Algebra II, SoSe 2012 – Lösung Blatt 9

9.1. Es genügt zu zeigen:

G besitzt einen Normalteiler H mit $\operatorname{ord} H = p^2$ oder $\operatorname{ord} H = q$. (*)

Denn nach Vorlesung ist H als Gruppe von Primzahlpotenzordnung auflösbar und analog wegen

$$\operatorname{ord} G/H = q \quad \text{oder} \quad \operatorname{ord} G/H = p^2$$

auch G/H. Da H Normalteiler ist, folgt die Auflösbarkeit von G damit aus Satz 26.5.

Wir zeigen also (*):

Sei s_p die Anzahl der p-Sylowgruppen in G und s_q die Anzahl der q-Sylowgruppen.

Nach Algebra I genügt es also zu zeigen:

$$s_p = 1 \quad \text{oder} \quad s_q = 1.$$

Die Sylowsätze liefern:

$$s_p \equiv 1 \bmod p, \quad s_p \mid q$$

$$s_q \equiv 1 \bmod q, \quad s_q \mid p^2.$$

$s_p \mid q \Rightarrow s_p \in \{1, q\}$. Ist $s_p = 1$, so sind wir fertig.

Gelte also $s_p = q$. Wir müssen zeigen, dass $s_q = 1$ gilt.

$s_p \equiv 1 \bmod p$

$\Rightarrow q = s_p = k \cdot p + 1$ für ein $k \in \mathbb{Z}$.

$\Rightarrow p \mid q-1$ (1)

Es ist $s_q \mid p^2$, d.h. $s_q \in \{1, p, p^2\}$. Gilt $s_q = 1$, so sind wir fertig. Analog zu eben erhalten wir aus $s_q \equiv 1 \bmod q$ zunächst

$$q \mid s_q - 1 \qquad (2)$$

- $s_q = p$. Dann haben wir mit (1) und (2):

  $p \mid q-1$, insb. $p \leq q-1$

  $q \mid p-1$, insb. $q \leq p-1$.

  Insgesamt ergibt sich $q \leq p-1 \leq q-2$ ↯

- $s_q = p^2$. Aus (2) folgt dann:

  $q \mid p^2 - 1$ d.h. $q \mid (p-1)(p+1)$.

  $\Rightarrow q \mid (p-1)$ oder $q \mid (p+1)$

Da der Fall $q \mid (p-1)$ wie oben zu einem Widerspruch führt, muss also $q \mid (p+1)$ gelten, d.h. insbesondere

$$q - 1 \leq p.$$

Andererseits haben wir mit (1) aber

$$p \mid (q-1).$$

$\Rightarrow$ Es muss $p = q-1$ gelten.

Da p und q Primzahlen sind muss also

$$p = 2 \text{ und } q = 3$$

gelten. (Denn: Wegen $p = q-1$ muss eine der Zahlen gerade, d.h. gleich 2 sein...)

Wir haben also $s_3 = 4$ (p^2..) sowie $s_2 = 3$ in einer Gruppe der Ordnung 12.

$s_3 = 4 \Rightarrow$ Haben 4 verschiedene Untergruppen der Ordnung 3

$\Rightarrow$ 8 Elemente in G haben Ordnung 3.

$s_2 = 3 \Rightarrow$ Haben 3 verschiedene Untergruppen der Ordnung 4

$\Rightarrow$ 9 Elemente, deren Ordnung > 1 ist und 4 teilt, d.h. ungleich 3 ist $\lightning$ $\operatorname{ord} G = 12$.

Es muss also doch $s_q = 1$ gelten und wir sind fertig.

$\blacksquare$

9.2. (i)

$$\mathbb{Z} \rhd 3\mathbb{Z} \rhd 12\mathbb{Z} \rhd 60\mathbb{Z} \rhd \{0\}$$

verfeinert die zweite Reihe und besitzt Faktoren isomorph zu $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/5\mathbb{Z}$, $\mathbb{Z}$.

Analog:

$$\mathbb{Z} \rhd 3\mathbb{Z} \rhd 15\mathbb{Z} \rhd 60\mathbb{Z} \rhd \{0\}$$

verfeinert die erste Reihe und besitzt Faktoren isomorph zu $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/5\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}$.

(ii) Möglichkeiten:

- $\mathbb{Z}/24\mathbb{Z} \rhd 3\mathbb{Z}/24\mathbb{Z} \rhd 6\mathbb{Z}/24\mathbb{Z} \rhd 12\mathbb{Z}/24\mathbb{Z} \rhd 24\mathbb{Z}/24\mathbb{Z}$

  Faktoren: $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}$ (alle einfach, also Kompositionsreihe)

- $\mathbb{Z}/24\mathbb{Z} \rhd 2\mathbb{Z}/24\mathbb{Z} \rhd 6\mathbb{Z}/24\mathbb{Z} \rhd 12\mathbb{Z}/24\mathbb{Z} \rhd 24\mathbb{Z}/24\mathbb{Z}$

  Faktoren: $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}$

- $\mathbb{Z}/24\mathbb{Z} \rhd 2\mathbb{Z}/24\mathbb{Z} \rhd 4\mathbb{Z}/24\mathbb{Z} \rhd 12\mathbb{Z}/24\mathbb{Z} \rhd 24\mathbb{Z}/24\mathbb{Z}$

  Faktoren: $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}$

- $\mathbb{Z}/24\mathbb{Z} \rhd 2\mathbb{Z}/24\mathbb{Z} \rhd 4\mathbb{Z}/24\mathbb{Z} \rhd 8\mathbb{Z}/24\mathbb{Z} \rhd 24\mathbb{Z}/24\mathbb{Z}$

  Faktoren: $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$.

(iii) $\mathbb{Z}/p^k\mathbb{Z}$ besitzt genau eine Kompositionsreihe:

$$\mathbb{Z}/p^k\mathbb{Z} \rhd p\mathbb{Z}/p^k\mathbb{Z} \rhd p^2\mathbb{Z}/p^k\mathbb{Z} \rhd \dots \rhd p^{k-1}\mathbb{Z}/p^k\mathbb{Z} \rhd p^k\mathbb{Z}/p^k\mathbb{Z}$$

in der alle Faktoren $\mathbb{Z}/p\mathbb{Z}$ sind. ∎

9.3. Wir verwenden die folgende Korrespondenz:

Sei $\varphi: G \to G'$ ein surjektiver Gruppenhomomorphismus mit $K = \operatorname{Kern} \varphi$. Dann wird durch

$$U \longmapsto \varphi(U)$$

eine Bijektion von der Menge

$$\mathcal{U} = \{U \subset G \mid U \text{ Untergruppe}, K \subset U\}$$

auf die Menge $\mathcal{U}'$ der Untergruppen von G' definiert.
Die Umkehrabbildung ist

$$U' \longmapsto \varphi^{-1}(U')$$

und es gilt für $U \in \mathcal{U}$ bzw. $U' \in \mathcal{U}'$ stets:

$$U \triangleleft G \iff \varphi(U) \triangleleft G'$$
$$U' \triangleleft G' \iff \varphi^{-1}(U') \triangleleft G. \qquad (*).$$

Damit zur Aufgabe.

(i) Sei

$$G = G_1 \overset{\triangleright}{\neq} G_2 \overset{\triangleright}{\neq} \cdots \overset{\triangleright}{\neq} G_m \overset{\triangleright}{\neq} G_{m+1} = \{e\}.$$

eine Kompositionsreihe ohne Wiederholungen.

Zu zeigen: $m = n$.

Die Faktoren G_i/G_{i+1} sind nach 26.7. auflösbar.

Also gilt für $i \in \{1, \dots, m\}$

Entweder ist G_i/G_{i+1} abelsch oder wir können (mit (*)) Gruppen $H^{(i)}_1, \dots, H^{(i)}_{l_{i+1}}$ finden, mit

$$G_i = H^{(i)}_1 \supsetneq H^{(i)}_2 \supsetneq \dots \supsetneq H^{(i)}_{l_{i+1}} = G_{i+1}$$

so dass $H^{(i)}_j / H^{(i)}_{j+1}$ für $j \in \{1, \dots, l_i\}$ abelsch ist.

Nach dem Hauptsatz über endlich erzeugte abelsche Gruppen können wir (wieder mit (*)) Gruppen

$$H^{(i)}_j = H^{(j,i)}_1 \supsetneq \dots \supsetneq H^{(j,i)}_{k_{j+1}} = H^{(i)}_{j+1}$$

konstruieren, so dass die Faktoren jeweils zyklisch von der Ordnung p sind.

<u>Also:</u> Entweder sind alle Faktoren der Reihe zyklisch von der Ordnung p, oder die Reihe kann verfeinert werden.

Letzteres ist aber nicht möglich, da wir eine Kompositionsreihe vorliegen haben.

$\Rightarrow$ Alle Faktoren sind isomorph zu $\mathbb{Z}/p\mathbb{Z}$.

Aber: Eine Gruppe der Ordnung p^n liefert nur n verschiedene Faktoren der Ordnung p.

$\Rightarrow$ Für die Kompositionsreihe zu Beginn gilt $m=n$ und $G_i/G_{i+1} \cong \mathbb{Z}/p\mathbb{Z}$ für $i \in \{1,\dots,n\}$.

(ii) Genügt zu zeigen:

$\exists$ Normalreihe von G, in der H einer der Terme ist (#).

Ist (#) gezeigt, dann liefert Anwendung von (*) eine Normalreihe mit abelschen Faktoren und H als Term.

Mit (*) und dem Hauptsatz über endlich erzeugte abelsche Gruppen erhalten wir Verfeinerung zu Normalreihe mit zyklischen Faktoren der Ordnung p und H als Term. $\Rightarrow$ Haben passende Kompositionsreihe konstruiert.

Wir müssen also (#) zeigen.

$\operatorname{ord} G = p^n$.

Beweis durch Induktion nach n:

- Induktionsanfang: $n=1$.
  Nichts zu zeigen, da die einzigen Untergruppen überhaupt G und $\{e\}$ sind.
- Induktionsschritt: „$(n-1) \to n$"
  Es ist $Z(G) \neq \{e\}$.
  Wir unterscheiden die Fälle

(a) $Z(G) \subset H$

(b) $Z(G) \not\subset H$

Zu (a):

Auf $G/Z(G)$ können wir die Induktionsvoraussetzung anwenden (mit der Untergruppe $H/Z(G)$). Wir erhalten Normalreihe mit $H/Z(G)$ als Term. Vermöge (*) liefert diese eine Normalreihe von G, welche H als Term enthält.

Zu (b):

Sei $U < G$ die von H und $Z(G)$ erzeugte Untergruppe. Es ist $H \trianglelefteq U$. Nach Induktionsvoraussetzung gibt es eine Normalreihe von $G/Z(G)$ mit $U/Z(G)$ als Term:

$$\frac{G}{Z(G)} = \frac{G_1}{Z(G)} \rhd \frac{G_2}{Z(G)} \rhd \dots \rhd \frac{U}{Z(G)} \rhd \frac{Z(G)}{Z(G)}.$$

Dann liefert (*) die Normalreihe

$$G = G_1 \rhd G_2 \rhd \dots \rhd U \rhd \{e\}$$

von G, welche wir mit H verfeinern können:

$$G = G_1 \rhd G_2 \rhd \dots \rhd U \rhd H \rhd \{e\}.$$

$\Rightarrow$ (#)

∎

9.4. (i) • Betrachte $\langle\sigma\rangle = \{\sigma^k \mid k \in \mathbb{Z}\}$. ← genügt sogar $k \in \mathbb{N}$.

$$\sigma\tau\sigma = \tau \Rightarrow \sigma^k \tau \sigma^k = \sigma^{k-1}\tau\sigma^{k-1} = \ldots = \tau$$

$$\Rightarrow \tau\sigma^k\tau^{-1} = (\sigma^k)^{-1}$$

Also ist $\tau\langle\sigma\rangle\tau^{-1} \subset \langle\sigma\rangle$ und natürlich

$$\sigma\langle\sigma\rangle\sigma^{-1} \subset \langle\sigma\rangle.$$

Da sich jedes $\delta \in D_n$ als Produkt mit Faktoren σ und τ schreiben lässt, erhalten wir

$$\delta\langle\sigma\rangle\delta^{-1} \subset \langle\sigma\rangle \quad \forall \delta \in D_n.$$

$$\Rightarrow \langle\sigma\rangle \triangleleft D_n \quad \text{(Normalteiler)}$$

• Jede Untergruppe von $\langle\sigma\rangle$ ist ebenfalls zyklisch, d.h. von der Form $\langle\sigma^m\rangle$ für ein $m \in \mathbb{N}$ mit $m \mid n$.
Es genügt also zu zeigen:

$$\delta\langle\sigma^m\rangle\delta^{-1} \subset \langle\sigma^m\rangle \quad \forall \delta \in D_n.$$

Nach dem ersten Punkt gilt zumindest $\delta\langle\sigma^m\rangle\delta^{-1} \leq \langle\sigma\rangle$.
(Untergruppe da Bild von $\langle\sigma^m\rangle$ unter Innerem Automorphismus)
Es ist $\operatorname{ord}\sigma^m = \frac{n}{m}$ und

$$\delta\sigma^m\delta^{-1}, \delta\sigma^{2m}\delta^{-1}, \ldots, \delta\sigma^{\frac{n}{m}\cdot m}\delta^{-1}$$

sind $\frac{n}{m}$ verschiedene Elemente. Es ist also

$\delta \langle \sigma^m \rangle \delta^{-1}$ eine Untergruppe von $\langle \sigma \rangle$ der Ordnung $\frac{n}{m}$.

Da $\langle \sigma \rangle$ zyklisch ist, ist $\langle \sigma^m \rangle < \langle \sigma \rangle$ die einzige Untergruppe der Ordnung $\frac{n}{m}$.

$\Rightarrow \quad \delta \langle \sigma^m \rangle \delta^{-1} = \langle \sigma^m \rangle$.

Insgesamt: Jede Untergruppe von $\langle \sigma \rangle$ ist Normalteiler in D_n.

(ii) Nach Vorlesung besteht $[D_n, D_n]$ aus allen endlichen Produkten von Kommutatoren in D_n. Wie in (i) gilt:

$$\tau \sigma^i \tau^{-1} = \sigma^{-i} \qquad (\forall i \in \mathbb{Z}).$$

- Zunächst: σ^2 kann als Kommutator geschrieben werden, liegt also in $[D_n, D_n]$:

$$[\sigma\tau, \tau] = \sigma\tau\tau\tau^{-1}\sigma^{-1}\tau^{-1} = \sigma \underbrace{\tau\sigma^{-1}\tau^{-1}}_{=\sigma} = \sigma^2.$$

$\Rightarrow \quad \langle \sigma^2 \rangle < [D_n, D_n]$.

- Wir zeigen nun: Jeder Kommutator liegt in $\langle \sigma^2 \rangle$.

Dazu:

$$D_n = \{ \sigma^i \tau^j \mid 0 \leq i \leq n-1, \ 0 \leq j \leq 1 \}.$$

Wir betrachten die verschiedenen Möglichkeiten für j getrennt:

„$j_1 = j_2 = 0$:"

$$[\sigma^{i_1}, \sigma^{i_2}] = \sigma^{i_1}\sigma^{i_2}\sigma^{-i_1}\sigma^{-i_2} = \sigma^0 = e \in \langle\sigma^2\rangle.$$

„$j_1 = j_2 = 1$:"

$$[\sigma^{i_1}\tau, \sigma^{i_2}\tau] = \sigma^{i_1}\tau\sigma^{i_2}\tau\tau^{-1}\sigma^{-i_1}\tau^{-1}\sigma^{-i_2}$$

$$= \sigma^{i_1}\underbrace{\tau\sigma^{i_2-i_1}\tau}_{=\sigma^{i_1-i_2}}{}^{-1}\sigma^{-i_2}$$

$$= \sigma^{i_1-i_2+i_1-i_2} = \sigma^{2(i_1-i_2)} \in \langle\sigma^2\rangle.$$

„$j_1 = 1,\ j_2 = 0$":

$$[\sigma^{i_1}\tau, \sigma^{i_2}] = \sigma^{i_1}\underbrace{\tau\sigma^{i_2}\tau}{}^{-1}\sigma^{-i_1}\sigma^{-i_2}$$

$$= \sigma^{i_1-i_2-i_1-i_2}$$

$$= \sigma^{2(-i_2)} \in \langle\sigma^2\rangle.$$

„$j_1 = 0,\ j_2 = 1$":

$$[\sigma^{i_1}, \sigma^{i_2}\tau] = \sigma^{i_1}\sigma^{i_2}\underbrace{\tau\sigma^{-i_1}\tau}{}^{-1}\sigma^{-i_2}$$

$$= \sigma^{i_1+i_2+i_1-i_2} = \sigma^{2i_1} \in \langle\sigma^2\rangle.$$

Damit liegen auch alle Produkte solcher Kommutatoren in $\langle\sigma^2\rangle$ (da Gruppe). $\Rightarrow [D_n, D_n] \subset \langle\sigma^2\rangle$.

▨