Algebra I, WiSe 2011\2012 - Lösung Blatt 6

6.1. Sei P eine p-Sylowgruppe in G.

Zu zeigen: $H \subset P$.

Nach Vorlesung (einer der Sylow-Sätze) ist H in einer zu P Konjugierten p-Sylowgruppe enthalten, d.h.

$$\exists \; a \in G : \; H \subset aPa^{-1}.$$

$$\Rightarrow \quad a^{-1}Ha \subset P$$

(denn $x \in a^{-1}Ha \Rightarrow x = a^{-1}ha$ für ein $h \in H \subset aPa^{-1}$, d.h. $h = apa^{-1}$ für ein $p \in P$. $\Rightarrow x = a^{-1}ha = a^{-1}apa^{-1}a = p \in P$)

Nach Voraussetzung ist $H \lhd G$, d.h.

$$\forall g \in G \text{ ist } gHg^{-1} = H$$

Speziell für $g = a^{-1}$ folgt:

$$a^{-1}Ha = a^{-1}H(a^{-1})^{-1} \overset{\text{s.o.}}{=} H$$

$$\Rightarrow \quad H = a^{-1}Ha \subset P.$$

$\blacksquare$

6.2. Überlegung vorab:

Sei U Gruppe mit $\operatorname{ord} U = p$ (p Primzahl).

$\overset{\text{Lagrange}}{\Longrightarrow}$ jedes Element $u \in U, u \neq e$ hat Ordnung p, erzeugt also die gesamte Gruppe U.

Also: Sind U_1, U_2 Untergruppen einer Gruppe G mit

$$\operatorname{ord} U_1 = \operatorname{ord} U_2 = p \quad (p \text{ Primzahl})$$

so ist entweder $U_1 \cap U_2 = \{e\}$ oder $U_1 = U_2$. $(*)$

(denn: $U_1 \cap U_2 \neq \{e\} \Rightarrow \exists\, u \in U_1 \cap U_2$ mit $u \neq e$.

$\overset{\text{s.o.}}{\Longrightarrow} U_1 = \langle u \rangle = U_2$)

Damit zur Aufgabe:

(i) $30 = 2 \cdot 3 \cdot 5$.

Sei s_p die Anzahl der p-Sylowgruppen in G.

- $s_3 \equiv 1 \mod 3$ und $s_3 \mid 10$

($s_3 \in \{1, 4, 7, 10, \ldots\}$ und $s_3 \in \{1, 2, 5, 10\}$)

$\Rightarrow s_3 = 1$ oder $s_3 = 10$

- $s_5 \equiv 1 \mod 5$ und $s_5 \mid 6$

($s_5 \in \{1, 6, 11, \ldots\}$ und $s_5 \in \{1, 2, 3, 6\}$)

$\Rightarrow s_5 = 1$ oder $s_5 = 6$.

$\lightning$ $s_3 = 10$ und $s_5 = 6$.

$\Rightarrow$ G enthält 10 <u>verschiedene</u> Gruppen der Ordnung 3, und jede dieser Gruppen 2 Elemente der Ordnung 3.

$\overset{(*)}{\Longrightarrow}$ G enthält 20 Elemente der Ordnung 3.

Außerdem: G enthält 6 <u>verschiedene</u> Gruppen der Ordnung 5 und jede dieser Gruppen 4 Elemente der Ordnung 5

$\overset{(*)}{\Longrightarrow}$ G enthält 24 Elemente der Ordnung 5.

$\Longrightarrow \quad |G| \geq 45 \quad \lightning \; |G| = 30.$

Also folgt:

$s_3 = 1$ oder $s_5 = 1$

$\Downarrow$ VL

Die 3-Sylowgruppe in G ist nichttrivialer Normalteiler

Die 5-Sylowgruppe in G ist nichttrivialer Normalteiler.

In jedem Fall besitzt G also nichttrivialen Normalteiler.

(ii) $56 = 2^3 \cdot 7$

Sei s_p die Anzahl der p-Sylowgruppen in G.

- $s_2 \equiv 1 \mod 2$ und $s_2 \mid 7$

  ($s_2 \in \{1, 3, 5, 7, \dots\}$ und $s_2 \in \{1, 7\}$)

  $\Longrightarrow s_2 = 1$ oder $s_2 = 7$

- $s_7 \equiv 1 \mod 7$ und $s_7 \mid 8$

  ($s_7 \in \{1, 8, 15, \dots\}$ und $s_7 \in \{1, 2, 4, 8\}$)

  $\Longrightarrow s_7 = 1$ oder $s_7 = 8$

↯ $s_2 = 7$ und $s_7 = 8$.

$s_7 = 8 \xRightarrow[\text{ord.}=7]{(*)}$ In G gibt es $6 \cdot 8 = 48$ verschiedene Elemente der Ordnung 7.

$s_2 = 7$ $(\text{ord.} = 2^3) \Rightarrow$ In G gibt es nach Lagrange <u>mehr als</u> 7 verschiedene Elemente deren Ordnung positive Potenz von 2 (und damit $\neq 7$) ist.

$\Rightarrow$ G besitzt mindestens $8 + 48 = 56$ Elemente, deren Ordnung > 1 ist ↯ $|G| = 56$, da $e \in G$ mit $\text{ord}\, e = 1$.

Also: $s_2 = 1$ oder $s_7 = 1$.

Wie in (i) muss G also entweder eine 2-Sylowgruppe oder eine 7-Sylowgruppe besitzen, welche Normalteiler (und nichttrivial) ist.

$\blacksquare$

6.3. (i) Seien $a_1, a_2 \in M$ mit $a_1 \neq a_2$.

Wir zeigen, dass a_1 und a_2 über $\mathbb{Z}$ nicht linear unabhängig sind.

Zunächst $\exists\, r_1, r_2 \in \mathbb{Z}$, $s_1, s_2 \in \mathbb{N}$ mit $r_1 \neq r_2$ so dass

$$a_1 = \frac{r_1}{s_1} \quad \text{und} \quad a_2 = \frac{r_2}{s_2} \quad \text{gilt.}$$

$$\Rightarrow \quad r_2 s_1 \cdot a_1 + (-r_1 s_2) \cdot a_2 = r_1 r_2 - r_1 r_2 = 0$$

Wegen $a_1 \neq a_2$ ist $r_1 s_2 \neq r_2 s_1$ und damit

$$(r_2 s_1, -r_1 s_2) \neq (0,0) \quad \text{(„nicht beide Null")}$$

$\Rightarrow$ Haben nichttriviale Linearkombination der 0 gefunden

$\Rightarrow$ M nicht frei.

(ii) $\lightning$ $f: \mathbb{Q} \to \mathbb{Z}$ ist Isomorphismus (bzgl. additiver Struktur)

$$\xRightarrow[\text{Aufgabe 4}]{\text{Blatt 2}} \quad f \equiv 0 \quad \lightning_{f \text{ Isomorphismus}}$$

(iii) $\lightning$ $(\mathbb{Q}, +)$ ist frei $\Rightarrow$ $(\mathbb{Q}, +)$ besitzt eine $\mathbb{Z}$-Basis $M \subset \mathbb{Q}$.

$\overset{(i)}{\Rightarrow}$ $|M| = 1$ Schreibe $M = \{m\}$ $(m \in \mathbb{Q})$

$\Rightarrow$ $\mathbb{Q} = \mathbb{Z} \cdot m$, d.h. zu jedem $q \in \mathbb{Q}$ $\exists!\, z_q \in \mathbb{Z}$ mit $q = z_q m$

$\Rightarrow$ $f: \mathbb{Q} \to \mathbb{Z}$, $q \mapsto z_q$ ist Isomorphismus (bzgl. additiver Struktur) $\lightning_{(ii)}$

$\blacksquare$

6.4. (i) Zeige zunächst: τ wohldefiniert, d.h.

- $g \in G \Rightarrow \tau(g)$ ist wohldefinierte Abbildung $G/U \to G/U$.

  Gelte $\bar{h} = \bar{k} \Rightarrow k^{-1} h \in U$

  $\Rightarrow (gk)^{-1}(gh) = k^{-1} g^{-1} g h = k^{-1} h \in U$

  $\Rightarrow \overline{gh} = \overline{gk}$ ok.

- $g \in G \Rightarrow \tau(g) \in \mathcal{S}(G/U)$, d.h. $\tau(g): G/U \to G/U$ ist bijektiv.

  $|G| < \infty \Rightarrow |G/U| < \infty \xRightarrow[\text{satz}]{\text{Schubladen-}}$ genügt zu zeigen $\tau(g)$ surjektiv.

  Sei also $\bar{k} \in G/U$ mit Repräsentant $k \in G$.

  G Gruppe $\Rightarrow l_g$ bijektiv $\Rightarrow \exists\, h \in G: g \cdot h = k$

  $\Rightarrow \tau(g)(\bar{h}) = \overline{gh} = \bar{k}$, also ist $\tau(g)$ surjektiv, ok.

Zeige nun: τ ist Gruppenhomomorphismus.

Es ist $\tau(g) \circ \tau(h)(\bar{k}) = \tau(g)(\overline{hk}) = \overline{g(hk)} = \overline{(gh)k}$

$= \tau(g \cdot h)(\bar{k})$

$\xRightarrow[\text{beliebig}]{\bar{k} \in G/U} \tau(g \cdot h) = \tau(g) \circ \tau(h) \quad \forall g, h \in G.$

Zeige: $\text{Kern}(\tau) \subset U$.

$g \in \text{Kern}(\tau) \Leftrightarrow \tau(g) = id$

$\Leftrightarrow \overline{gh} = \bar{h} \quad \forall h \in G$

$\xRightarrow[h=e]{\text{speziell für}} \bar{g} = \bar{e}$, d.h. $g \in U$

Also: $\text{Kern}(\tau) \subset U$.

(ii) Wegen $m = [G:U] = |G/U|$ folgt

$$|\mathcal{S}(G/U)| = m!$$

Es ist $\mathrm{Kern}\,\varphi \trianglelefteq G$ (als Kern), also folgt aus dem Homomorphiesatz:

$$G/\mathrm{Kern}(\varphi) \cong \mathrm{Bild}(\varphi) \subset \mathcal{S}(G/U) \text{ Untergruppe}$$

Mit dem Satz von Lagrange folgt also

$$[G:\mathrm{Kern}(\varphi)] = |G/\mathrm{Kern}(\varphi)| \overset{\text{s.o.}}{=} |\mathrm{Bild}(\varphi)| \underset{\text{Lagrange}}{\mid} m!$$

(d.h. die zweite Aussage ist gezeigt.)

Andererseits gilt wegen $\mathrm{Kern}(\varphi) \subset U \subset G$ nach Vorlesung

$$\begin{aligned}[G:\mathrm{Kern}(\varphi)] &= [G:U]\,[U:\mathrm{Kern}(\varphi)] \\ &= m \cdot [U:\mathrm{Kern}(\varphi)]\end{aligned}$$

$$\Rightarrow \quad m \mid [G:\mathrm{Kern}(\varphi)]$$

(d.h. die erste Aussage ist gezeigt.

(iii) $|G| = 36 = 3^2 \cdot 4$

Sei $U \subset G$ eine 3-Sylowgruppe von G (existiert nach Vorlesung)

$\Rightarrow |U| = 9 \Rightarrow [G : U] = 4$

Für den zugehörigen Homomorphismus φ (vgl. (i)) folgt also nach (ii):

- $[G : \mathrm{Kern}(\varphi)] \mid 4! = 24 < 36$

  $\Rightarrow \mathrm{Kern}(\varphi) \neq \{e\}$

- $4 \mid [G : \mathrm{Kern}(\varphi)]$, d.h. $[G : \mathrm{Kern}(\varphi)] > 1$

  $\Rightarrow \mathrm{Kern}(\varphi) \neq G$

Also: $\mathrm{Kern}(\varphi)$ ist der gesuchte nichttriviale Normalteiler von G.

$\blacksquare$