/H,\ gN \mapsto gH$ ist wohldefiniert und surjektiv ($N \subset H$)

Der Kern $\ker(\varphi) = \{gN \mid gH = H\} = \{gN \mid g \in H\} = H/N$

Mit dem Homomorphiesatz folgt nun $(G/N)/(H/N) \simeq (G/N)/\ker(\varphi)$

$\simeq \operatorname{Im}\varphi = G/N$ $\square$

§2 Die Sylowsätze

Def 2.1 Sei p eine Primzahl. Eine p-Gruppe G ist eine Gruppe in der jedes Element als Ordnung eine Primzahlpotenz hat, d.h. $\mathrm{Ord}(\underbrace{g}_{\in G}) = p^l$ für ein $l \geq 0$

Beispiel: Eine endl. Gruppe G der Ordnung $|G| = p^k$ ist eine p-Gruppe, da nach dem Satz von Lagrange $\mathrm{ord}(g)$ ein Teiler von $|G| = p^k$ ist. Die Umkehrung für endl. Gruppen ergibt sich aus dem folgenden Satz:

Satz 2.2 (Existenz von p-Untergruppen) Sei G eine endliche Gruppe der Ordnung $|G| = p^k \cdot m$ mit p teilt nicht m ($p \nmid m$). Dann existiert für jedes $0 \leq l \leq k$ eine Untergruppe $H \subset G$ der Ordnung $|H| = p^l$.

Kor 2.3 Sei G eine endliche Gruppe und p eine Primzahl.
(1) (Cauchy) Teilt p die Gruppenordnung $|G|$ ($p \mid |G|$) Dann gibt es ein Element der Ordnung p in G.
(2) G ist eine p-Gruppe genau dann, wenn $|G| = p^l$ mit $l \geq 0$

Beweis von (2.3)
(1) Nach dem Existenzsatz (2.2) existiert eine Untergruppe $H \subset G$ der Ordnung p. Sei $e \neq g \in H$ dann gilt $|\langle g \rangle| = |H|$, da $1, p$ die einzigen Teiler von $|H| = p \Rightarrow \mathrm{ord}(g) = p$.
(2) $|G| = p^l \Rightarrow G$ p-Gruppe (nach Bsp)
Ist umgekehrt $|G|$ keine p-Potenz, dann existiert eine Primzahl $q \neq p$, die $|G|$ teilt. Nach (1) ex. dann ein Element der Ordnung $q \neq p^l \Rightarrow G$ keine p-Gruppe □

Beispiel Wir illustrieren die Beweisidee des Existenzsatzes (2.2) am Beispiel der S_3. Wir werden eine Methode beschreiben, um Untergruppen der Ordnung 3 zu ~~fin~~ finden.

Betr. dazu die Menge X aller 3-elementigen Teilmengen von $G = S_3$ und ein Element $A \in X$, s.d. die Länge der Bahn GA unter der Operation $G \times X \to X \quad (g, A) \mapsto gA = \{ga \mid a \in A\}$ nicht durch 3 teilbar ist.

In diesem Fall gilt dann $2 \overset{(*)}{=} |GA| = [G : Stab(A)] = \frac{|G|}{|Stab(A)|} = \frac{6}{3}$

$\rightsquigarrow$ also $Stab(A)$ ist dann die gesuchte 3-Gruppe

(*): insg. kommt für $|GA| = 1, 2, 3, 6$ in Frage

n.V. $3 \nmid |GA|$ also bleibt nur $|GA| = 1, 2$

$GA = \bigcup_{g \in G} gA = \bigcup_{A' \in GA} A' \not\ni A$ ungültig

$\Rightarrow$ es gibt keine Bahn der Länge 1

Bleibt die Existenz eines solchen $A \in X$ ($|GA| = 2 \Leftrightarrow 3 \nmid |GA|$) zu zeigen.

Es ist $|X| = \binom{6}{3} = 20$ einerseits und andererseits $|X| = \sum_{GA \in G \backslash X} |GA| = \sum_{GA \in G/X} (G : Stab(A))$

Da 3 kein Teiler von $|X| = 20$ ist, können nicht alle Bahnen Länge 3 oder 6 haben.

$\Rightarrow \exists A$ mit $|GA| = 2 \Rightarrow Stab(A)$ def eine 3-Gruppe.

Allgemeiner verwenden wir für die Existenz einer Bahn mit gesuchter Länge das folgende Lemma:

<u>Lemma 2.4</u> Sei p eine Primzahl, $k, m \in \mathbb{Z}_{\geq 1}$ mit $p \nmid m$. Dann sind p^{k-l+1} für $1 \leq l \leq k$ keine Teiler von $\binom{p^k m}{p^l}$

Statt $GA \in G \backslash X$ schreibt man häufig auch einfach $A \in R$ für ein vollst. Repräsentantensystem der Bahnen, d.h. R ist eine Menge s.d. jede Bahn $GA \in G \backslash X$ genau ein Element $A \in R$ enthält d.

$$\sum_{GA \in G\backslash X} |GA| = \sum_{A \in R} |GA|$$

Beweis 2.4

Es gilt $\binom{p^k m}{p^l} = \frac{p^k m}{p^l} \binom{p^k m-1}{p^l-1}$

Wegen $p \nmid m$ bleibt z.Z., dass $p \nmid \binom{p^k m-1}{p^l-1}$

Bemerken, dass der Faktor $i \leq p^l - 1$ der Faktor p höchstens mit Exponent $l \leq k$ vorkommt: (kann als vollst. gekürzt werden)

Schreibe $i \in \{1, \dots, p^l-1\}$ als $i = p^{n_i} \cdot t_i$ mit $p \nmid t_i$

Wegen $i \leq p^l - 1$ gilt $n_i < l \leq k$

Nun ist $\binom{p^k m-1}{p^l-1} = \prod_{i=1}^{p^l-1} \frac{p^k m - i}{p^l - i} \underset{i=p^{k_i}+t_i}{=} \prod \frac{p^{k-n_i} m - t_i}{p^{l-n_i} - t_i}$

Wegen $p \nmid t_i$ ist dieses (gekürzte Prod) ein Produkt von rationalen Zahlen s.d. weder Nenner noch Zähler durch p teilbar sind

$\Rightarrow p \nmid \binom{p^k m-1}{p^l-1}$ $\square$

Beweis des Existenzsatzes (2.2):

Sei $|G| = p^k m$ mit $p \nmid m$ und $1 \leq l \leq k$

$X = \{A \subset G \mid |A| = p^l\}$

G operiert auf X durch $G \times X \to X$ $(g, A) \mapsto gA$

Wegen Lemma 2.4 ist p^{k-l+1} „eins" kein Teiler von $|X| = \binom{p^k m}{p^l}$. Also existiert ein $A \in X$ mit $p^{k-l+1} \nmid |GA|$, da nach der Bahngleichung $|X| = \sum_{A \in R} |GA|$, wobei R ein vollst. Repräsentantensystem der Bahnen ist.

Wenn also alle $|GA|$ von p^{k-l+1} geteilt werden würden, dann auch $|X|$ ↯ wegen Lemma 2.4

Wir halten dieses $A \in X$ mit $p^{k-l+1} \nmid |GA|$ fest. Wir zeigen nun, dass $\mathrm{Stab}(A)$ eine Untergruppe der Ordnung p^l ist.

Schreibe $|\mathrm{Stab}(A)| = p^r v$ & $(G : \mathrm{Stab}(A)) = p^s w$ mit $r, s \in \mathbb{Z}$, $v, w \in \mathbb{Z}_{\geq 1}$ und $p \nmid v$ & $p \nmid w$. Wegen $|GA| = (G : \mathrm{Stab}(A))$ ist $s \leq k - l$

Mit der Indexformel folgt: $p^{r+s} v \cdot w = (G : Stab(A)) \cdot |Stab(A)|$
$= |G| = p^k m$
$\Rightarrow r+s = k$ (wegen d. Eindeutigkeit der Primfaktorzerlegung &
$p \nmid v$, $p \nmid w$
$\Rightarrow r = k - s \overset{\uparrow}{\geq} l$

$p^{k-l+1} \nmid |GA| = p^s w$
$k-l+1 \geq s$

Für $a \in A$ und ein $g \in Stab(A)$ ist $ga \in gA \overset{g \in Stab(A)}{=} A$
Daher ist die Abb (induziert durch die Verknüpfung in G)

$$Stab(A) \to A \;,\; g \mapsto gA$$

wohldefiniert und injektiv.
$\Rightarrow p^l \leq |Stab(A)| \leq |A| = p^l$
$\Rightarrow Stab(A)$ ist eine UG der Ordnung p^l.

Sylowuntergruppen

Def 2.5 Sei p prim und G eine Gruppe mit $|G| = p^k m$ und $p \nmid m$. Eine Untergruppe $H \subset G$ heißt p-Sylowuntergruppe, falls $|H| = p^k$.

Satz 2.6 (Sylowsätze)
1) Jede p-UG $H \subset G$ liegt in einer p-Sylow UG von G.
2) Jede konjugierte p-Sylowuntergruppe ist wieder eine p-SylowUG von G.
Je 2 p-Sylowuntergruppen sind konjugiert zueinander.
D. h. die Menge p-Sylow UG bilden eine Konjugationsklasse
3) Sei $S_p = |\{U \mid U \subset G \text{ ist } p\text{-Sylow UG von } G\}|$
Dann ist a) $S_p \mid |G|$ b) $S_p \equiv 1 \bmod p$ (lässt beim Teilen durch p den Rest 1)

Kor 2.7 Schreibe $|G| = p^k m$ mit $p \nmid m$. Dann gilt $S_p \mid m$.
Beweis: klar, wegen $S_p \mid |G| = p^k m$ & $S_p \equiv 1 \bmod p$ $\square$

Kor 2.8 Sei G eine endl. Gruppe mit $|G| = p^k m$ & $p \nmid m$
H ist p-Sylow UG von G $\Leftrightarrow$ H ist eine maximal große p-Untergruppe $H \subset G$.
Beweis: „$\Leftarrow$" Sei $|G| = p^k m$ mit $p \nmid m$ und sei $H \subset G$ eine Maximalgröße p-UG von G. Nach dem ersten Sylowsatz liegt H in einer p-Sylow UG $H' \subset G$. Falls $H \subsetneq H'$, dann wäre H' eine größere p-UG ↯ zur Maximal.
„$\Rightarrow$" klar, mit Kor 2.3, da jede endl. p-Gruppe von der Ordnung $|U| = p^l$ für ein $l \leq k$ ist □

Lemma 2.9: Sei $H \subset G$ eine p-UG und sei $S \subset G$ eine p-Sylow UG.
Sei $N_G(S) = \{g \in G \mid gSg^{-1} = S\}$ der Normalisator von S
(= gr. Untergruppe $N \subset G$ s.d. S Normalteiler in N ist)
Falls $H \subset N_G(S)$, dann ist schon $H \subset S$.
Beweis: Schreibe $|G| = p^k m$ mit $p \nmid m$
Nach Vor ist $H \subset N_G(S)$ und nach Konstruktion von $N_G(S)$ ist $S \subset N_G(S)$ ein Normalteiler.
Wenden wir den 1. Isomorphiesatz an: $HS/S \simeq H/H \cap S$
$\Rightarrow |HS/S|$ ein Teiler von $|H|$, also eine p-Potenz
$\Rightarrow |HS| = |HS/S| \cdot |S| \geq |S| = p^k$
$\Rightarrow |HS| = p^k$ also folgt $HS = S$, was wiederum $H \subset S$ impliziert. □

Lemma 2.10: Ist $U \subset G$ eine p-Sylow UG und $H \subset G$ eine p-UG, dann gilt:
$\exists b \in G: H \subset bUb^{-1}$ und bUb^{-1} ist wieder eine p-Sylow UG.
Beweis: Sei $U^G = \{gUg^{-1} \mid g \in G\} (= C_G)$
Betr. Konjugationsoperation auf U^G
$$G \times U^G \to U^G,\ (g, S) \mapsto gSg^{-1}$$
Diese Operation ist wegen def von U^G transitiv (d.h. hat nur eine Bahn) $\Rightarrow \mathrm{Stab}(U) = N_G(U) \overset{\text{Bahnformel}}{\Rightarrow} |G| = |U^G| \cdot |N_G(U)|$

Schreibe $|G| = p^k m$ mit $p \nmid m$. Wegen $U \subset N_G(U)$ gilt
$|U| = p^k \mid |N_G(U)|$ und deswegen $p \nmid |U^G|$

Betrachte nun die Operation der UG $H \subset G$ $H \times U^G \to U^G, (a,S) \mapsto (aSa^{-1})$

In diesem Fall zerfällt U^G in die disjunkte Vereinigung der Bahnen.

Sei R ein volst. Repräsentantensystem der Bahnen

Dann gilt $|U^G| = \sum_{S \in R} \frac{|H|}{|Stab_H(S)|} \overset{H\ p\text{-UG}}{=} \sum_{S \in R} p^{j_S}$ $j_S \geq 0$

Wegen $p \nmid |U^G|$ ex. ein $S \in R$ mit $j_S = 0$, also

ex. ein S mit $H = Stab_H(S) = \{a \in H \mid aS = S\} \subset \{g \in G \mid gSg^{-1} = S\}$
$= N_G(S)$

$\Rightarrow H \subset N_G(S) \overset{2.9}{\Longrightarrow} H \subset S \in U^G$

$S \in U^G$ hat eine Darstellung $S = bUb^{-1}$ mit $b \in G$

$\Rightarrow H \subset S = bUb^{-1}$ und $|S| = |U| = p^k$ $\Rightarrow S$ ist p-Sylow UG

Beweis der Sylowsätze

(1) Nach dem Existenzsatz 2.2 ex. eine p-Sylowuntergruppe $U \subset G$.
Nach Lemma 2.10 $\exists\, b \in G$ mit $\underbrace{bUb^{-1}}_{p\text{-Sylow UG}} \supset H$.

(2) Wende den 1. Sylowsatz auf p-Sylowuntergruppe H an
Je zwei Sylow UG haben gleiche Ordnung, also ist $H = bUb^{-1}$
$\Rightarrow$ alle p-Sylow UG liegen in der selben Konjugationsklasse
mit Lemma 2.10 ist die Konjugierte einer p-Sylow UG auch wieder eine p Sylow UG

(3) Sei U eine p-Sylow UG. Nach Teil (2) ist $U^G = \{gUg^{-1} \mid g \in G\}$
die Menge aller p-Sylow UG von G $\Rightarrow s_p = |U^G|$
$\Rightarrow s_p = [G : Stab_G(U)] = \frac{|G|}{|Stab_G(U)|}$ ist also ein Teiler von $|G|$

Dies zeigt (a). Für Teil (b) betr. Operation $U \times U^G \to U^G, (a,S) \mapsto aSa^{-1}$

Sei R ein vollst. Repräsentantensystem der Bahnen.

Die Bahn von $U \in U^G$ enthält offensichtlich U.

Keine andere Bahn enthält nur ein Element: Wäre $S \in R$ mit $aSa^{-1} = S$ $\forall a \in U$, dann wäre $U \subset N_G(S) \overset{2.9}{\Rightarrow} U \subset S \overset{|U|=|S|}{\Rightarrow} U = S$

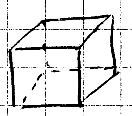
Mit der Bahngleichung bekommen wir $S_p = |U^G| = \sum_{S \in R} \frac{|U|}{|Stab_U(S)|}$

$$= \underbrace{\frac{|U|}{Stab_U(U)}}_{=1} + \sum_{S \in R} \frac{|U|}{|Stab_U(S)|} = 1 + \sum_{S \in R \setminus \{U\}} p^{j_S} \quad \text{mit } j_S \geq 1 \ \forall S \in R \setminus \{U\}$$

$$\Rightarrow S_p \equiv 1 \mod p \qquad \square$$

<u>Bsp:</u> Wir untersuchen die Symmetriegruppe (G) des Würfels

$|G| = 2^4 \cdot 3 = 48$



- Für die Anzahl der 2-Sylow UG gilt

  $S_2 \mid 3$ & $S_2 \equiv 1 \mod 2 \Rightarrow S_2 \in \{1, 3\}$

Es gibt 3 Seitenmittendiagonalen L_i und $|Stab(L_i)| = 16$

$Stab(L_1) = \langle (1234)(5678), (13)(57), (15)(26)(37)(48) \rangle$

Für die 3-Sylow UG gilt $S_3 \mid 16$ & $S_3 \equiv 1 \mod 3$

$\Rightarrow S_3 \in \{1, 4, 16\}$

Wäre $S_3 = 16$, so gäbe es $16 \cdot 2$ Elemente der Ordnung 3, da es 32 El. der Ordnung 2 gibt, kann dies nicht sein.

Die Gruppen der Drehungen um die 4 Eckendiagonalen haben Ordnung 3 z.B. $(\langle (245)(638) \rangle \Rightarrow S_3 = 4$