Satz (8.1)

Sei G eine endliche Gruppe, p eine Primzahl und $k \in \mathbb{N}_0$ derart, dass p^k ein Teiler der Gruppenordnung $|G|$ ist. Dann gibt es in G eine Untergruppe der Ordnung p^k.

(Dieser Satz wird gelegentlich als „Nullter Sylowsatz“ bezeichnet.)

Folgerung (8.2)

Ist G eine endliche Gruppe und p ein Primteiler von $|G|$, dann existiert in G ein Element der Ordnung p.

(Diese Ausage ist bekannt als „Satz (oder Lemma) von Cauchy“.)

Anmerkungen zu Satz 8.1

- Ist G eine endliche abelsche Gruppe, dann gibt es sogar für jeden Teiler d der Gruppenordnung eine Untergruppe der Ordnung d. Die Zahl d braucht also keine Primzahlpotenz zu sein. Dies kann leicht aus dem Hauptsatz über endliche abelschen Gruppe (§ 5) abgeleitet werden.

- Für nicht-abelsche Gruppen ist das im Allgemeinen falsch. Beispielsweise ist 6 ein Teiler der Ordnung $|A_4| = 12$, aber es gibt in A_4 keine Untergruppe der Ordnung 6.

Definition der p-Sylowgruppen

Definition (8.3)

Sei p eine Primzahl und G eine endliche Gruppe der Ordnung $n = p^r m$, wobei m und p teilerfremd sind.

- Eine p-Untergruppe von G ist eine Untergruppe der Ordnung p^s mit $0 \leq s \leq r$.
- Ist $r = s$, dann sprechen wir von einer p-Sylowgruppe.

Die Rolle des Normalisators

Proposition (8.4)

Sei G eine Gruppe und U eine Untergruppe. Dann ist $N_G(U)$ die größte Untergruppe H von G mit der Eigenschaft, dass U Normalteiler von H ist.

Lemma (8.5)

Sei G eine Gruppe mit Untergruppen S, H, und es gelte $hSh^{-1} = S$ für alle $h \in H$. Dann ist das Komplexprodukt HS eine Untergruppe von G, und es gilt $S \trianglelefteq HS$.

Die Sylowsätze *(Peter Sylow, Norwegen, 1832-1918)*

Satz (8.6)

Sei G eine endliche Gruppe und p eine Primzahl.

(i) *Erster Sylowsatz:*
Jede p-Untergruppe von G ist in einer p-Sylowgruppe enthalten.

(ii) *Zweiter Sylowsatz:*
Je zwei p-Sylowgruppen sind zueinander konjugiert.

(iii) *Dritter Sylowsatz:*
Für die Anzahl ν_p der p-Sylowgruppen gilt
$\nu_p \equiv 1 \mod p$ und $\nu_p \mid m$.

Beweis von Satz 8.6:

- geg.: endl. Gruppe G, p Primzahl.
  $m \in \mathbb{N}$, $r \in \mathbb{N}_0$ mit $|G| = p^r m$ und $p \nmid m$.

zzg: (i) Jede p-Untergr. ist enthalten in einer p-Sylowgr. von G.

(ii) Je zwei p-Sylowgr. sind konjugiert

(iii) $\nu_p \equiv 1 \bmod p$, $\nu_p \mid m$ für die Anzahl ν_p der p-Sylowgruppen

Sei $\mathcal{U}$ die Menge der Untergruppen von G.

Nullter Sylowsatz $\Rightarrow \exists$ eine p-Sylowgr. P

Betrachte die Bahn $U = G(P)$ von P unter der Operation von G auf V durch Konjugation.

Beh.: $p \nmid |U|$

Es gilt $|U| = (G : N_G(P))$, weil $|U|$ die Bahnlänge und $N_G(P)$ der Stabilisator von P ist. Es gilt $P \leq N_G(P)$ (gilt für jede Untergr. von G) $\Rightarrow |P|$ teilt $|N_G(P)|$, und $m = \frac{|G|}{p^r} = \frac{|G|}{|P|} = \frac{|G|}{|N_G(P)|} \cdot \frac{|N_G(P)|}{|P|} =$

$(G : N_G(P)) \cdot (N_G(P) : P) = |U| \cdot (N_G(P) : P)$

$\Rightarrow |U|$ teilt m Aus $p \nmid m$ folgt $p \nmid |U|$.

zu (1) Sei H eine p-Untergruppe von G.
Betrachte die Operation von H auf U.

Beh. (1) Die Operation hat einen Fixpunkt.
(2) Ist $S \in U$ ein bel. Fixpunkt der Operation, dann folgt $H \subseteq S$.

(Aus (1) und (2) folgt die Aussage des 1. Sylowsatzes.)

zu (1) Sei $F \subseteq U$ die Fixpunktmenge der Operation und $R \subseteq U$ ein Repr.-system der Bahnen mit mehr als einem Element. Bahngleichung $\Rightarrow$

$$|U| = |F| + \sum_{Q \in R} (H : H_Q)$$

Da $(H : H_Q)$ jeweils > 1 und eine p-Potenz ist, ist

$(H : H_\alpha)$ jeweils durch p teilbar

aber s.o. $\rightarrow p \nmid |\Omega| \Rightarrow |F| \neq 0 \Rightarrow F \neq \emptyset$

zu (2) Sei S ein Fixpunkt der Operation $\circ$.

z.Zg.: $H \subseteq S$

Nach Vor. gilt $h \circ S = S$, also $hSh^{-1} = S$ für alle $h \in H$. Lemma 8.5 $\Rightarrow$ HS ist Untergp. von G. und $S \trianglelefteq HS$ §4 Erster Isomorphiesatz

$\rightarrow H/S \cap H \cong HS/S \rightarrow \frac{|H|}{|S \cap H|} = \frac{|HS|}{|S|} \Rightarrow$

$|HS| = \frac{|S| \cdot |H|}{|S \cap H|} \Rightarrow |HS|$ ist eine p-Potenz

außerdem $S \subseteq HS$ Da S als p-Untergruppe bereits maximale Ordnung hat, folgt $S = HS \Rightarrow H \subseteq S$

zu (ii) Sei Q eine beliebige p-Sylowgruppe. Betrachte die Operation von Q auf $\mathcal{U}$, wende (i) an $\Rightarrow$ Es gibt eine p-Sylowgruppe $P'' \in \mathcal{U}$ mit $Q \subseteq P''$. $\overset{|P''| = p^r = |Q|}{\Longrightarrow} Q = P''$

Da P'' in $\mathcal{U} = G(P)$ liegt, existiert ein $g \in G$ mit

$$Q = P'' = gPg^{-1}$$

zu (iii) zzg: $\nu_p \mid m$ und $\nu_p \equiv 1 \bmod p$

Oben wurde gezeigt, dass $|\mathcal{U}|$ Teiler von m ist

Nach (ii) ist $\mathcal{U}$ die Menge alle p-Sylowgruppen von G.

$\rightarrow \nu_p = |\mathcal{U}| \Rightarrow \nu_p \mid m$

Betrachte nun die Operation von P auf U durch Konjugation.

(ii) $\Rightarrow$ P ist in jedem Fixpunkt der Operation enthalten

also: $Q \in U$ Fixpunkt $\Rightarrow P \subseteq Q \overset{|P|=p^n=|Q|}{\Rightarrow} P = Q$

Daraus folgt, dass die Fixpunktmenge der Operation durch $F = \{P\}$ gegeben ist. Sei $R \subseteq U$ ein Repr.-system der Bahnen mit mehr als einem Element. Bahngleichung $\Rightarrow$

$$|U| = |F| + \sum_{U \in R} (P : P_U) \quad \Rightarrow \quad v_p = 1 + \sum_{U \in R} (P : P_U)$$

Da jeder Summand $(P : P_U)$ durch p teilbar ist (siehe (i)), folgt $v_p \equiv 1 \mod p$. $\square$

Folgerung aus dem Zweiten Sylowsatz

Folgerung (8.7)

Sei G eine Gruppe und p eine Primzahl. Eine p-Sylowgruppe P ist genau dann ein Normalteiler von G, wenn die Anzahl ν_p der p-Sylowgruppen von G gleich 1 ist.

Beweis von Folgerung 8.7

geg. endl. Gruppe G, p Primzahl, P eine p-Sylowgr.

Sei ν_p die Anzahl der p-Sylowgruppen von G

2. Sylowsatz $\Rightarrow$ Ist Q eine beliebige p-Sylowgr. von G, dann gibt es ein $g \in G$ mit $Q = gPg^{-1}$

Beh.: $\nu_p = 1 \iff P \trianglelefteq G$

„$\Rightarrow$" Sei $g \in G$ zzg: $gPg^{-1} = P$

Da $G \to G$, $h \mapsto ghg^{-1}$ ein Automorphismus von G ist, ist auch gPg^{-1} eine p-Sylowgruppe von G

$n_p = 1 \Longrightarrow gPg^{-1} = P$

$\Longleftarrow$ " Sei Q eine bel p-Sylowgp. 2. Sylowsatz $\Rightarrow \exists g \in G$:

$Q = gPg^{-1} = P \Rightarrow n_p = 1$

$\uparrow P \trianglelefteq G$

$\square$

Gruppen der Ordnung ≤ 15 bis auf Isomorphie

n	$r(n)$	Gruppen bis auf Isomorphie
1	1	$\mathbb{Z}/1\mathbb{Z}$
2	1	$\mathbb{Z}/2\mathbb{Z}$
3	1	$\mathbb{Z}/3\mathbb{Z}$
4	2	$\mathbb{Z}/4\mathbb{Z},\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
5	1	$\mathbb{Z}/5\mathbb{Z}$
6	2	$\mathbb{Z}/6\mathbb{Z},\ S_3$
7	1	$\mathbb{Z}/7\mathbb{Z}$
8	5	$\mathbb{Z}/8\mathbb{Z},\ \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z},\ (\mathbb{Z}/2\mathbb{Z})^3,\ D_4,\ Q_8$

Gruppen der Ordnung ≤ 15 bis auf Isomorphie (Forts.)

n	$r(n)$	Gruppen bis auf Isomorphie
9	2	$\mathbb{Z}/9\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$
10	2	$\mathbb{Z}/10\mathbb{Z}$, D_5
11	1	$\mathbb{Z}/11\mathbb{Z}$
12	5	$\mathbb{Z}/12\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$, D_6, A_4, $\mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$
13	1	$\mathbb{Z}/13\mathbb{Z}$
14	2	$\mathbb{Z}/14\mathbb{Z}$, D_7
15	1	$\mathbb{Z}/15\mathbb{Z}$

Anwendung: Gruppen der Ordnung 15

Lemma (8.8)

Jede Gruppe der Ordnung 15 besitzt einen Normalteiler der Ordnung 3 und einen Normalteiler der Ordnung 5.

Folgerung (8.9)

Jede Gruppe der Ordnung 15 ist zyklisch.

Beweis von Lemma 8.8:

Vfg. Gruppe G mit $|G| = 15$

Für $p \in \{3, 5\}$ sei ν_p die Anzahl der p-Sylowgruppen von G.

3. Sylowsatz $\Rightarrow \nu_5 \mid 3 \Rightarrow \nu_5 \in \{1, 3\}$, außerdem $\nu_5 \equiv 1 \bmod 5$

$3 \not\equiv 1 \bmod 5 \Rightarrow \nu_5 = 1$

3. Sylowsatz $\Rightarrow \nu_3 \mid 5 \Rightarrow \nu_3 \in \{1, 5\}$, außerdem $\nu_3 \equiv 1 \bmod 3$

$5 \equiv 2 \not\equiv 1 \bmod 3 \Rightarrow \nu_3 = 1$

Sei P die einzige 3- und Q die einzige 5-Sylowgruppe. Dann gilt $|P| = 3$ und $|Q| = 5$. Aus $\nu_3 = 1$ und $\nu_5 = 1$ folgt $P \trianglelefteq G$ und $Q \trianglelefteq G$, nach Folgerung 8.7. □

Beweis von Satz 8.9.

Sei G eine Gruppe der Ordnung 15. zeige. $G \cong \mathbb{Z}/15\mathbb{Z}$

Lemma 8.8 $\Rightarrow$ 7 Normalteiler $P, Q \trianglelefteq G$ mit $|P| = 3$ und $|Q| = 5$ Beh.: G ist innere direktes Produkt von P und Q

zu überprüfen: (i) $P \cap Q = \{e\}$ (ii) $PQ = G$

zu (i) folgt aus der Teilerfremdheit von $|P| = 3$ und $|Q| = 5$

zu (ii) $P, Q \trianglelefteq G \Rightarrow PQ$ ist Untergr. von G (sogar Normalteiler)

$P \subseteq PQ \Rightarrow |P| = 3$ teilt $|PQ|$
$Q \subseteq PQ \Rightarrow |Q| = 5$ teilt $|PQ|$
$\Rightarrow$ kgV$(3,5) = 15$ teilt $|PQ|$

$\Rightarrow |PQ| \geq 15 = |G| \overset{PQ \subseteq G}{\Rightarrow} PQ = G$ ($\Rightarrow$ Beh.)

Aus der Beh. folgt $G \cong P \times Q$.

$|P| = 3$, $|Q| = 5$ sind Primzahlen $\Rightarrow$ P, Q sind zyklisch $\Rightarrow$ $P \cong \mathbb{Z}/3\mathbb{Z}$, $Q \cong \mathbb{Z}/5\mathbb{Z}$

$\Rightarrow G \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ $\overset{\text{Chin. Restsatz}}{\Longrightarrow}$ $ggT(3,5) = 1$

$\Rightarrow G \cong \mathbb{Z}/15\mathbb{Z}$ □

Anwendung: Gruppen der Ordnung $2p$

Proposition (8.10)

Sei $n \in \mathbb{N}$ mit $n \geq 3$, G eine Gruppe und $\{g, h\}$ ein Erzeugendensystem von G, wobei $\mathrm{ord}(g) = n$, $\mathrm{ord}(h) = 2$ und $ghgh = e_G$ gilt. Dann ist G isomorph zur Diedergruppe D_n.

Satz (8.11)

Sei p eine ungerade Primzahl und G eine nicht-abelsche Gruppe der Ordnung $2p$. Dann ist G isomorph zur Diedergruppe D_p.

Beweis von Proposition 8.10

geg.: $n \in \mathbb{N}$, $n \geq 3$, G Gruppe mit einem zweielementigen Erz.-system $\{g, h\}$, wobei $\operatorname{ord}(g) = n$, $\operatorname{ord}(h) = 2$ und $ghgh = e$.

bereits bekannt: $D_n = \langle \rho, \tau \rangle$ mit $\operatorname{ord}(\rho) = n$, $\operatorname{ord}(\tau) = 2$, $\rho\tau\rho\tau = id$. Daraus hatten wir gefolgert: $D_n = \langle \rho \rangle \langle \tau \rangle = \{\rho^a \tau^b \mid 0 \leq a < n, b \in \{0,1\}\}$ und $|D_n| = 2n$. Ebenso erhalten wir aus den Voraussetzungen von oben: $G = \langle g \rangle \langle h \rangle = \{g^a h^b \mid 0 \leq a < n, b \in \{0,1\}\}$, $|G| = 2n$.

Daraus folgt, dass $\varphi: D_n \to G$ geg. durch

$\rho^a \tau^b \mapsto g^a h^b$ für $0 \leq a < n$, $b \in \{0,1\}$ eine Bijektion. noch z.zg.: Ψ ist ein Homomorphismus

bekannt: Aus $\rho\tau\rho\tau = id$ folgt $\tau\rho = \rho^{-1}\tau$ und $\tau\rho^c = \rho^{-c}\tau$ $\forall c \in \mathbb{N}$. genauso erhalten wir $hg^c = g^{-c}h$ $\forall c \in \mathbb{N}$. Seien nun $a, c \in \{0, \dots, n-1\}$, $b, d \in \{0,1\}$. z.zg: $\Psi((\rho^a\tau^b)\cdot(\rho^c\tau^d)) = \Psi(\rho^a\tau^b)\,\Psi(\rho^c\tau^d)$.

1. Fall: $b = 0$ $\Psi((\rho^a\tau^b)(\rho^c\tau^d)) = \Psi(\rho^{a+c}\cdot\tau^d)$

Aus $\Psi(\rho^a \cdot \tau^d) = g^a h^d$ für $0 \leq a < n$ und $\mathrm{ord}(\rho) = \mathrm{ord}(g) = n$ folgt $\Psi(\rho^a\tau^d) = g^a\tau^d$ für alle $a \in \mathbb{Z}$, wobei $d \in \{0,1\}$.

$\Rightarrow \Psi((\rho^a\tau^b)(\rho^c\tau^d)) = g^{a+c}\cdot h^d = g^a h^b g^c h^d$

$= \varphi(\rho^a \tau^b) \cdot \varphi(\rho^c \tau^d)$

2. Fall: $b = 1$

$\varphi((\rho^a \tau)\cdot(\rho^c \tau^d)) \overset{s.o.}{=} \varphi(\rho^{a-c} \cdot \tau^{1+d}) =$

$g^{a-c} h^{1+d} = g^a g^{-c} h h^d \overset{s.o.}{=} g^a h g^c h^d =$

$\varphi(\rho^a \tau) \cdot \varphi(\rho^c \tau^d)$ □

Beweis von Satz 8.11:

geg: Gruppe G der Ordnung $2p$, p Primzahl ≥ 3
G nicht-abelsch

z.zg: $G \cong D_p$ genügt nach Prop. 8.10:
$\exists\, g, h \in G$ mit $G = \langle g, h \rangle$, $\mathrm{ord}(g) = p$, $\mathrm{ord}(h) = 2$,
und $ghgh = e$

Für die Anzahl ν_p der p-Sylowgr. von G gilt: $\nu_p \mid 2$
$\Rightarrow \nu_p \in \{1, 2\}$, außerdem $\nu_p \equiv 1 \bmod p$, $2 \not\equiv 1 \bmod p \Rightarrow \nu_p = 1$
Sei N die einzige p-Sylowgr. von G. $\nu_p = 1 \overset{\text{Folg. 8.7}}{\Rightarrow} N \trianglelefteq G$
außerdem: $|N| = p$ Primzahl $\Rightarrow N$ ist zyklisch $\rightarrow \exists\, g \in G$
mit $N = \langle g \rangle$, wobei $\mathrm{ord}(g) = |\langle g \rangle| = |N| = p$

$2 \mid |G|$, 2 Primzahl $\xrightarrow[\text{Cauchy}]{\text{Lemma von}}$ $\exists\, h \in G$ mit $\operatorname{ord}(h) = 2$

$\Rightarrow$ gilt $p \mid |\langle g, h\rangle|$ wegen $\operatorname{ord}(g) = p$, $g \in \langle g, h\rangle$. Aus $h \in \langle g, h\rangle$

folgt $2 \mid |\langle g, h\rangle| \Rightarrow 2p$ teilt $|\langle g, h\rangle| \overset{|G|=2p}{\Rightarrow} G = \langle g, h\rangle$

Wegen $N \trianglelefteq G$ gilt $hNh^{-1} = N$. $\Rightarrow hgh = hgh^{-1} \in \langle g\rangle \Rightarrow$

$\exists\, c \in \mathbb{Z}$ mit $hgh = g^c$ $\Rightarrow$ gilt $h^2 g h^2 = h(hgh^{-1})h^{-1} =$

$h g^c h^{-1} = (hgh^{-1})^c = (g^c)^c = g^{c \cdot c} = g^{c^2}$, andererseits

$h^2 g h^2 = g$ wg. $h^2 = e$ $\Rightarrow g^{c^2} = g = g^1 \overset{\operatorname{ord}(g)=p}{\Rightarrow} c^2 \equiv 1 \bmod p$

$\Rightarrow \bar{c}^2 - \bar{1} = \bar{0}$ in $\mathbb{F}_p$ $\Rightarrow (\bar{c} - \bar{1})(\bar{c} + \bar{1}) = c^2 - \bar{1} = \bar{0}$ in $\mathbb{F}_p$

$\Rightarrow \bar{c} \in \{\pm \bar{1}\}$ in $\mathbb{F}_p$ $\Rightarrow c \equiv \pm 1 \bmod p \Rightarrow hgh \in \{g, g^{-1}\}$

Aus $hgh = g$ folgt $hg = gh^{-1} = gh$. In diesem Fall ist G inneres dir.

Produkt von $\langle g\rangle \cong \mathbb{Z}/p\mathbb{Z}$ und $\langle h\rangle \cong \mathbb{Z}/2\mathbb{Z}$ $\overset{\text{Chin. RS}}{\Rightarrow} G \cong \langle g\rangle \times \langle h\rangle \cong \mathbb{Z}/2p\mathbb{Z}$

Nachtrag: Aus der Gleichung $hg = gh \Leftrightarrow ghg^{-1} = h$ folgt, dass g im Normalisator $N_G(\langle h \rangle)$ enthalten ist. Wegen $h \in N_G(\langle h \rangle)$ folgt $\{g, h\} \subseteq N_G(\langle h \rangle)$, $\langle g, h \rangle \subseteq N_G(\langle h \rangle)$ und somit $N_G(\langle h \rangle) = G$. Die Untergruppe $\langle h \rangle$ ist somit ein Normalteiler von G, und wegen $(G : \langle g \rangle) = \frac{2p}{p} = 2$ gilt dasselbe für $\langle g \rangle$. Wie im Beweis von Satz 8.9 überprüft man die übrigen Eigenschaften eines inneren direkten Produkts.

Als einzige Möglichkeit bleibt somit $hgh = g^{-1}$, was zu was zu $ghgh = e$ umgeformt werden kann.