WS 05/06
Priv.-Doz. Dr. S. Wewers

Algebra I

5. Übungsblatt

Aufgabe 1: (2+1+1=4 P) Die abelsche Gruppe G sei gegeben durch drei Erzeuger x, y, z und die Relationen

$$\begin{aligned} 3x - 2y + 4z &= 0, \\ 2x - 3y + z &= 0, \\ 8x - 7y + 9z &= 0. \end{aligned}$$

(a) Bestimmen Sie die Elementarteiler $d_1, \ldots, d_m$ und den Rang von G.

(b) Bestimmen Sie ein Element von G mit der Ordnung 5 (als Linearkombination von x, y, z).

(c) Wieviele Elemente der Ordnung 5 gibt es in G?

Lösung:

(a) Es gilt also

$$G = \mathbb{Z}^3/H ,$$

wobei

$$H := \langle (3,-2,4), (2,-3,1), (8,-7,9) \rangle \leq \mathbb{Z}^3 .$$

Sind e_1, e_2, e_3 die drei Einheitsvektoren in $\mathbb{Z}^3$, so gilt $x = e_1 + H$, $y = e_2 + H$ und $z = e_3 + H$. Wir verwenden umkehrbare ganzzahlige Zeilen- und Spaltenumformungen, und erhalten

$$\begin{aligned} \begin{pmatrix} 3 & -2 & 4 \\ 2 & -3 & 1 \\ 8 & -7 & 9 \end{pmatrix} &\rightsquigarrow \begin{pmatrix} 1 & -3 & 2 \\ 4 & -2 & 3 \\ 9 & -7 & 8 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & -3 & 2 \\ 0 & 10 & -5 \\ 0 & 20 & -10 \end{pmatrix} \\ &\rightsquigarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 10 & -5 \\ 0 & 20 & -10 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 5 & 10 \\ 0 & 10 & 20 \end{pmatrix} \\ &\rightsquigarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 5 & 10 \\ 0 & 0 & 0 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 5 & 0 \\ 0 & 0 & 0 \end{pmatrix} . \end{aligned}$$

Also gibt es eine Basis (x_1, x_2, x_3) von $\mathbb{Z}^3$ derart, daß $H = \mathbb{Z} \cdot x_1 + \mathbb{Z} \cdot 5x_2$. Setzt man $x' := x_1 + H = 0$, $y' := x_2 + H$ und $z' := x_3 + H$, so wird G also von Elementen y', z' erzeugt unter der Relation $5y' = 0$. Folglich ist

$$\begin{aligned} G &= \mathbb{Z}^3/H \cong \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}/(\mathbb{Z} \times 5\mathbb{Z} \times 0\mathbb{Z}) \\ &\cong (\mathbb{Z}/\mathbb{Z}) \times (\mathbb{Z}/5\mathbb{Z}) \times (\mathbb{Z}/0\mathbb{Z}) \cong (\mathbb{Z}/5\mathbb{Z}) \times \mathbb{Z} . \end{aligned}$$

Daher hat G den Elementarteiler 5 und den Rang 1.

(b) Nach obigem ist y' ein Element der Ordnung 5, denn dieses wird unter dem Ismomorphismus $G \to (Z/5\mathbb{Z}) \times \mathbb{Z}$ auf das Elememt $(\bar{1}, 0)$ abgebildet, welches in $(\mathbb{Z}/5\mathbb{Z}) \times \mathbb{Z}$ die Ordnung 5 hat. Um y' als Linearkombination von x, y und z auszudrücken, müssen wir die die Variablensubstutionenen im Algorithmus, die durch Spaltenumformungen entstanden sind, wieder rückgängig machen.

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & -1 \\ 0 & 1 & 0 \end{pmatrix}$$
$$\rightsquigarrow \begin{pmatrix} 1 & -3 & 2 \\ 0 & 2 & -1 \\ 0 & 1 & 0 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 2 & -3 & 1 \\ -1 & 2 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

Also gilt $x' = 2x - 3y + z = 0$, $y' = -x + 2y$, $z' = y$. Somit ist $y' = -x + 2y$ ein Element der Ordnung 5.

(c) Die Gruppe G hat wegen der Isomorphie genau so viele Elemente der Ordnung 5 wie $(\mathbb{Z}/5\mathbb{Z}) \times \mathbb{Z}$. Letztere Gruppe hat genau vier Elemente der Ordnung 5, nämlich $(\bar{1}, 0)$, $(\bar{2}, 0)$, $(\bar{3}, 0)$ und $(\bar{4}, 0)$. Also hat auch G genau vier Elemente der Ordnung 5.

Aufgabe 2: (1+1=2 P) Sei G eine abelsche Gruppe der Ordnung 100. Zeigen Sie:

(a) G enthält ein Element der Ordnung 10.

(b) Wenn G kein Element der Ordnung > 10 enthält, dann gilt

$$G \cong \mathbb{Z}/\mathbb{Z} \cdot 10 \times \mathbb{Z}/\mathbb{Z} \cdot 10.$$

Lösung:

(a) Nach dem Hauptsatz über enndlich erzeugte abelsche Gruppen gibt es abgesehen von Isomorphie genau die folgenden abelschen Gruppen der Ordnung 100.

- $\mathbb{Z}/100\mathbb{Z}$
- $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/50\mathbb{Z}$
- $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/20\mathbb{Z}$
- $\mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$.

Jede dieser Gruppen enthält ein Element der Ordnung 10; z.B.

- $\overline{10} \in \mathbb{Z}/100\mathbb{Z}$
- $(0, \bar{5}) \in \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/50\mathbb{Z}$
- $(0, \bar{2}) \in \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/20\mathbb{Z}$
- $(\bar{1}, 0) \in \mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$.

(b) Offenbar gibt es in jeder der drei anderen Gruppen Element der Ordnung > 10, z.B.

- $\operatorname{ord} \bar{1} = 100$ in $\mathbb{Z}/100\mathbb{Z}$
- $\operatorname{ord}(\bar{0}, \bar{1}) = 50$ in $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/50\mathbb{Z}$
- $\operatorname{ord}(\bar{0}, \bar{1}) = 20$ in $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/20\mathbb{Z}$.

Daraus folgt die Behauptung.

Aufgabe 3: (1+1+1=3 P)

(a) Zeigen Sie: jede endlich erzeugte Untergruppe von $(\mathbb{Q}, +)$ ist zyklisch.

(b) Zeigen Sie: jede endlich erzeugte Untergruppe von $(\mathbb{Q}^\times, \cdot)$ ist frei.

(c) Bestimmen Sie eine Untergruppe von $(\mathbb{Q}^\times, \cdot)$ vom Rang 5 (durch Angabe einer Basis).

Lösung:

(a)

- 1. Möglichkeit: Es sei G eine endlich erzeugte Untergruppe von $(\mathbb{Q}, +)$. Also gibt es $q_1, \ldots, q_r \in \mathbb{Q}$ so, daß

$$G = \mathbb{Z}q_1 + \ldots + \mathbb{Z}q_r .$$

Schreibt man $q_i = \frac{m_i}{n_i}$, so folgt

$$G \subseteq \mathbb{Z}\frac{1}{n_1} + \ldots + \mathbb{Z}\frac{1}{n_r} \subseteq \mathbb{Z}\frac{1}{n_1 \cdot \ldots \cdot n_r} := U \quad \leq \mathbb{Q} .$$

Also ist G Untergruppe der zyklischen Gruppe U. Nach Vorlesung ist dann auch G zyklisch.

- 2. Möglichkeit: Nach dem Haupsatz für endlich erzeugte abelsche Gruppen gilt folgendes

Korollar *Eine endlich erzeugte abelsche Gruppe ist genau dann frei, wenn sie keine nicht-trivialen Elemente endlicher Ordnung hat.*

In $(\mathbb{Q}, +)$ gibt es keine Elemente endlicher Ordnung außer 0. Folglich ist jede endlich erzeugte Untergruppe G von $(\mathbb{Q}, +)$ frei. Also besitzt G eine Basis $(q_1, \ldots, q_r)$. Wäre $r \geq 2$, $q_1 = \frac{m_1}{n_1}$, $q_2 = \frac{m_2}{n_2}$, so sind m_1, n_1, m_2, n_2 jeweils $\neq 0$, und die Gleichung

$$n_1 m_2 q_1 + n_2 m_1 q_2 = 0$$

zeigt, daß q_1 und q_2 linear abhängig sind, ein Widerspruch. Daher gilt $r \leq 1$ und G ist zyklisch

(b)

- Die Aussage stimmt nicht. Zum Beispiel ist die Untergruppe $\{-1, 1\}$ von $(\mathbb{Q}^\times, \cdot)$ endlich erzeugt, aber nicht frei, da sie nicht-triviale Elemente endlicher Ordnung enthält, nämlich -1 wegen $(-1)^2 = 1$.
- Richtig ist jedoch, daß jede endlich erzeugte Untergruppe von $(\mathbb{Q}_{>0}, \cdot)$ frei ist. Dies liegt daran, daß es in $(\mathbb{Q}_{>0}, \cdot)$ keine nicht-trivialen Elemente endlicher Ordnung gibt, denn aus $q^n = 1$ und $q \in \mathbb{Q}_{>0}$ folgt stets $q = 1$. Also folgt die Behauptung aus obigem Korollar.
- Man kann auch direkt beweisen, daß jede endlich erzeugte Untergruppe von $(\mathbb{Q}_{>0}, \cdot)$ frei ist. Es sei etwa $G = \langle q_1, \ldots, q_n \rangle$ eine endlich erzeugte Untergruppe. Es seien $p_1, \ldots, p_r$ alle Primzahlen, die in den Primfaktorzerlegungen der Zähler und Nenner der q_i auftreten. Also gilt

$$G \subseteq \langle p_1, \ldots, p_r \rangle := U .$$

Betrachte nun die Abbildung

$$\mathbb{Z}^r \to U,\ (m_1, \ldots, m_r) \mapsto p_1^{m_1} \cdot \ldots \cdot p_r^{m_r} .$$

Dies ist offenbar ein surjektiver Gruppenhomomorphismus. Er ist auch injektiv, da die $p_1, \ldots, p_r$ paarweise verschiedene Primzahlen sind. Also ist U eine freie abelsche Gruppe, und G ist eine Untergruppe davon. Nach Vorlesung ist G daher auch eine freie abelsche Gruppe.

(c) Wir nehmen die Idee aus dem letzten Paragraphen zur Lösung von Teil (b), angewandt auf die Primzahlen $2, 3, 5, 7, 11$. Wie dort erklärt, ist die Abbildung

$$\begin{array}{rcl} \mathbb{Z}^5 & \to & U := \langle 2, 3, 5, 7, 11 \rangle \,, \\ (m_1, m_2, m_3, m_4, m_5) & \mapsto & 2^{m_1} 3^{m_2} 5^{m_3} 7^{m_4} 11^{m_5} \end{array}$$

ein Isomorphismus. Also ist

$$U \;=\; \langle 2, 3, 5, 7, 11 \rangle$$

eine Untergruppe von $(\mathbb{Q}, \cdot)$ vom Rang 5 mit Basis $(2, 3, 5, 7, 11)$.

Aufgabe 4: (3 P) Sei $G = (\mathbb{Z}/\mathbb{Z} \cdot 70)^{\times}$. Bestimmen Sie die Elementarteiler von G, und finden Sie ein Element der Ordnung 12. (Hinweis: benutzen Sie den Chinesischen Restsatz.)

Lösung: Es gilt $70 = 2 \cdot 5 \cdot 7$. Nach dem Chinesischen Restsatz folgt

$$\begin{array}{rcl} (\mathbb{Z}/70\mathbb{Z})^{\times} & \cong & (\mathbb{Z}/2\mathbb{Z})^{\times} \times (\mathbb{Z}/5\mathbb{Z})^{\times} \times (\mathbb{Z}/7\mathbb{Z})^{\times} \\ & \cong & (\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/6\mathbb{Z}) \\ & \cong & (\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z} \times 2\mathbb{Z}) \\ & \cong & (\mathbb{Z}/12\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \\ & \cong & (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/12\mathbb{Z}) \,. \end{array}$$

Also sind 2 und 12 die Elementarteiler von G. Nun hat $\overline{2} \in (\mathbb{Z}/5\mathbb{Z})^{\times}$ die Ordnung 4, und $\overline{2} \in (\mathbb{Z}/7\mathbb{Z})^{\times}$ hat die Ordnung 3. Folglich hat das Element

$$\left(\overline{1}, \overline{2}, \overline{2}\right) \;\in\; (\mathbb{Z}/2\mathbb{Z})^{\times} \times (\mathbb{Z}/5\mathbb{Z})^{\times} \times (\mathbb{Z}/7\mathbb{Z})^{\times}$$

die Ordnung $3 \cdot 4 = 12$. Wir suchen ein Urbild x davon unter obigem Isomorphismus. Also suchen wir ein $x \in \mathbb{Z}$ derart, daß

$$\begin{array}{rclcl} x & \equiv & 1 & \mod & 2 \\ x & \equiv & 2 & \mod & 5 \\ x & \equiv & 2 & \mod & 7 \,. \end{array}$$

Die Lösungen von $x \equiv 1 \mod 2, x \equiv 2 \mod 5$ sind offenbar von der Form $7, 17, 27, \ldots$. Die erste Zahl in dieser Reihe die auch $\equiv 2 \mod 7$ ist, ergibt sich als 37. Also löst $x = 37$ das Kongruenzsystem, und $\overline{37} \in (\mathbb{Z}/70\mathbb{Z})^{\times}$ hat die Ordnung 12.

Bemerkung: Jedes $x \in \mathbb{Z}$ mit $x \equiv 1 \mod 2$, $x \equiv 2$ oder $3 \mod 5$ und $x \equiv 2$ oder $4 \mod 7$ erfüllt $\operatorname{ord} \overline{x} = 12$ in $(\mathbb{Z}/70\mathbb{Z})^{\times}$.