Merkmale der Operation durch Konjugation

Proposition (7.13)

Der Stabilisator eines Elements $h \in G$ unter der Operation durch Konjugation ist gegeben durch $C_G(h) = \{g \in G \mid gh = hg\}$. Die Fixpunkte der Operation sind die Elemente der Menge

$$Z(G) \quad = \quad \{g \in G \mid gh = hg \ \forall \ h \in G\} \quad ,$$

dem sogenannten Zentrum. Auch $Z(G)$ ist eine Untergruppe, darüber hinaus sogar ein Normalteiler von G.

Die Klassengleichung

Satz (7.14)

Sei G eine endliche Gruppe, die durch Konjugation auf sich selbst operiert. Sei R ein Repräsentantensystem der Konjugationsklassen mit mehr als einem Element. Dann gilt

$$|G| \quad = \quad |Z(G)| + \sum_{g \in R} (G : C_G(g)).$$

Diese Gleichung erhält man durch Anwendung der Bahngleichung auf die Operation durch Konjugation der Gruppe G auf der Menge ihrer Elemente.

Das nichttriviale Zentrum der p-Gruppen

Definition (7.20)

Sei p eine Primzahl. Eine endliche Gruppe G wird als p-Gruppe bezeichnet, wenn sie von p-Potenzordnung ist, also $|G| = p^e$ für ein $e \in \mathbb{N}_0$ erfüllt ist.

Satz (7.21)

Sei G eine nichttriviale p-Gruppe. Dann ist das Zentrum $Z(G)$ von G ebenfalls nichttrivial, besteht also aus mindestens p Elementen.

Gruppen von Primzahlquadratordnung

Lemma (7.22)

Ist G eine Gruppe mit der Eigenschaft, dass die Faktorgruppe $G/Z(G)$ zyklisch ist, dann ist G selbst abelsch.

Satz (7.23)

Sei p eine Primzahl. Dann ist jede Gruppe der Ordnung p^2 abelsch. Bis auf Isomorphie sind also $\mathbb{Z}/p^2\mathbb{Z}$ und $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ die einzigen Gruppen der Ordnung p^2.

Die Auflösbarkeit der p-Gruppen

Satz (7.24)

Jede p-Gruppe ist auflösbar.

Beweis von Satz 7.24:

Sei p eine Primzahl, $e \in \mathbb{N}_0$ und G eine Gruppe der Ordnung p^e. Dann ist G auflösbar.

Beweis durch vollständige Induktion über e

Ind.-Anf.: $e = 0$ Dann ist $G = \{e\} \Rightarrow G$ abelsch
$\rightarrow G$ ist auflösbar

Ind.-Schritt: Sei $e \in \mathbb{N}$, setze die Aussage für Werte $< e$ voraus. Sei G eine Gruppe der Ordnung p^e.
Satz 7.21 $\Rightarrow Z(G) \neq \{e\} \Rightarrow |G/Z(G)| \leq p^{e-1}$
$\overset{\text{Ind.V.}}{\Rightarrow} G/Z(G)$ ist auflösbar

bekannt: $Z(G)$ ist abelsch, somit ebenfalls auflösbar

Aus der Auflösbarkeit von $Z(G)$ und $G/Z(G)$ folgt die Auflösbarkeit von G. $\square$

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“.)

Beweis von Satz 8.1:

z.zg.: Jede endliche Gruppe G besitzt für jede Primzahlpotenz, die |G| teilt, zumindest eine Untergruppe dieser Primzahlpotenzordnung

Beweis durch vollständige Induktion über die Ordnung n der Gruppe

Ind.-Anf.: $n=1$ Sei G eine Gruppe der Ordnung 1 $\Rightarrow G=\{e\}$ Die einzige Primzahlpotenz, die |G| teilt ist 1, und $\{e\}$ ist eine Untergruppe dieser Ordnung

Sei nun $n > 1$. G eine Gruppe der Ordnung n.
Setze die Aussage für Gruppen der Ordnung $< n$
voraus. Sei p eine Primzahl und $k \in \mathbb{N}_0$ mit
$p^k \mid n$. z.zg: G hat eine Untergruppe U mit
$|U| = p^k$ O.B.d.A. sei $k \geq 1$.

1. Fall: Es gibt eine (echte) Untergr. $H \leq G$ mit $p \nmid (G:H)$.
(d.h. $H \subsetneq G$)

Dann ist $|H| < |G|$, und wegen $|G| = (G:H) \cdot |H|$
und $p \nmid (G:H)$, $p^k \mid |G|$ folgt $p^k \mid |H|$.
Ind.-V. $\Rightarrow$ Es gibt eine Untergr. U von H mit
$|U| = p^k$. Dies ist auch eine Untergr. von G.

2. Fall: Für jede echte Untergruppe H von G gilt $p \mid (G:H)$.

Sei R ein Repräsentantensystem der Konjugationsklassen von G mit mehr als einem Element. Klassengleichung $\Rightarrow$

$$|G| = |Z(G)| + \sum_{h \in R} (G : C_G(h))$$

Wegen $(G : C_G(h)) = |G(h)| > 1$ ist $C_G(h)$ jeweils eine echte Untergr. von G, und p somit ein Teiler von $(G : C_G(h))$, für jedes $h \in R$.

$\Rightarrow p \mid \left(\sum_{h \in R} (G : C_G(h)) \right)$

$p^k \mid |G|, \; k \geq 1 \Rightarrow p \mid |G| \overset{\text{klassengl.}}{\Rightarrow} p \mid |Z(G)|$

$Z(G)$ ist eine endl. abelsche Gruppe $\overset{\S 5}{\Rightarrow}$ $Z(G)$ ist isomorph zu einem Prod. $C_1 \times \dots \times C_r$ zyklischer Gruppen $C_1 \times \dots \times C_r$ $p \mid |Z(G)| \Rightarrow$ $p \mid |C_i|$ für mind. ein i. Dieses C_i enthält ein Element der Ordnung p. $\Rightarrow \exists\, g \in Z(G)$ mit $p = \operatorname{ord}(g)$.

Sei $N = \langle g \rangle$. Aus $N \subseteq Z(G)$ folgt $N \trianglelefteq G$.

(denn: Sei $h \in G$ und $n \in N$. $\Rightarrow hnh^{-1} = hh^{-1}n = en = n$, $\uparrow n \in Z(G)$

$\Rightarrow hnh^{-1} \in N$) Sei $\bar{G} = G/N$. Es gilt

$$|\bar{G}| = (G:N) = \frac{|G|}{|N|} = \frac{|G|}{\operatorname{ord}(g)} = \frac{|G|}{p} < |G|$$

$p^k \mid |G| \Rightarrow p^{k-1} \mid |\bar{G}|$ Ind. Voraussetzung, angewendet auf $\bar{G}$ $\Rightarrow \exists$ Untergp. $\bar{U}$ von $\bar{G}$ mit

$|\bar{U}| = p^{k-1}$. Sei $\pi: G \to \bar{G}$ der kan. Epimorphismus $(h \mapsto hN)$ und $U = \pi^{-1}(\bar{U})$. Nach dem Korrespondenzsatz (§4) gilt $(G:U) = (\bar{G}:\bar{U}) \Rightarrow$

$$|U| = \underset{\text{Lagrange}}{\frac{|G|}{(G:U)}} = \frac{|G|}{(\bar{G}:\bar{U})} = \frac{p|\bar{G}|}{(\bar{G}:\bar{U})} \underset{\text{Lagrange}}{=} p|\bar{U}| = p\,p^{k-1} = p^k$$

Also besitzt G eine Untergr. der Ordnung p^k. $\square$

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 $S \trianglelefteq HS$.

Beweis von Prop. 8.4:

geg: Gruppe G, $U \leq G$, zzg:

(1) Der Normalisator $N_G(U) = \{g \in G \mid gUg^{-1} = U\}$ ist eine Untergruppe von G.

(2) $U \trianglelefteq N_G(U)$ (3) $H \leq G$ mit $U \trianglelefteq H \Rightarrow H \subseteq N_G(U)$

zu (1) Nach Def ist $N_G(U)$ der Stabilisator von U bzgl. der Operation von G auf der Menge $\mathcal{U}$ der Untergr. von G gegeben durch $g \circ U = gUg^{-1}$. bekannt: Jeder Stabilisator einer Gruppenop. ist eine Untergruppe der operierenden Gruppe (hier G)

zu (2) bekannt: Ist $u \in U$, dann ist $\tau_u : U \to U$, $v \mapsto uvu^{-1}$ ein Automorphismus von U, insb. gilt $uUu^{-1} = \tau_u(U) = U$. Daraus folgt $U \subseteq N_G(U)$

zu (3) Sei H wie angeg. Wegen $U \trianglelefteq H$ gilt $hUh^{-1} = U \; \forall h \in H$.
$\Rightarrow h \in N_G(U) \; \forall h \in H \Rightarrow H \subseteq N_G(U)$. □

Beweis von Lemma 8.5:

geg: Gruppe G, $H, S \leq G$, $hSh^{-1} = S \quad \forall h \in H$

z.zg. (1) $HS \leq G$ (2) $S \trianglelefteq HS$

zu (1) Nach § 4 reicht es z.zg: $HS = SH$

„$\subseteq$" Sei $g \in HS \Rightarrow \exists h \in H, s \in S$ mit $g = hs \Rightarrow$

$g = hsh^{-1}h$ Vor. $\Rightarrow hsh^{-1} \in S$, $h \in H \Rightarrow g \in SH$

„$\supseteq$" Sei $g \in SH \Rightarrow \exists s \in S, h \in H$ mit $g = sh$

$\Rightarrow g = hh^{-1}s(h^{-1})^{-1}$ Vor. $\Rightarrow h^{-1}s(h^{-1})^{-1} \in S$

und $h \in H \Rightarrow g \in HS$

zu (2) Zeige: H und S sind im ~~Normalisator~~ $N_{HS}(S)$ enthalten. (Dann ist $HS \leq N_{HS}(S)$, und nach Proposition 8.4 folgt aus $HS = N_{HS}(S)$ die Aussage $S \trianglelefteq HS$.)
Für jedes $h \in H$ gilt nach Vor. $hSh^{-1} = S$, also $h \in N_{HS}(S)$ und somit $H \leq N_{HS}(S)$. Außerdem folgt $S \leq N_{HS}(S)$ direkt aus Prop 8.4. □

Die Sylowsätze

Satz (8.6)

Sei G eine Gruppe der Ordnung n, p eine Primzahl und $n = mp^r$ mit $p \nmid m$.

(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 der Sylowsätze

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

(i) Jede p-Untergr. liegt in einer p-Sylowgruppe

(ii) $P, P' \leq G$ p-Sylowgruppen $\Rightarrow$ $\exists g \in G$ mit $gPg^{-1} = P'$

(iii) Es gelt $n_p \mid m$ und $n_p \equiv 1 \bmod p$ für die Anzahl n_p der p-Sylowgruppen.

Betrachte die Operation $\bullet$ von G auf der

mit $p \in \mathbb{N}_0$, $m \in \mathbb{N}$, $p \nmid m$ z.Zg.:

(i) Jede p-Untergr. liegt in einer p-

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

Satz 8.1 $\Rightarrow$ Es gibt eine p-Sylowgruppe P.

Sei $\boxed{\mathcal{U} = G(P)} = \{gPg^{-1} \mid g \in G\}$

Für jedes $g \in G$ gilt $gPg^{-1} = \tau_g(P)$ mit dem Automorphismus $\tau_g : G \to G,\ h \mapsto ghg^{-1}$.

$\Rightarrow$ Alle Elemente von $\mathcal{U}$ sind isomorph zu P, d.h. $\mathcal{U}$ besteht nur aus p-Sylowgruppen

Auf Grund des Zusammenhangs zwischen Bahnlänge und Stabilisator gilt $|\mathcal{U}| = |G(P)|$

$= (G : N_G(P))$. Daraus folgt $\boxed{p \nmid |\mathcal{U}|}$ denn:

Es gilt $P \subseteq N_G(P)$ und $|P| = p^r$

$$\Rightarrow (G:P) = \frac{|G|}{|P|} = \frac{p^r m}{p^r} = m$$

außerdem: $|G| = (G:N_G(P))\,|N_G(P)| =$

$(G:N_G(P))\,(N_G(P):P)\,|P| \Rightarrow$

$m = \frac{|G|}{|P|} = (G:N_G(P))\,(N_G(P):P)$

$\Rightarrow |\mathcal{U}| = (G:N_G(P))$ ist Teiler von m

$\overset{p \nmid m}{\Rightarrow} p \nmid |\mathcal{U}|$.

zu (i) Sei H eine p-Untergruppe von G, $\{e\} \neq H$.
Betrachte die Operation von H auf $\mathcal{U}$.
Sei $R \subseteq \mathcal{U}$ ein Repräsentantensystem der Bahnen mit mehr als einem Element.

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

Wobei $F \subseteq U$ die Fixpunktmenge der Operation bezeichnet. Beh.:

(1) $F \neq \emptyset$ (2) $\forall S \in F : H \subseteq S$

Da F aus p-Sylowgruppen besteht, ist damit (i) bewiesen

zu (1) H ist p-Gruppe. $|H| > 1 \Rightarrow |H|$ ist p-Potenz größer als 1. Da für jedes $Q \in R$ $(H : H_Q) = |H(Q)| > 1$ gilt, ist auch $(H : H_Q)$ p-Potenz > 1 und somit durch p teilbar. andererseits: $p \nmid |U|$

Aus der Bahngl. und $p \mid \left(\sum_{Q \in R} (H : H_Q)\right)$ folgt somit $p \nmid |F| = |F| + 0 \Rightarrow F \neq \emptyset$

zu (2) Sei $S \in F$, z.zg: $H \leq S$ S Fixpunktl der Operation $\Rightarrow h \cdot S = S \ \forall h \in H \Rightarrow hSh^{-1} = S \ \forall h \in H$

Lemma 8.5 $\Rightarrow HS \leq G$ und $S \trianglelefteq HS$

Isomorphiesätze (§4) $\Rightarrow HS/S \cong H/S \cap H$

$|H|$ ist p-Potenz $\Rightarrow |H/S \cap H| = \frac{|H|}{|S \cap H|}$ ist p-Potenz

$\Rightarrow \frac{|HS|}{|S|} = |HS/S|$ ist p-Potenz $\Rightarrow$ $|HS|$ ist p-Potenz insgesamt: HS ist p-Untergr., $HS \geq S$.

S ist p-Sylowgruppe $\Rightarrow HS = S$ (da die p-Sylowgr. die maximalen p-Untergr. sind) $\Rightarrow H \leq S$

zu (ii) Sei P' eine beliebige p-Sylowgruppe. Betrachte die Operation von P' auf $\mathcal{U}$. Siehe (i) $\Rightarrow \exists$ Fixpunkt $P'' \in \mathcal{U}$ der Operation, und $P' \subseteq P''$ $\xrightarrow[\text{beides } p\text{-Sylowgr.}]{P', P''}$ $P' = P''$

$P'' \in \mathcal{U}$, $\mathcal{U} = G(P) \Rightarrow P' = P'' = gPg^{-1}$ für ein $g \in G$.

zu (iii) z.zg: $\nu_p \mid m$ und $\nu_p \equiv 1 \bmod p$

Teil (ii) $\Rightarrow \mathcal{U} = G(P)$ ist die Menge aller p-Sylowgruppen

$\Rightarrow \nu_p = |\mathcal{U}| = (G : N_G(P))$ so $\Rightarrow$ Dies ist ein Teiler von $(G:P) = m$

Betrachte die Operation von P auf $\mathcal{U}$. Sei $F \subseteq \mathcal{U}$ die Fixpunktmenge und $R \subseteq \mathcal{U}$ ein Repr. der Bahnen mit mehr als einem Elt.

BahnGl. $\Rightarrow \nu_p = |\mathcal{U}| = |F| + \sum_{Q \in R} (P : P_Q)$ Wie oben sieht man, dass p Teiler von $\sum_{Q \in R} (P : P_Q)$ ist. Für jedes $S \in F$ gilt $P \subseteq S$, nach (i) Da P und S beides p-Sylowgruppen sind, gilt $P = S$

Beweis der Sylowsätze (Abschluss)

Daraus folgt, dass P das einzige Element der Fixpunktmenge F ist. Es gilt also $F = \{P\}$ und $|F| = 1$. Da für die Summe in der Bahngleichung $\sum_{Q \in R}(P : P_Q) \equiv 0 \mod p$ gilt, erhalten wir insgesamt $\nu_p \equiv 1 + 0 \equiv 1 \mod p$.