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

Einführung in Algebra und Zahlentheorie – Übungsblatt 12 – Musterlösung

Aufgabe 0 (0 Punkte)
Besuche das Sommerfest der Fakultät für Mathematik am 12.07.2013, ab 17:30 Uhr.
`http://www.math.kit.edu/event/sommerfest/`

Lösung:
Das habe ich live vorgeführt.

Aufgabe 1 (4 Punkte)
Berechne die Elementarteiler von $M = \begin{pmatrix} 1 & 2 & 3 \\ -2 & 2 & 4 \\ 0 & 4 & 6 \end{pmatrix} \in \mathbb{Z}^{3\times 3}$. Gib unimodulare Matrizen L, R an, so dass LMR in Normalform ist.
Für $a, b \in \mathbb{Z}$ seien $c_1 = \begin{pmatrix} a \\ b \\ 1 \end{pmatrix}, c_2 = \begin{pmatrix} a \\ b \\ 2 \end{pmatrix}$ gegeben. Untersuche jeweils, für welche a, b das lineare Gleichungssystem $Mz = c_1$ beziehungsweise $Mz = c_2$ lösbar ist und gib gegebenenfalls die Lösung an.

Lösung: Für $L = \begin{pmatrix} 1 & 0 & 0 \\ 2 & 1 & -1 \\ 4 & 2 & -3 \end{pmatrix}, R = \begin{pmatrix} 1 & -2 & 1 \\ 0 & 1 & -2 \\ 0 & 0 & 1 \end{pmatrix}$ gilt $LMR = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}$ $(*)$, die Elementarteiler sind also 1|2|2.
Für $i = 1, 2$ gilt $Mz = b_i \Leftrightarrow LMR(R^{-1}z) = Lb_i \Leftrightarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix} (R^{-1}z) = \begin{pmatrix} a \\ 2a + b - i \\ 4a + 2b - 3i \end{pmatrix}$. Das letzte LGS ist offensichtlich genau dann ganzzahlig lösbar, wenn $2a + b - i, 4a + 2b - 3i$ jeweils durch 2 teilbar sind. Für $i = 1$ gibt es nie eine Lösung (denn dann ist $4a + 2b - 3$ stets ungerade), für $i = 2$ gibt es genau dann eine Lösung, wenn b gerade ist.
Für gerades b löst $R^{-1}z = \begin{pmatrix} a \\ a + \frac{b}{2} - 1 \\ 2a + b - 3 \end{pmatrix}$ das letzte LGS und wir berechnen $z = R(R^{-1}z) = \begin{pmatrix} a - 1 \\ -3a - \frac{3}{2}b + 5 \\ 2a + b - 3 \end{pmatrix}$ als eindeutige Lösung des ursprünglichen LGS.

$(*)$ Dies kann etwa mit folgenden Schritten verifiziert werden:
Addition der ersten Zeile auf die zweite Zeile; Subtraktion der ersten Spalte zweimal von der zweiten, dreimal von der dritten Spalte; Zwischenergebnis $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 6 & 10 \\ 0 & 4 & 6 \end{pmatrix}$
ab sofort wird die 2×2-Teilmatrix unten rechts betrachtet und mit Zeilen- und Spaltenumformungen per Euklid der ggT (= 2) der Einträge erzeugt: Subtraktion der dritten Zeile von der zweiten; Subtraktion der zweiten Zeile zweimal von der dritten; Subtraktion der zweiten Spalte zweimal von der dritten Spalte; Zwischenergebnis $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & -2 \end{pmatrix}$
ab sofort wieder Betrachten der Restmatrix (1×1); Multiplikation der dritten Zeile mit -1 - fertig.

Aufgabe 2 (4 Punkte) – *eine alte Klausuraufgabe*
Sei G eine endliche abelsche Gruppe von Ordnung $n \in \mathbb{N}$. Zeige die Äquivalenz der folgenden Aussagen:

i) G ist zyklisch.

ii) Für alle Teiler d von n gibt es genau eine Untergruppe von G mit Ordnung d.

iii) Für alle Teiler d von n gibt es höchstens eine Untergruppe von G mit Ordnung d.

Lösung: Nach dem Struktursatz für endlich erzeugte abelsche Gruppen ist G isomorph zu einem Produkt zyklischer Gruppen. Stärker ist $\mathbb{Z}$ kein Faktor in G, denn G ist endlich.
Also ist $G \cong \mathbb{Z}/e_1\mathbb{Z} \times ... \times \mathbb{Z}/e_r\mathbb{Z}$ (für ein $r \in \mathbb{N}_0$) und im Beweis haben wir gesehen, dass wir $e_1|e_2|...|e_r \in \mathbb{N}$ wählen können. Dabei können wir auf Faktoren $\mathbb{Z}/1\mathbb{Z}$ verzichten, also ist $e_1 \neq 1$.
Weiterhin gilt $\#G = n = \prod_{i=1}^{r} e_i$.
„$(i) \Rightarrow (ii)$“ Ohne Einschränkung ist $G = \mathbb{Z}/n\mathbb{Z}$. Sei d ein Teiler von n.
$U = \langle \overline{\frac{n}{d}} \rangle$ ist eine Untergruppe der Ordnung d. Das zeigt die **Existenz**.
Für die **Eindeutigkeit** reicht es zu zeigen, dass jede Untergruppe V der Ordnung d das Element $\overline{\frac{n}{d}}$ enthält – dann gilt $V \subseteq U$ und wegen der Mächtigkeit sogar Gleichheit. Das sehen wir recht elegant mit dem Satz von Lagrange. Dabei benutzen wir, dass V sogar ein Normalteiler ist, denn G ist abelsch.
Es ist $\#(G/V) = \frac{\#G}{\#V} = \frac{n}{d}$, also ist die Ordnung von jedem Element $g + V \in G/V$ ein Teiler von $\frac{n}{d}$, das heißt $\frac{n}{d}(g + V) = 0 + V$, also $\frac{n}{d} \cdot g \in V$ für alle $g \in G$.
Der Spezialfall $g = 1$ zeigt $\frac{n}{d} \cdot \overline{1} = \overline{\frac{n}{d}} \in V$, was zu zeigen war.

Alternativ identifiziert man alle Elemente mit ihrem Vertreter in $\{0, ..., n-1\}$. Für $d \neq 1$ gibt es dann ein minimales Element $m \neq 0$ in einer Gruppe V der Ordnung d. Wäre m kein Teiler aller anderen Elemente und kein Teiler von n, so ließe sich durch Division mit Rest ein kleineres Element konstruieren.
Also ist m ein Erzeuger und ein Teiler von $n = 0 \in V$ und die Ordnung der Gruppe verrät $m = \frac{n}{d}$.

„$(ii) \Rightarrow (iii)$“ Das stimmt!

„$(iii) \Rightarrow (i)$“ Sei G nicht zyklisch. Dann gibt es mindestens zwei Elementarteiler, also $G \cong \mathbb{Z}/e_1\mathbb{Z} \times \mathbb{Z}/e_2\mathbb{Z} \times R$ mit $1 \neq e_1|e_2$, wobei uns der Rest R nicht interessiert.
Dann erzeugen $(1, 0, 0)$ und $(0, \frac{e_2}{e_1}, 0)$ verschiedene Gruppen der Ordnung $e_1|n$.

Aufgabe 3 (4 Punkte)
Sei $R \neq 0$ ein kommutativer Ring. Zeige, dass R genau dann ein Hauptidealring ist, wenn für jedes $n \in \mathbb{N}$ jeder R-Untermodul von R^n eine R-Basis besitzt.

Lösung:
„$\Leftarrow$“ Insbesondere sind alle Untermoduln von $R = R^1$ frei. Die Untermoduln von R sind aber gerade die Ideale von R. In R sind zwei Elemente r_1, r_2 stets linear abhängig, denn für $r_1, r_2 \neq 0$ ist $r_2 \cdot r_1 + (-r_1) \cdot r_2 = 0$ eine nichttriviale Darstellung der Null. Jedes Ideal $\neq 0$ besitzt also eine einelementige Basis und ist somit ein Hauptideal, 0 ist ebenfalls Hauptideal.

Es verbleibt zu zeigen, dass R nullteilerfrei ist (nur hier benötigen wir $R \neq 0$).
Annahme: Sei $ab = 0$ für $a, b \neq 0 \in R$. Wir betrachten das von a erzeugte Ideal $I = (a) \neq 0$.
Hinweis: Wir halten fest, dass $\{a\}$ keine Basis von I ist, da $\{a\}$ wegen $ba = 0$ nicht linear unabhängig ist.
I besitzt eine Basis $\{r\}$ für ein $r \neq 0$ und wegen der linearen Unabhängigkeit ist r kein Nullteiler. Aber wegen $(r) = (a)$ ist $r = sa$ für ein $s \in R$ und damit gilt $rb = sab = s \cdot 0 = 0$ und r eben doch ein Nullteiler. Dies ist ein Widerspruch.
Achtung: wir können nicht davon ausgehen, dass a und r assoziiert sind, denn dafür bräuchten wir bereits die Nullteilerfreiheit.

„⇒“ Wir schreiben den Beweis aus der Vorlesung für den Spezialfall $R = \mathbb{Z}$ (fast) ab.
Für $n = 0$ glauben wir die Aussage.
$n = 1$: R ist ein Hauptidealring. Für ein Ideal $I \neq 0$ existiert ein Erzeuger $a \neq 0$ und wegen der Nullteilerfreiheit ist $\{a\}$ eine Basis von I.
Natürlich ist $\emptyset$ eine Basis des Nullideals.

Sei nun die Aussage wahr für $n \geq 1$ und $A \leq R^{n+1}$ eine Untergruppe. $\Phi\colon R^{n+1} \to R$ sei die Projektion auf die letzte Komponente. $K := \mathrm{Kern}(\Phi|_A) = \mathrm{Kern}(\Phi) \cap A = \{\begin{pmatrix} x_1 \\ \cdots \\ x_n \\ 0 \end{pmatrix} \in A\}$ ist Untermodul von $\{\begin{pmatrix} x_1 \\ \cdots \\ x_n \\ 0 \end{pmatrix} \in R^{n+1}\} \cong R^n$.
K kann also als Untermodul von R^n aufgefasst werden und besitzt nach Induktionsvoraussetzung eine Basis B.
Ist bereits $\Phi(A) = 0$, so ist $A = K$ und wir sind fertig.
Ohne Einschränkung sei also $\Phi(A) \neq 0$ ein echter Untermodul von R, dann gibt es eine einelementige Basis $\{z\}$, das haben wir für $n = 1$ gesehen. Es gibt ein Urbild $y = \begin{pmatrix} x_1 \\ \cdots \\ x_n \\ z \end{pmatrix}$ von z in A.

Behauptung: $B \cup \{y\}$ ist eine Basis von A.
Erzeugendensystem: Für $a \in A$ beliebig ist $\Phi(a) = rz$ für ein $r \in R$, denn z erzeugt $\Phi(A)$. Wegen $rz = r\Phi(y) = \Phi(ry)$ ist $0 = \Phi(a) - \Phi(ry) = \Phi(a - ry)$, also $a - ry \in K$ (denn wegen $a \in A, y \in A$ ist $a - ry \in A$). Also kann $a = ry + (a - ry)$ als Summe von Elementen in (y) und K geschrieben werden, was zu zeigen war.
lineare Unabhängigkeit: Ist $\sum_{b \in B} r_b \cdot b + ry = 0$, so ist $ry = -\sum_{b \in B} r_b \cdot b$. Das impliziert $ry \in K$, also $0 = \Phi(ry) = rz$. Aber wegen der Nullteilerfreiheit (und da im Fall $\Phi(A) \neq 0$ sicher $z \neq 0$ ist) impliziert das $r = 0$. Die Linearkombination ist also eine Linearkombination über B und da B eine Basis ist, müssen alle Koeffizienten 0 sein.

Aufgabe 4 (4 Punkte) – *alte Klausuraufgaben, wo man hinschaut...*
Seien $a, b, c \in \mathbb{Z} \setminus \{0\}$.

a) Bestimme die Elementarteiler der Matrix $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$.

b) Bestimme die Elementarteiler der Matrix $\begin{pmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & c \end{pmatrix}$.

c) Sei $n \in \mathbb{N}$, $M \in \mathbb{Z}^{n \times n}$, es gelte $p^2 \nmid \det(M) \neq 0$ für alle $p \in \mathbb{P}$. Bestimme die Elementarteiler der Matrix M.

Lösung: Vorüberlegung: Wir haben in der Vorlesung gesehen, dass wir die Elementarteiler einer Matrix M als Elementarteiler des Bildes der zugehörigen Abbildung berechnen können, das ist das Erzeugnis der Spalten.
Die Elementarteiler seien stets mit $e_1|...|e_r$ bezeichnet. Wir wissen die folgenden Aussagen:

- e_1 ist der ggT aller Matrixeinträge.
- e_r ist die kleinste Zahl d, so dass $d\mathbb{Z}^n \subseteq M\mathbb{Z}^n$ (für n passend).
- $\prod_{i=1}^{r} e_i = \det(S^{-1}MT) = |\det(M)|$, denn die Basiswechselmatrizen S, T haben Determinante ± 1.
  Mit ggT und kgV sei nachfolgend stets (wie üblich) der positive Wert gemeint.

a) Es ist $e_1 = \text{ggT}(a, b)$ und $e_1 \cdot e_2 = \det(\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}) = a \cdot b$.
   Also ist $e_2 = \frac{|ab|}{\text{ggT}(a,b)} = kgV(a, b)$.

b) Es ist $e_1 = \text{ggT}(a, b, c)$. Die Elemente der Untergruppe haben die Form $\begin{pmatrix} az_1 \\ bz_2 \\ cz_3 \end{pmatrix}$, $z_1, z_2, z_3 \in \mathbb{Z}$ und mit der zweiten Vorbemerkung sehen wir $e_3 = \text{kgV}(a, b, c)$.
   Es verbleibt dann $e_2 = |\frac{abc}{\text{ggT}(a,b,c)\text{kgV}(a,b,c)}|$.
   Hinweis: Achtung, $e_r = \text{kgV}...$ ist im Allgemeinen falsch, hier wegen der speziellen Form aber richtig!
   Zum Beispiel besitzt $\begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$ den doppelten Elementarteiloer $e_1 = e_2 = 1$, die Spalten erzeugen $\mathbb{Z}^2$.

c) Wegen $\det(M) \neq 0$ gibt es n Elementarteiler. Jeder Primteiler, der $e_1, ..., e_{n-1}$ teilt, teilt auch e_n, kommt also zweimal vor.
   Es folgt $e_1 = ... = e_{n-1} = 1, e_n = |\det(M)|$.