Universität Konstanz
Fachbereich Mathematik und Statistik
Sommersemester 2011

Christoph Hanselka
Aaron Kunert
Markus Schweighofer

Lösungsblatt 5 zur Zahlentheorie

Aufgabe 1.
Wir schreiben Gruppen U und V jeweils als Bild einer gewissen Matrix und berechnen deren Smithsche Normalform über $\mathbb{Z}$.

(a) Wir betrachten dazu die Matrix

$$\begin{pmatrix} 1 & 2 & 1 \\ 2 & 10 & -10 \\ 5 & 16 & -7 \\ 3 & 12 & -9 \end{pmatrix}.$$

Um den Isomorphismus angeben zu können, werden wir die Zeilenoperationen ebenfalls dokumentieren.

$$\left(\begin{array}{ccc|cccc} 1 & 2 & 1 & 1 & 0 & 0 & 0 \\ 2 & 10 & -10 & 0 & 1 & 0 & 0 \\ 5 & 16 & -7 & 0 & 0 & 1 & 0 \\ 3 & 12 & -9 & 0 & 0 & 0 & 1 \end{array}\right) \longrightarrow \left(\begin{array}{ccc|cccc} 1 & 2 & 1 & 1 & 0 & 0 & 0 \\ 0 & 6 & -12 & -2 & 1 & 0 & 0 \\ 0 & 6 & -12 & -5 & 0 & 1 & 0 \\ 0 & 6 & -12 & -3 & 0 & 0 & 1 \end{array}\right) \longrightarrow$$

$$\left(\begin{array}{ccc|cccc} 1 & 2 & 1 & 1 & 0 & 0 & 0 \\ 0 & 6 & -12 & -2 & 1 & 0 & 0 \\ 0 & 0 & 0 & -3 & -1 & 1 & 0 \\ 0 & 0 & 0 & -1 & 1 & 0 & 1 \end{array}\right) \longrightarrow \left(\begin{array}{ccc|cccc} 1 & 2 & 1 & 1 & 0 & 0 & 0 \\ 0 & 6 & 0 & -2 & 1 & 0 & 0 \\ 0 & 0 & 0 & -3 & -1 & 1 & 0 \\ 0 & 0 & 0 & -1 & 1 & 0 & 1 \end{array}\right) \longrightarrow$$

$$\left(\begin{array}{ccc|cccc} 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 6 & 0 & -2 & 1 & 0 & 0 \\ 0 & 0 & 0 & -3 & -1 & 1 & 0 \\ 0 & 0 & 0 & -1 & 1 & 0 & 1 \end{array}\right).$$

Daher haben wir einen Isomorphismus

$$\begin{aligned} \phi\colon \mathbb{Z}^4/U &\longrightarrow (0) \times \mathbb{Z}/(6) \times \mathbb{Z} \times \mathbb{Z} \\ \overline{(x_1,x_2,x_3,x_4)} &\longmapsto (0, \overline{x_2 - x_1}, x_3 - x_2 + x_1, -x_1 - x_2 + x_4) \end{aligned}$$

(b) Hier betrachten wir die Matrix

$$\begin{pmatrix} 5 & 10 & -10 \\ 15 & 40 & 80 \\ 5 & 10 & 20 \end{pmatrix},$$

und berechnen die Smithsche Normalform wie folgt

$$\left(\begin{array}{ccc|ccc} 5 & 10 & -10 & 1 & 0 & 0 \\ 15 & 40 & 80 & 0 & 1 & 0 \\ 5 & 10 & 20 & 0 & 0 & 1 \end{array}\right) \longrightarrow \left(\begin{array}{ccc|ccc} 5 & 10 & -10 & 1 & 0 & 0 \\ 0 & 10 & 110 & -3 & 1 & 0 \\ 0 & 0 & 30 & -1 & 0 & 1 \end{array}\right) \longrightarrow$$

$$\left(\begin{array}{ccc|ccc} 5 & 10 & -10 & 1 & 0 & 0 \\ 0 & 10 & 0 & -3 & 1 & 0 \\ 0 & 0 & 30 & -1 & 0 & 1 \end{array}\right) \longrightarrow \left(\begin{array}{ccc|ccc} 5 & 0 & 0 & 1 & 0 & 0 \\ 0 & 10 & 0 & -3 & 1 & 0 \\ 0 & 0 & 30 & -1 & 0 & 1 \end{array}\right).$$

Somit erhalten wir einen Isomorphismus

$$\begin{aligned}\phi\colon \mathbb{Z}^3/V &\longrightarrow \mathbb{Z}/(5)\times\mathbb{Z}/(10)\times\mathbb{Z}/(30),\\ \overline{(x,y,z)} &\longmapsto (\overline{x},\ \overline{-3x+y},\ \overline{-x+z}).\end{aligned}$$

Nun sind $\mathbb{Z}/(10)$ und $\mathbb{Z}/(30)$ keine einfachen $\mathbb{Z}$–Moduln. Allerdings wissen wir aus dem Chinesischem Restsatz, dass $\mathbb{Z}/(10)\cong\mathbb{Z}/(2)\times\mathbb{Z}/(5)$ sowie $\mathbb{Z}/(30)\cong\mathbb{Z}/(2)\times\mathbb{Z}/(3)\times\mathbb{Z}/(5)$. Verketten wir ϕ mit den entsprechenden Isomorphismen erhalten wir

$$\begin{aligned}\psi\colon \mathbb{Z}^3/V &\longrightarrow \mathbb{Z}/(5)\times\mathbb{Z}/(2)\times\mathbb{Z}/(5)\times\mathbb{Z}/(2)\times\mathbb{Z}/(3)\times\mathbb{Z}/(5),\\ \overline{(x,y,z)} &\longmapsto (\overline{x},\ \overline{-3x+y},\ \overline{-3x+y},\ \overline{-x+z}\ \overline{-x+z},\ \overline{-x+z}).\end{aligned}$$

Aufgabe 2. Wir berechnen die Smithsche Normalform. Da wir beide Übergangsmatrizen benötigen, dokumentieren wir Spalten–und Zeilenoperationen. Zuvor bemerken wir noch $X^3-X^2+X-1=(X-1)(X^2+1)$.

$$\begin{array}{ccc|cc}
(X-1) & (X^2-1) & 0 & 1 & 0\\
(X^3-X^2+X-1) & (X^4+X^2-2) & (X^2-1) & 0 & 1\\
\hline
1 & 0 & 0 & & \\
0 & 1 & 0 & & \\
0 & 0 & 1 & &
\end{array}\quad\longrightarrow$$

$$\begin{array}{ccc|cc}
(X-1) & (X^2-1) & 0 & 1 & 0\\
0 & (X^2-1) & (X^2-1) & (-X^2-1) & 1\\
\hline
1 & 0 & 0 & & \\
0 & 1 & 0 & & \\
0 & 0 & 1 & &
\end{array}\quad\longrightarrow$$

$$\begin{array}{ccc|cc}
(X-1) & (X^2-1) & (-X^2+1) & 1 & 0\\
0 & (X^2-1) & 0 & (-X^2-1) & 1\\
\hline
1 & 0 & 0 & & \\
0 & 1 & -1 & & \\
0 & 0 & 1 & &
\end{array}\quad\longrightarrow$$

$$\begin{array}{ccc|cc}
(X-1) & 0 & 0 & 1 & 0\\
0 & (X^2-1) & 0 & (-X^2-1) & 1\\
\hline
1 & (-X-1) & (X+1) & & \\
0 & 1 & -1 & & \\
0 & 0 & 1 & &
\end{array}\quad\longrightarrow$$

Somit gilt also

$$\begin{pmatrix} 1 & 0\\ -(X^2-1) & 1\end{pmatrix}\cdot\begin{pmatrix} X-1 & X^2-1 & 0\\ X^3-X^2+X-1 & X^4+X^2-2 & X^2-1\end{pmatrix}\cdot\begin{pmatrix} 1 & -X-1 & X+1\\ 0 & 1 & -1\\ 0 & 0 & 1\end{pmatrix}$$

$$=\begin{pmatrix} X-1 & 0 & 0\\ 0 & X^2-1 & 0\end{pmatrix}.$$

Aufgabe 3.
Es ist schon bekannt, dass die Menge M^N aller Abbildungen von M nach N mit punktweiser Addition und Skalarmultiplikation ein R–Modul ist. Zu zeigen ist noch, dass $\hom(M,N) \subseteq M^N$ ein Untermodul, also abgeschlossen unter Addition und Skalarmultiplikation ist. Seien also $f,g \in \mathrm{Hom}(M,N)$, sowie $x,y \in M$ und $r,s \in R$. Dann gilt $(f+g)(x+y) = f(x+y) + g(x+y) = f(x) + f(y) + g(x) + g(y) = f(x) + g(x) + f(y) + g(y) = (f+g)(x) + (f+g)(y)$. Weiter ist $(f+g)(rx) = f(rx)+g(rx) = rf(x)+rg(x) = r(f+g)(x)$. Was zeigt, dass auch $f+g$ in $\mathrm{Hom}(M,N)$ liegt. Ferner ist $(rf)(x+y) = r(f(x+y)) = r(f(x)+f(y)) = rf(x)+rf(y) = (rf)(x)+rf(y)$. Schließlich ist $(rf)(sx) = r(f(sx)) = rsf(x) = srf(x) = s(rf)(x)$, woraus $rf \in \mathrm{Hom}(M,N)$ folgt. Man beachte, dass die letzten Gleichungen nur gelten, wenn R ein kommutativer Ring ist. Für nichtkommutative Ringe ist $\mathrm{Hom}(M,N)$ unter der Skalarmultiplikation im Allgemeinen nicht abgeschlossen.

Aufgabe 4.

(a) Sei $A = (a_{ij})$, $B = (b_{kl})$ und $X = (x_{ab})$. Dann ist

$$\begin{aligned}
(AB)(X)_{pq} &= \sum_{i=1}^{r} (AB)_{pi} X_{iq} \\
&= \sum_{i=1}^{r} \left(\sum_{j=1}^{n} A_{pj} B_{ji} \right) X_{iq} \\
&= \sum_{i=1}^{r} \sum_{j=1}^{n} (A_{pj} B_{ji}) X_{iq} \\
&= \sum_{i=1}^{r} \sum_{j=1}^{n} A_{pj} (B_{ji} X_{iq}) \\
&= \sum_{j=1}^{n} \sum_{i=1}^{r} A_{pj} (B_{ji} X_{iq}) \\
&= \sum_{j=1}^{n} A_{pj} \left(\sum_{i=1}^{r} B_{ji} X_{iq} \right) \\
&= \sum_{j=1}^{n} A_{pj} (BX)_{jq} \\
&= A(BX)_{pq}.
\end{aligned}$$

(b) Diese Aussage folgt sofort aus der Teilaufgabe zuvor unter der Verwendung der Tatsache, dass man R als Modul über sich selbst auffassen kann. Übrig ist nur noch, dass für alle $A \in R^{r \times r}$ gilt, dass $AI_r = I_r A = A$ ist. Dies lässt sich jedoch unmittelbar nachrechnen.

(c) Auch diese Behauptung folgt sofort aus den beiden Vorhergehenden.