Die Bahngleichung

Satz (7.11)

Sei G eine Gruppe, die auf einer endlichen Menge X operiert. Sei $F \subseteq X$ die Fixmpunktmenge der Operation und $R \subseteq X$ ein Repräsentantensystem der Menge aller Bahnen $G(x)$ mit mindestens zwei Elementen. Dann gilt

$$|X| \quad = \quad |F| + \sum_{x \in R} (G : G_x)$$

und $(G : G_x) > 1$ für alle $x \in R$.

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.

Beweis von Satz 7.21

geg: Primzahl p, $e \in \mathbb{N}$, G Gruppe der Ordnung p^e

Beh: $|Z(G)| > 1$

Sei $R \subseteq G$ ein Repr.-system der Konjugationsklassen mit mehr als einem Element. Klassengleichung $\Rightarrow$

$$p^e = |G| = |Z(G)| + \sum_{g \in R} (G : C_G(g))$$

Es gilt $p^e \equiv 0 \bmod p$, ebenso $(G : C_G(g)) \equiv 0 \bmod p$ für alle $g \in R$, denn: $(G : C_G(g)) = |[g]| > 1$, und $(G : C_G(g))$ ist Teiler von $|G| = p^e$ [Konjugationsklasse

Aus der Gleichung folgt also $|Z(G)| \equiv 0 \bmod p$.

Wegen $|Z(G)| \geq |\{e\}| = 1$ folgt $|Z(G)| \geq p > 1$. $\square$

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.

Beweis von Lemma 7.22:

geg.: Gruppe G mit der Eigenschaft, dass $G/Z(G)$ zyklisch ist

z.zg.: G ist abelsch

Weil $G/Z(G)$ zyklisch ist, existiert ein $g \in G$ mit $G/Z(G) = \langle gZ(G) \rangle$.

Seien $a, b \in G$. z.zg.: $ab = ba$

$aZ(G)$ liegt in $G/Z(G) = \langle gZ(G) \rangle$

$\Rightarrow \exists\, m \in \mathbb{Z}$ mit $aZ(G) = (gZ(G))^m$

ebenso: $bZ(G) = (gZ(G))^n$ für ein $n \in \mathbb{Z}$

$aZ(G) = (gZ(G))^{\text{Kg}} = g^m Z(G) \Rightarrow a \in g^m Z(G)$

$\Rightarrow \exists h \in Z(G)$ mit $a = g^m h$ ebenso:

$\exists k \in Z(G)$ mit $b = g^n k$ Damit erhalten

wir insgesamt $ab = g^m h g^n k =$

$g^m g^n hk = g^{m+n} hk = g^{n+m} hk =$

$g^n g^m hk = g^n k g^m h = ba$ $\square$

$\uparrow k \in Z(G)$

$\uparrow h \in Z(G)$

Beweis von Satz 7.23:

Sei p eine Primzahl und G eine Gruppe der Ordnung p^2. z.zg.: G ist abelsch

$Z(G) \leq G \overset{\text{Lagrange}}{\Rightarrow} |Z(G)| \in \{1, p, p^2\} \overset{\text{Satz 7.21}}{\Rightarrow}$

$|Z(G)| \in \{p, p^2\}$

1. Fall: $|Z(G)| = p^2 \Rightarrow |Z(G)| = |G| \overset{Z(G) \leq G}{\Rightarrow} G = Z(G)$

Daraus folgt, dass G abelsch ist.

2. Fall: $|Z(G)| = p$

$|G/Z(G)| = \frac{|G|}{|Z(G)|} = \frac{p^2}{p} = p$ p ist Primzahl $\Rightarrow$

$G/Z(G)$ ist zyklisch $\overset{\text{Lemma 7.22}}{\Rightarrow}$ G ist abelsch $\square$

$n \in \mathbb{Z}$

Die Auflösbarkeit der p-Gruppen

Satz (7.24)

Jede p-Gruppe ist auflösbar.

Beweis von Satz 7.24

geg: G Gruppe, p Primzahl, $e \in \mathbb{N}_0$ mit $|G| = p^e$

z.zg.: G ist auflösbar

Ind.-anfang: $e \leq 2$ Dann ist G abelsch, und somit insbesondere auflösbar (Satz 7.23).

Ind.-schritt: Sei $e \geq 3$, setze die Aussage für kleinere Werte als e voraus. Satz 7.21 $\Rightarrow |Z(G)| > 1$

$\Rightarrow |G/Z(G)| = \frac{|G|}{|Z(G)|} = \frac{p^e}{|Z(G)|} < p^e \Rightarrow |G/Z(G)| = p^{e'}$

für ein $e' \in \mathbb{N}_0$ mit $e' < e$. Ind.-V. $\Rightarrow G/Z(G)$ ist auflösbar, außerdem: $Z(G)$ abelsch $\Rightarrow Z(G)$ auflösbar

$Z(G) \trianglelefteq G$, $Z(G)$ und $G/Z(G)$ auflösbar $\overset{\S 6}{\Longrightarrow} G$ ist auflösbar. $\square$

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

geg. endl. Gruppe G, p Primzahl, $k \in \mathbb{N}_0$ mit $p^k \mid |G|$

z.zg.: Es gibt eine Untergr. $U \leq G$ mit $|U| = p^k$

O.B.d.A. sei $k \geq 1$. Der Beweis läuft durch vollst. Ind. über $n = |G|$. Im Ind.-Anf. ($n = 1$) ist nichts zu zeigen.

Ind.-schritt: Sei $n = |G| > 1$, setze die Aussage für Gruppen kleinerer Ordnung voraus.

1. Fall: Es gibt eine Untergr. V von G mit $p \nmid (G:V)$ und $(G:V) > 1$ (also $V \subsetneq G$)

Aus $p^k \mid |G|$, also $p^k \mid (G:V)|V|$, und $p \nmid (G:V)$ folgt $p^k \mid |V|$. Wegen $|V| < |G|$ kann somit die Ind.-V.

auf V angewendet werden $\Rightarrow$ erhalte eine Untergr. $U \leq V$ mit $|U| = p^k$. Dies ist auch eine Untergr. von G

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

Sei $R \subseteq G$ ein Repr.-system der Konjugatenklassen mit mehr als einem Element. Klassengleichung $\Rightarrow |G| = |Z(G)| + \sum_{g \in R} (G : C_G(g))$

Wegen $(G:C_G(g)) = |[g]| > 1$ ist $C_G(g)$ jeweils eine echte Untergr. von G. Nach Vor. des 2. Falls gilt also $(G:C_G(g)) \equiv 0 \bmod p$

$p^k \mid |G|$, $k \geq 1$ $\Rightarrow |G| \equiv 0 \bmod p \overset{\text{Klassengl.}}{\Rightarrow} |Z(G)|$ ist durch p teilbar

Hauptsatz über abelsche Gruppen $\Rightarrow$ $\exists$ zyklische Gruppen $C_1, \dots, C_t$ ($t \in \mathbb{N}$) mit $Z(G) \cong C_1 \times \dots \times C_t$. $p \mid |Z(G)| \Rightarrow p \mid |C_j|$ für ein $j \in \{1, \dots, t\}$ $\Rightarrow$ C_j enthält ein Element der Ordnung p

$\Rightarrow$ Es gibt ein Element g der Ordnung p in $Z(G)$

Sei $N = \langle g \rangle$. Wegen $N \leq Z(G)$ gilt $N \trianglelefteq G$.
Sei $\bar{G} = G/N$ und $\pi : G \to \bar{G}$ der kanonische Epimorphismus. Dann gilt $|\bar{G}| = \frac{|G|}{|N|} = \frac{|G|}{p} < |G|$.
Wende die Ind.-vor. auf $\bar{G}$ und den Teiler p^{k-1} von $|\bar{G}|$ an (Aus $p^k \mid |G|$ und $|\bar{G}| = \frac{|G|}{p}$ folgt $p^{k-1} \mid |\bar{G}|$.) $\Rightarrow$ erhalte eine Untergr. $\bar{U} \leq \bar{G}$ mit $|\bar{U}| = p^{k-1}$. Sei $U = \pi^{-1}(\bar{U})$.
Korrespondenzsatz $\Rightarrow (G : U) = (\bar{G} : \bar{U}) \Rightarrow$

$$|U| = \frac{|G|}{(G:U)} = \frac{p \cdot |\bar{G}|}{(\bar{G} : \bar{U})} = p|\bar{U}| = p \cdot p^{k-1} = p^k$$

□

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 $S \trianglelefteq HS$.

Beweis von Lemma 8.5:

geg: Gruppe G, Untergruppen $S, H \leq G$

Vor: $hSh^{-1} = S \quad \forall h \in H$

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

zu (1) Es ist $HS = SH$, denn

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

s.o. $\Rightarrow hsh^{-1} \in S \Rightarrow \Rightarrow hs = \underbrace{(hsh^{-1})}_{\in S} h \in SH$

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

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

$\Rightarrow sh = h(h^{-1}sh) \in HS$

Laut §5 folgt aus $SH = HS$, dass HS eine Untergruppe von G ist.

zu (2) Auf Grund der Voraussetzung $\forall h \in H: hSh^{-1} = S$ gilt $H \subseteq N_{HS}(S)$.

Außerdem gilt $U \subseteq N_G(U)$ für jede Gruppe G und jede Untergr. $U \subseteq G$. Anwendung hier auf $U = S \Rightarrow S \subseteq N_{HS}(S)$

Weil HS eine Untergr. von G ist, gilt $HS = \langle H \cup S \rangle$. $S \cup H \subseteq N_{HS}(S)$

$\Rightarrow HS = \langle S \cup H \rangle \subseteq N_{HS}(S)$

$\Rightarrow S \trianglelefteq HS$ □

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

Satz (8.6)

Sei G eine endliche Gruppe, und seien p, m wie in Definition 8.3.

(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 $\nu_p \mid m$.