Algebra I, WiSe 2011\2012 – Lösung Blatt 13

13.1. $\forall a \in G$ ist $aUa^{-1} \cong U$, d.h. insbesondere

$$|aUa^{-1}| = |U| = k$$

Da $aUa^{-1} \subset G$ Untergruppe ist, und $U \subset G$ die einzige Untergruppe der Ordnung k ist, folgt

$$aUa^{-1} = U \qquad \forall a \in G$$

$\Rightarrow U \triangleleft G$.

(Bemerkung: Der Isomorphismus ist wie üblich für $a \in G$ durch den inneren Automorphismus (vgl. VL!)

$$\begin{aligned} \tau_a : G &\longrightarrow G \\ g &\longmapsto aga^{-1} \end{aligned}$$

gegeben.)

$\blacksquare$

<u>13.2.</u> Sei

$$G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}.$$

G' sei homomorphes Bild von G, d.h. es gibt einen surjektiven Homomorphismus

$$\varphi : G \longrightarrow G'.$$

Da $\operatorname{Kern}\varphi \lhd G$ ist, folgt mit dem Homomorphiesatz:

$$G' \cong G/\operatorname{Kern}\varphi .$$

Da G abelsch ist, wird jede Untergruppe von G in dieser Weise als Kern realisiert (vgl. VL.).

Wir müssen also alle Untergruppen von G bestimmen!

Untergruppen der Faktoren: (mit Lagrange, u.a.)

$\mathbb{Z}/2\mathbb{Z}$: $\quad U_0^{(2)} = \{e\}$, $\quad U_1^{(2)} = \mathbb{Z}/2\mathbb{Z}$

$\mathbb{Z}/3\mathbb{Z}$: $\quad U_0^{(3)} = \{e\}$, $\quad U_1^{(3)} = \mathbb{Z}/3\mathbb{Z}$

$\mathbb{Z}/4\mathbb{Z}$: $\quad U_0^{(4)} = \{e\}$, $\quad U_1^{(4)} = 2\mathbb{Z}/4\mathbb{Z}$, $\quad U_2^{(4)} = \mathbb{Z}/4\mathbb{Z}$.

Da es in $\mathbb{Z}/2\mathbb{Z}$ und $\mathbb{Z}/3\mathbb{Z}$ nur die trivialen Untergruppen gibt, erhalten wir alle Untergruppen von G durch

$$U_i^{(2)} \times U_j^{(3)} \times U_k^{(4)} \quad \text{mit } i \in \{0,1\},\ j \in \{0,1\},\ k \in \{0,1,2\}.$$

Für G' gibt es also (bis auf Isomorphie) nur die Möglichkeiten

$$\frac{G}{U_i^{(2)} \times U_j^{(3)} \times U_k^{(4)}} \quad \text{mit } i \in \{0,1\},\ j \in \{0,1\},\ k \in \{0,1,2\}.$$

Vereinfachung: Definieren wir i', j', k' durch

$$i + i' = 1 \quad , \quad j + j' = 1 \quad , \quad k + k' = 2$$

mit $i' \in \{0,1\}$, $j' \in \{0,1\}$, $k' \in \{0,1,2\}$, dann:

$$\frac{G}{U_i^{(2)} \times U_j^{(3)} \times U_k^{(4)}} \cong U_{i'}^{(2)} \times U_{j'}^{(3)} \times U_{k'}^{(4)} .$$

$\blacksquare$

(Bemerkung: Es ist $U_1^{(4)} = 2\mathbb{Z}/4\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z}$.)

<u>13.3.</u> Untergruppen von $\mathbb{Z}/12\mathbb{Z}$ sind von der Form

$$k\mathbb{Z}/12\mathbb{Z} \quad \text{mit } k \in \mathbb{N},\ k \mid 12.$$

(d.h. $k \in \{1, 2, 3, 4, 6, 12\}$).

Nach dem 2. Isomorphiesatz gilt:

$$\left(\mathbb{Z}/12\mathbb{Z}\right) \Big/ \left(4\mathbb{Z}/12\mathbb{Z}\right) \cong \mathbb{Z}/4\mathbb{Z}.$$

Wähle also $U = 4\mathbb{Z}/12\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z}$, dann ist U

die gesuchte Untergruppe. ∎

13.4. Es ist $111 = 3 \cdot 37$.

$\Rightarrow$ Es gibt die trivialen Untergruppen und (Lagrange) die Untergruppen der Ordnungen 3 und 37 (das sind Sylowgruppen!). $(*)$

Sei s_{37} die Anzahl der 37-Sylowgruppen und s_3 die Anzahl der 3-Sylowgruppen. Dann:

- $s_{37} \equiv 1 \mod 37$ und $s_{37} \mid 3 \Rightarrow s_{37} = 1$.

  Also gibt es eine Untergruppe der Ordnung 37 und diese ist ein nichttrivialer Normalteiler.

- $s_3 \equiv 1 \mod 3$ und $s_3 \mid 37 \Rightarrow s_3 = 1$ oder $s_3 = 37$

  $s_3 = 37 \Rightarrow$ Es gibt 37 zueinander Konjugierte Untergruppen der Ordnung 3.

  $\Rightarrow$ Diese sind keine Normalteiler.

  Mit $(*)$ folgt also: Es gibt genau einen nichttrivialen Normalteiler $\lightning$ Voraussetzung.

$\Rightarrow s_3 = 1$.

Seien U_3 bzw. U_{37} die 3- bzw. 37-Sylowgruppen.

$\Rightarrow U_3, U_{37}$ sind Normalteiler

$\operatorname{ord} G = 111 = 3 \cdot 37 = \operatorname{ord} U_3 \cdot \operatorname{ord} U_{37}$

und $\operatorname{ggT}(\operatorname{ord} U_3, \operatorname{ord} U_{37}) = \operatorname{ggT}(3, 37) = 1.$

$$\xRightarrow[(i)]{\text{ÜA 7.2}} \quad G = U_3 \oplus U_{37} \cong U_3 \times U_{37}$$

$$\cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/37\mathbb{Z}$$

3, 37 Primzahlen

$$\cong \mathbb{Z}/111\mathbb{Z}.$$

$\operatorname{ggT}(3,37)=1$

Also ist $G \cong \mathbb{Z}/111\mathbb{Z}$ und damit zyklisch.

$\blacksquare$

13.5. Vorüberlegung:

Die Elemente der Gestalt $a_1 x_1 + \dots + a_n x_n$ für $(x_1, \dots, x_n) \in \mathbb{Z}^n$ sind genau die Elemente des Ideals

$$(a_1, \dots, a_n) \subset \mathbb{Z}.$$

Sei $d = \operatorname{ggT}(a_1, \dots, a_n)$. Dann folgt (VL):

$$(a_1, \dots, a_n) = (d).$$

- Sei nun für $b \in \mathbb{Z}$ die Gleichung lösbar (in $\mathbb{Z}^n$).

$$\overset{\text{Vorüber-}}{\underset{\text{legung}}{\Longrightarrow}} \quad b \in (a_1, \dots, a_n) = (d)$$

$$\Rightarrow \quad d \mid b \qquad \text{ok.}$$

- Gelte umgekehrt für $b \in \mathbb{Z}$: $d \mid b$.

Wegen $(d) = (a_1, \dots, a_n)$, $\exists\ (y_1, \dots, y_n) \in \mathbb{Z}^n$ mit

$$y_1 a_1 + \dots + y_n a_n = d.$$

$d \mid b \Rightarrow \exists\ t \in \mathbb{Z}$ mit $d \cdot t = b$. Definiere

$x_1 := t \cdot y_1, \dots, x_n := t \cdot y_n \Rightarrow (x_1, \dots, x_n) \in \mathbb{Z}^n$ und

$$x_1 a_1 + \dots + x_n a_n = t y_1 a_1 + \dots + t y_n a_n = t(y_1 a_1 + \dots + y_n a_n)$$
$$= td = b.$$

Die Gleichung ist also lösbar. $\blacksquare$

13.6.

$\mathfrak{p}$ Primideal $\Rightarrow$ $R/\mathfrak{p}$ ist Integritätsbereich.

In der Vorlesung wurde gezeigt, dass ein endlicher Integritätsbereich ein Körper ist.

Da nach Voraussetzung $R/\mathfrak{p}$ endlich ist, folgt:

$$R/\mathfrak{p} \text{ ist Körper}$$

$\Rightarrow$ $\mathfrak{p}$ ist maximales Ideal. $\blacksquare$