Karlsruher Institut für Technologie
Institut für Algebra und Geometrie
PD Dr. Stefan Kühnlein Dipl.-Math. Jochen Schröder

Einführung in Algebra und Zahlentheorie – Übungsblatt 7 – Musterlösung

Schreibweise: Für eine endliche Gruppe G und eine Primzahl p schreiben wir s_p für die Anzahl der p-Sylowgruppen von G.

Wiederholung eines Arguments: Ist G eine Gruppe und U die einzige Untergruppe von G mit dieser Mächtigkeit, so ist U ein Normalteiler von G – denn für alle $g \in G$ ist gUg^{-1} eine Untergruppe, die gleichmächtig zu U ist, also nach Voraussetzung gleich U.
Insbesondere gilt dies im Fall einer endlichen Gruppe G, wenn $s_p = 1$ ist für eine Primzahl p – dann ist die eine p-Sylowgruppe normal. Ist also $p|\#G$, aber $\#G$ keine p-Potenz, so ist diese p-Sylowgruppe nichttrivial und insgesamt G nicht einfach.

Aufgabe 1 (4 Punkte)
Zeige, dass A_6 einfach ist.
(*Hinweis:* In der Vorlesung haben wir gesehen, dass A_5 einfach ist. Wir finden A_5 als Untergruppe in A_6.)

Lösung: Sei $i \in \{1, ..., 6\}$ zunächst beliebig.
Wir finden A_5 auf natürliche Art uns Weise als Untergruppe von A_6: $A_5^{(i)} := \{\sigma \in A_6 : \sigma(i) = i\} \cong A_5$ ist der Stabilisator des Elements i unter der natürlichen Operation von A_6 auf $\{1, ..., 6\}$.

Sei nun $N \trianglelefteq A_6$ ein Normalteiler. Zu zeigen ist $N \overset{(!)}{\in} \{\{\mathrm{id}\}, A_6\}$.
Behauptung 1: $N_i := N \cap A_5^{(i)} \subseteq A_5^{(i)}$ ist ein Normalteiler.
Beweis der Behauptung 1: N_i ist als Schnitt zweier Untergruppen von A_6 wieder eine Gruppe.
Sei $a \in A_5^{(i)}$ und $n \in N_i$, so gilt $ana^{-1} \in N$ (denn $n \in N$ und N ist ein Normalteiler von $A_6 \supseteq A_5^{(i)}$) und $ana^{-1} \in A_5^{(i)}$ (als Produkt von Elementen in $A_5^{(i)}$), also $ana^{-1} \in N_i$.

Da $A_5 \cong A_5^{(i)}$ einfach ist, ist $N \cap A_5^{(i)} \in \{\{\mathrm{id}\}, A_5^{(i)}\}$.

Fall 1: $N_i = \{\mathrm{id}\}$ für alle $i \in \{1, ..., 6\}$. Das heißt, in N gibt es kein Element $\sigma \neq \mathrm{id}$ mit $\sigma(i) = i$ für ein $i \in \{1, ..., 6\}$. Wir wollen zeigen, dass in diesem Fall $N \overset{(!)}{=} \{\mathrm{id}\}$ ist.
Annahme: Es gebe $\sigma \neq \mathrm{id}$ in N. σ hat keinen Fixpunkt und σ hat Signum 1. Es folgt, dass σ von der Form $(ab)(cdef)$ (**Fall 1.1**) oder $(abc)(def)$ (**Fall 1.2**) ist, wobei $\{a, b, c, d, e, f\} = \{1, 2, 3, 4, 5, 6\}$.
Im Fall 1.1 ist $\sigma^2 \in N$ mit Fixpunkt $\sigma^2(a) = a$, aber $\sigma^2 \neq \mathrm{id}$ wegen $\sigma^2(c) = e$. WIDERSPRUCH
Im Fall 1.2 konjugieren wir σ mit $(abd) \in A_6$. Es ist $\sigma' = (abd) \circ \sigma \circ ((abd)^{-1}) = (bdc)(aef) \in N$, denn N ist ein Normalteiler in A_6.
Es ist $\sigma' \circ \sigma \in N$, aber $\sigma'(\sigma(b)) = b$ und $\sigma' \circ \sigma \neq \mathrm{id}$ wegen $\sigma'(\sigma(d)) = f$. WIDERSPRUCH

Fall 2: Sei $N_i = A_5^{(i)}$ für ein $i \in \{1, ..., 6\}$. Ohne Einschränkung sei das $i = 6$, sonst geht der Beweis analog.
Behauptung 2: Alle Dreizykel sind in N enthalten.
Dann ist $N = A_6$, denn die Dreizykel erzeugen A_6 laut Vorlesung.
Beweis der Behauptung 2: Alle Dreizykel (abc) mit paarweise verschiedenen $a, b, c \in \{1, ..., 5\}$ sind in

N enthalten. Sei nun $(ab6)$ (mit $a, b \in \{1, ..., 5\}$ paarweise verschieden) ein anderer Dreizykel:
Wähle $c \in \{1, .., 5\} \setminus \{a, b\}$. Es ist $(abc) \in N$.
(**Bemerkung:** Es ist $(ab6) = (c6) \circ (abc) \circ (c6)^{-1}$, aber $(c6)$ kein Element von A_6. Wir haben aber genug Elemente in $\{1, ..., 6\}$, um das zu umgehen.)
Wähle weiterhin $i \neq j \in \{1, ..., 5\} \setminus \{a, b, c\}$. Dann ist $(ij)(6c) = ((ij)(6c))^{-1} \in A_6$ und es ist
$(ab6) = (ij)(6c) \circ (abc) \circ ((ij)(6c))^{-1} \in N$, denn N ist ein Normalteiler in A_6.

Nachtrag: Für den Beweis benötigen wir genug Elemente, um geeignet konjugieren zu können. Man beachte, dass zwei Dreizykel in S_n stets konjugiert sind, für kleine $n \in \mathbb{N}$ aber nicht notwendigerweise auch in A_n. Zum Beispiel ist $(123) = (12) \circ (132) \circ (12)^{-1}$, aber (123) und (132) sind nicht konjugiert in A_3.
Darum können wir aus der Einfachheit der Gruppe A_3 nicht folgern, dass A_4 einfach ist.
Für große n kann der Beweis aber analog geführt werden und wir sehen induktiv, dass A_n für $n \geq 5$ einfach ist. Es reicht für hinreichend große n, wenn ein einziger Dreizykel in einem Normalteiler N enthalten ist, um $N = A_n$ zu zeigen.

Aufgabe 2 (4 Punkte)
Seien p, q nicht notwendigerweise verschiedene Primzahlen. Weiterhin sei G eine Gruppe der Mächtigkeit $\#G = p^2 q$.
Zeige, dass G nicht einfach ist.

Lösung:
Fall 1: Sei zunächst $p = q$, also G eine Gruppe der Ordnung p^3.
Ist G nicht abelsch, so ist das Zentrum ein nichttrivialer Normalteiler, wie wir auf dem letzten Übungsblatt gesehen haben.
Ist G abelsch, so ist jede Untergruppe ein Normalteiler und es gibt sicher eine nichttriviale Untergruppe – es ist eine schöne Übungsaufgabe, dass die Gruppen $\mathbb{Z}/p\mathbb{Z}$ und die triviale Gruppe (bis auf Isomorphie) die einzigen Gruppen sind, die keine triviale Untergruppe haben. Konkret können wir hier z.B. für nichtzyklisches G ein beliebiges $a \in G, a \neq e_G$ hernehmen und uns eine echte Untergruppe erzeugen lassen; ist G hingegen zyklisch, so ist G isomorph zu $\mathbb{Z}/p^3\mathbb{Z}$, das als echte Untergruppe das Erzeugnis von p^2 enthält (dieses hat Ordnung p).
In beiden Fällen ist G nicht einfach.

Fall 2: Sei nun $p \neq q$. Sicher gilt auch $q \neq p^2$, denn $q \in \mathbb{P}$.
Fall 2.1: Ist $q < p$, so gelten die Bedingungen $s_p \equiv 1\ (p) \Rightarrow s_p \in \{1, p+1, .2p+1, \dots\}$ und $s_p | q$. Wegen $q < p$ folgt $s_p = 1$ und mit der Vorüberlegung des Blattes sind wir fertig.
Fall 2.2: Analog finden wir für $q > p^2$, dass es genau eine q-Sylowgruppe gibt, denn $s_q | p^2$ und $s_q \equiv 1\ (q)$, was wegen $q > p^2$ nur von $s_q = 1$ erfüllt wird.
Fall 2.3: Der letzte Fall ist $p < q < p^2$. Es gilt $s_q | p^2$, also $s_q \in \{1, p, p^2\}$: Für $s_q = 1$ sind wir direkt fertig, der Fall $s_q = p$ ist wegen $p = s_q \equiv 1\ (q)$ und $p < q$ nicht möglich.
Sei also $s_q = p^2$. Dann gibt es p^2 Untergruppen der Ordnung q, die jeweils von allen Elementen ungleich e_G erzeugt werden. Also enthalten sie je $q - 1$ Elemente der Ordnung q und der Schnitt zweier solcher Gruppen ist trivial.
Also gibt es $p^2 \cdot (q - 1) = p^2 q - p^2$ Elemente der Ordnung q in G. Es verbleibenden p^2 Elemente anderer Ordnung.
In einer p-Sylowgruppe – diese besitzt Ordnung p^2 – besitzt jedes Element Ordnung $1, p$ oder p^2 nach dem Satz von Lagrange. Da es eine p-Sylowgruppe gibt und nur p^2 Elemente Ordnung $\neq q$ haben, müssen all diese Elemente in dieser p-Sylowgruppe enthalten sein – also gilt $s_p = 1$ und wir sind fertig.

Aufgabe 3 (4 Punkte)
Zeige die folgenden Aussagen:

a) Sei $\#G = 40$. Dann ist G nicht einfach.

b) Sei $\#G = 24$. Dann ist G nicht einfach.
(*Hinweis:* Für eine Primzahl p operiert G auf der Menge der p-Sylowgruppen durch Konjugation.)

Lösung:

a) Es ist $40 = 8 \cdot 5$ und für die Anzahl s_5 der 5-Sylowgruppen gilt nach den Sylowsätzen:
$s_5 \equiv 1\ (5)$ und $s_5|8$, woraus $s_5 \equiv 1$ folgt. Es gibt also genau eine 5-Sylowgruppe. Dies ist die einzige Gruppe mit 5 Elementen, also ein Normalteiler nach der Vorbemerkung des Übungsblattes.

b) Es ist $24 = 2^3 \cdot 3$ und für die Anzahl s_2 der 2-Sylowgruppen[1] gilt
$s_3 \equiv 1\ (2)$ und $s_3|3$. Dazu gibt es zwei Möglichkeiten.
Im **Fall 1** ist $s_3 = 1$ und die Argumentation aus a) gibt uns auch hier einen nichttrivialen Normalteiler.
Im **Fall 2** gibt es drei 2-Sylowgruppen U_1, U_2, U_3. G operiert durch Konjugation auf $H := \{U_1, U_2, U_3\}$ (das haben wir in der Vorlesung gesehen) und nach dem zweiten Sylowsatz besitzt diese Operation genau eine Bahn.
Die Gruppenoperation entspricht einem Gruppenhomomorphismus $\varphi\colon G \mapsto \mathrm{Sym}(H)$.
Wieder mit dem zweiten Sylowsatz gibt es ein $g \in G$ mit $gU_1g^{-1} = U_2$, also ist $g \notin \mathrm{Kern}(\varphi)$, also $\mathrm{Kern}(\varphi) \neq G$.
Wegen $\#G > \#\mathrm{Sym}(H) = 6$ ist φ nicht injektiv, also $\mathrm{Kern}(\varphi) \neq \{e_G\}$.
Also ist der Kern ein nichttrivialer Normalteiler in G, G nicht einfach.

Nachtrag: Man überlege sich selbst, warum in a) die Anzahl der 2-Sylowgruppen und in b) die Anzahl der 3-Sylowgruppen nicht zum Erfolg geführt hätte. Es gibt weitere Argumente, mit denen ein nichttrivialer Normalteiler gefunden werden kann, zum Beispiel Elementezählen wie in Aufgabe 2.

Aufgabe 4 (4 Punkte) – Das ist ja schon wieder eine alte Klausuraufgabe!
Seien p eine Primzahl und $G = S_p$.

a) Wie viele Elemente der Ordnung p und wie viele p-Sylowgruppen gibt es in G?

b) Sei P eine p-Sylowgruppe und $N := \{g \in G : gPg^{-1} = P\}$ ihr *Normalisator*. Bestimme $\#N$.

c) Zeige, dass es in G keine Untergruppe mit $p(3p-1)$ Elementen gibt.

Lösung:

a) Das Argument haben wir schon in der Vorlesung gesehen, es sei deswegen hier nur kurz skizziert.
Die Elemente der Ordnung p sind genau die p-Zykel, davon gibt es $(p-1)!$ Stück – das ist ein einfaches Kombinatorikargument.
Wegen $\#S_p = p!$ und da p als Primteiler genau einmal in $p!$ steckt, besitzt jede p-Sylowgruppe genau p Elemente, ist also zyklisch und wird von einem p-Zykel erzeugt. Je $p-1$ p-Zykel erzeugen die gleiche Gruppe, also verbleiben $\frac{(p-1)!}{p-1} = (p-2)!$ Gruppen der Ordnung p.

b) Wir benutzen wieder die transitive Gruppenoperation von G durch Konjugation auf der Menge der p-Sylowgruppen durch Konjugation. Nach Definition ist N der Stabilisator $\mathrm{Stab}_G(P)$ von P.
P ist ein Vertreter der einen Bahn aller p-Sylowgruppen. Mit der Bahnbilanzformel und a) lernen wir $(p-2)! = [G : \mathrm{Stab}_G(P)] = [G : N] = \frac{\#G}{\#N} = \frac{p!}{\#N}$ und Umstellen ergibt $\#N = p(p-1)$.

[1] mit 8 Elementen

c) Nehmen wir an, es gebe eine solche Untergruppe U. Wir berechnen die Anzahl s_p der p-Sylowgruppen (mit p Elementen) in U.
Es gilt $s_p | 3p - 1$, also insbesondere $s_p \leq 3p - 1$ und $s_p \equiv 1$ (p). Beide Bedingungen erfordern $s_p \in \{1, p + 1, 2p + 1\}$.
– **Annahme 1:** $s_p = 2p + 1 \Rightarrow 2p + 1 | 3p - 1$ und da $2 \cdot (2p + 1) > 3p - 1$ ist, folgt $2p + 1 = 3p - 1$, also $p = 2$. Aber in S_2 gibt es sicher keine Untergruppe mit $2 \cdot (3 \cdot 2 - 1) = 10$ Elementen! WIDERSPRUCH
– **Annahme 2:** $S_p = p + 1$. Wegen $p + 1 < 3p - 1$ und $3(p + 1) > 3p - 1$ folgt $2(p + 1) = 3p - 1$, also $p = 3$ und U ist eine Untergruppe mit 24 Elementen in der S_3. WIDERSPRUCH.
– Also ist $s_p = 1$, es gibt genau eine p-Sylowgruppe P, auf der U trivial durch Konjugation operiert, also ist $U \subseteq \mathrm{Stab}_G(P)$. Wegen $\#U = p(3p - 1) > p(p - 1) = \#\mathrm{Stab}_G(P)$ ist das ein WIDERSPRUCH, es kann keine solche Gruppe U geben.