Heinrich-Heine-Universität Düsseldorf

Zusammenstellung der Vorträge aus dem Seminar

Anzahlen endlicher Gruppen

Veranstalter:
Prof. Benjamin Klopsch
Moritz Petschick

29. Oktober 2020

Dies ist eine Zusammenstellung der schriftlichen Ausarbeitungen, die wegen der weltweiten Pandemie anstatt von Präsenzvorträgen für das Seminar *Anzahlen endlicher Gruppen* an der Heinrich-Heine-Universität Düsseldorf im Sommersemester 2020 abgegeben wurden. Die Vorträge nähern sich anhand des Buches 'Enumeration of Finite Groups' von S. R. Blackburn, P. M. Neumann und G. Venkataraman dem Satz von Pyber über die Anzahl der Isomorphieklassen endlicher Gruppen einer bestimmten Ordnung an.

KAPITEL 1

Einführung ins Thema

Moritz Petschick

1. Die Fragestellung und ihre Formulierung

Dieses Seminar beschäftigt sich mit folgender Fragestellung:

Wieviele Gruppen der Ordnung $n \in \mathbb{N}$ gibt es?

Liest man dies wörtlich erhält man keine sinnvolle Antwort, denn natürlich kann man durch Umbennung der Elemente einer einzigen Gruppe beliebig viele neue Gruppen erhalten. Jede Menge derselben Kardinalität stellte eine Gruppe dar, und die folgerichtige Antwort auf die Frage wäre: „Die Klasse aller Gruppen der Ordnung n ist unabhängig von n eine echte Klasse (und damit keine Menge)."

Diese Antwort ist nicht jene, die wir suchen. Daher schränken wir uns weiter ein und fragen:

Wieviele Isomorphieklassen von Gruppen der Ordnung $n \in \mathbb{N}$ gibt es?

Die Antwort auf diese Frage kann man nun in einer Funktion darstellen. Als generelle Konvention nennen wir diese

$$\begin{aligned} f : \mathbb{N} &\to \mathbb{N} \\ n &\mapsto \#\text{ Menge aller Isomorphieklassen von Gruppen der Ordnung } n. \end{aligned}$$

Andere solche *Zählfunktionen* werden wir ähnlich benennen und eventuell mit Subskripten ausstatten.

Zurück zu unserer Frage. Ein sinnvoller erster Versuch zu einer Antwort wäre es, die ersten Werte von f zu berechnen. Für kleine Zahlen sind diese Werte schon lange bekannt, und mit Hilfe grundlegender Sätze und Methoden kann man sie selbst nachrechnen. Bis $n = 16$ sind die Werte in Tabelle 1 wiedergegeben.

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$f(n)$	1	1	1	2	1	2	1	5	2	2	1	5	1	2	1	14

Tabelle 1. $f(n)$ für kleine Werte von n.

Wer mehr sehen möchte, kann sich diese (die erste!) Folge der *The On-Line Encyclopedia of Integer Sequences* ansehen. Noch mehr findet man in der Arbeit von Besche, Eick und O'Brien, wobei wir vor allen an den beiden folgenden Resultaten daraus interessiert sind:

$$f(2^{10}) = f(1024) = 49487365422$$
$$\sum_{n=1}^{2000} f(n) = 49910529484$$

Das heißt, dass $\frac{49487365422}{49910529484} \approx 99,15\%$ aller (Isomorphieklassen von) Gruppen der Ordnung ≤ 2000 von Ordnung 2^{10} sind! Schaut man sich die obige Tabelle noch einmal an, stellt man ein ganz ähnliches Verhalten im kleinen fest. Es sind 14 von 42, also immerhin ein Drittel, der Gruppen von Ordnung ≤ 16 genau von Ordnung 16.

Auf der anderen Seite kennen wir den Satz, dass alle Gruppen von Primzahlordnung zyklisch sind, das heißt, dass für alle Primzahlen p gerade $f(p) = 1$ gilt. (Andersherum gilt das nicht: Obwohl 15 nicht prim ist, gilt $f(15) = 1$.) Damit drängt sich folgende Vermutung auf: Der Wert $f(n)$ is groß, wenn n viele Teiler hat, und klein, wenn n wenige Teiler hat. Konkreter wollen wir folgende Maße für die *arithmetische Größe* einer natürlichen Zahl definieren:

DEFINITION 1.1. Sei $n \in \mathbb{N}$ eine positive ganze Zahl mit Primfaktorzerlegung

$$n = \prod_{i=1}^{\ell} p_i^{\alpha_i},$$

dass heißt p_i ist prim und $\alpha_i \in \mathbb{N}$ für $i = 1, \ldots, \ell$, und $p_i = p_j$ impliziert $i = j$. Wir definieren

$$\mu(n) := \max_{i=1}^{\ell} \alpha_i$$
$$\lambda(n) := \sum_{i=1}^{\ell} \alpha.$$

Achtung! Die Funktion μ ist *nicht* die häufig in der Zahlentheorie verwendete *Möbius-Funktion*, die oft ebenfalls mit μ bezeichnet wird.

Außerdem erkennen wir, dass unmöglich scheint eine exakte Formel für $f(n)$ anzugeben. Was wir suchen ist also eine *Abschätzung* für den Wert von f abhängig von n. Um auch dieses zu präzisieren definieren wir:

DEFINITION 1.2. Seien $k, l : \mathbb{N} \to \mathbb{R}$ zwei Funktionen. Wir schreiben

$$k(n) \leq \mathcal{O}(l(n))$$

(und analog $\leq, =$) falls eine positive Zahl $M \in \mathbb{R}_+$ existiert, sodass ein $n_0 \in \mathbb{N}$ exisiert, ab welchem für alle $n > n_0 \in N$ die folgende Abschätzung gilt:

$$k(n) \leq Ml(n).$$

Diese Konvention nennt man *Landau*-$\mathcal{O}$-Notation.

BEISPIEL 1.3.

(1) Einige Klassen von Funktionen lassen sich durch das Landau-$\mathcal{O}$ einfach beschreiben. Zum Beispiel sind die beschränkten Funktionen gerade die Funktionen k, für welche $k \leq \mathcal{O}(1)$ gilt. Dabei beschreibt 1 die konstante Funktion.

(2) Von großem Interesse ist es, wie sich Zählfunktionen in die Hierarchie von polynomiellen, also $\mathcal{O}(P)$ mit einem Polynom P, und exponentiellen, also $\mathcal{O}(\exp)$, einordnen.

2. Resultate

Im Verlaufe des Seminars werden wir die Beweise für die beiden folgenden Resultate über die approximative von f untersuchen. Dabei gelten diese zunächst nur für Primzahlpotenzen, was aber im Angesicht der im vorherigen Abschnitt erklärten Vermutung ein plausibler Startpunkt ist.

SATZ 2.1. *Sei p eine Primzahl. Dann gilt für natürliche Zahlen $m \in \mathbb{N}$*

$$f(p^m) \geq p^{\frac{2}{27}m^3 - \mathcal{O}(m^2)}.$$

SATZ 2.2. *Sei p eine Primzahl. Dann gilt für natürliche Zahlen $m \in \mathbb{N}$*

$$f(p^m) \leq p^{\frac{2}{27}m^3 + \mathcal{O}(m^{\frac{8}{3}})}.$$

Tatsächlich liegen wir damit schon in einem engen Wachstumsfenster. Beachtet man, dass $\mu(p^m) = m = \lambda(p^m)$ gilt, stellt sich die Frage danach, welches arithmetische Größenmaß die Potenz verallgemeinert.

In der zweiten Hälfte des Seminars beschäftigen wir uns mit einem Spezialfall des Satzes von Pyber, dessen allgemeine Form eine sehr präzise Antwort auf unsere zentrale Frage liefert:

SATZ 2.3. *Es gilt:*

$$f(n) \leq n^{\frac{2}{27}\mu(n)^3 + \mathcal{O}(\mu(n)^{\frac{5}{3}})}.$$

3. Elementare Abschätzungen

DEFINITION 3.1 (Hierachie von gruppenähnlichen algebraischen Strukturen).

(1) Eine nicht-leere Menge M mit einer Operation
$$\cdot : M \times M \to M$$
heißt *Magma*.

(2) Ein Magma M mit einem Element 1_M mit der Eigenschaft
$$1_M \cdot m = m = m \cdot 1_M$$
für alle $m \in M$ heißt *unitäres Magma*. Das Element 1_M heißt neutrales Element.

(3) Ein Magma, in dem das Assoziativgesetz gilt, heißt *Halbgruppe*.

(4) Ein Magma M mit der Eigenschaft, daß für alle $m, n \in M$ Elemente $x, y \in M$ existieren, sodaß
$$m \cdot x = n \text{ und } y \cdot m = n$$
gelten, heißt *Quasigruppe*.

Jedes endliche Magma wird vollständig durch seine Multiplikationstafel (auch *Cayley-Tafel* genannt) beschrieben, also durch die Matrix $(m \cdot n)_{m,n \in M} \in M^{|M|^2}$. Dadurch läßt sich die Anzahl der möglichen Magmas einer bestimmten Größe einfach abschätzen. Es gilt:

$$f_{\text{Magma}}(n) \leq n^{n^2}.$$

Da Magmas keine algebraischen Eigenschaften (wie Assoziativität, Kommutativität, &c.) erfüllen müssen, definieren wir den *Isomorphimsus von Magmas* als Bijektion der unterliegenden Mengen. Natürlich soll f_{Magma} die Zahl der Magmas bis auf Isomorphie beschreiben. Also wissen wir, daß eine untere Schranke für f_{Magma} durch

$$\frac{n^{n^2}}{n!}$$

gegeben wird.

Wie zu erwarten bringt uns diese Abschätzung noch kaum einen Schritt an die Resultate für Gruppen heran. Auch der Übergang zu unitären Magmas ist nicht bedeutsam, da bei diesen lediglich eine Spalte und Zeile in der Cayley-Tafel festgelegt ist (die des neutralen Elementes), d.h.

$$\frac{n^{n-1^2}}{(n-1)!} \leq f_{\text{uni.Magma}}(n) \leq n^{n-1^2}.$$

Größere Hoffnung einer Annäherung an die Ergebnisse für Gruppen liegt im Übergang zu Halb- oder Quasigruppen.

SATZ 3.2. *Sei $\epsilon > 0$. Dann existiert ein $n_0 \in \mathbb{N}$, sodaß für alle $n > n_0$ folgendes gilt:*

$$f_{\text{Halbgruppen}}(n) \geq n^{(1-\epsilon)n^2}.$$

BEWEIS. Die Idee ist es, strukturell sehr einfach zu beschreibenden Halbgruppen zu konstruieren. Sei $M \neq \emptyset$ eine durch $<$ linear geordnete Menge, d.h. bis auf Umbenennung $\{0, \ldots, |M| - 1\}$ mit der natürlichen Ordnung. Wähle $m \in M$ beliebig und definiere

$$i \cdot j = \begin{cases} 0, & \text{falls } i < m \text{ oder } j < m \\ \text{beliebig in } \{n \in M \mid n < m\} & \text{andernfalls.} \end{cases}$$

Unabhängig von der konkreten Wahl im zweiten Fall erhalten wir eine Halbgruppe: Es gilt für alle $i, j, k \in M$

$$\underbrace{(i \cdot j)}_{<m} \cdot k = 0 = i \cdot \underbrace{(j \cdot k)}_{<m}.$$

Es gilt also für jedes $m \in M$

$$f_{\text{Halbgruppen}}(n) \geq \frac{m^{(n-m)^2}}{n!}.$$

Wählt man $m := n^{(1-\frac{1}{2}\epsilon)}$ ergibt sich

$$f_{\text{Halbgruppen}}(n) \geq n^{(1-\frac{1}{2}\epsilon)(n-n^{1-\frac{1}{2}\epsilon})}.$$

Für große $n \in N$ gilt damit $f_{\text{Halbgruppen}}(n) \geq n^{(1-\epsilon)n^2}$. □

Trotz Assoziativität bleiben wir also sehr dicht an n^{n^2}. Die nächste Hoffnung sind die Quasi-Gruppen. Um diese besser zu verstehen betrachten wir folgendes Lemma:

LEMMA 3.3. *Ein Magma M ist genau dann eine Quasigruppe, wenn seine Multiplikationstafel ein* lateinisches Quadrat *ist, d.h. wenn in jeder Zalte und Speile jedes Element von M genau einmal vorkommt.*

BEWEIS. Angenommen M ist eine Quasigruppe. In der Spalte von $m \in M$ taucht $n \in M$ auf, denn es existiert $x \in M$ mit $m \cdot x = n$. Analoges gilt für die Zeilen der Tafel, mit der Existenz von $y \in M$, sodaß $y \cdot m = n$. Die Rückrichtung ist klar. □

Leider ist die Zahl der Lateinischen Quadrate einer fixen Größe ein Mysterium; es ist keine Asymptotik bekannt. Aber ein Satz von M. Hall besagt:

$$n^{\frac{1}{2}n^2 - \mathcal{O}(n)} \leq f_{\text{Lateinische Quadrate}}(n) \leq n^{n^2}.$$

Also reicht auch die Invertierbarkeit nicht für eine signifikante Reduktion der Anzahl der Objekte aus. Man muß also tatsächlich alle drei Eigenschaften der Gruppe – Assoziativität, Invertierbarkeit und Unitarität – gleichzeitig betrachten.

SATZ 3.4 (Elementare obere Schranke). *Es gilt*

$$f(n) \leq n^{n\lambda(n)}.$$

BEWEIS. Definiere den Rang von G durch

$$\mathrm{d}(G) := \min\{|X| \mid X \subseteq G, \langle X \rangle = G\},$$

also als die minimale Größe eines Erzeugendensystems von G. Dann gilt

$$\lambda(|G|) \geq \mathrm{d}(G).$$

Dies wird wie folgt bewiesen: Sei

$$G = G_r > G_{r-1} > \cdots > G_1 > G_0 = \{1\}$$

eine maximale Kette ineinander enthaltener Untergruppen von G. Wähle für jedes $i \in \{1, \ldots, r\}$ ein Element $g_i \in G_i \setminus G_{i-1}$. Dann gilt $\langle g_i \mid i \in \{1, \ldots, j\}\rangle = G_j$, denn wäre $\langle g_i \mid i \in \{1, \ldots, j\}\rangle < G_j$ könnte man die Kette verfeinern. Damit ist $r > \mathrm{d}(G)$. Nach dem Satz von Lagrange gilt

$$|G| = \prod_{i=1}^{r} |G_i : G_{i-1}|.$$

Damit ist nun $r \leq \lambda(|G|)$, denn $\lambda(|G|)$ ist die maximale Länge eines Produktes von Zahlen aus $\mathbb{N}_{>1}$, welches $|G|$ ergibt. Dies beweist die Behauptung $\lambda(|G|) \geq \mathrm{d}(G)$.

Nach dem Satz von Cayley gilt bis auf Isomorphie $G \leq \mathsf{Sym}(|G|)$. Also

$$\begin{aligned} f(n) &\leq \#\text{Untergruppen der Ordnung } n \text{ von } \mathsf{Sym}(n) \\ &\leq \#\lambda(n)\text{-erzeugte Untergruppen der Ordnung } n \text{ von } \mathsf{Sym}(n), \end{aligned}$$

nach obiger Behauptung, und konsequenterweise

$$\begin{aligned} f(n) &\leq \#\lambda(n)\text{-elementige Teilmengen von } \mathsf{Sym}(n) \\ &= (n!)^{\lambda(n)} \\ &\leq n^{n\lambda(n)}. \end{aligned}$$

□

KAPITEL 2

p-Gruppen: Grundlagen

Lassaad Methnani

1. Die Kommutatoruntergruppe

Definition 1.1. Sei G eine Gruppe, für $x, y \in G$ nennt man $[x, y] = x^{-1}y^{-1}xy$ den Kommutator von x und y. Die von allen Kommutatoren erzeugte Untergruppe G' heißt Kommutatorgruppe von G. Die Kommutatorgruppe von G' bezeichnen wir mit $G - G^{(2)}$, allgemein betrachten wir die höhere Kommutatorgruppe $G^{(k+1)} = (G^{(k)})'$.

Bemerkung 1.2. Sei G eine Gruppe und $X, Y \subseteq G$.

(1) $X, Y \subseteq G \to [X, Y] \trianglelefteq \langle X, Y\rangle \subseteq G$.
(2) $[X, Y] \leq X \leftrightarrow Y \leq N_G(X)$.
(3) Für jede Gruppenhomomorphismus $f : G \to H$ gilt

$$f([X, Y]) = [f(X), f(Y)].$$

Beispiel 1.3. Zu Kommutatoruntergruppen:

(1) $[S_n, S_n] = A_n$, für $n \geq 1$.
(2) $[A_n, A_n] = \begin{cases} \{\mathrm{id}\} & \text{für } n = 1, 2, 3 \\ V_4 & \text{für } n = 4 \\ A_n & \text{für } n \geq 5. \end{cases}$

Lemma 1.4. *Sei G eine Gruppe, für $x, y, z \in G$ und $\forall n \in \mathbb{N}$ gilt:*

$$\begin{aligned}
[x, y] &= [y, x]^{-1} \\
[xy, z] &= [x, z]^y[y, z] = [x, z][x, z, y][y, z] \\
[x, yz] &= [x, z][x, y]^z = [x, z][x, y][x, y, z] \\
1 &= [x, y^{-1}, z]^y[y, z^{-1}, x]^z[z, x^{-1}, y]^x \quad (\textit{Die Wittsche Identität}) \\
[x^{-1}, y] &= ([x, y]^{-1})^{x^{-1}} = [x, y, x^{-1}]^{-1}[x, y]^{-1} \\
[x, y^{-1}] &= ([x, y]^{-1})^{y^{-1}} = [x, y, y^{-1}]^{-1}[x, y]^{-1} \\
[x, y, z] &= ([z, x^{-1}, y^{-1}]^{-1})^{xy}([y^{-1}, z^{-1}, x]^{-1})^{zy} \\
[y, x^n] &= [y^n, x] = [y, x]^n \\
(xy)^n &= x^n y^n [y, x]^{\frac{1}{2}n(n-1)}
\end{aligned}$$

Beweis. Durch einfaches Nachrechnen. □

LEMMA 1.5 (Das drei Untergruppen-Lemma). *Sei G eine Gruppe und A, B, C Untergruppen von G. Gelten $[A, B, C] = 1$ und $[B, C, A] = 1$, dann auch $[C, B, A] = 1$.*

BEWEIS. Sind $a \in A$, $b \in B$ und $c \in C$, so folgt $[a, b, c] = [b, c, a] = 1$ nach Voraussetzung und daher auch $[c, b, a] = 1$ nach der Wittschen Identität, denn die Konjugation ist ein Automorphismus und muss 1 auf 1 abbilden. Also vertauscht jedes $a \in A$ mit jedem $[c, b]$ und daher mit der davon erzeugte Gruppe $[C, B]$ und daraus folgt $[C, B, A] = 1$. □

DEFINITION 1.6. Sei G eine Gruppe, die untere Zentralreihe G_1, G_2, G_3 ... von G ist definiert durch $G_1 = G$ und $G_{i+1} = [G_i, G]$ für jede positive ganze Zahl i.
G_i heißt der $i - te$ Term der unteren Zentralreihe von G und diese sind charakteristische Untergruppen von G.

SATZ 1.7. *Sei G eine Gruppe,$\forall i, j \in \mathbb{Z}$ gilt*

$$[G_i, G_j] \leq G_{i+j}.$$

BEWEIS. Induktion nach j:
$j = 1$ ist klar (Definition der unteren Zentralreihe).
$j \geq 1$: Wenn wir G bei Bedarf durch den Quotient G/G_{i+j} ersetzen, können wir annehmen, dass $G_{i+j} = \{1\}$. Unsere induktive Hypothese impliziert, dass

$$[G_i, G_{j-1}, G] \leq [G_{i+j-1}, G] = G_{i+j} = \{1\}$$

und $[G, G_i, G_{j-1}] = [G_i, G, G_{j-1}] = [G_{i+1}, G_{j-1}] \leq G_{i+j} = \{1\}$. Das Lemma 1.5 impliziert, dass

$$[G_i, G_j] = [G_j, G_i] = [G_{j-1}, G, G_i] \leq [G_i, G_{j-1}, G][G, G_i, G_{j-1}] = \{1\} = G_{i+j}.$$

□

2. Nilpotente Gruppen

DEFINITION 2.1. Eine Gruppe G heißt nilpotent, wenn es eine in der trivialen Gruppe endenden Zentralreihe in G gibt. Das heißt es gibt Normalteiler $N_i \trianglelefteq G$ mit $1 = N_0 \trianglelefteq N_1 \trianglelefteq N_2 \cdots \trianglelefteq N_c = G$ und $N_{i+1}/N_i = Z(G/N_i)$.

Sei G eine Gruppe, $Z_0(G) = 1$, $Z_1(G) = Z(G)$ und $\forall i : Z_{i+1}(G)/Z_i(G) = Z(G/Z_i(G))$. $Z_i(G)$ heißt die i-te Zentrum von G und $Z_0(G) \leq Z_1(G) \leq \cdots \leq Z_i(G)$ die aufsteigende Zentralreihe von G. G ist nilpotent, falls $Z_n(G) = G$ für ein $n \in \mathbb{N}$.

LEMMA 2.2. *Für eine nilpotente Gruppe G gilt:*

- *$U < G \to U < N_G(U)$ (G erfüllt die Normalisator-Bedingung).*
- *Jede maximale Untergruppe in G ist normal.*
- *G ist direktes Produkt seiner Sylowgruppen.*

BEISPIEL 2.3. Zu nilpotenten Gruppen:

(1) Abelsche Gruppen sind nilpotent ($Z(G) = G$).
(2) Jede endliche p-Gruppe ist nilpotent. (*Jede endliche p-Gruppe besitzt ein nichttriviales Zentrum.*)
(3) Die Frattinigruppe ist nilpotent.
(4) S_3 ist nicht nilpotent, da $Z_i(S_3) = 1, \forall i \geqslant 0$.

SATZ 2.4. *Sei G eine Gruppe, die durch eine Menge S erzeugt ist. Sei T eine Teilmenge von G_i, deren Bild in G_i/G_{i+1} erzeugt. Dann wird G_{i+1}/G_{i+2} von der Menge $\{[t,s]G_{i+2}/t \in T, s \in S\}$ erzeugt.*

SATZ 2.5. *Sei G nilpotent und H eine Untergruppe von G. Wenn $H_2G_3 = G_2$, dann ist $H_i = G_i \ \forall i \geqslant 2$.*

IDEE DES BEWEISES. Wir beweisen zuerst, dass $H_rG_{r+1} = G_r \ \forall r \geqslant 2$. Induktion nach r :
$r = 2$: Ist klar nach Induktionsannahme. Also angenommen $r > 2$ und $H_sG_{s+1} = G_s$ für $2 \leqslant s \leqslant r$

$$H_rG_{r+1} \leqslant G_r$$

ist klar und wir müssen beweisen, dass $G_r \leqslant H_rG_{r+1}$.

Wir betrachten zwei Ergebnisse (ohne Beweis):

$$[KL, M] \leqslant [K, M][L, M]G_{r+1} \qquad \text{(3.10 im Buch)}$$
$$[H_{r-1}, G] \leqslant [G, H_{r-2}, H][H, G, H_{r-2}]G_{r+1} \qquad \text{(3.11 im Buch)}$$

Es folgt

$$\begin{aligned}
G_r &= [G_{r-1}, G] \\
&= [H_{r-1}G_r, G] \\
&= [H_{r-1}, G]G_{r+1} && (3.10) \\
&\leq [G, H_{r-2}, H][H, G, H_{r-2}]G_{r+1} && (3.11) \\
&\leq [G_{r-1}, H][G_2, H_{r-2}]G_{r+1} && \text{(Proposition 1.7)} \\
&= [H_{r-1}G_r, H][H_2G_3, H_{r-2}]G_{r+1} \\
&= [H_{r-1}, H][G_r, H][H_2, H_{r-2}][G_3, H_{r-2}]G_{r+1} && (3.10) \\
&= H_rG_{r+1} && \text{(Proposition 1.7).}
\end{aligned}$$

Als nächstes beweisen wir, dass $G_i = H_iG_{i+k}$ für $k \geqslant 1$ und $i \geqslant 2$. Für $k = 1$ ist das schon bewiesen. Für $k > 1$ und $G_i = H_iG_{i+k-1}$ gilt: $G_i = H_iG_{i+k-1} = H_iH_{i+k-1}G_{i+k} = H_iG_{i+k}$. Wir gehen davon aus, dass G nilpotent ist, also $G_{i+k} = \{1\}$ und es folgt: $G_i = H_i$ □

3. Die Frattiniuntergruppe

Die Frattinigruppe oder genauer die Frattiniuntergruppe ist eine spezielle Untergruppe einer gegebenen Gruppe. Mit ihrer Hilfe kann insbesondere die Struktur endlicher p-Gruppen untersucht werden. Sie ist benannt nach dem italienischen Mathematiker Giovanni Frattini.

DEFINITION 3.1. Ist G eine Gruppe, dann ist die Frattinigruppe $\Phi(G)$ definiert als der Schnitt aller maximalen Untergruppen von G.

$$\Phi(G) = \cap\{U \mid U \leqslant_{\max} G\}$$

Hat G keine maximale Untergruppe, so setzt man $\Phi(G) = G$.

LEMMA 3.2 (Frattini-Argument). *Ist $N \trianglelefteq G$ und P eine p-Sylowgruppe von N, dann gilt*

$$G = N_G(P)N.$$

LEMMA 3.3. *Für alle Gruppen G gilt:*

(1) $\Phi(G)$ *ist nilpotent.*
(2) $\Phi(G) \leqslant_{\text{char}} G$.

BEISPIEL 3.4. Zu Frattiniuntergruppen:

- $\Phi(S_3) = 1$.
- $\Phi(D_4) = Z(D_n) \cong C_2$.

LEMMA 3.5. *Sei G eine endliche Gruppe und X eine Teilmenge von G. Dann erzeugen $\Phi(G)$ und X zusammen G, genau dann wenn X die Gruppe G erzeugt. (Das heißt $\Phi(G)$ ist die Menge der Nichterzeuger von G.)*

BEWEIS. Eindeutig bedeutet $G = \langle X \rangle$, dass $G = \langle X \bigcup \Phi(G) \rangle$.
Für das Gegenteil nehmen wir an, dass $G \neq \langle X \rangle$. Dann ist $\langle X \rangle$ in einem maximalen Untergruppe M von G enthalten.

Da $\Phi(G)$ der Schnitt aller maximalen Untergruppe von G ist, haben wir $\Phi(G) \leqslant M$. Aber jetzt $\langle X \bigcup \Phi(G) \rangle \leq M < G$ und so ist $G \neq \langle X \bigcup \Phi(G) \rangle$. □

Wenn G eine p-Gruppe ist, dann haben die maximale Untergruppen von G eine besondere einfache Form.

KOROLLAR 3.6. *Sei G eine endliche p-Gruppe. Dann ist jede maximale Untergruppe M von G normal und hat den Index p in G.*

LEMMA 3.7. *Sei G eine endliche p-Gruppe. Dann ist $G/\Phi(G)$ eine elementare abelsche p-Gruppe der Ordnung p^d, wobei d die minimale Anzahl der Erzeuger von G ist.*

Außerdem ist $\Phi(G) = G^p G'$, wobei G^p die von der Menge $\{x^p : x \in G\}$ erzeugte Untergruppe ist.

LEMMA 3.8. *Sei G eine endliche p-Gruppe und B die Gruppe von Automorphismen von G, die den Identitätsautomorphismen auf $G/\Phi(G)$ induziert. Dann ist B eine p-Gruppe.*

BEWEIS. Angenommen B ist keine p-Gruppe. Es gibt also $x \in B$ und die Ordnung von x ist keine Potenz von p. Sei q die Ordnung von x, wobei $q \neq p$ (q ist ein Primzahl). Sei $g \in G$. Da x den Identitätsautomorphismus auf $G/\Phi(G)$ induziert, vertauscht x die Elemente in der Nebenklasse $g\Phi(G)$. Jede Zyklus von x hat entweder die Länge 1 oder q.

Da $|g\Phi(G)|$ eine Potenz von p hat (und ein Potenz von p kein Vielfaches von q ist), können nicht alle diese Zyklen die Länge q haben. Daher fixiert x ein Element in jeder Nebenklasse $g\Phi(G)$ von $\Phi(G)$ in G. Insbesondere erzeugen G die Elemente in G, die durch x festgelegt sind. Da x ein Erzeugendensystem von G festhält, stellen wir fest, dass x der Identitätsautomorphismus ist.

Diese widerspricht der Tatsache, dass x die Ordnung q hat. □

SATZ 3.9. *Sei G eine endliche Gruppe. Dann ist G genau dann nilpotent, wenn $G' \leq \Phi(G)$.*

BEWEIS. Angenommen G ist nilpotent.

Das heißt jede Untergruppe H von G ist in ihrem Normalisator enthalten. Um dies zu sehen, sei i die größte ganze Zahl, so dass G_i nicht in H enthalten ist. Dann $[G_i, H] \leq G_{i+1} < H$ und damit $G_i \leq N_G(H)$). Insbesondere ist jede maximale Untergruppe M von G normal. $(G/M)'$ ist eine echte Untergruppe von G/M, $(G/M)'$ ist trivial und daher ist G/M abelsch. Somit ist $G' \leq M$ für jede maximale Untergruppe M von G und G' in der Schnittmenge $\Phi(G)$ aller maximalen Untergruppen von G enthalten.

Um das Gegenteil zu beweisen, nehmen wir an, dass $G' \leq \Phi(G)$. (Und damit insbesondere, dass jede maximale Untergruppe von G normal ist).
Sei P eine Sylowuntergruppe von G und wir suchen nach einem Widerspruch, dass $N_G(P)$ eine echte Untergruppe von G ist. Dann ist $N_G(P) \leq M$ für eine maximale Untergruppe M von G. Nun ist $P \leq M$ und damit P eine Sylowuntergruppe der normale Untergruppe M. Nach dem Frattini-Argument ist $N_G(P).M = G$, aber $N_G(P) \leq M$. Widerspruch!

Somit ist jede Sylowuntergruppe von G normal und daher ist G nilpotent. □

KAPITEL 3

p-Gruppen: Higmans untere Schranke

Christin Katzgrau

1. Wichtige Ergebnisse aus der Linearen Algebra

Hier geht es um die Aufzählung von Ergebnissen aus der L.A., Wiederholung von Standardsachen und den daraus reslutierenden Folgerungen für einfache abelsche Gruppen. Hierbei wird q eine p-Potenz sein und $\mathbb{F}_q$ ein endlicher Körper mit q Elementen. Beweise werden hier keine geführt.

Satz 1.1. *Sei V ein d dimensionaler Vektorraum über $\mathbb{F}_q$. Dann existieren*

$$(q^d-1)\cdot(q^d-q)\cdot\ldots\cdot(q^d-q^{k-1})$$

Möglichkeiten für eine Reihenfolge $v_1,\ldots,v_k$ von linear unabhängigen Vektoren. Im Besonderen gilt

$$|\operatorname{GL}(d,q)| = (q^d-1)\cdot(q^d-q)\cdot\ldots\cdot(q^d-q^{d-1}) \leq q^{d^2}.$$

Beweis. Anwendung der linearen Algebra und einfaches Nachrechnen. □

Satz 1.2. *Sei V ein Vektorraum über $\mathbb{F}_q$ mit Dimension d. Für $0 \leq k \leq d$ sei $n_{d,k}$ die Anzahl der k-dimensionalen Untervektorräume von V. Dann gilt:*

$$n_{d,k} = \frac{(q^d-1)\cdot(q^d-q)\cdot\ldots\cdot(q^d-q^{k-1})}{(q^k-1)\cdot(q^k-q)\cdot\ldots\cdot(q^k-q^{k-1})}.$$

Desweiteren gilt:

$$q^{k(d-k)} \leq n_{d,k} \leq q^{k(d-k-1)}.$$

Beweis. Folgt aus dem ersten Satz. □

Da man eine einfache p-Gruppe als Vektorraum über $\mathbb{F}_q$ auffassen können, erhalten wir aus dem oberen Satz folgendes Korollar.

Korollar 1.3. *Sei p eine Primzahl und sei P eine einfache abelsche Gruppe der Ordnung p^d . Dann hat P exakt $n_{k,d}$ Untergruppen der Ordnung p^k.*

Nun wollen wir ein paar Standardergebnisse für die alternierenden Abbildungen anschauen.

Seien V und W Vektorräume über einem Körper F. Genau wie für abelsche Gruppen ist eine Abbildung $\phi : V \times V \to W$alternierend, wenn $\phi(v,v) = 0\ \forall\ v \in V$ gilt.

Hat W die Dimension 1 über F, so sagen wir, dass ϕ eine alternierende Abbildung von V ist. Für einen Untervektorraum U von F definieren wir $U^\perp$ durch

$$U^\perp = \{u \in V | \phi(u, v) = 0 \forall v \in V\}.$$

Das Radikal R einer alternierenden Abbildung auf V ist die Untergruppe, die durch $V^\perp$ definiert wird. Also

$$R = \{u \in V | \phi(u, v) = 0 \forall v \in V\}.$$

Ist R trivial, so sagen wir, dass ϕ nicht ausartend ist. Nicht ausartend bedeuted, dass die Darstellungsmatrix invertierbar bezüglich der Basis ist.

Eine Basis $u_1, \ldots, u_r, v_1, \ldots, v_r$ von V ist symplektisch (im Bezug auf ϕ), wenn für alle $i, j \in \{1, \ldots, r\}$ gilt:

$$\phi(u_i, u_j) = 0$$
$$\phi(v_i, v_j) = 0$$
$$\phi(u_i, v_j) = \begin{cases} 1, & \text{wenn } i = j \\ 0, & \text{sonst} \end{cases}$$

SATZ 1.4. *Sei V ein endlich dimensionaler Vektorraum über F und sei $\phi : V \times V \to F$ eine nicht ausartende Abbildung auf V. Dann existiert eine Basis $u_1, \ldots, u_r, v_1, \ldots, v_r$ auf V, die symplektisch ist im Bezug auf V. Hierbei muss die Dimension gerade sein.*

BEWEIS. Anwendung von Prinzipien aus der linearen Algebra. □

SATZ 1.5. *Sei V ein endlicher $2r$ dimensionaler Vektorraum über $\mathbb{F}_q$ und sei ϕ eine nicht ausartende Abbildung auf V. Dann ist die Anzahl der Basen für V, die symplektisch im Bezug auf ϕ sind:*

$$(q^{2r} - 1) \cdot q^{2r-1} \cdot (q^{2r-2} - 1) \cdot q^{2r-3} \cdot \ldots \cdot (q^2 - 1) \cdot q = q^{r^2} \cdot (q^{2r} - 1) \cdot (q^{2r-2} - 1) \cdot \ldots \cdot (q^2 - 1)$$

Dies ist genau die Ordnung von $\mathrm{Sp}(2r, q)$.

BEWEIS. Induktion über die Dimension. □

2. p-Gruppen : Eine untere Schranke

Sei p nun eine bestimmte Primzahl. Für jede ganze Zahl m ist $f(p^m)$ die Anzahl der Gruppen (bis auf Isomorphie) mit Ordnung p^m.
Dieses Kapitel wird zeigen, dass

$$f(p^m) \geq p^{\frac{2}{27}m^2(m-6)}$$

ist.
Diese Gleichung wollen wir in diesem Kapitel beweisen.

DEFINITION 2.1 (relativ freie Gruppen). Sei r eine positive ganze Zahl. Sei F_r eine freie Gruppe von Rang r, und N der Normalteiler erzeugt von allen Wörtern der Form $x^{p^2}, [x, y]^p$ und $[x, y, z]$. Beachte, dass alle Wörter der Form $[x^p, y]$ in N liegen.
Die Gruppe $G_r = F_r/N$ ist die relativ freie Gruppe in der Varietät von p-Gruppen von ϕ-Klasse 2. Eine p-Gruppe hat ϕ-Klasse 2, wenn es eine Untergruppe $H \in \mathrm{Z}(G)$ von G gibt, so dass G/H abelsch ist.

Wir identifizieren die Elemente x_i mit ihrem Bild in G_r. Durch diese Abbildung $x_1, \ldots, x_r$ erzeugen wir G_r.

LEMMA 2.2. *Sei H eine Gruppe der ϕ-Klasse 2 und seien $y_1, \ldots, y_r \in H$. Dann existiert ein Homomorphismus $\phi : G_r \to H$, so dass $\phi(x_i) = y_i$ für $i \in \{1, \ldots, r\}$.*

BEWEIS. Da F_r eine freie Gruppe ist, existiert ein eindeutiger Homomorphismus $\psi : F_r \to H$ so dass $\psi(x_i) = y_i \forall i \in \{1, 2, \ldots, r\}$ gilt. Durch unsere Bedingungen, die wir an H gestellt haben, erhalten wir: $N \leq \ker(\psi)$ somit induziert ψ den Homomorphismus $\phi : G_r \to H$ so dass $\phi(x_i) = y_i \; \forall \, i \in \{1, 2, \ldots, r\}$. □

LEMMA 2.3. *Sei G_r eine p-Gruppe. Die Frattini-Untergruppe $\phi(G_r)$ von G_r ist von Ordnung $p^{\frac{1}{2}r(r+1)}$ und hat Index p^r und liegt im $\mathrm{Z}(G_r)$. Auch gilt, dass jeder Automorphismus $x \in \mathrm{Aut}(G_r)$, der die Identitätsabbildung von $G_r/\phi(G_r)$ induziert, $\phi(G_r)$ punktweise fixiert.*

BEWEIS. Da jeder Kommutator oder p-te Potenz in G_r im Zentrum von G liegt und Ordnung p hat, liegt auch $G_r^p G'$ im Zentrum und ist somit eine abelsche Gruppe. Auch $G_r/G_r^p G'$ ist abelsch und somit ist G_r eine p-Gruppe.
Aus einem Lemma zur Frattini-Untergruppe wissen wir, dass $\phi(G_r) = G_r^p G'$ ist und somit liegt $\phi(G_r)$ im Zentrum.
$\phi(G_r)$ wird von Elementen x_i^p für $i \in \{1, 2, \ldots, r\}$ und $[x_i, x_j]$ mit $1 \leq i < j \leq r$ erzeugt.
Da diese Elemente einen minimalen Erzeuger von $\phi(G_r)$ bilden zeigt man wie folgt:
Angenommen es existiert $a_i \in \{0, \ldots, p-1\}$ für $i = 1, 2, \ldots, r$ und $b_{i,j} \in 0, 1, \ldots, p-1$ für $1 \leq i < j \leq r$, so dass

$$\prod_{i=1}^{r} (x_i^p)^{a_i} \cdot \prod_{1 \leq i < j \leq r} [x_j, x_i]^{b_{i,j}} = 1.$$

Sei H eine von h erzeugte zyklische Gruppe der Ordnung p^2. Da H der ϕ-Klasse 2 ist, impliziert Lemma 2.2, dass es für alle k mit $1 \leq k \leq r$ ein Homomorphismus $\Psi_k : G_r \to H$ existiert, so dass

$$\Psi_k(x_i) = \begin{cases} 1, \text{wenn } i \neq k \\ h, \text{wenn } i = k. \end{cases}$$

Unter dem Homomorphismus Ψ_k bekommen wir für die obere Gleichung folgende Ergebnisse: $(h^p)^{a_k} = 1$ und somit $a_k = 0$. Deshalb gilt $a_1 = a_2 = \ldots = a_r = 0$.
Durch ein ähnliches Argument kann gezeigt werden, dass $b_{i,j} = 0$ für alle i und j ist.
Hierbei bildet der Homomorphismus ϕ die x_i und x_j auf die erzeugenden Elemente $\left(\begin{smallmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right)$ und $\left(\begin{smallmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{smallmatrix}\right)$ der Gruppe H mit 3×3 oberen Dreiecksmatritzen der Form $\left(\begin{smallmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{smallmatrix}\right)$ über $\mathbb{F}_p$ ab. Hierbei bildet ϕ alle anderen Erzeuger auf 1 ab.
Somit ist die erzeugenden Menge von $\phi(G_r)$ minimal und es gilt :

$$|\phi(G_r)| = p^{r + \frac{1}{2}r(r-1)}$$

Nun ist $G_r/\phi(G_r)$ wieder eine abelsche Gruppe und hat die Bilder von $x_1, \ldots, x_r$ als minimales Erzeugendensystem.
$\Rightarrow \phi(G_r)$ hat Index p^r.

Sei nun $\alpha \in \mathrm{Aut}(G_r)$ ein Automorphismus, der die Identitätsabbildung auf G/G_r induziert. Es existiert also $h_1, \ldots, h_r \in \phi(G_r)$, so dass $\alpha(x_i) = x_i h_i$ für $i = 1, \ldots, r$ gilt. Da $\phi(G_r) \in Z(G_r)$ liegt und den Exponent p hat, gilt :

$$\alpha(x_i^p) = \alpha(x_i)^p = (x_i h_i)^p = x_i^p h_i^p = x_i^p.$$

Es gilt weiterhin

$$\alpha([x_j, x_i]) = [\alpha(x_j), \alpha(x_i)] = [x_j h_j, x_i h_i] = [x_j, x_i].$$

Somit wird $\phi(G_r)$ punktweise durch α fixiert. □

LEMMA 2.4. *Seien $N_1, N_2 \leq \phi(G_r)$. Dann ist $G_r/N_1 \cong G_r/N_2$ genau dann wenn ein $\alpha \in \mathrm{Aut}(G_r)$ existiert, so dass $\alpha(N_1) = N_2$ gilt.*

BEWEIS. Ein Element $\alpha \in G_r$, dass N_1 auf N_2 abbildet, induziert einen Isomorphismus α' von G_r/N_1 auf G_r/N_2. Wir müssen nun die Rückrichtung zeigen.
Sei $\alpha'(x_i N_1) = y_i N_2$. Da G_r aus der ϕ-Klasse 2 ist, impliziert Lemma 2.2, dass ein Homomorphismus $\alpha : G_r \to G_r$ existiert, so dass $\alpha(x_i) = y_i$. Da nun α^i ein Isomorphismus ist, erzeugen $y_1, \ldots, y_r$ und N_2 zusammen G_r. Aber auch $y_1, \ldots, y_r$ und $\phi(G_r)$ erzeugen G_r, da $N_2 \leq \phi(G_r)$ gilt. Somit folgt aus einem Lemma aus dem ersten Vortrag, dass $y_1, \ldots, y_r$ G_r erzeugt. Die Elemente $y_1, \ldots, y_r$ sind nun auf das Bild von α beschränkt. Somit ist α surjektiv.
Aus der Endlichkeit von G_r folgt nun, dass es $\alpha \in Aut(G_r)$ ist.
Es bleibt noch zu zeigen, dass $\alpha(N_1) = N_2$ gilt. Die Definition von α zeigt uns, dass $\alpha(x)N_2 = \alpha'(xN_1)$ gilt, wenn x einer der Erzeuger ist. Somit gilt dann, dass $\alpha(x)N_2 = \alpha'(xN_1) \forall x \in G_r$. Anders gesagt kommutiert die folgende Abbildung:

$$\begin{array}{ccc} G_r & \xrightarrow{\alpha} & G_r \\ \downarrow & & \downarrow \\ G_r/N_1 & \xrightarrow{\alpha'} & G_r/N_2. \end{array}$$

Man kann hier sehen, dass $\alpha(N_1) = N_2$ gilt. □

SATZ 2.5. *Sei r eine positive ganze Zahl und sei s ganzzahlig, so dass $1 \leq s \leq \frac{1}{2}r(r+1)$ gilt. Dann existieren mindestens $p^{\frac{1}{2}rs(r+1)-r^2-s^2}$ Isomorphieklassen von Gruppen der Ordnung p^{r+s}.*

BEWEIS. Sei G_r eine Gruppe, wie oben. Sei X die Menge der Untergruppen $N \leq \phi(G_r)$ mit Index p^s in $\phi(G_r)$. Für jede Untergruppe $N \in X$ erhalten wir eine Gruppe G_r/N mit Ordnung p^{r+s}. Dank Lemma 2.4 wissen wir, dass die Menge der Isomorphieklassen für Gruppen, die man auf diese Weise erhält, in Bijektion mit der Menge der Bahnen von $\mathrm{Aut}(G_r)$ auf X steht.
Sei θ ein natürlicher Homomorphismus für $\mathrm{Aut}(G_r)$ nach $\mathrm{Aut}(G_r/\phi(G_r))$. Durch Lemma 2.3 wissen wir, dass jedes $\alpha \in \ker(\theta)$ $\phi(G_r)$ punktweise fixiert und somit trivial auf X operiert. Somit enthält $\ker(\theta)$ den Stabilisator von jedem Element von X. Die Länge jeder Bahn von $\mathrm{Aut}(G_r)$, die auf X operiert, maximal

$$|\mathrm{Aut}(G_r)|/|\ker(\theta)| \leq |\mathrm{Aut}(G_r/\phi(G_r))|$$

Wir können nun $G_r/\phi(G_r)$ als Vektorraum über $\mathbb{F}_p$ auffassen. Die Gruppenautomorphismen korrespondieren dann direkt mit inversen linear Transformationen.

Somit gilt:

$$|\operatorname{Aut}(G_r/\phi(G_r))| = |\operatorname{GL}(r,p)| \leq p^{r^2} \tag{1}$$

Somit hat jede Bahn von X die maximale Länge p^{r^2}. □

SATZ 2.6. *Die Anzahl von p-Gruppen mit Ordnung p^m, $f(p^m)$ ist mindestens*

$$p^{\frac{2}{27}m^2(m-6)}.$$

BEWEIS. Für $m \leq 6$ ist es trivial, da hier $p^0 = 1$ gilt.
Für $m > 6$ definieren wir s wie folgt:

$$s = \begin{cases} \frac{1}{3}m, \text{ wenn } m \equiv 0 \bmod 3 \\ \frac{1}{3}(m+2), \text{ wenn } m \equiv 1 \bmod 3 \\ \frac{1}{3}(m+1), \text{ wenn } m \equiv 2 \bmod 3. \end{cases}$$

und wir definieren $r = m - s$. Nun können wir Satz 2.5 anwenden. Am Beispiel von $s = \frac{1}{3}$ zeigen wir, wie sich die Wahl von s ergibt:

$$s = \frac{1}{3} \Rightarrow r = m - s = \frac{2}{3}m \Rightarrow \frac{1}{2}r(r+1) = \frac{1}{3}m(\frac{5}{3}m) = \frac{5}{9}m^2$$

$$m \bmod 3 = 0 \Rightarrow m = 3n \rightarrow s = n, r = 2n \rightarrow \frac{1}{2}r(r+1) = 5n^2 \Rightarrow s \leq \frac{r(r+1)}{2}.$$

Somit wissen wir nun, dass $f(p^m) \geq p^{\frac{1}{2}rs(r+1)-r^2-s^2}$ gilt. Setzen wir nun unser s ein, so können wir die Schranke bestimmen. Zum einfacheren berechnen, betrachten wir das p nicht.

1. Fall: $s = \frac{1}{3}m \Rightarrow r = \frac{2}{3}m$, d.h.

$$\begin{aligned} &\frac{1}{2}(\frac{2}{3}m)(\frac{1}{3}m)(\frac{2}{m}m+1) - (\frac{2}{3}m)^2 - (\frac{1}{3}m)^2 \\ &= \frac{2}{27}m^3 + \frac{1}{9}m^2 - \frac{4}{9}m^2 - \frac{1}{9}m^2 \\ &= \frac{2}{27}m^3 - \frac{4}{9}m^2 \\ &= \frac{2}{27}m^2 \cdot (m-6). \end{aligned}$$

2. Fall: $s = \frac{1}{3}(m+2) \Rightarrow r = m - \frac{1}{3}(m+2) = \frac{2}{3}m - \frac{2}{3}$, d.h.

$$\begin{aligned} &\frac{1}{2}(\frac{2}{3}m - \frac{2}{3})(\frac{1}{3}m + \frac{2}{3})(\frac{2}{3}m - \frac{2}{3} + 1) - (\frac{2}{3}m - \frac{2}{3})^2 - (\frac{1}{3}m + \frac{2}{3})^2 \\ &= \frac{2}{27}(m^3 - 6^m 2 + \frac{9}{2}m - 13) \geq \frac{2}{27}m^2(m-6). \end{aligned}$$

3. Fall: $s = \frac{1}{3}(m+1) \Rightarrow r = m - \frac{1}{3}(m+1) = \frac{2}{3}m - \frac{1}{3}$, d.h.

$$\begin{aligned} &\frac{1}{2}(\frac{2}{3}m - \frac{1}{3})(\frac{1}{3})(m+1)(\frac{2}{3}m - \frac{1}{3} + 1) - (\frac{1}{3}m + \frac{1}{3})^2 - (\frac{2}{3}m - \frac{1}{3})^2 \\ &= \frac{2}{27}(m^3 - 6m^2 + 3m - \frac{7}{2}) \geq \frac{2}{27}m^2(m-6). \end{aligned}$$

Somit ist das Ergebnis aus Fall 1 unsere untere Schranke. □

KAPITEL 4

Sylowsysteme und Fittingsuntergruppe

Viktor Nikolai

1. Einleitung

Dieses Seminar dient der Vorbereitung auf den Beweis des Satzes von Pyber für auflösbare Gruppen. Da die Eigenschaft der Auflösbarkeit einer Gruppe zentral für die folgenden Definitionen und Zusammenhänge ist, wird der Begriff zunächst einmal wiederholt und es werden naheliegende Beispiele dafür angeführt.

Definition 1.1 (auflösbare Gruppen). Eine Gruppe G heißt *auflösbar*, wenn es eine Kette

$$\{1_G\} = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_n = G$$

von Untergruppen von G gibt, sodass G_{i-1} für alle $i = 1, \ldots, n$ ein Normalteiler in G_i ist und die zugehörigen Faktorgruppen G_i/G_{i-1} abelsch sind.
Beispiele:

(1) abelsche Gruppen, nilpotente Gruppen
(2) Gruppen der Ordnung $p^n q^m$ mit p, q prim und $n, m \in \mathbb{N}$ (Satz von Burnside)
(3) endliche Gruppen ungerader Ordnung (Satz von Feit-Thompson)

2. Hallsche Untergruppen

Nun werden die hallschen Untergruppen eingeführt und es wird eine Verallgemeinerung der Sylow-Sätze für auflösbare Gruppen bewiesen.

Definition 2.1 (Hallsche Untergruppen). Sei G eine endliche Gruppe. Eine Untergruppe H von G heißt *hallsche Untergruppe*, falls $|H|$ und $|G : H|$ teilerfremd sind.
Sei π eine Menge von Primzahlen. Eine Untergruppe H von G heißt *hallsche π-Untergruppe*, falls $|H|$ ein Produkt von Primzahlen in π ist und $|G : H|$ ein Produkt von Primzahlen nicht in π ist.

Satz 2.2 (Satz von Hall). *Sei G eine auflösbare Gruppe der Ordnung $p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$. Seinen weiterhin $r \in \mathbb{N}$ mit $1 \leq r \leq k$ und $\pi = \{p_1, p_2, \ldots, p_r\}$. Dann gelten:*

(1) *G hat eine hallsche π-Untergruppe (der Ordnung $p_1^{\alpha_1} \cdot \ldots \cdot p_r^{\alpha_r}$).*
(2) *Je zwei hallsche π-Untergruppen sind konjugiert in G.*
(3) *Jede π-Untergruppe von G ist in einer hallschen π-Untergruppe von G enthalten.*

Beweis. Der Beweis erfolgt per vollständiger Induktion nach $|G|$. Für $|G| = 1$ ist der Satz trivial. Seinen im Folgenden $|G| > 1$ und der Satz wahr für alle Gruppen der Ordnung kleiner $|G|$.

Sei nun M ein minimaler Normalteiler von G. Da G auflösbar ist, ist $M/\{1_G\} = M$ abelsch und kann zudem als endliche einfache Gruppe aufgefasst werden. Damit ist $|M| = p$ für eine Primzahl p, die n teilt. Nach der Induktionsvoraussetzung hat G/M eine hallsche π-Untergruppe K/M. Weiterhin sind solche Untergruppen konjugiert in G/M und jede π-Untergruppe von G/M ist in einer hallschen π-Untergruppe von G/M enthalten. Der Beweis wird nun in zwei Fälle aufgeteilt.
Fall 1: $p \in \pi$. Dann ist K eine hallsche π-Untergruppe von G und (1) ist erfüllt.
Falls H eine beliebige hallsche π-Untergruppe von G ist, dann ist $M \subseteq H$, da HM eine π-Untergruppe ist. Außerdem ist H/M eine hallsche π-Untergruppe von G/M und nach der Induktionsvoraussetzung gilt $(gM)^{-1}(H/M)(gM) = K/M$ für ein $gM \in G/M$. Das bedeutet aber, dass $K = g^{-1}Hg$. Also gilt (2).
Sei schließlich L eine π-Untergruppe von G. Dann ist LM/M eine hallsche π-Untergruppe von G/M und damit in einer hallsche π-Untergruppe H/M von G/M enthalten. Doch dann ist H eine hallsche π-Untergruppe von G und $L \subseteq H$. So folgt (3) und der Induktionsschritt ist für Fall 1 gezeigt.
Fall 2: $p \notin \pi$. (Hier wird der Satz von Schur-Zassenhaus benötigt, welcher in Kapitel 7 des Buches 'Enumeration of Finite Groups' von S. R. Blackburn, P. M. Neumann und G. Venkataraman bewiesen wird.) In diesem Fall sind $|K/M|$ und $|M|$ teilerfremd. Der Satz von Schur-Zassenhaus impliziert dann, dass ein Komplement H zu M in K existiert und dass je zwei Komplemente konjugiert in K sind. Dann aber gilt $|H| = |K/M|$. Also ist H eine hallsche π-Untergruppe von G und es folgt (1).
Sei nun H_1 eine hallsche π-Untergruppe von G. Dann ist H_1M/M eine hallsche π-Untergruppe von G/M und nach Induktionsvoraussetzung existiert ein g_1 in G, sodass $(g_1M)^{-1}(H_1M/M)(g_1M) = K/M$. Damit ist $H_2 := g_1^{-1}H_1g_1 \leq K$. Weiter ist H_2 ein Komplement zu M in K und der Satz von Schur-Zassenhaus besagt, dass H_2 und H konjugiert sind, womit (2) eintritt.
Sei jetzt L eine π-Untergruppe von G. Dann ist LM/M enthalten in einer hallschen π-Untergruppe K_1/M von G/M. Da alle hallschen π-Untergruppen von G/M konjugiert in G/M sind, sind auch K_1 und K konjugiert in G. Also existiert ein Konjugat L_1 von L, sodass $L_1 \leq K$. Mit $K = HM$ ist dann $L_1M = L_1M \cap HM = (L_1M \cap H)M$. Nun sind L_1 und $L_1M \cap H$ Komplemente zu M in L_1M und folglich konjugiert nach dem Satz von Schur-Zassenhaus. Damit ist L_1 konjugiert zu einer Untergruppe von H und L ist enthalten in einer hallschen π-Untergruppe von G. Also gilt (3) und der Induktionsschritt ist auch für Fall 2 gezeigt. □

3. Sylowsysteme

Die Resultate aus Kapitel 2 werden im Folgenden unter Zuhilfenahme der Sylowsysteme weiter präzisiert.

Definition 3.1 (Sylowsysteme). Sei G eine Gruppe der Ordnung $p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$. Ein *Sylowsystem* in G ist eine Familie von Untergruppen $\{P_1, \ldots, P_k\}$, wobei P_i eine Sylow-p_i-Untergruppe ist und $P_iP_j = P_jP_i$ für alle $i, j \in \{1, \ldots, k\}$ gilt.
Bemerkung: Falls $i \neq j$, dann ist P_iP_j eine Untergruppe von G der Ordnung $p_i^{\alpha_i}p_j^{\alpha_j}$. Falls weiter $\pi \subseteq \{p_1, p_2, \ldots, p_k\}$, dann ist $\prod_{p_i \in \pi} P_i$ eine hallsche π-Untergruppe von G.

Satz 3.2 (Satz von Hall, präzisere Version). *Sei G eine auflösbare Gruppe der Ordnung $p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$. Dann gelten:*

(1) *G hat ein Sylowsystem.*

(2) *Je zwei Sylowsysteme sind konjugiert in G.*
(3) *Falls $H \leq G$ und $\{Q_1, \ldots, Q_k\}$ ein Sylowsystem in H ist, dann existiert ein Sylowsystem $\{P_1, \ldots, P_k\}$ in G, sodass $Q_i = H \cap P_i$ für alle $i \in \{1, \ldots, k\}$.*

4. Fittinguntergruppe

Dieses Kapitel enthält grundlegende Resultate, die sich auf die Fittinguntergruppe beziehen, welche unter bestimmten Voraussetzungen als der maximale nilpotente Normalteiler einer Gruppe verstanden werden kann.

BEMERKUNG 4.1. Falls P und Q normale p-Untergruppen von G sind, dann ist PQ eine normale p-Untergruppe, die P und Q enthält. Falls P und Q zudem maximal sind, dann gilt $P = PQ = Q$. Damit existiert eine eindeutige maximale normale p-Untergruppe von G. Bezeichne diese mit $O_p(G)$.

DEFINITION 4.2 (Fittinguntergruppe). $F(G) := \langle O_p(G) \mid p \textit{ ist eine Primzahl} \rangle$ heißt *Fittinguntergruppe* von G.
Bemerkung: Falls p und q unterschiedliche Primzahlen sind, gilt $[O_p(G), O_q(G)] \leq \overline{O_p(G) \cap O_q(G)} = \{1_G\}$. Somit folgt $F(G) = O_{p_1}(G) \times \cdots \times O_{p_k}(G)$, wobei $p_1, \ldots, p_k$ paarweise verschiedene Primzahlen sind, die $|G|$ teilen. Insbesondere ist $F(G)$ das direkte Produkt seiner Sylowuntergruppen und damit nilpotent.

HILFSSATZ 4.3. *Sei G eine endliche Gruppe. Dann ist $F(G)$ der eindeutige maximale nilpotente Normalteiler von G.*

SATZ 4.4. *Sei G eine endliche Gruppe, und sei S der eindeutige maximale auflösbare Normalteiler von $C_G(F(G)) = \{g \in G \mid \forall f \in F(G) : fg = gf\}$. Dann ist $S = Z(F(G))$.*

KOROLLAR 4.5. *Falls G eine endliche auflösbare Gruppe ist, gilt*

$$C_G(F(G)) = Z(F(G))$$

.

BEWEIS. Da G auflösbar ist, ist $C_G(F(G))$ als Untergruppe von G ebenfalls auflösbar. Der maximale auflösbare Normalteiler von $C_G(F(G))$ ist also $C_G(F(G))$ selbst. Mit Satz 4.4 und $S = C_G(F(G))$ folgt die Behauptung. □

5. Verhältnis zwischen Fittinguntergruppe und Frattiniuntergruppe

Schließlich wird der Satz von Gaschütz bewiesen, der eine wichtige Aussage über die Beziehung zwischen der Fittinguntergruppe und der Frattiniuntergruppe liefert. Zur Vorbereitung des Beweises werden die folgenden Lemmata benötigt.

LEMMA 5.1. *Seien N eine endliche Gruppe und K ein Normalteiler von N, wobei N/K nilpotent ist. Dann sind je zwei Sylow-p-Untergruppen von N konjugiert durch ein Element in K.*

BEWEIS. Seien P_1 und P_2 Sylow-p-Untergruppen von N. Dann sind P_1K/K und P_2K/K Sylow-p-Untergruppen von N/K. Da N/K nilpotent ist, ist dessen Sylow-p-Untergruppe eindeutig. Somit ist $P_1K/K = P_2K/K$. Also ist $P_1K = P_2K$ und und P_2 ist eine Sylow-p-Untergruppe von P_1K. Damit ist $P_2 = y^{-1}P_1y$ für $y \in P_1K$. Setze nun $y = xk$ für $x \in P_1$ und $k \in K$. Dann folgt $P_2 = y^{-1}P_1y = k^{-1}P_1k$. □

LEMMA 5.2 (Verallgemeinerung des Frattini-Arguments). *Seien G eine endliche Gruppe und N ein Normalteiler von G. Sei weiterhin K ein Normalteiler von N, sodass N/K nilpotent ist. Dann gilt für jede Sylow-Untergruppe P von N der Zusammenhang $G = N_G(P)K = \{g \in G \mid g^{-1}Pg = P\}K$.*

BEWEIS. Sei $g \in G$. Dann ist $g^{-1}Pg$ eine Sylow-Untergruppe von N. Nach Lemma 5.1 existiert ein $k \in K$, sodass $g^{-1}Pg = k^{-1}Pk$. Daraus folgt $kg^{-1}Pgk^{-1} = P$ und damit $gk^{-1} \in N_G(P)$. Also ist $g \in N_G(P)K$ und folglich $G = N_G(P)K$. □

DEFINITION 5.3 (Frattiniuntergruppe). $\Phi(G)$ definiert als der Schnitt aller maximalen Untergruppen von G heißt *Frattiniuntergruppe* von G.

HILFSSATZ 5.4. *Seien G eine endliche Gruppe und N ein Normalteiler von G. Falls $\Phi(G) \subseteq N$ und $N/\Phi(G)$ nilpotent ist, ist auch N nilpotent. Insbesondere ist dann $\Phi(G)$ nilpotent und folglich gilt $\Phi(G) \leq F(G)$.*

SATZ 5.5 (Satz von Gaschütz). *Falls G endlich ist, gilt*

$$F(G/\Phi(G)) = F(G)/\Phi(G)$$

.

BEWEIS. Sei N eine Untergruppe von G mit $\Phi(G) \subseteq N$ und $N/\Phi(G) = F(G/\Phi(G))$. Es genügt, zu zeigen: $F(G) = N$.
Nach Hilfssatz 5.4 ist $\Phi(G) \subseteq F(G)$. Da außerdem $F(G)/\Phi(G)$ ein nilpotenter Normalteiler von $G/\Phi(G)$ ist, gilt nach Hilfssatz 4.3 $F(G)/\Phi(G) \subseteq F(G/\Phi(G))$. Damit ist $F(G) \subseteq N$. Weiterhin ist N nach Hilfssatz 5.4 nilpotent, weil $F(G/\Phi(G))$ nilpotent ist. Also ist $N \subseteq F(G)$ und somit $N = F(G))$. □

KAPITEL 5

Primitive Permutationsgruppen

Ahmed Sato

Satz 0.1. *Sei X eine Menge der Ordnung n und sei G eine Permutationsgruppe, die auf X wirkt. Wenn G r Bahnen auf X hat, dann kann G von $(n-r)$ Elementen erzeugt werden.*

Beweis. Wir beweisen diesen Satz per Induktion.

$n = r \implies G$ ist trivial und dann man erhält das Ergebnis, da jedes Element eine Bahn ist, also keine echte Wirkung vorliegt.

Angenommen, G hat r Bahnen auf X und sei ω ein Element, das in einer nicht-trivialen Bahn Δ liegt. Wir können Δ schreiben: $\Delta = \Delta_1 \cup \Delta_2 \cup \cdots \cup \Delta_k$, wobei die Menge Δ_i die Bahnen des Stabilisators G_ω von ω in G seien.

Wir können annehmen, dass $\Delta_k = \{\omega\}$ ist. Da Δ eine nicht-triviale Bahn ist; $k > 1$; für $i \in \{1, 2, 3, \ldots, k\}$, sei $g_i \in G$, sodass $g_i\omega \in \Delta_i$ liegt. Nun wird G von G_ω und $(k-1)$ Elementen $g_1, g_2, \ldots, g_{k-1}$, zusammen erzeugt. Aber G_ω hat mindestens $k + (r-1)$ Bahnen auf X.

Nach unserer Induktionsannahme kann G_ω von $n - (r - k - 1)$ Elementen erzeugt werden. Folglich, wenn man die Zahlen zusammen rechnet, kann G von $n - r$ Elementen erzeugt werden. □

1. Primitivität

Definition 1.1. Die Gruppe G operiere auf der Menge X.

(1) Eine Teilmenge $B \subset X$ heißt *Block* unter der Operation von G (kurz G-Block), wenn gilt: $\sigma B = B \bigvee \sigma B \cap B = \Phi$ für alle $\sigma \in G$. Offenbar sind X , Φ Blöcke bezüglich jeder Operation auf X. Diese sind die sog. trivialen Blöcke.

(2) Die Operation von G heißt *primitiv* auf X, wenn sie transitiv ist und nur die trivialen Blöcke besitzt.

Zur Erinnerung: Eine Gruppenoperation heißt transitiv, wenn sie nur eine Bahn hat, wenn also jedes Element überall hin abgebildet wird.

- Jede transitive Gruppe von Primzahlgrad ist primitiv.
- S_3 wirkt auf $X = \{1, 2, 3\}$ primitiv. Im allgemeinen S_n wirkt auf der Menge $X = \{1, 2, 3, \ldots, n\}$ primitiv, für alle $n > 2$.

Lemma 1.2. *Sei G eine primitive Permutationsgruppe, die auf X wirkt. Sei N ein Normalteiler von G (nicht trivial), dann N ist transitiv.*

Beweis. Wir definieren eine Äquivalenzrelation ρ auf der Menge X, sodass $\alpha \sim_\rho \beta$ genau dann wenn $\exists\ h \in N$; $h\alpha = \beta$. Mit anderen Worten: $\alpha \sim_\rho \beta \Leftrightarrow \alpha$ und β liegen in der selben Bahn (N-Bahn).

Sei $g \in G$ und α , $\beta \in X$; $\alpha \sim_\rho \beta$ und $h \in N$; $h\alpha = \beta$. Da N ein Normalteiler ist, gilt $gh = h'g$ für manche $h' \in N$, also $h'g\alpha = gh\alpha = g\beta$, und $g\alpha \sim_\rho g\beta$ analog $g\alpha \sim_\rho g\beta$, was bedeutet $\alpha \sim_\rho \beta$ und so ist ρ eine Kongruenz. Die Bahnen von N sind die Blöcke von ρ. Da N nicht trivial ist, ist ρ nicht die triviale Äquivalenzrelation. Da G primitiv ist, bedeutet das, dass ρ die Äquivalenzrelation ist, die alles miteinander identifzieret. Mittels der Defintion von ρ wird N transitiv gezeigt. □

DEFINITION 1.3. *Das Kranzprodukt* (engl. Wreath product) bezeichnet ein spezielles semidirektes Produkt von Gruppen. Seien G und H endliche Gruppen, und sei $H^G := \{f \ ; \ G \to H \ \}$, die Menge aller Funktionen von G nach H bezüglich punktweiser Operationen : $(f_1 \ f_2)(x) := f_1(x) \ f_2(x)$, sodass H^G eine Gruppe ist. Dann G wirkt auf H^G ; $g \to f^g$ mit $f^g(x) = f(xg)$.

Das reguläre Kranzprodukt $H \wr G$ von H mit G ist das semidirekte Produkt von H^G mit G bezüglich ebendieser Wirkung.

$$H \wr G := H^G \rtimes G \text{ oder anderes Symbol } H \wr G := H \mathrm{wr} G$$

DEFINITION 1.4. *Das semidirekte Produkt*: Seien N, H zwei Gruppen und H wirkt auf N durch Automorphismen : $\alpha : H \to \mathrm{Aut}(N)$. Die kartesische Produkt $N \times H = \{(n, h) \mid n \in N, h \in H\}$ mit der Komposition $(n_1, h_1)(n_2, h_2) = (n_1\alpha(h_1)(n_2), h_1h_2)$ ist eine Gruppe G, genannt das externe semidirekte Produkt von N mit H.

Notation : $G = N \rtimes_\alpha H$, das externe semidirekte Produkt von N mit H bezüglich der Wirkung α.

SATZ 1.5. *Sei G eine primitive auflösbare Permutationsgruppe, die auf Ω wirkt. Sei M ein minimaler Normalteiler von G.*

(1) *M wirkt regulär auf Ω, also $|\Omega| = |M| = p^d$.*
(2) *$\alpha \in \Omega$. Sei G_α der Stabilisator von α in G. Dann ist $G = M \rtimes G_\alpha$.*

SATZ 1.6. *Sei G eine transitive Permutationsgruppe, die auf der Menge Ω wirkt.*

Sei $\rho_0 < \rho_1 < \rho_2 \cdots < \rho_r$ eine maximale Kette von Äquivalenzrelationen. Wir definieren eine Ordnung der Menge der Äquivalenzrelationen $\rho \leq \rho\prime$, sodass jede eine Äquivalenzklasse von ρ in der Äquivalenzklasse von $\rho\prime$ enthalten ist. Seien $\Delta_0 \subseteq \Delta_1 \subseteq \cdots \subseteq \Delta_r$ die Äquivalenzklassen, sodass Δ_i die Klasse von ρ_i ist.

Für alle $i \in \{1, 2, \ldots, r\}$ sei x_i die Menge aller Äquivalenzklassen von $\rho_i - 1$ enthalten in Δ_i.

Sei G_i die Gruppe $(G_{\Delta_i})^{x_i}$ der Permutationen von x_i und G_i wird von dem Stabilisator G_{Δ_i} von Δ_i erzeugt.

Dann sind diese Gruppe G_i primitiv und wir können X mit

$$\Omega_1 \times \Omega_2 \times \cdots \times \Omega_r$$

in der Weise identifizieren, dass $G \leq G_1 \wr G_2 \wr \cdots \wr G_r$.

BEWEIS. Zuerst notieren wir, dass ρ_0 die triviale Äquivalenzrelation und ρ_r die universale Äquivalenzrelation, da die Kette maximal ist, was bedeutet, dass $\Delta_r = \Omega$. Es ist nicht schwerig, zu sehen, dass die Äquvalenzrelation ρ in G_i erhalten sind (Eins-zu- eins-Korrespondenz) mit dieser Äquivalenzrelationen ρ', die in G erhalten sind, sodass $\rho_{i-1} \leq \rho' \leq \rho_i$.

Hier, steht ein Block B von ρ in Korrespondenz zum Block $\bigcup_{\Gamma \in B} \Gamma$ von ρ' . Die restliche Blöcke von ρ' sind verschoben durch Elemente von G. Da die Kette $\rho_0 < \rho_1 < \cdots < \rho_r$ maximal ist, liegt keine Äquivalenzrelation echt zwischen ρ_{i-1}

und ρ_i und so ist G_i primitiv. Zu zeigen, dass G eingebettet in dem Kranzprodukt ist, benutzen wir Induktion nach der Länge r von der maximalen Kette der Äquivalenzrelationen.

Angenommen das Ergebnis ist wahr für eine maximale Kette von Äquivalenzrelation von kürzerer Länge. Sei $\Delta = \Delta_{r-1}$ und $H = (G_\Delta)^\Delta$, da G transitive Permutationsgruppe auf Ω, dann haben wir, dass H eine transitive Permutationsgruppe auf Δ ist. Die Beschränkung von $\rho_0, \rho_1, \ldots, \rho_{r-1}$ in Δ Formen ist eine maximale Kette von Äquivalenzrelationen enthalten in H. Nach unsererer Induktionsannahme kann Δ mit $\Omega_1 \times \Omega_2 \times \cdots \times \Omega_{r-1}$ identifiziert werden, sodass $H \leq G_1 \wr G_2 \wr \cdots \wr G_{r-1}$. Um die Proposition zu beweisen, ist daher ausreichend zu zeigen, dass Ω mit $\Delta \times \Omega_r$ identifiziert wird in der Weise , dass $G \leq H \wr G_r$. Sei $\Omega_r = \{\Gamma_1, \Gamma_2, \ldots, \Gamma_k\}$, da $\Delta_r = \Omega$, haben wir Ω_r ist die Menge alle Blöcke von ρ_{r-1} und Ω ist die disjunkte Vereinigung der Menge Γ_i. Da G transitiv ist, ist jede Block Γ_i von ρ_{r-1} Verschoben durch Δ Δ. Für $i \in \{1, 2, \ldots, k\}$ können wir $x_i \in G$ wählen, sodss $x_i \Delta = \Gamma_i$ ist.

Wir definieren eine Bijektion $f : \Omega \to \Delta \times \Omega_r$; mit $f(\alpha) = (x_i^{-1}\alpha, \Gamma_i)$ für alle $\alpha \in \Gamma_i$. Es ist nicht schwer zu überprüfen, sei $g \in G$ mit $fgf^{-1} \in \mathrm{Sym}\ (\Delta \times \Omega_r)$ eingebettet in $H \wr G_r$. Der Beweis folgt im folgenden.

Sei $g \in G$ und $y \in G$ eine Permutation von Ω_r wird induziert durch g. Sei $i \in \{1, 2, \ldots, k\}$, dann existiert $j \in \{1, 2, \ldots, k\}$, sodass $g^{-1}\Gamma_i = \Gamma_j$ ist. Nun $x_i^{-1} g x_j$ ist erhalten in Δ und $\implies$ $x_i^{-1} g x_j \in G_\Delta$. Sei h_i ein Element von H und wird durch $x_i^{-1} g x_j$ induziert. Dann ist es nicht schwer zu überprüfen, dass $fgf^{-1} = (h_1, h_2, \ldots, h_k)y \in H \wr G_r$ ist. □

Satz 1.7. *Sei G eine Gruppe wirkt treu und irreduziebel auf einem Vektorraum V. Angenommen, sei G imprimitiv, dann existiert eine Zahl $k \in \mathbb{Z}$, $k \leq 2$ und eine Zerlegung $V = V_1 \bigoplus V_2 \bigoplus \cdots \bigoplus V_k$ von V , sodass die Gruppe G die direkten Summanden permutiert.*

Sei $Q \leq Sym(k)$ eine Permutationsgruppe, die von der Wirkung von G auf der Menge des Summandes V_i induziert wird. Definiere $W = V_1$ und $H \leq \mathrm{GL}(W)$. (Die Gruppe H wird von dem Stabilisator von W in G induziert). Dann ist Q transitiv und H ist irreduzibel. Außerdem ist G isomorph zu einer linearen Gruppe und eine Untergruppe von $H \wr Q$.

Definition 1.8. Eine Darstellung ist *irreduzibel* ,wenn sie sich nicht auf blockdiagonale Form transformieren lässt.

Ist eine Darstellung Γ irreduzibel, bilden die einzelnen Blöcke der blockdiagonalen Form (Γ_i) selber Darstellungen der Gruppe. Die Darstellung Γ ist dann eine sog. *direkte Summe* der einzelnen Darstellungen Γ_i:

$$\Gamma = \Gamma_1 \bigoplus \Gamma_2 \bigoplus \cdots \bigoplus \Gamma_i.$$

KAPITEL 6

Gruppenerweiterungen

Niklas Schaumann

1. Einleitung

Ziel dieses Abschnittes ist die Einführung von Gruppenerweiterungen. Dabei werden wir spezifisch auf die zweidimensionale Kohomologiegruppe und einige grundlegende Eigenschaften dieser eingehen.

2. Gruppenerweiterungen

Definition 2.1. Sei $M \trianglelefteq E$ und $G = E/\mathrm{M}$. Dann nennen wir E die Gruppenerweiterung von M durch G. Formal bedeutet dies, dass wir eine Kette folgender Form erhalten:

$$1 \longrightarrow M \overset{i}{\hookrightarrow} E \overset{\rho}{\twoheadrightarrow} G \longrightarrow 1$$

Dabei beschreibt i die natürliche Einbettung von M in E und $\rho : E \longrightarrow\!\!\!\!\!\rightarrow G$ die surjektive Abbildung, mit $\ker(\rho) = i(M)$.

Definition 2.2. Zwei Erweiterungen E und E' von M heißen äquivalent, falls ein Homomorphismus $\Phi : E \to E'$ existiert, sodass folgendes Diagramm kommutiert:

$$\begin{array}{ccccccc} 1 & \longrightarrow & M & \overset{i}{\hookrightarrow} & E & \overset{\rho}{\twoheadrightarrow} & G \longrightarrow 1 \\ & & \mathrm{id}\downarrow & & \Phi\downarrow & & \mathrm{id}\downarrow \\ 1 & \longrightarrow & M & \overset{i}{\hookrightarrow} & E' & \overset{\rho}{\twoheadrightarrow} & G \longrightarrow 1 \end{array}$$

Dies bedeutet insbesondere, dass gelten muss:

$$\rho'(\Phi(i(m))) = \rho(\Phi^{-1}(i'(m))) \text{ (für } m \in M).$$

Bemerkung 2.3. Aus der Tatsache, dass Φ^{-1} eindeutig und wohldefiniert sein muss, erkennt man, dass Φ bijektiv sein muss. Also haben wir einen bijektiven Homomorphismus und für zwei äquivalente Erweiterungen E und E' gilt:

$$E \cong E'.$$

Für den Rest des Vortrags betrachten wir den Fall, dass M eine abelsche multiplikative Gruppe ist.

Bemerkung 2.4. Da $i : M \to E$ einen Homomorphismus darstellt und wir M als abelsch voraussetzen, können wir M in Form von $i(M)$ als abelsche Untergruppe von E interpretieren. Dann ist $i(M) \trianglelefteq E$ und E operiert auf natürliche Weise durch Konjugation auf M. Damit liegt M dann im Kern dieser Gruppenoperation und $E/M \cong G$ operiert auch auf natürliche Weise auf M.

BEMERKUNG 2.5. Falls E und E' äquivalent sind, induzieren Sie dieselbe Gruppenoperation von G auf M.

Wir betrachten nun den Fall, dass M ein $\mathbb{Z}G$-Modul ist. Dann existiert immer eine natürliche Gruppenerweiterung E auf M, welche die Gruppenoperation von G auf M induziert. Diese erhält man dann aus dem semi-direkten Produkt von M und G ($E = M \rtimes G$), welche man durch die Gruppenoperation von G auf M erhält.

3. Die zweite Kohomologie-Gruppe

Wir wollen nun alle Gruppenerweiterungen E beschreiben, welche durch die Gruppenoperation von G auf M induziert werden. Dabei werden wir die zweite Kohomologie-Gruppe $H^2(G, M)$ Schritt für Schritt konstruieren und einige Eigenschaften dieser festhalten.

DEFINITION 3.1. Zunächst sei $S := \{s_g \in E \mid g \in G\}$ eine Vertretermenge von Elementen aus M in E und ρ die surjektive Einbettung von E in G, sodass gilt: $\rho(s_g) = g$. Dabei können wir o.B.d.A. annehmen, dass $s_1 = 1$ gilt. Für $g \in G$ beschreibt $g \cdot m = m^{s_g} = s_g m s_g^{-1}$ die durch Konjugation erhaltene Gruppenoperation von G auf M.

BEMERKUNG 3.2. Wir wollen nun einige Eigenschaften der s_g betrachten. Zunächst stellen wir fest, dass für $g, h \in G$ die Elemente $s_g s_h$ und s_{gh} das selbe Bild unter der Abbildung ρ haben, da ρ ein Homomorphismus ist. Also gilt: $\rho(s_g s_h) = \rho(s_{gh})$.

Nun wissen wir, dass es ein eindeutiges Element $f(g, h) \in M$ geben muss, sodass:

$$s_g s_h = f(g, h) s_{gh} \text{ (für } f : G \times G \to M)$$

Da wir $s_1 = 1$ voraussetzen folgt:

$$f(g, 1) = 1 = f(1, h) \ (\forall g, h \in G).$$

Die Gruppeneigenschaften von E implizieren direkt folgende Eigenschaften von f, seien $g, h, k \in G$:

$$f(g, h) f(gh, k) = (g \cdot f(h, k)) f(g, hk).$$

DEFINITION 3.3. Eine Abbildung $f : G \times G \to M$, welche diese Eigenschaften erfüllt nennen wir eine Faktorgruppe. Die Menge aller Faktorgruppen von $G \times G \to M$ bezeichnen wir mit $Z^2(G, M)$.

BEMERKUNG 3.4. Wir können nun $Z^2(G, M)$ selbst als Gruppe auffassen, indem wir uns folgende Addition definieren.
Seien dazu $f, f' \in Z^2(G, M)$, $g, h \in G$:

$$(f + f')(g, h) = f(g, h) f'(g, h).$$

Da f und f' nach M abbilden, erkennt man sofort, dass diese Gruppe auch abelsch sein muss, denn wir setzten M selbst als abelsch voraus.
Das heißt, dass f eindeutig bestimmt wird von einem gegebenen $\mathbb{Z}G$-Modul M, einer Gruppenerweiterung E auf M, welche durch G induziert wird und einer Vertretermenge $S = \{s_g \mid g \in G\}$ für M in E, mit $s_1 = 1$. Dabei ist es wichtig zu merken, dass f auch tatsächlich von der Wahl der Vertretermenge S abhängt. Seien dazu S und S' zwei verschiedene Vertretermengen, mit $s_1 = s'_1 = 1$. Dann

existiert für jedes $g \in G$ ein Element $a(g) \in M$, sodass $s'_g = a(g)s_g$ gilt. Dann beschreibt $a : g \to M$ eine Funktion, mit $a(1) = 1$ und wir erhalten eine neue Faktorgruppe $f' \in Z^2(G, M)$. Für f, f' und $g, h \in G$ gilt dann:

$$\begin{aligned} f'(g,h) &= s'_g s'_h s_{gh}^{-1} \\ &= a(g)s_g a(h)s_h(a(gh)s_{gh}^{-1}) \\ &= a(g)(s_g a(h)s_g^{-1})s_g s_h s_{gh}^{-1} a(gh)^{-1} \\ &= a(g)(g \cdot a(h))f(g,h)a(gh)^{-1} \\ &= (g \cdot a(h))a(gh)^{-1}a(g)f(g,h). \end{aligned}$$

Dann sind f und f' für verschiedene S und S' auch verschieden.

Definition 3.5. Zu einer gegebenen Abbildung $a : G \to M$ definieren wir uns eine Abbildung $\delta a : G \times G \to M$, sodass für alle $g, h \in G$ gilt:

$$\delta a(g,h) = (g \cdot a(h))a(gh)^{-1}a(g)f(g,h) \quad [1]$$

Dann ist δa eine Faktorgruppe aus $Z^2(G, M)$ und wir definieren

$$B^2(G, M) := \{\delta a | a : G \to M, a(1) = 1\}.$$

Bemerkung 3.6. Wir betrachten nun zwei Abbildungen $a : G \to M$ und $b : G \to M$, mit $a(1) = b(1) = 1$. Für $g \in G$ können wir dann eine Addition auf der Menge $H := \{a : G \to \mathrm{M} |\ a(1) = 1\}$ folgendermaßen definieren:

$$(a + b)(g) = a(g)b(g).$$

Dann beschreibt $\delta : H \to Z^2(G, M)$ einen Gruppenhomomorphismus, denn für $a, b \in H$ und $g, h \in G$ gilt:

$$\begin{aligned} (\delta(a+b)(g,h) &= (g \cdot (a+b)(h))((a+b)(gh))^{-1}(a+b)(g) \\ &= (g \cdot a(h)(b(h))(a(gh)b(gh))^{-1}a(g)b(g) \\ &= (s_g a(h)b(h)s_g^{-1})(a(gh)b(gh))^{-1}a(g)b(g) \\ &= (s_g a(h)s_g^{-1}s_g b(h)s_g^{-1})b(gh)^{-1}a(gh)^{-1}a(g)b(g) \\ &= (s_g a(h)s_g^{-1}a(gh)^{-1}a(g)(s_g b(gh)s_g^{-1}b(gh)^{-1}b(g) \\ &= \delta a(g,h) + \delta b(g,h). \end{aligned}$$

Somit ist also δ ein Gruppenhomomorphismus und das Bild von $B^2(G, M)$ unter δ ist eine Untergruppe von $Z^2(G, M)$.

Definition 3.7. Wir definieren: $H^2(g, M) := Z^2(G, M)/B^2(G, M)$. Diese Gruppe nennen wir zweidimensionale Kohomologie-Gruppe auf M über G.

Bemerkung 3.8. Mit [1] folgt für $f, f' \in Z^2(G, M)$, welche von der gleichen Erweiterung E induziert werden:

$$f - f' = \delta a$$

Daher gilt schon:

$$f' - f \in B^2(G, M) \text{ oder } f + B^2(G, M) = f' + B^2(G, M).$$

Somit beschreiben also f und f' das selbe Element in $H^2(G, M)$.

Also beschreibt die durch eine Gruppenerweiterung induzierte Faktorgruppe ein eindeutiges Element aus $H^2(G,M)$ und jeder Gruppenerweiterung E lässt sich ein eindeutiges Element aus $H^2(G,M)$ zuordnen.

Damit haben wir die zweidimensionale Kohomologie-Gruppe eingeführt und uns bereits einige Eigenschaften klar gemacht, mit denen wir nun folgende Sätze beweisen können.

SATZ 3.9. *Zwei Erweiterungen von M über G sind genau dann äquivalent (d.h. isomorph) zu einander, wenn Sie dieselbe Gruppenoperation von G auf M und somit dasselbe Element aus $H^2(G,M)$ beschreiben.*

Den Beweis werden wir hier nicht genauer ausführen, allerdings schauen wir uns einmal die Idee dazu an.

BEWEIS. Wir wissen bereits, dass zwei äquivalente Erweiterungen, diesselbe Wirkung von G auf M induzieren, und es folgt leicht, dass äquivalente Erweiterungen dasselbe Element in $H^2(G,M)$ bestimmen.

Wenn wir nun zwei Erweiterungen E und E' betrachten, die dieselbe Wirkung von G auf M induzieren und dasselbe Element in $H^2(G,M)$ bestimmen, müssen wir zeigen, dass diese auch äquivalent sind. Dies geschieht, indem wir zeigen, dass die Multiplikation in E vollständig durch die Wirkung von G auf M und das Element $f+B^2(G,M)$ bestimmt wird. Dazu identifiziert man die Elemente in E und E' mit ms_g und ms'_g für Transversale $\{s_g \mid g\in G\}$ und $\{s'_g \mid g\in G\}$ für M in E und E'. Dann bildet die Abbildung

$$\Phi : E \to E', \quad \Phi(ms_g) = ma(g)^{-1}s'_g$$

einen gewünschten Homomorphismus, wobei a durch $f'-f=\delta a$ bestimmt ist. □

SATZ 3.10. *Sei M ein $\mathbb{Z}G$-Modul und sei*

$$\mathcal{M} := \{E \mid E \text{ ist Gruppenerweiterung von } M \text{ über } G\}.$$

Dann gelten:

1. *Es existieren eine bijektive Abbildung zwischen den Äquivalenzklassen auf $\mathcal{M}$ und $H^2(G,M)$.*
2. *Die Anzahl der Isomorphieklassen auf $\mathcal{M}$ beträgt höchstens $|H^2(G,M)|$.*

BEWEIS. Wir können eine Abbildung von den Äquivalenzklassen auf $\mathcal{M}$ nach $H^2(G,M)$ definieren, indem wir f mit $f+B^2(G,M)$ identifizieren. Mit Satz 3.9 folgt nun auch direkt, dass diese Abbildung injektiv und wohldefiniert sein muss. Also bleibt uns nur noch zu zeigen, dass diese Abbildung auch surjektiv ist.
Sei dazu $f'+B^2(G,M)\in H^2(G,M)$. Wir setzen $E := M\times G$ und definieren uns folgende Abbildung:

$$\phi : E'\times E' \to E', (m,g)(m',h) = (m(g\cdot m')f'(g,h), gh) \in E',$$

für $m,m'\in M$ und $g,h\in G$. Mit dieser Multiplikation können wir E' als Gruppe auffassen. Diese ist dann eine Erweiterung von M durch G und somit in $\mathcal{M}$ enthalten, welche das Element $f'+B^2(G,M)\in H^2(G,M)$ vollständig bestimmt. Also wird $f'+B^2(G,M)$ durch $E'\in\mathcal{M}$ bestimmt und wir erkennen, dass unsere Abbildung also surjektiv sein muss.
Die zweite Aussage folgt direkt aus Bemerkung 2.3 und (1). □

4. Die erste Kohomologie-Gruppe

Zuletzt wollen wir noch, der Vollständigkeit halber, die Definition der ersten Kohomologie-Gruppe einführen.

DEFINITION 4.1. Sei G eine Gruppe und M ein $\mathbb{Z}G$-Modul. Wie gewohnt sei die Wirkung von $g \in G$ auf $m \in M$ als $g \cdot m$ geschrieben. Sei $Z^1(G, M)$ die Menge aller Funktionen $f : G \to M$, mit $f(1) = 1$ und:

$$f(g_1 g_2) = (g_1 \cdot f(g_2))f(g_1) \quad \forall\ g_1, g_2 \in G$$

Solche Funktionen nennen wir Derivationen von G nach M. Mit der folgenden Verknüpfung wird auch $Z^1(G, M)$ zu einer Gruppe:

$$(f + f')(g) = f(g)f'(g) \text{ für } f, f' \in Z^1(G, M),\ g \in G$$

Wir betrachten nun die Funktionen $\delta_m : G \to M$, mit:

$$\delta_m(g) = (g \cdot m^{-1}m\ \forall g \in G$$

Diese Funktionen sind offensichtlich Derivationen, denn $\delta_m(1) = 1$ und es gilt:

$$\begin{aligned}\delta_m(g_1 g_2) &= (g_1 g_2 m^{-1}) \\ &= (g_1 \cdot ((g_2 \cdot m^{-1})mm^{-1}))m \\ &= (g_1 \cdot ((g_2 \cdot m^{-1})m))(g_1 \cdot m^{-1})m \\ &= (g_1 \cdot \delta_m(g_2))\delta_m(g_1).\end{aligned}$$

Die Funktionen δ_m bezeichnen wir als innere Derivationen. Die inneren Derivationen δ_m bilden dann als Menge eine Untergruppe von $Z^1(G, M)$ und die erste Kohomologie-Gruppe wird dann mit $H^1(G, M) := Z^1(G, M)/B^1(G, M)$ bezeichnet.

KAPITEL 7

Gruppenkohomologie

Niclas Janssen

1. Kohomologiegruppen n-ter Dimension

Sei $n \in \mathbb{N}$ und M ein $\mathbb{Z}G$-Modul. Wir definieren $C^n(G, M)$ als die Menge aller Abbildungen

$$f : G \times \cdots \times G \longrightarrow M$$

mit

$$f(g_1, \ldots, g_n) = 0,$$

wenn

$$\exists\, i \in \{1, \ldots, n\} : g_i = 1_G.$$

Weiter definieren wir für $f, f' \in C^n(G, M)$ folgende Addition:

$$(f + f')(g_1, \ldots, g_n) = f(g_1, \ldots, g_n) + f'(g_1, \ldots, g_n)$$

und erhalten somit $C^n(G, M)$ als abelsche Gruppe.
Für jedes $f \in C^n(G, M)$ definieren wir nun eine Funktion $\delta_n f \in C^{n+1}(G, M)$ mit

$$\begin{aligned}\delta_n f(g_1, \ldots, g_{n+1}) &= g_1 \cdot f(g_2, \ldots, g_n) \\ &\quad + \sum_{i=1}^{n} (-1)^i f(g_1, \ldots, g_{i-1}, g_i g_{i+1}, g_{i+2}, \ldots, g_{n+1}) \\ &\quad + (-1)^{n+1} f(g_1, \ldots, g_n).\end{aligned}$$

Wir zeigen, dass $\delta_n f \in C^{n+1}(G, M)$ gilt:
Hierfür müssen wir also zeigen, dass $\delta_n f$ eine Abbildung von $G \times \cdots \times G$ nach M ist und dass für jedes Tupel $(g_1, \ldots, g_{n+1})$ mit $g_i = 1_G$, $i \in \{1, \ldots, n+1\}$ außerdem $\delta_n f(g_1, \ldots, g_{n+1}) = 0$ gilt.
Dass $\delta_n f$ die gewünschten Definitions- und Zielbereiche hat, wird sofort aus der Definition und der Tatsache, dass M ein $\mathbb{Z}G$-Modul ist, klar.
Sei nun exemplarisch $g_1 = 1_G$. Dann folgt:

$$\begin{aligned}\delta_n f(1_G, g_2, \ldots, g_{n+1}) &= 1_G \cdot f(g_2, \ldots, g_{n+1}) + (-1)^1 f(1_G \cdot g_2, \ldots, g_{n+1}) \\ &\quad + \sum_{i=2}^{n} (-1)^i f(g_1, \ldots, g_{i-1}, g_i g_{i+1}, g_{i+2}, \ldots, g_{n+1}) \\ &\quad + (-1)^{n+1} f(g_1, \ldots, g_n) \\ &= f(g_2, \ldots, g_{n+1}) - f(g_2, \ldots, g_{n+1}) + \sum_{i=2}^{n} 0 + 0 \\ &= 0.\end{aligned}$$

Wir sehen nun, dass für $i \in \{1, \dots, n+1\}$ beliebig die Gleichung

$$\delta_n f(g_1, \dots, g_{n+1}) \\ = f(g_1, \dots, g_{i-1}, g_{i+1}, \dots, g_{n+1}) - f(g_1, \dots, g_{i-1}, g_{i+1}, \dots, g_{n+1}) = 0$$

gilt und somit ist die Behauptung bewiesen.
Insbesondere ist die Abbildung $\delta_n : C^n(G, M) \longrightarrow C^{n+1}(G, M)$ ein Homomorphismus.
Wir betrachten nun den Kern dieses Homomorphismus δ_n und bezeichnen diesen als $Z^n(G, M)$, d.h.

$$Z^n(G, M) := \text{Kern}(\delta_n) = \{f \in C^n(G, M) | \delta_n f = 0\}$$

und das Bild von δ_{n-1}, welches wir als $B^n(G, M)$ bezeichnen, d.h.

$$B^n(G, M) := \text{Bild}(\delta_{n-1}) = \{\delta_{n-1} f | f \in C^{n-1}(G, M)\}$$

Wählt man nun eine beliebige Abbildung $f \in C^{n-1}(G, M)$ und wendet auf diese Abbildung $\delta_n \delta_{n-1}$ an, so stellt man fest, dass $\delta_n \delta_{n-1} f = 0$ gilt.
Also ist das Bild von δ_{n-1} im Kern von δ_n enthalten.
Hiermit können wir nun die n-dimensionale Kohomologiegruppe definieren:

$$H^n(G, M) := {}^{Z^n(G,M)}\!/_{B^n(G,M)}.$$

Wir wollen nun n-dimensionale Kohomologiegruppen über freie Auflösungen bestimmen. Hierzu sei G eine Gruppe und M ein $\mathbb{Z}G$-Modul.
Wir können $\mathbb{Z}$ als $\mathbb{Z}G$-Modul auffassen, indem wir $(\sum_{g \in G} n_g g)n = (\sum_{g \in G} n_g)n$ setzen. Wir bezeichnen $\mathbb{Z}$ dementsprechend als das triviale $\mathbb{Z}G$-Modul.
Wir definieren nun den Begriff des „freien Moduls":
Sei R ein Ring mit 1 und A ein R-Modul. Sei weiter $X \subseteq A$ und M ein R-Modul derart, dass jede Abbildung $\iota : X \longrightarrow M$ eindeutig zu einem R-Modul Homomorphismus von A nach M erweiterbar ist. Dann heißt A ein *freies R-Modul* mit freiem Erzeuger X.
Wir konstruieren nun ein freies $\mathbb{Z}G$-Modul auf einer Menge X, um deren Existenz zu beweisen.
Sei hierbei R der Gruppenring $\mathbb{Z}G$ und X eine nichtleere Menge.
Betrachte: $RX = \{\sum_{i=1}^{n} r_i x_i | r_i \in R, x_i \in X, n \geq 0\}$.
Jedes Element von RX kann nun eindeutig geschrieben werden durch $\sum_{x \in X} r_x x$, mit $r_x = 0$ für fast alle $x \in X$.
Definieren wir nun die Addition für zwei Elemente aus RX durch
$\sum_{x \in X} r_x x + \sum_{x \in X} s_x x = \sum_{x \in X} (r_x + s_x)x$, so erhalten wir RX als abelsche Gruppe, wobei sich die Kommutativität sofort aus der Kommutativität des Rings R ergibt.
Definieren wir weiter $r(\sum_{x \in X} r_x x) = \sum_{x \in X} (r r_x)x$, erhalten wir ein R-Modul.
Somit können wir jede Abbildung von X nach M eindeutig zu einem R-Modul Homomorphismus zwischen RX und M erweitern.
Also ist RX nach Definition ein freies R-Modul mit freiem Erzeuger X.

Eine Sequenz $\mathcal{X}$ von freien $\mathbb{Z}G$-Modulen X_i und $\mathbb{Z}G$-Modul Homomorphismen d_i heißt eine *freie Auflösung* des trivialen $\mathbb{Z}G$-Moduls $\mathbb{Z}$, falls

$$\mathcal{X} : \dots \longrightarrow X_n \xrightarrow{d_n} X_{n-1} \xrightarrow{d_{n-1}} \dots \longrightarrow X_1 \xrightarrow{d_1} X_0 \xrightarrow{d_0} \mathbb{Z} \longrightarrow 0$$

exakt ist, d.h. falls $\text{im}(d_n) = \ker(d_{n-1})$ für alle $n \geq 1$ gilt
und außerdem $\text{im}(d_0) = \mathbb{Z}$ ist.

Die Existenz freier Auflösungen lässt sich leicht nachvollziehen, indem wir das triviale $\mathbb{Z}G$-Modul $\mathbb{Z}$ als das homomorphe Bild eines freien $\mathbb{Z}G$-Moduls X_0 betrachten. Sei

$$X_0/K_1 \cong \mathbb{Z}.$$

Dann gibt es ein freies $\mathbb{Z}G$-Modul X_1, sodass K_1 das homomorphe Bild von X_1 ist. Also gibt es ein Modul K_2 mit $X_1/K_2 \cong K_1$. Wenden wir diese Methode kontinuierlich an, so erhalten wir eine Sequenz freier $\mathbb{Z}G$-Module und $\mathbb{Z}G$-Modul Homomorphismen, sodass

$$\ldots \longrightarrow X_n \xrightarrow{d_n} X_{n-1} \xrightarrow{d_{n-1}} \ldots \longrightarrow X_1 \xrightarrow{d_1} X_0 \xrightarrow{d_0} \mathbb{Z} \longrightarrow 0$$

exakt ist.
Wir stellen nun fest, dass der $\mathbb{Z}G$-Modul Homomorphismus $d_i : X_i \longrightarrow X_{i-1}$ einen (abelschen) Gruppenhomomorphismus

$$d_i^* : \mathrm{Hom}_{\mathbb{Z}G}(X_{i-1}, M) \longrightarrow \mathrm{Hom}_{\mathbb{Z}G}(X_i, M)$$

induziert. Für $f \in \mathrm{Hom}_{\mathbb{Z}G}(X_{i-1}, M)$ und $x \in X_i$ gilt $d_i^*(f)(x) = f(d_i(x))$.
Also folgt $d_i^*(f) = f d_i$. Da die Sequenz $\mathcal{X}$ exakt ist gilt nun $d_i d_{i+1} = 0$ und somit auch $d_{i+1}^* d_i^* = 0$. Demzufolge ist also das Bild von d_i^* im Kern von d_{i+1}^* enthalten.
Wir definieren nun die n-dimensionale Kohomologiegruppe $H^n(G, M)$ als den Quotienten

$$\ker(d_{n+1}^*)/\mathrm{im}(d_n^*).$$

Diese Definition scheint von der Wahl der freien Auflösung abzuhängen, jedoch ist dies nicht der Fall, wie folgendes Theorem zeigen wird:

Satz 1.1. *Die Definition einer n-dimensionalen Kohomologiegruppe hängt nicht von der freien Auflösung $\mathcal{X}$ ab.*

Beweis. Seien $\mathcal{X}$ und $\bar{\mathcal{X}}$ zwei freie Auflösungen des trivialen $\mathbb{Z}G$-Moduls $\mathbb{Z}$. Wir zeigen, dass es einen Morphismus π zwischen $\mathcal{X}$ und $\bar{\mathcal{X}}$ gibt, d.h. dass eine Sequenz $\pi_0, \pi_1, \ldots$ von $\mathbb{Z}G$-Modul Homomorphismen existiert, sodass das folgende Diagramm kommutiert:

$$\begin{array}{lccccccccccc}
\mathcal{X} : \ldots & \xrightarrow{d_{n+1}} & X_n & \xrightarrow{d_n} & X_{n-1} & \xrightarrow{d_{n-1}} & \ldots & \xrightarrow{d_1} & X_0 & \xrightarrow{d_0} & \mathbb{Z} & \longrightarrow 0 \\
 & & \downarrow{\scriptstyle \pi_n} & & \downarrow{\scriptstyle \pi_{n-1}} & & & & \downarrow{\scriptstyle \pi_0} & & \downarrow{\scriptstyle \mathrm{id}} & \\
\bar{\mathcal{X}} : \ldots & \xrightarrow{\bar{d}_{n+1}} & \bar{X}_n & \xrightarrow{\bar{d}_n} & \bar{X}_{n-1} & \xrightarrow{\bar{d}_{n-1}} & \ldots & \xrightarrow{\bar{d}_1} & \bar{X}_0 & \xrightarrow{\bar{d}_0} & \mathbb{Z} & \longrightarrow 0
\end{array}$$

Da $\mathcal{X}$ und $\bar{\mathcal{X}}$ exakt sind, gilt $\mathrm{im}(\bar{d}_0) = \mathrm{im}(d_0) = \mathbb{Z}$ und da X_0 frei ist, folgt somit, dass eine Abbildung π_0 mit $d_0 = \bar{d}_0 \pi_0$ existiert. Wir nehmen nun als Induktionshypothese an, dass $\pi_0, \pi_1, \ldots, \pi_{n-1}$ bereits so gewählt wurden, dass $\bar{d}_i \pi_i = \pi_{i-1} d_i$ für alle $0 \leq i < n$ gilt. Hierbei ist π_{-1} die Identitätsabbildung.
Es gilt weiterhin $\bar{d}_{n-1} \pi_{n-1} d_n = \pi_{n-2} d_{n-1} d_n = 0$.
Also folgt: $\mathrm{im}(\pi_{n-1} d_n) \subseteq \ker(\bar{d}_{n-1}) = \mathrm{im}(\bar{d}_n)$.
Da X_n frei ist, existiert nun ein Homomorphismus π_n mit $\bar{d}_n \pi_n = \pi_{n-1} d_n$.
Per Induktion existiert demnach ein Morphismus $\pi : \mathcal{X} \longrightarrow \bar{\mathcal{X}}$.
Nun induziert π einen Homomorphismus $\pi_n^* : \mathrm{Hom}_{\mathbb{Z}G}(\bar{X}_n, M) \longrightarrow \mathrm{Hom}_{\mathbb{Z}G}(X_n, M)$ mit $\pi_n^*(f) = f \pi_n$. Weiter gilt $\pi_n^*(\ker(\bar{d}_{n+1}^*)) \subseteq \ker(d_{n+1}^*)$ und
$\pi_n^*(\mathrm{im}(\bar{d}_n^*)) \subseteq \mathrm{im}(d_n^*)$ und somit induziert π sogar einen Homomorphismus $\pi_n' :$

$\ker(\bar{d}^*_{n+1})/\mathrm{im}(\bar{d}^*_n) \longrightarrow \ker(d^*_{n+1})/\mathrm{im}(d^*_n)$.
Auf ganz ähnliche Weise finden wir einen Morphismus $\bar{\pi} : \bar{\mathcal{X}} \longrightarrow \mathcal{X}$ der Homomorphismen

$$\bar{\pi}'_n : \ker(d^*_{n+1})/\mathrm{im}(d^*_n) \longrightarrow \ker(\bar{d}^*_{n+1})/\mathrm{im}(\bar{d}^*_n)$$

induziert.

Um zu zeigen, dass π'_n Isomorphismen sind behaupten wir nun $\bar{\pi}'_n = (\pi'_n)^{-1}$.
Beweis dieser Aussage: Betrachte den Morphismus $\rho : \mathcal{X} \longrightarrow \mathcal{X}$ mit $\rho = \bar{\pi}\pi$.
Das bedeutet $\rho_n = \bar{\pi}_n\pi_n, \quad \rho^*_n = \pi^*_n\bar{\pi}^*_n, \quad \rho'_n = \pi'_n\bar{\pi}'_n$ für $n \geq 0$.
Wir behaupten nun es existieren Homomorphismen $\sigma_n : X_n \longrightarrow X_{n+1}$ mit $\rho_n - \mathrm{id} = d_{n+1}\sigma_n + \sigma_{n-1}d_n$ für $n \geq 0$, wobei wir $\sigma_{-1} = 0$ setzen.
Um dies zu beweisen, zeigen wir, dass folgendes Diagramm kommutiert:

$$\begin{array}{ccccccccccccc}
\ldots & \xrightarrow{d_{n+1}} & X_n & \xrightarrow{d_n} & X_{n-1} & \xrightarrow{d_{n-1}} & \ldots & \xrightarrow{d_1} & X_0 & \xrightarrow{d_0} & \mathbb{Z} & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \rho_n - \mathrm{id}} & & \downarrow{\scriptstyle \rho_{n-1} - \mathrm{id}} & & & & \downarrow{\scriptstyle \rho_0 - \mathrm{id}} & & \downarrow{\scriptstyle 0} & & \\
\ldots & \xrightarrow{d_{n+1}} & X_n & \xrightarrow{d_n} & X_{n-1} & \xrightarrow{d_{n-1}} & \ldots & \xrightarrow{d_1} & X_0 & \xrightarrow{d_0} & \mathbb{Z} & \longrightarrow & 0
\end{array}$$

Im Besonderen ist $d_0(\rho - \mathrm{id}) = d_0(d_1\sigma_0 + 0d_0) = d_0(d_1\sigma_0) = (d_0d_1)\sigma_0 = 0$.
Also gilt $\mathrm{im}(\rho_0 - \mathrm{id}) \subseteq \ker(d_0) = \mathrm{im}(d_1)$.
Da X_0 frei ist, existiert also ein gewünschter Homomorphismus σ_0
mit $d_1\sigma_0 = \rho_0 - \mathrm{id}$.
Induktionshypothese: Seien $\sigma_0, \sigma_1, \ldots, \sigma_n$ bereits wie gewünscht gewählt.
Es gilt:

$$\begin{aligned}
d_{n+1}(\rho_{n+1} - \mathrm{id} - \sigma_n d_{n+1}) &= (\rho_n - \mathrm{id})d_{n+1} - d_{n+1}\sigma_n d_{n+1} \\
&= (d_{n+1}\sigma_n + \sigma_{n-1}d_n)d_{n+1} - d_{n+1}\sigma_n d_{n+1} \\
&= d_{n+1}\sigma_n d_{n+1} + \sigma_{n-1}(d_n d_{n+1}) - d_{n+1}\sigma_n d_{n+1} \\
&= 0
\end{aligned}$$

also gilt $\mathrm{im}(\rho_{n+1} - \mathrm{id} - \sigma_n d_{n+1}) \subseteq \ker(d_{n+1}) = \mathrm{im}(d_{n+2})$.
Da X_{n+1} frei ist existiert also σ_{n+1} mit $d_{n+2}\sigma_{n+1} = \rho_{n+1} - \mathrm{id} - \sigma_n d_{n+1}$. Per Induktion folgt also nun die Behauptung und das Diagramm kommutiert.
Um nun zu zeigen, dass ρ'_n Identitätsabbildungen sind muss gelten, dass $(\rho^*_n - \mathrm{id})f \in \mathrm{im}(d^*_n)$, falls $f \in \ker(d^*_{n+1})$ gilt. Allerdings ist:

$$\begin{aligned}
(\rho^*_n - \mathrm{id})f &= f(\rho_n - \mathrm{id}) = f(d_{n+1}\sigma_n + \sigma_{n-1}d_n) \\
&= f\sigma_{n-1}d_n, \mathrm{da} f \in \ker(d^*_{n+1}) \\
&\in \mathrm{im}(d^*_n).
\end{aligned}$$

Es folgt also $\rho'_n = \pi'_n\bar{\pi}'_n = \mathrm{id}$.
Analog funktioniert dieser Beweis für $\bar{\rho} = \pi\bar{\pi}, \bar{\rho} : \bar{\mathcal{X}} \longrightarrow \bar{\mathcal{X}}$, also folgt $\bar{\pi}'_n\pi'_n = \mathrm{id}$.
Daher ist nun also π'_n ein Isomorphismus zwischen

$$\ker(d^*_{n+1})/\mathrm{im}(d^*_n)$$

und

$$\ker(\bar{d}^*_{n+1})/\mathrm{im}(\bar{d}^*_n)$$

Somit ist der Satz bewiesen. □

2. Standard Bar-Auflösung

Sei $n \in \mathbb{N}$. Betrachte die Sammlung aller Symbole $[x_1|x_2|\dots|x_n]$,
wobei $x_i \in G \setminus \{\mathrm{id}\}$ gilt. Sei B_n das freie $\mathbb{Z}G-$Modul welches durch diese Symbole erzeugt wird. Für $x_i = \mathrm{id}_G$ setzen wir $[x_1|x_2|\dots|x_n] = 0$. Für $n = 0$ gilt außerdem, dass B_0 das freie $\mathbb{Z}G-$Modul ist, welches durch das Symbol $[\ ]$ erzeugt wird. Offenbar ist $B_0 \cong \mathbb{Z}G$. Daher existiert ein surjektiver $\mathbb{Z}G-$Modul Homomorphismus $\delta_0 : B_0 \longrightarrow \mathbb{Z}$ welcher in Korrespondenz zu der Abbildung $\epsilon : \mathbb{Z}G \longrightarrow \mathbb{Z}$ gegeben durch $\epsilon(\sum_{g\in G} n_g g) = \sum_{g\in G} n_g$ steht. Für $n \in \mathbb{N}$ definieren wir nun $\delta_n : B_n \longrightarrow B_{n-1}$ als den $\mathbb{Z}G-$Modul Homomorphismus mit

$$\begin{aligned}\delta_n[x_1|x_2|\dots|x_n] = x_1 \cdot [x_2|\dots|x_n] \\ + \sum_{i=1}^{n}(-1)^i[x_1|\dots|x_ix_{i+1}|\dots|x_n] \\ + (-1)^n[x_1|\dots|x_{n-1}]\end{aligned}$$

für $x_1, \dots, x_n \in G \setminus \{\mathrm{id}\}$.
Die Standard Bar-Auflösung ist nun die freie Auflösung, die durch die Sequenz $\mathcal{B}$ der $\mathbb{Z}G-$Module B_n und den $\mathbb{Z}G-$Modul Homomorphismen δ_n beschrieben wird. Da B_n ein freies $\mathbb{Z}G-$Modul ist, ist jedes Element $f \in \mathrm{Hom}_{\mathbb{Z}G}(B_n, M)$ eindeutig durch den Wert der $[x_1|\dots|x_n]$ bestimmt. Umgekehrt können beliebige Werte in M diesen Symbolen zugewiesen werden, um so Elemente in $\mathrm{Hom}_{\mathbb{Z}G}(B_n, M)$ zu erzeugen. Daraus folgt, dass $\mathrm{Hom}_{\mathbb{Z}G}(B_n, M)$ isomorph zu der additiven Gruppe $C^n(G, M)$ ist. Hiermit können wir zeigen, dass die n-dimensionale Kohomologiegruppe die von der Sequenz $\mathcal{B}$ erzeugt wird isomorph zu dem Quotienten

$$H^n(G, M) := {}^{Z^n(G,M)}\!/_{B^n(G,M)}$$

ist und die Definitionen somit kompatibel sind.

Satz 2.1. *Seien A, B $\mathbb{Z}G$-Moduln. Es gilt:*

$$H^n(G, A + B) \cong H^n(G, A) + H^n(G, B)$$

Beweis. Sei $\{X_n\}$ eine freie Auflösung des trivialen $\mathbb{Z}G-$Moduls $\mathbb{Z}$. So gilt für $n \in \mathbb{N}$:

$$\mathrm{Hom}_{\mathbb{Z}G}(X_n, A + B) \cong \mathrm{Hom}_{\mathbb{Z}G}(X_n, A) + \mathrm{Hom}_{\mathbb{Z}G}(X_n, B)$$

als abelsche Gruppen.
Sei Θ ein solcher Isomorphismus und seien π_A, π_B die entsprechenden Projektionen. Wir sehen $\pi_A(\Theta)d_n^* = d_n^*\pi_A(\Theta)$, sowie $\pi_B(\Theta)d_n^* = d_n^*\pi_B(\Theta)$. Folglich induziert Θ einen Isomorphismus von $H^n(G, A + B)$ nach $H^n(G, A) + H^n(G, B)$. □

KAPITEL 8

Auflösbare Untergruppen in symmetrischen und endlichen linearen Gruppen

Marvin Agristean

Im Folgenden werden Obergrenzen für die Ordnungen von auflösbaren Untergruppen der endlichen symmetrischen Gruppen und der endlichen linearen Gruppen gezeigt.

Dafür muss man aber zunächst ein paar Sätze wiederholen.

1. Wiederholung

Die folgenden Sätze stammen aus Kapitel 9 und haben im Buch die Nummerierungen 9.1, 9.2, 9.3, 9.5 und 9.7. Sie werden hier nicht wortwörtlich aufgeführt, sondern es werden nur die für die folgenden Beweise relevanten Aussagen erwähnt. Außerdem werden die Sätze hier nicht bewiesen.

Grundvoraussetzung:

- Seien G eine Gruppe, die treu und primitiv auf einem $\mathbb{F}_q G$-Modul V operiert,
- A ein maximaler abelscher Normalteiler von G,
- K die von A erzeugte Unteralgebra,
- C der Zentralisator von A in G,
- B eine maximale Untergruppe von C, für die $B/A \trianglelefteq G/A$ abelsch ist,
- X ein irreduzibler $\mathbb{F}_q A$-Untermoduln von V,
- d_1 die Dimension von X und
- d_2 die Multiplizität von X in V.

Satz 1.1. *A ist zyklisch und $K \cong \mathbb{F}_{q^{d_1}}$ als $\mathbb{F}_q$-Algebra.*

Satz 1.2. *C lässt sich als Untergruppe von $\mathrm{GL}(d_2, K)$ realisieren.*

Satz 1.3. *G/C ist isomorph zu einer Untergruppe von $\mathrm{Gal}(K : \mathbb{F}_q)$.*

Satz 1.4. *$|B/A| = \dim_{\langle A \rangle_{\mathbb{F}_q}} \langle B \rangle_{\mathbb{F}_q}$ und $|B/A| \leq d_2^2$.*

Satz 1.5. *C/B operiert per Konjugation treu auf B/A.*

2. Resultate

Die folgenden Sätze haben im Buch die Nummerierung 10.1, 10.2 und 10.3.

Satz 2.1. *Sei $n \in \mathbb{N}$, $G \leq \mathsf{Sym}(n)$ und G auflösbar. Dann gilt:*

$$|G| \leq k^{n-1}$$

für einen Konstante $k = \sqrt[3]{24}$.

BEWEIS. Der Beweis erfolgt per Induktion nach n.
Für $n = 1$ ist G bereits trivial und damit gilt: $|G| = 1 \leq 1 = k^0$.
Sei nun $2 \leq n$.
Definiere $\Omega := \{1, 2, ..., n\}$ als die Menge, auf der die $\mathsf{Sym}(n)$ operiert.

Fall 1: Sei G nicht transitiv.

Dann existieren nicht leere $\Omega_1, \Omega_2 \subset \Omega$ mit $\Omega = \Omega_1 \dot\cup \Omega_2$, die eine G-invariante Partitionierung von Ω darstellen.
Nun ist G isomorph zu einer Untergruppe von $G^{\Omega_1} \times G^{\Omega_2}$, wobei $G^{\Omega_i} := G/\sim_i$ für die Äquivalenzrelation $\sim_i$, welche Elemente von G nur aufgrund ihrer Wirkung auf Ω_i unterscheidet, gilt.
Diese G^{Ω_i} sind als Bilder von auflösbaren Gruppen auflösbar.
Um die Auffassung des Rausteilens der Relation als Bild zu rechtfertigen, kann man die Einschränkung von Elementen aus G auf Ω_i betrachten, um so einen Homomorphismus von G nach $\mathsf{Sym}(\Omega_i)$ zu erhalten.
Da die Partitionen beide nicht leer sind, gilt außerdem $|\Omega_i| \lneq n$.
Damit kann man hier bereits die Induktionsannahme verwenden und erhält so:

$$|G| \leq |G^{\Omega_1}| * |G^{\Omega_2}| \leq k^{|\Omega_1|-1} * k^{|\Omega_2|-1} \leq k^{|\Omega|-1}.$$

Fall 2: Sei G transitiv und imprimitiv.

Nun gibt es eine Äquivalenzrelation ρ auf Ω die G-invariant, nicht trivial und nicht universal ist.
Sei $\alpha \in \Omega$, $\Omega_1 := \bar\alpha$ die zugehörige Äquivalenzklasse und Ω_2 die Menge der Äquivalenzklassen.
Betrachte ähnlich wie im obigen Fall $G_2 := G^{\Omega_2} := G/\rho$, die Wirkung von G auf den Äquivalenzklassen. Den Kern der Projektion von G nach G_2 bezeichnen wir mit $N = \{g \in G | \forall \omega \in \Omega : w\rho(g.w)\}$.
Bezeichne mit $\bar\alpha_1, \bar\alpha_2, ..., \bar\alpha_{|\Omega_2|}$ die verschiedenen Elemente von Ω_2. $N_i := N^{\bar\alpha_i}$ ist analog auch wieder eine auflösbare Untergruppe von $\mathsf{Sym}(\bar\alpha_i)$ und $N \leq N_1 \times ... \times N_{|\Omega_2|}$. Also kann man hier wieder die Induktionsannahme anwenden:

$$|G| = |N| * \ |G_2| \leq (k^{|G_1|-1})^{|G_2|} * k^{|G_2|} = k^{|\Omega|-1}.$$

In die letzte Gleichung fliesst ein, dass $|\Omega| = |\Omega_1| * |\Omega_2|$ gilt. Hierfür kann man sich überlegen, dass alle Äquivalenzklassen gleich viele Elemente haben müssen, da das vertreterweise Rechnen in G_2 für jede nicht triviale Wirkung eine Bijektion zwischen den Äquivalenzklassen vermittelt. Die Transitivität sichert hierbei, dass alle Äquivalenzklassen untereinander Bijektionen besitzen.

Fall 3: Sei G primitiv.

Setze $\alpha \in \Omega$ fest und wähle einen minimalen Normalteiler $M \triangleleft G$.
Die Endlichkeit von G sichert uns die Existenz dieses Normalteilers.
Nach Satz 1.5 gilt bereits $G = M \rtimes H$, für den Stabilisator $H \leq \mathrm{GL}(d, \mathbb{F}_p)$ von α und $|\Omega| = |M| = p^d$ für eine Primzahl p

und ein natürliches d.
Für $32 \leq n$ gilt nun:

$$|G| = |M| * |H| \leq n * |\operatorname{GL}(d, \mathbb{F}_p)| < n * p^{d^2} \leq n^{1+log(n)} < k^{n-1}.$$

Für $n \leq 31$ muss man die übrigen Fälle konkret nachrechnen.

Damit ist die Aussage in jedem Fall gezeigt. □

Der Beweis des nächsten Satzes ist ähnlich zum obigen aufgebaut. Auch hier will man die Gruppe wieder anhand einer Eingenschaft aufteilen um die Induktionsannahme zu verwenden. Hierfür braucht man den Begriff der kompletten Reduzibilität für lineare Gruppen. Dieser sichert uns, dass man den Vektorraum, auf welchem die Gruppe wirkt, als direkte Summe von G -invarianten irreduziblen Unterräumen schreiben kann.

Satz 2.2. *Sei $G \leq \operatorname{GL}(d, \mathbb{F}_q)$ auflösbar und komplett reduzibel für geeignete d, q. Dann gilt:*

$$|G| \leq q^{3d-2}$$

Beweis. Der Beweis erfolgt per Induktion nach der Dimension d.
Für $d = 1$ ist $\operatorname{GL}(d, \mathbb{F}_q) = \operatorname{GL}(1, \mathbb{F}_q) \cong \mathbb{F}_q$ und damit

$$|G| \leq |\operatorname{GL}(1, \mathbb{F}_q)| = q - 1 \leq q = q^{3-2}$$

Sei $V := \mathbb{F}_q^d$ und G als lineare Gruppe treu.
Für den Induktionsschritt sei nun $2 \leq d$.

Fall 1: Sei G reduzibel.

Dann existiert ein G-invarianter echter, nicht trivialer Untervektorraum $V_1 \leq V$. Die komplette Reduzibilität sichert uns auch noch die Existenz eines G-invarianten Komplements V_2 mit $V = V_1 \oplus V_2$. Analog zum ersten Beweis lassen sich wieder $G^{V_i} \leq \operatorname{GL}(V_i)$, die Auflösbarkeit und komplette Reduzibilität von G erben, bilden und man erkennt, dass G isomorph zu einer Untergruppe von $G^{V_1} \times G^{V_2}$ ist. Jetzt kann man die Induktionsannahme verwenden:

$$|G| \leq q^{3\dim(V_1)-2} * q^{3\dim(V_2)-2} = q^{3\dim(V)-4} < q^{3\dim(V)-2} = q^{3d-2}$$

Fall 2: Sei G irreduzibel und imprimitiv.

Nun existieren Untervektorräume $V_1, V_2, ..., V_{m_2}$ der Dimension m_1 mit $V = V_1 \oplus V_2 \oplus ... \oplus V_{m_2}$ und $G \leq \mathsf{Sym}(\{V_i | 1 \leq i \leq m_2\})$. Mit Satz 1.7 erhalten wir, dass $G \leq G_1 \wr G_2$ für transitive und auflösbare $G_1 \leq \operatorname{GL}(m_1, \mathbb{F}_q)$ und $G_2 \leq \mathsf{Sym}(m_2)$ ist. Mit der Induktionsannahme und Satz 2.1 gilt nun:

$$|G| = |G_1|^{m_2} * |G_2| \leq (q^{3m_1-2})^{m_2} * k^{m_2-1} \leq q^{3d-2}$$

wobei k die Konstante aus 2.1 ist und $d = m_1 m_2$ gilt.

Fall 3: Sei G irreduzibel und primitiv.

Hier werden die wiederholten Sätze aus Kapitel 9 angewandt. Dafür müssen wir aber erstmal die Voraussetzungen schaffen. Sei $d := |G|$, $A \trianglelefteq G$ ein maximaler abelscher Normalteiler, C sein Zentralisator und $K \leq \operatorname{End}_{\mathbb{F}_q}(V)$ die von A erzeugte Unteralgebra. Nach 1.1 gilt also ohne Einschränkung $K = \mathbb{F}_{q^{d_1}}$ für

einen positiven Teiler d_1 von d. Setze $d_2 = d/d_1$ fest.
Mit 1.2 erhält man, dass $C \leq \mathrm{GL}(d_2, \mathbb{F}_{q^{d_1}})$ auflösbar ist und 1.3 liefert, dass $G/C \leq \mathrm{Gal}(\mathbb{F}_{q^{d_1}} : \mathbb{F}_q)$ ist und als Galoisgruppe einer endlichen Körpererweiterung eines endlichen Körpers ist G/C zyklisch mit einer Ordnung von maximal d_1.
Fall 3.1: Sei $2 \leq d_1$.

Hier kann man direkt die Induktionsannahme verwenden:

$$|G| \leq |G/C| * |C| \leq d_1 * (q^{d_1})^{3d_2-2} < q^{3d-2}$$

wobei $d_1 \leq q^{d_1}$ zusätzlich in die letzte Ungleichung einfliesst.

Fall 3.2: Sei $d_1 = 1$.

Dann ist G/C trivial und damit gilt bereits $G = C$. Außerdem ist die Algebra $\langle A \rangle = K = \mathbb{F}_q$. Damit ist $|K| \leq q$ und weil A bzgl. Multiplikation eine Gruppe und F_q ein Körper ist, kann das 0-Element aus K nicht in A vorkommen. Das ergibt die Abschätzung $|A| \leq q - 1$ für die Ordnung von A.
Sei $A \trianglelefteq B \leq G$ mit B/A abelsch und maximal in G/A. 1.4 liefert die Abschätzung $|B/A| \leq d^2$ für die Ordnung von B/A. 1.5 liefert uns die Treue der Operation per Konjugation von G/B auf B/A und damit $G/B \leq Aut(B/A)$. Betrachte die Abschätzung $|\mathrm{Aut}(B/A)| \leq d^{4*log(d)}$, welche hier nicht bewiesen wird.
Für $45 \leq d$ gilt nun die folgende Abschätzung:

$$\begin{aligned} |G| &\leq |A| * |B/A| * |G/B| \leq (q-1) * d^2 * d^{4*\log(d)} \\ &\leq q^{1+2\log(d)+4\log(d)^2} \leq q^{3d-2}, \end{aligned}$$

wobei die erste Abschätzung aus zweifacher Anwendung des Satzes von Laplace folgt.
Für $d \leq 44$ hingegen muss man wieder die einzelnen Fälle konkret nachrechnen.

Damit ist die Aussage in jedem Fall gezeigt. □

Der letzte Satz bietet eine praktische leicht zu merkende Formel, mit der man auflösbare Untergruppen der endlichen Symmetrischen Gruppen abschätzen kann.

Satz 2.3. *Sei $G \leq Sym(n)$ auflösbar und primitiv, für geeignetes natürliches n. Dann gilt:*

$$|G| \leq n^4.$$

Beweis. Sei $n \in \mathbb{N}$, $\alpha \in \{1, 2, ..., n\}$ fest, $G \leq \mathsf{Sym}(n)$ auflösbar und primitiv, $M \trianglelefteq G$ minimal und H der Stabilisator von α.
Nach Satz 1.5 ist $n = p^d = |M|$ und $|G| = |H| * |M|$ für eine Primzahl p und ein natürliches d. Außerdem kann H mit einer Untergruppe von $\mathrm{GL}(d, p)$ realisiert

werden und ist irreduzibel und auflösbar als Untergruppe der primitiven und auflösbaren Gruppe G. Damit ist H insbesondere komplett reduzibel und 2.2 liefert uns:

$$|H| \leq p^{3d-2} < p^{3d} = n^3.$$

Damit folgt bereits die Behauptung:

$$|G| = |H| * |M| \leq n^3 * n \leq n^4.$$

□

KAPITEL 9

Pybers Satz - für auflösbare Gruppen

Karina Tulchinskaja

1. Ziel des Vortrags

Das Ziel dieses Vortrags ist es, den folgenden Satz von Pyber zu beweisen:

> Die Anzahl auflösbarer Gruppen G der Ordnung $n = p_1^{\alpha_1} \cdot ... \cdot p_k^{\alpha_k}$ mit Sylow-p_i-Untergruppen $P_1, ..., P_k$ ist höchstens $n^{8\mu+278833}$, wobei $\mu = \mu(n) = \max\{\alpha_1, ..., \alpha_k\}$ ist.

Als Korollar erhalten wir eine obere Schranke für die Anzahl der auflösbaren A-Gruppen G der Ordnung n.

Dieser Vortrag orientiert sich an [Enumeration of Finite Groups, §15].

2. Notationen, Erinnerungen, erste Überlegungen

n sei durchgehend fest und $n = p_1^{\alpha_1} \cdot ... \cdot p_k^{\alpha_k}$ die Primfaktorzerlegung. $P_1, ..., P_k$ seien p_i-Gruppen der Ordnungen $|P_i| = p_i^{\alpha_i}$. $\mathcal{S}$ sei eine Familie dieser Gruppen.

$F_1, ..., F_k$ seien die maximalen normalen p_i-Untergruppen von G. Es gilt also $F_i \leq P_i$. Die davon erzeugte Untergruppe ist die Fittinguntergruppe von G. Wir bezeichnen diese mit F. Es gilt $F = F_1 \times ... \times F_k$, F ist also das Produkt seiner Sylow-p_i-Untergruppen.

Sei $A_i = \mathrm{Aut}(F_i)$ und $A = \mathrm{Aut}(F)$. Es gilt $A = A_1 \times ... \times A_k$.

Sei Z das Zentrum von F und seinen $Z_1, ..., Z_k$ die Zentren der $F_1, ..., F_k$. Es gilt $Z = Z_1 \times ... \times Z_k$. Die Z_i sind die Sylow-p_i-Untergruppen von Z.

Sei $H = G/Z$. Die Sylow-p_i-Untergruppen von H sind Quotienten der Sylow-p_i-Untergruppen von G. Wir bezeichnen diese mit $Q_i = P_i/Z_i$.

Es ist also Z eine Untergruppe von G und H der entsprechende Quotient. Das bedeutet, dass G eine Gruppenerweiterung von Z durch H ist. Diese Tatsache werden wir benutzen, um den Satz von Pyber zu beweisen.

3. Vorbereitung

Lemma 3.1. *Seien die zwei Gruppen Z und H wie oben gegeben sowie eine Wirkung von H auf Z. Dann ist die Anzahl der Gruppen G, die Erweiterungen von*

Z durch H sind und deren Sylow-p_i-Untergruppen $P_1, ..., P_k$ sind, höchstens

$$\prod_{i=1}^{k} p_i^{\alpha_i^2} \leq n^{\mu}.$$

BEWEIS. Erweiterungen von Z durch H sind Gruppen G, für die die Sequenz

$$1 \longrightarrow Z \longrightarrow G \longrightarrow H \longrightarrow 1$$

exakt ist. Sei $\mathrm{H}^2_{\mathcal{S}}(\mathrm{H}, \mathrm{Z})$ die Menge der Äquivalenzklassen solcher Erweiterungen, deren Sylow-p_i-Untergruppen in $\mathcal{S}$ liegen, also genau die $P_1, ..., P_k$ sind. $\mathrm{H}^2_{\mathcal{S}}(\mathrm{H}, \mathrm{Z})$ enthält alle Isomorphieklassen solcher Erweiterungen, also wollen wir $|\,\mathrm{H}^2_{\mathcal{S}}(\mathrm{H}, \mathrm{Z})\,|$ abschätzen.
Aus $Z = Z_1 \times ... \times Z_k$ folgt für die Kohomologiegruppen

$$H^2(H, Z) \cong H^2(H, Z_1) \times ... \times H^2(H, Z_k).$$

Man kann nachrechnen, dass die Einschränkung dieses Isomorphismus auf $\mathrm{H}^2_{\mathcal{S}}(\mathrm{H}, \mathrm{Z})$ liefert, dass

$$\mathrm{H}^2_{\mathcal{S}}(\mathrm{H}, \mathrm{Z}) \cong H^2_{\mathcal{S}_1}(H, Z_1) \times ... \times H^2_{\mathcal{S}_k}(H, Z_k) \tag{2}$$

gilt, wobei $\mathcal{S}_i$ die p_i-Gruppe P_i und für $j \neq i$ die p_j-Gruppen $Q_j = P_j/Z_j$ enthält. Da $Q_i \to H$ injektiv ist, ist die induzierte Abbildung auf den Kohomologiegruppen

$$H^2(H, Z_i) \to H^2(Q_i, Z_i) \text{ injektiv.}$$

Auch hier wollen wir uns auf die fest gewählten Sylow-p_i-Untergruppen $P_1, ..., P_k$ beschränken, daher schränken wir obige Abbildung auf $H^2_{\mathcal{S}_i}(H, Z_i)$ ein. Das liefert, dass

$$H^2_{\mathcal{S}_i}(H, Z_i) \to H^2_{\{P_i\}}(Q_i, Z_i) \text{ injektiv} \tag{3}$$

ist. Aus (2) und (3) folgt

$$|\,\mathrm{H}^2_{\mathcal{S}}(\mathrm{H}, \mathrm{Z})\,| \leq \prod_{i=1}^{k} |H^2_{\mathcal{S}_i}(H, Z_i)| \leq \prod_{i=1}^{k} |H^2_{\{P_i\}}(Q_i, Z_i)|, \tag{4}$$

daher schätzen wir $|H^2_{\{P_i\}}(Q_i, Z_i)|$ ab.
Die Sequenz

$$1 \longrightarrow Z_i \longrightarrow P_i \longrightarrow Q_i \longrightarrow 1$$

soll exakt sein. Die drei Gruppen Z_i, P_i und Q_i sind gegeben, daher müssen wir abschätzen, wie viele Abbildungen für die Pfeile

$$Z_i \longrightarrow P_i \text{ und } P_i \longrightarrow Q_i$$

in obiger Sequenz möglich sind.
Zuerst untersuchen wir den Pfeil $Z_i \to P_i$. Wegen $Z_i \leq P_i$ ist $|Z_i| = p_i^{\beta_i}$ für ein $\beta_i \leq \alpha_i$. Die für diesen Pfeil möglichen Abbildungen sind genau die Homomorphismen $Z_i \to P_i$, die injektiv sind und deren Bild ein Normalteiler in P_i ist. Ihre Anzahl ist beschränkt durch

$$\begin{aligned}
&|\{\text{Homomorphismen } Z_i \to P_i\}| \\
=&|\{\text{Abbildungen } \{e_1, ..., e_{\beta_i}\} \to P_i\}|,\ e_1, ..., e_{\beta_i} \text{ Erzeuger von } Z_i \\
=&|P_i|^{\beta_i} = p_i^{\alpha_i \beta_i}.
\end{aligned}$$

Nun betrachten wir den Pfeil $P_i \to Q_i$. Es gilt $|Q_i| = |P_i/Z_i| = p_i^{\alpha_i-\beta_i}$. Die möglichen Abbildungen für diesen Pfeil sind genau die surjektiven Homomorphismen $P_i \to Q_i$ mit Kern Z_i. Eine obere Schranke für ihre Anzahl ist

$$\begin{aligned}&|\{\text{Homomorphismen } P_i/Z_i \to Q_i\}|\\ =&|\{\text{Abbildungen } \{f_1,...,f_{\alpha_i-\beta_i}\} \to Q_i\}|,\ f_1,...,f_{\alpha_i-\beta_i} \text{ Erzeuger von } P_i/Z_i\\ =&|Q_i|^{\alpha_i-\beta_i} = p_i^{(\alpha_i-\beta_i)^2}.\end{aligned}$$

Insgesamt erhalten wir eine obere Schranke für die Anzahl möglicher Pfeile durch

$$p_i^{\alpha_i\beta_i} \cdot p_i^{(\alpha_i-\beta_i)^2} \leq p_i^{\alpha_i\beta_i} \cdot p_i^{(\alpha_i-\beta_i)\alpha_i} = p_i^{\alpha_i^2}.$$

Nach dieser Abschätzung zusammen mit (3) ist

$$|\,\mathrm{H}^2_{\mathcal{S}}(\mathrm{H},\mathrm{Z})\,| \leq \prod_{i=1}^{k} |H^2_{\{P_i\}}(Q_i,Z_i)| \leq \prod_{i=1}^{k} p_i^{\alpha_i^2} \leq \prod_{i=1}^{k} p_i^{\alpha_i\mu} = n^\mu$$

eine obere Schranke für die Anzahl der Gruppenerweiterungen von Z durch H mit Sylow-p_i-Untergruppen $P_1,...,P_k$. □

Definition 3.2. Sei G eine Gruppe. Wir definieren

$$\mathrm{Mss}(G) = \{H \mid H \text{ ist maximale auflösbare Untergruppe von } G\}.$$

An dieser Stelle fassen wir die Resultate, die wir im nächsten Teilkapitel brauchen werden, als ein Lemma zusammen. Für die Herleitung siehe [Enumeration of Finite Groups, §15.1].

Lemma 3.3. *(i) Sei $M \leq A_i$ eine auflösbare Untergruppe der Ordnung $|M| = p_i^m x_i$ mit $p_i \nmid x_i$. Dann gilt $x_i \leq p_i^{3\alpha_i}$.*
(ii) Es gilt $|\mathrm{Mss}(A_i)| \leq p_i^{\alpha_i^2+278833}$ und $\mathrm{Mss}(A) = \mathrm{Mss}(A_1) \times ... \times \mathrm{Mss}(A_k)$, somit $|\mathrm{Mss}(A)| \leq n^{\mu+278833}$.

4. Pybers Satz für auflösbare Gruppen

Satz 4.1. *Die Anzahl auflösbarer Gruppen G der Ordnung n mit Sylow-p_i-Untergruppen $P_1,...,P_k$ ist höchstens*

$$n^{8\mu+278833}.$$

Beweis. Wir wissen bereits, dass wenn G gegeben ist, die beiden Gruppen Z und H eindeutig sind. Umgekehrt sahen wir in Lemma 3.1, dass wenn Z und H gegeben sind, höchstens n^μ Gruppen G mit Sylow-p_i-Untergruppen $P_1,...,P_k$ Erweiterung von Z durch H sein können. Die Kernidee dieses Beweises ist es, abzuschätzen, wie viele Paare von Gruppen Z, H auftreten können, sodass $Z = Z(F(G))$ und $H = G/Z$ für eine auflösbare Gruppe G der Ordnung n mit Sylow-p_i-Untergruppen $P_1,...,P_k$ gilt.
Wir wollen die Beweisidee noch etwas ausführlicher durchgehen. Angenommen, F ist bekannt. Dann sind Z und A, das Zentrum beziehungsweise die Automorphismengruppe von F, eindeutig. Die Konjugationswirkung $G \to A$ hat den Kern Z, somit kann man $H = G/Z$ als Untergruppe von A auffassen. Da G auflösbar ist, ist auch H auflösbar, also ist H in einer maximalen auflösbaren Untergruppe von A enthalten. Die Möglichkeiten für H zählen wir ab, indem wir mithilfe von Sylowsystemen die Untergruppen von Elementen aus $\mathrm{Mss}(A)$ zählen und die Schranke

für $|\mathrm{Mss}(A)|$ aus Lemma 3.3 benutzen. Damit beginnen wir den Beweis.
Sei $M \in \mathrm{Mss}(A)$. Es gilt $M = M_1 \times ... \times M_k$ mit $M_i = M \cap A_i \in \mathrm{Mss}(A_i)$. Wir wählen $R_1, ..., R_k$ als Teil eines Sylowsystems von M aus. Das Sylowsystem einer Untergruppe H von M ist von der Form $Q_1, ..., Q_k$ mit $Q_i = H \cap R_i$. Wir könnten also die Anzahl der Untergruppen von M durch die Anzahl der Möglichkeiten für $R_1, ..., R_k$ und $Q_1, ..., Q_k$ mit $Q_i \leq R_i$ abschätzen.
Es gilt $R_i = R_{i1} \times ... \times R_{ik}$, wobei die R_{ij} Sylow-p_i-Untergruppen von M_j sind. Sei

$$X_j = \prod_{\substack{i=1,...,k \\ i \neq j}} R_{ij} \subseteq M_j.$$

Da $R_1, ..., R_k$ ein Sylowsystem ist, gilt $R_s R_t = R_t R_s$, und daher ist X_j eine Untergruppe von M_j, also auch $X_j \leq A_j$. Da X_j das Produkt von p_i-Gruppen für $i = 1, ..., k,\ i \neq j$ ist, gilt $p_j \nmid |X_j|$. Wir können Lemma 3.3 anwenden und erhalten $|X_j| \leq p_j^{3\alpha_j}$. Das zeigt, dass $|R_{ij}|$ für $i \neq j$ nicht allzu groß ist. Wir bräuchten auch eine ähnliche Schranke für $|R_{ii}|$, da die Anzahl der Möglichkeiten für H von allen $|R_i| = |R_{i1}| \cdot ... \cdot |R_{ik}|$ abhängt. Dafür wollen wir die $R_1, ..., R_k$ durch $S_1, ..., S_k$ ersetzen, sodass $Q_i \leq S_i$ erhalten bleibt und $|S_i|$ klein ist.
Wir definieren S_{ij} als

$$S_{ij} = \begin{cases} R_{ij} & , \text{ falls } i \neq i \\ \phi_i(P_i) & , \text{ falls } i = j \end{cases}$$

wobei $\phi_i = \pi_i \circ \phi$ die Verkettung der Konjugationswirkung $\phi : G \to A$ und der Projektion $\pi_i : A \to A_i$ ist. Und S_i definieren wir als

$$S_i = S_{i1} \times ... \times S_{ik}.$$

Es gilt $\phi_i(P_i) = \pi_i(P_i/Z_i) = \pi_i(Q_i)$. Aus der Definition von S_i und $Q_i \leq R_i$ folgt $Q_i \leq S_i$. Für $|S_{ii}|$ haben wir die Schranke

$$|S_{ii}| = |\phi_i(P_i)| \leq |P_i| = p_i^{\alpha_i}.$$

Wir überlegen uns, welche weiteren Abschätzungen nötig sind, um die behauptete Schranke $n^{8\mu+278833}$ herzuleiten. Dazu definieren wir die vier Zahlen

$n_1 =$ Anzahl der Möglichkeiten für F
$n_2 =$ Anzahl der Möglichkeiten für M, gegeben F
$n_3 =$ Anzahl der Möglichkeiten für $S_1, ..., S_k$, gegeben $F,\ M$
$n_4 =$ Anzahl der Möglichkeiten für $Q_1, ..., Q_k$, gegeben $F,\ M,\ S_1, ..., S_k$

Wir haben uns bereits überlegt, dass

$$n_1 \cdot n_2 \cdot n_3 \cdot n_4 \geq \text{Anzahl der Möglichkeiten für } H$$

gilt. Für Z gibt es nur eine Möglichkeit, wenn F gegeben ist. Und pro gegebenes Paar $Z,\ H$ gibt es höchstens n^μ Möglichkeiten für G nach Lemma 3.1. Insgesamt gilt

$$n_1 \cdot n_2 \cdot n_3 \cdot n_4 \cdot n^\mu \geq \text{Anzahl der Möglichkeiten für } G$$

Jetzt widmen wir uns den Abschätzungen für diese vier Zahlen.
Es gilt $F = F_1 \times ... \times F_k$. Da $F_i \leq P_i$ gilt, ist F_i von bis zu α_i Elementen von P_i

erzeugt. Also gibt es für F_i höchstens $|P_i|^{\alpha_i}$ Möglichkeiten, daher gilt

$$n_1 \leq \prod_{i=1}^{k} |P_i|^{\alpha_i} = \prod_{i=1}^{k} p_i^{\alpha_i^2} \leq \prod_{i=1}^{k} p_i^{\alpha_i \mu} = n^{\mu}. \tag{5}$$

Es gilt $n_2 = |\mathrm{Mss}(A)|$, Lemma 3.3 liefert die Abschätzung

$$n_2 \leq n^{\mu+278833}. \tag{6}$$

Nun widmen wir uns der Abschätzung von n_3. Zunächst schätzen wir die Anzahl der Möglichkeiten für $R_1, ..., R_k$ ab. Diese sind Teil eines Sylowsystems von M. Da alle Sylowsysteme von M konjuiert sind, gibt es höchstens $|M|$ Stück, und

$$\begin{aligned} |M| &\leq |A| = \prod_{i=1}^{k} |A_i| \\ &\leq \prod_{i=1}^{k} |F_i|^{\gamma_i}, \text{ wobei } \gamma_i \leq \alpha_i \text{ die minimale Anzahl der Erzeuger von } F_i \text{ ist} \\ &\leq \prod_{i=1}^{k} |P_i|^{\alpha_i} = \prod_{i=1}^{k} p_i^{\alpha_i^2} \leq \prod_{i=1}^{k} p_i^{\alpha_i \mu} \leq n^{\mu}. \end{aligned}$$

Als nächstes müssen wir abschätzen, wie viele $S_1, ..., S_k$ für gegebene $R_1, ..., R_k$ existieren. Bei der Wahl von F wird auch eine Einbettung $F \hookrightarrow P$ festgelegt, somit auch eine Konjugationswirkung $P_i \to A_i$. Diese ist gerade die Einschränkung der Konjugationswirkung $\phi_i : G \to A_i$. Da S_i über R_i und $\phi_i(P_i)$ definiert ist, sind $S_1, ..., S_k$ eindeutig bestimmt durch F und $R_1, ..., R_k$. Daher gilt

$$n_3 \leq n^{\mu}. \tag{7}$$

Schließlich widmen wir uns n_4. Dazu schätzen wir die Anzahl der Untergruppen der $S_1, ..., S_k$ ab. Eine Untergruppe $Q_i \leq S_i$ ist von bis zu α_i Elementen von S_i erzeugt, daher ist

$$n_4 \leq \prod_{i=1}^{k} |S_i|^{\alpha_i} \leq \left(\prod_{i=1}^{k} |S_i| \right)^{\mu}.$$

Mit

$$\prod_{i=1}^{k} |S_i| = \prod_{i=1}^{k} \left(|X_i| \cdot |S_{ii}| \right) \leq \prod_{i=1}^{k} \left(p_i^{3\alpha_i} \cdot p_i^{\alpha_i} \right) = \prod_{i=1}^{k} p_i^{4\alpha_i} = n^4$$

folgt

$$n_4 \leq n^{4\mu}. \tag{8}$$

Aus (5), (6), (7) und (8) folgt, dass

$$n_1 \cdot n_2 \cdot n_3 \cdot n_4 \cdot n^{\mu} \leq n^{\mu} \cdot n^{\mu+278833} \cdot n^{\mu} \cdot n^{4\mu} \cdot n^{\mu} = n^{8\mu+278833}$$

eine obere Schranke für die Anzahl der auflösbaren Gruppen der Ordnung n mit Sylow-p_i-Untergruppen $P_1, ..., P_k$ ist. □

KOROLLAR 4.2. *Die Anzahl auflösbarer A-Gruppen G der Ordnung n ist höchstens*

$$n^{8\mu+278834}.$$

BEWEIS. Die Sylow-p_i-Untergruppen einer A-Gruppe sind abelsch. Es gibt höchstens m abelsche Gruppen Gruppen der Ordnung m nach [Enumeration of Finite Groups, 17.3], also gibt es höchstens $p_1^{\alpha_1} \cdot ... \cdot p_k^{\alpha_k} = n$ mögliche Paare von Sylow-p_i-Untergruppen $P_1, ..., P_k$ einer Gruppe der Ordnung n. Mit Theorem 4.1 folgt die Behauptung, da $n \cdot n^{8\mu+278833} = n^{8\mu+278834}$. □