Die Klassengleichung

Satz (10.14)

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

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

Das Zentrum der p-Gruppen

Definition (10.15)

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 (10.16)

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 sind abelsch

Lemma (10.17)

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

Satz (10.18)

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 10.17

geg.: Gruppe G, so dass $G/Z(G)$ zyklisch

Beh.: G ist abelsch

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

$G/Z(G)$ zyklisch $\Rightarrow \exists\, \bar{g} \in G/Z(G) : G/Z(G) = \langle \bar{g} \rangle$

Sei $g \in G$ mit $\bar{g} = gZ(G)$

$aZ(G) \in \langle \bar{g} \rangle \Rightarrow \exists\, m \in \mathbb{Z} : aZ(G) = \bar{g}^m =$

$g^m Z(G) \Rightarrow a \in g^m Z(G) \Rightarrow \exists\, c \in Z(G) : a = g^m c$

genamos. $bZ(G) \in \langle \bar{g} \rangle \Rightarrow \exists n \in \mathbb{Z}, d \in Z(G) : b = g^n d$

$\Rightarrow ab = g^m c g^n d = g^m g^n cd = g^{m+n} cd$

$\uparrow c \in Z(G)$

$= g^n g^m cd = g^n g^m dc = g^n d g^m c = ba$

$\uparrow d \in Z(G)$ $\uparrow d \in Z(G)$ $\square$

Beweis von Satz 10.18

geg.: Gruppe G der Ordnung p^2, wobei p Primzahl ist

G ist p-Gruppe, somit bekannt: $Z(G) \geq p$, außerdem (vg. Satz von Lagrange) $|Z(G)| \mid p^2$

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

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

$\underset{\Rightarrow}{Z(G) \leq G}$ $Z(G) = G \Rightarrow G$ ist abelsch

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

$|G/Z(G)| = (G : Z(G)) = \frac{|G|}{|Z(G)|} = \frac{p^2}{p}$

$= p$ (Primzahl) $\Rightarrow$ $G/Z(G)$ zyklisch

$\xrightarrow{\text{Lemma 10.17}}$ G abelsch $\Rightarrow G = Z(G)$

$\Rightarrow |Z(G)| = |G| = p^2$ ↯ (Der 2. Fall kann nicht eintreten.) □

Die Auflösbarkeit der p-Gruppen

Satz (10.19)

Jede p-Gruppe ist auflösbar.

Beweis von Satz 10.19.

Erinnerung: Ist G eine Gruppe und $N \trianglelefteq G$, dann gilt die Äquivalenz

G ist auflösbar $\iff$ N, G/N beide auflösbar

Sei nun G eine p-Gruppe, $G = p^n$ für ein $n \in \mathbb{N}_0$. Wir zeigen die Auflösbarkeit durch vollständige Induktion über n.

bereits bekannt: Für $n \leq 2$ ist G abelsch, somit insbesondere auflösbar.

Sei nun $n \geq 3$, $|G| = p^n$, setze die Aussage für p^m mit $m < n$ voraus. Satz 10.16 $\Rightarrow$ $|Z(G)| \geq p$, außerdem bekannt: $Z(G) \trianglelefteq G$

$|G/Z(G)| = \frac{|G|}{|Z(G)|} < |G| \overset{\text{Ind-V.}}{\Rightarrow} G/Z(G)$ ist auflösbar. Als abelsche Gruppe ist auch $Z(G)$ auflösbar. also:

$Z(G)$, $G/Z(G)$ beide auflösbar $\overset{\text{s.o.}}{\Rightarrow}$ G auflösbar

□

□

„Nullter“ Sylowsatz und Satz von Cauchy

Satz (10.20)

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.

Folgerung (10.21)

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

Beweis von Satz 10.20:

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

zzg: $\exists$ Untergr. U von G mit $|U| = p^k$

OBdA sei $k \geq 1$, beweise die Aussage durch vollst. Ind. über $|G|$

Ind.-Anf. $|G| = 1$ nichts zu zeigen

Ind.-Schritt: Sei $|G| > 1$, setze die Aussage für Gruppen der Ordnung $< |G|$ voraus.

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

Wegen $H \subsetneq G$ gilt $|H| < |G| \Rightarrow$ Ind.-V. auf H anwendbar. Lagrange $\Rightarrow |G| = (G:H)|H|$

$p^k \mid |G|$, p^k teilerfremd zu $(G:H) \Rightarrow p^k \mid |H|$

Ind.-V. $\Rightarrow \exists$ Untergr. U von H mit $|U| = p^k$

Dieses U ist dann auch eine Untergruppe von G.

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

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

$$|G| = |Z(G)| + \sum_{g \in R} \underbrace{(G : C_G(g))}_{>1}$$

Für alle $g \in R$ gilt $(G : C_G(g)) > 1$ nach Def $\Rightarrow C_G(G) \subsetneq G \overset{\text{Ann. 2. Fall}}{\Rightarrow} p \mid (G : C_G(g))$

$\Rightarrow \sum_{g \in R} (G : C_G(g))$ ist teilbar durch p

ebenso: $p^k \mid |G|$ und $k \geq 1$

Klassengleichung $\Rightarrow p \mid |Z(G)|$

Beh.: Es gibt in $Z(G)$ eine Untergruppe N mit $|N| = p$.

$Z(G)$ ist endliche abelsche Gruppe $\Rightarrow$

$\exists r \in \mathbb{N}_0$, zykl. Gruppen $C_1, \ldots, C_r$ mit

$Z(G) \cong C_1 \times \dots \times C_r$ $\quad p \mid |Z(G)| \Rightarrow$

$p \mid |C_j|$ für ein $j \in \{1, \dots, r\}$ In zyklischen Gruppen gibt es zu jedem Teiler d der Gruppenordnung (genau) eine Untergr. der Ordnung d.

$\Rightarrow C_j$ hat eine Untergr. der Ordnung p

$\Rightarrow Z(G)$ " " " " " "

($\Rightarrow$ Beh.)

Wegen $N \subseteq Z(G)$ gilt $N \trianglelefteq G$. (denn: Sei $g \in G$, $n \in N \Rightarrow gng^{-1} \overset{n \in Z(G)}{=} gg^{-1}n = en = n \in N$)

Sei $\overline{G} = G/N \Rightarrow |\overline{G}| = (G:N) = \frac{|G|}{|N|} = \frac{|G|}{p} < |G|$

Ind.-V. anwendbar

Wegen $p^k \mid |G|$ und $|\bar{G}| = \frac{1}{p}|G|$ gilt

$p^{k-1} \mid |\bar{G}| \overset{\text{Ind. V.}}{\Longrightarrow}$ Es gibt eine Untergr.

$\bar{U}$ von $\bar{G}$ mit $|\bar{U}| = p^{k-1}$ Sei

$U = \pi_N^{-1}(\bar{U})$, wobei $\pi_N : G \to \bar{G}$ kan.

Epimorphismus Korrespondenzsatz

$\Rightarrow (G:U) = (\bar{G}:\bar{U}) \Rightarrow$

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

□

Definition der Sylowgruppen

Definition (10.22)

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.

Bedeutung des Normalisators

Proposition (10.23)

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.

Beweis von Prop. 10.23

geg: Gruppe G, $U \leq G$

Erinnerung: Definition des Normalisators:

$N_G(U) = \{g \in G \mid gUg^{-1} = U\}$

Beh: (1) $U \trianglelefteq N_G(U)$

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

zu (1) Sei $g \in N_G(U)$. Dann gilt

$gUg^{-1} = U \rightarrow U \trianglelefteq N_G(U)$

zu (2) Sei $h \in H$. $U \trianglelefteq H \Rightarrow hUh^{-1}$

$= U$ Daraus folgt $h \in N_G(U)$, nach Definition des Normalisators. $\square$

Beweis der Sylowsätze (Vorbereitung)

Lemma (10.24)

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 10.24:

geg: Gruppe G, Untergruppen S, H, wobei $hSh^{-1} = S$ für alle $h \in H$.

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

zu (1) bekannt: Für die Untergruppeneigenschaft von HS genügt es, $HS = SH$ zu beweisen.

„$\subseteq$" Sei $g \in HS \Rightarrow \exists h \in H, s \in S: g = hs = hsh^{-1}h$

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

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

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

$hh^{-1}s(h^{-1})^{-1} \in HS \Rightarrow g \in HS$

zu (2) zeige: $N_{HS}(S) = HS$ Nach Prop. 10 23 gilt $S \trianglelefteq N_{HS}(S)$, aus der Gleichung folgt dann also $S \trianglelefteq HS$ wie gewünscht.

Für jedes $s \in S$ gilt $sSs^{-1} = S \rightarrow S \subseteq N_{HS}(S)$

Vor: $hSh^{-1} = S \; \forall h \in H \Rightarrow H \subseteq N_{HS}(S)$

Da $N_{HS}(S)$ eine Untergruppe von HS und somit abgeschlossen unter der Verknüpfung ist, folgt aus $H \subseteq N_{HS}(S)$ und $S \subseteq N_{HS}(S)$ auch $hs \in N_{HS}(S) \; \forall h \in H, s \in S$, also $HS \subseteq N_{HS}(S)$ andererseits: $N_{HS}(S) \subseteq HS$

insgesamt: $N_{HS}(S) = HS$ □

Die Sylowsätze

Satz (10.25)

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

(i) Jede p-Untergruppe von G ist in einer p-Sylowgruppe enthalten.

(ii) Je zwei p-Sylowgruppen sind zueinander konjugiert.

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