MA3201 Rings and Modules, 2014

Solution Sheet 6

To be discussed on Friday 14 November and Friday 21 November.

Problems from: Bhattacharya, P. B.; Jain, S. K.; Nagpaul, S. R. Basic abstract algebra. Second edition. Cambridge University Press, Cambridge, 1994.

Page	Problem numbers
401	1, 3(b)
409	(c)

Problems from old exams:

Exam	Problem number
2013	1
2011	1
2009	2

Page 401, Question 1(a). We carry out the following operations on A to get the Smith normal form.

$$\begin{pmatrix} 0 & 2 & -1 \\ -3 & 8 & 3 \\ 2 & -4 & -1 \end{pmatrix} \xrightarrow[C_1\leftrightarrow C_3]{} \begin{pmatrix} -1 & 2 & 0 \\ 3 & 8 & -3 \\ -1 & -4 & 2 \end{pmatrix} \xrightarrow[C_2+2C_1]{} \begin{pmatrix} -1 & 0 & 0 \\ 3 & 14 & -3 \\ -1 & -6 & 2 \end{pmatrix} \xrightarrow[R_3-R_1]{R_2+3R_1} \begin{pmatrix} -1 & 0 & 0 \\ 0 & 14 & -3 \\ 0 & -6 & 2 \end{pmatrix} \xrightarrow[C_2\leftrightarrow C_3]{}$$

$$\begin{pmatrix} -1 & 0 & 0 \\ 0 & -3 & 14 \\ 0 & 2 & -6 \end{pmatrix} \xrightarrow[R_2\leftrightarrow R_3]{} \begin{pmatrix} -1 & 0 & 0 \\ 0 & 2 & -6 \\ 0 & -3 & 14 \end{pmatrix} \xrightarrow[C_3+3C_2]{} \begin{pmatrix} -1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & -3 & 5 \end{pmatrix} \xrightarrow[R_3+R_2]{} \begin{pmatrix} -1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & -1 & 5 \end{pmatrix} \xrightarrow[R_2\leftrightarrow R_3]{}$$

$$\begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 5 \\ 0 & 2 & 0 \end{pmatrix} \xrightarrow[C_3+5C_2]{} \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 2 & 10 \end{pmatrix} \xrightarrow[R_3+2R_2]{} \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 10 \end{pmatrix} \xrightarrow[(-1)\cdot R_2]{(-1)\cdot R_1} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 10 \end{pmatrix}$$

Page 401, Question 1(b). We carry out the following operations on A to get the Smith normal form.

$$\begin{pmatrix} -x-3 & 2 & 0 \\ 1 & -x & 1 \\ 1 & -3 & -x-2 \end{pmatrix} \xrightarrow[R_1\leftrightarrow R_2]{} \begin{pmatrix} 1 & -x & 1 \\ -x-3 & 2 & 0 \\ 1 & -3 & -x-2 \end{pmatrix} \xrightarrow[C_3-C_1]{C_2+xC_1}$$

$$\begin{pmatrix} 1 & 0 & 0 \\ -x-3 & -x^2-3x+2 & x+3 \\ 1 & x-3 & -x-3 \end{pmatrix} \xrightarrow[R_3-R_1]{R_2+(x+3)R_1} \begin{pmatrix} 1 & 0 & 0 \\ 0 & -x^2-3x+2 & x+3 \\ 1 & x-3 & -x-3 \end{pmatrix} \xrightarrow[C_2\leftrightarrow C_3]{}$$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & x+3 & -x^2-3x+2 \\ 0 & -x-3 & x-3 \end{pmatrix} \xrightarrow[C_3+xC_2]{} \begin{pmatrix} 1 & 0 & 0 \\ 0 & x+3 & 2 \\ 0 & -x-3 & -x^2-2x-3 \end{pmatrix} \xrightarrow[C_2\leftrightarrow C_3]{}$$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & x+3 \\ 1 & -x^2-2x-3 & -x-3 \end{pmatrix} \xrightarrow[C_3-\frac{x+3}{2}C_2]{} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & -x^2-2x-3 & \frac{1}{2}(x^3+5x^2+7x+3) \end{pmatrix} \xrightarrow[2R_3]{\frac{1}{2}R_2}$$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -2x^2-4x-6 & x^3+5x^2+7x+3 \end{pmatrix} \xrightarrow[R_3+(2x^2+4x+6)R_2]{} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & (x+1)^2(x+3) \end{pmatrix}$$

Page 401, Question 3(b). The subgroup G of $\mathbb{Z}^4$ generated by these elements is

$$G = \{x(2,3,1,4) + y(1,2,3,0) + z(1,1,1,4) \,:\, x,y,z \in \mathbb{Z}^3\}.$$

Let A be the 4×3 matrix whose columns are the three given vectors. Suppose that P is a 4×4 matrix and Q is a 3×3 matrix, both invertible (over $\mathbb{Z}$). Then, since Q is invertible,

$$G = \{A\mathbf{x} \,:\, \mathbf{x} \in \mathbb{Z}^3\}$$

$$= \{AQ\mathbf{x} \,:\, \mathbf{x} \in \mathbb{Z}^3\}.$$

Since P is invertible, it gives a $\mathbb{Z}$-module isomorphism from $\mathbb{Z}^4$ to $\mathbb{Z}^4$. This takes G to PG, so P also gives an isomorphism from G to PG. We have

$$PG = \{PAQ\mathbf{x} \,:\, \mathbf{x} \in \mathbb{Z}^3\}.$$

So if A is equivalent to a matrix B, the corresponding subgroups are isomorphic, and hence have the same rank. So the rank of G is the number of invariant factors in the Smith normal form of A. We thus compute the Smith normal form of A:

$$\begin{pmatrix}2&1&1\\3&2&1\\1&3&1\\4&0&4\end{pmatrix} \xrightarrow[R_1\leftrightarrow R_3]{} \begin{pmatrix}1&3&1\\3&2&1\\2&1&1\\4&0&4\end{pmatrix} \xrightarrow[C_3-C_1]{C_2-3C_1} \begin{pmatrix}1&0&0\\3&-7&-2\\2&-5&-1\\4&-12&0\end{pmatrix} \xrightarrow[R_4-4R_1]{\substack{R_2-3R_1\\R_3-2R_1}} \begin{pmatrix}1&0&0\\0&-7&-2\\0&-5&-1\\0&-12&0\end{pmatrix} \xrightarrow[R_2\leftrightarrow R_3]{}$$

$$\begin{pmatrix}1&0&0\\0&-5&-1\\0&-7&-2\\0&-12&0\end{pmatrix} \xrightarrow[C_2\leftrightarrow C_3]{} \begin{pmatrix}1&0&0\\0&-1&-5\\0&-2&-7\\0&0&-12\end{pmatrix} \xrightarrow[(-1)R_4]{\substack{(-1)R_2\\(-1)R_3}} \begin{pmatrix}1&0&0\\0&1&5\\0&2&7\\0&0&12\end{pmatrix} \xrightarrow[C_3-5C_2]{} \begin{pmatrix}1&0&0\\0&1&0\\0&2&-3\\0&0&12\end{pmatrix} \xrightarrow[R_3-2R_2]{}$$

$$\begin{pmatrix}1&0&0\\0&1&0\\0&0&-3\\0&0&12\end{pmatrix} \xrightarrow[R_4+4R_3]{} \begin{pmatrix}1&0&0\\0&1&0\\0&0&-3\\0&0&0\end{pmatrix} \xrightarrow[(-1)R_3]{} \begin{pmatrix}1&0&0\\0&1&0\\0&0&3\\0&0&0\end{pmatrix}$$

We see that A has three invariant factors, so the rank of G is 3.

Page 409, Question (c). We perform operations on the matrix A whose columns are the vectors coming from the coefficients of the relations given.

$$\begin{pmatrix}0&-3&2\\2&8&-4\\-1&3&-1\end{pmatrix} \xrightarrow[R_1\leftrightarrow R_3]{} \begin{pmatrix}-1&3&-1\\2&8&-4\\0&-3&2\end{pmatrix} \xrightarrow[C_3-C_1]{C_2+3C_1} \begin{pmatrix}-1&0&0\\2&14&-6\\0&-3&2\end{pmatrix} \xrightarrow[R_2+2R_1]{} \begin{pmatrix}-1&0&0\\0&14&-6\\0&-3&2\end{pmatrix} \xrightarrow[C_2\leftrightarrow C_3]{}$$

$$\begin{pmatrix}-1&0&0\\0&-6&14\\0&2&-3\end{pmatrix} \xrightarrow[R_2\leftrightarrow R_3]{} \begin{pmatrix}-1&0&0\\0&2&-3\\0&-6&14\end{pmatrix} \xrightarrow[C_3+C_2]{} \begin{pmatrix}-1&0&0\\0&2&-1\\0&-6&8\end{pmatrix} \xrightarrow[C_2\leftrightarrow C_3]{} \begin{pmatrix}-1&0&0\\0&-1&2\\0&8&-6\end{pmatrix}$$

$$\xrightarrow[C_3+2C_2]{} \begin{pmatrix}-1&0&0\\0&-1&0\\0&8&10\end{pmatrix} \xrightarrow[R_3+8R_2]{} \begin{pmatrix}-1&0&0\\0&-1&0\\0&0&10\end{pmatrix} \xrightarrow[(-1)\cdot R_2]{(-1)\cdot R_1} \begin{pmatrix}1&0&0\\0&1&0\\0&0&10\end{pmatrix}$$

Hence the abelian group is $\mathbb{Z}/1\mathbb{Z} \times \mathbb{Z}/1\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$, which is isomorphic to $\mathbb{Z}/10\mathbb{Z}$.

Exam 2013, Problem 1. For part (a), we carry out operations on the matrix given to reduce it to Smith normal form.

$$\begin{pmatrix}2-X&1&2\\0&1-X&2\\1&0&1-X\end{pmatrix} \xrightarrow[R_1\leftrightarrow R_3]{} \begin{pmatrix}1&0&1-X\\0&1-X&2\\2-X&1&2\end{pmatrix} \xrightarrow[C_3-(1-X)C_1]{} \begin{pmatrix}1&0&0\\0&1-X&2\\2-X&1&-X^2\end{pmatrix} \xrightarrow[R_3-(2-X)R_1]{}$$

$$\begin{pmatrix}1&0&0\\0&1-X&2\\0&1&-X^2\end{pmatrix} \xrightarrow[R_2\leftrightarrow R_3]{} \begin{pmatrix}1&0&0\\0&1&-X^2\\0&1-X&2\end{pmatrix} \xrightarrow[C_3+X^2C_2]{} \begin{pmatrix}1&0&0\\0&1&0\\0&1-X&2+X^2-X^3\end{pmatrix} \xrightarrow[R_3-(1-X)R_2]{}$$

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

For part (b), we need to compute the invariant factors of $A - XI$, which is the matrix in part (a). So the invariant factors are $1, 1$ and $2 + X^2 - X^3$. The monic version of the last one is $-2 - X^2 + X^3$ (multiplying by the unit -1). So there is only one non-unit invariant factor, $-2 - X^2 + X^3$. The corresponding companion matrix is:

$$\begin{pmatrix} 0 & 0 & 2 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix}$$

Since there is only one non-unit invariant factor, this is the rational canonical form of A.

We finally consider part (c). If $P, Q \in \mathbb{Z}_3[X]$ then $\Phi_A(P+Q) = (P+Q)(A) = P(A)+Q(A) = \Phi_A(P)+\Phi_A(Q)$. We also have $\Phi_A(PQ) = (PQ)(A) = P(A)Q(A) = \Phi_A(P)\Phi_A(Q)$ and $\Phi_A(1_{\mathbb{Z}_3[X]}) = 1_{\mathbb{Z}_3[X]}(A) = I$, the identity matrix in $\mathbb{Z}_3[X]$. Hence Φ_A is a ring homorphism. By the Fundamental theorem of ring homomorphisms,

$$\mathbb{Z}_3[X]/\ker\Phi_A \cong \operatorname{im}\Phi_A.$$

The kernel of Φ_A consists of the polynomials P in X over $\mathbb{Z}_3$ which satisfy $P(A) = 0$, which is the ideal generated by the minimum polynomial of A. This minimum polynomial is the last invariant factor of A, which is $m_A = -2-X^2+X^3$ by part (b). We have $m_A(0) = -2$, $m_A(1) = -2-1+1 = -1$ and $m_A(2) = -2-4+8 = 2$ (recall we are working over $\mathbb{Z}_3$). Since none of these are zero, m_A has no linear factors, so cannot be factorized, i.e. it is irreducible.

If I was an ideal of $\mathbb{Z}_3[X]$ containing (m_A) it would be principal (as $\mathbb{Z}_3[X]$ is a PID), of form (P) for some polynomial P. But then $(m_A) \subseteq (P)$ so $P|m_A$. Since m_A is irreducible, P is either a unit times m_A or a unit, so (P) is either (m_A) or $\mathbb{Z}_3[X]$. Hence $\ker\Phi_A = (m_A)$ is a maximal ideal of $\mathbb{Z}_3[X]$. So the quotient $\mathbb{Z}_3[X]/\ker\Phi_A \cong \operatorname{im}\Phi_A$ is a field.

Exam 2011, Problem 1. For part (a), we apply operations to $A - xI_4$, reducing it to Smith normal form.

$$\begin{pmatrix} 2-x & 0 & -1 & 0 \\ 0 & 2-x & 0 & -1 \\ 0 & 0 & 2-x & 0 \\ 0 & 0 & 0 & 2-x \end{pmatrix} \xrightarrow[C_2\leftrightarrow C_4]{C_1\leftrightarrow C_3} \begin{pmatrix} -1 & 0 & 2-x & 0 \\ 0 & -1 & 0 & 2-x \\ 2-x & 0 & 0 & 0 \\ 0 & 2-x & 0 & 0 \end{pmatrix} \xrightarrow[C_4+(2-x)C_2]{C_3+(2-x)C_1}$$

$$\begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 2-x & 0 & (2-x)^2 & 0 \\ 0 & (2-x) & 0 & (2-x)^2 \end{pmatrix} \xrightarrow[R_4+(2-x)R_2]{R_3+(2-x)R_1} \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & (2-x)^2 & 0 \\ 0 & 0 & 0 & (2-x)^2 \end{pmatrix} \xrightarrow[(-1)\cdot R_2]{(-1)R_1}$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & (2-x)^2 & 0 \\ 0 & 0 & 0 & (2-x)^2 \end{pmatrix}$$

For part (b), we note that the non-unit invariant factors of $A-xI_4$ are $(2-x)^2$ and $(2-x)^2$. The companion matrix of $(2-x)^2 = 4-4x+x^2$ is:

$$\begin{pmatrix} 0 & -4 \\ 1 & 4 \end{pmatrix}.$$

Taking two copies of this block, we see that the rational canonical form of A is

$$\begin{pmatrix} 0 & -4 & 0 & 0 \\ 1 & 4 & 0 & 0 \\ 0 & 0 & 0 & -4 \\ 0 & 0 & 1 & 4 \end{pmatrix}.$$

For part (c), we note that the non-unit invariant factors of $A-xI_4$ are $(2-x)^2$ and $(2-x)^2$. This expression for the invariant factors already gives a factorization into irreducible polynomials, since $2-x$ is irreducible. Hence the elementary divisors are $(2-x)^2$ and $(2-x)^2$.

The Jordan normal form is determined by the elementary divisors: the Jordan block corresponding to $(2-x)^2$ is: $\begin{pmatrix} 2 & 0 \\ 1 & 2 \end{pmatrix}$. The Jordan normal form of A is obtained by taking two copies of this block:

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

Exam 2009, Problem 2. The Smith normal form of an $m \times n$ matrix A over a PID R is an $m \times n$ matrix D with entries in R of the form:

$$\begin{pmatrix} a_1 & & & & \\ & a_2 & & & \\ & & \ddots & & \\ & & & a_k & \\ & & & & \\ & & & & \end{pmatrix}$$

where $a_{ii} = a_i$ for $1 \leq i \leq k$ and all other entries are zero, such that $a_1|a_2$, $a_2|a_3, \ldots, a_{k-1}|a_k$ and there is an invertible $m \times m$ matrix P with entries in R and an invertible $n \times n$ matrix Q with entries in R such that $PAQ = D$.

We find the Smith normal form of A by applying row and column operations to it.

$$\begin{pmatrix} 6 & 4 & 2 \\ 4 & 2 & 2 \\ 8 & 6 & 6 \end{pmatrix} \xrightarrow[C_1 \leftrightarrow C_3]{} \begin{pmatrix} 2 & 4 & 6 \\ 2 & 2 & 4 \\ 6 & 6 & 8 \end{pmatrix} \xrightarrow[C_3 - 3C_1]{C_2 - 2C_1} \begin{pmatrix} 2 & 0 & 0 \\ 2 & -2 & -2 \\ 6 & -6 & -10 \end{pmatrix} \xrightarrow[R_3 - 3R_1]{R_2 - R_1} \begin{pmatrix} 2 & 0 & 0 \\ 0 & -2 & -2 \\ 0 & -6 & -10 \end{pmatrix} \xrightarrow[(-1)\cdot R_3]{(-1)\cdot R_2}$$
$$\begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 2 \\ 0 & 6 & 10 \end{pmatrix} \xrightarrow[C_3 - C_2]{} \begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 6 & 4 \end{pmatrix} \xrightarrow[R_3 - 3R_2]{} \begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 4 \end{pmatrix}$$

Let A be a 6×6 matrix over $\mathbb{R}$ with minimum polynomial $(x-2)(x-1)^3$. Then the last invariant factor of A must be $(x-2)(x-1)^3$, with the others dividing it. Furthermore, the product of the non-unit invariant factors must be the characteristic polynomial, hence of degree 6. So the invariant factors before the last one must have total degree 2, with each dividing the next (so the following one must always have degree at least that of the preceeding one). We can write $2 = 2$, $2 = 1 + 1$ as a sum of increasing positive integers. Hence the possibilities for the (non-unit) invariant factors are:

$$\begin{gathered} (x-1)^2, (x-2)(x-1)^3 \\ (x-2)(x-1), (x-2)(x-1)^3 \\ (x-1), (x-1), (x-2)(x-1)^3 \\ (x-2), (x-2), (x-2)(x-1)^3 \end{gathered}$$

In the first case, the companion matrices of the non-unit invariant factors, $(x-1)^2 = x^2 - 2x + 1$ and $(x-2)(x-1)^3 = x^4 - 5x^3 + 9x^2 - 7x + 2$ are

$$\begin{pmatrix} 0 & -1 \\ 1 & 2 \end{pmatrix} \qquad \text{and} \qquad \begin{pmatrix} 0 & 0 & 0 & -2 \\ 1 & 0 & 0 & 7 \\ 0 & 1 & 0 & -9 \\ 0 & 0 & 1 & 5 \end{pmatrix},$$

so the rational canonical form of A, obtained by taking the block matrix with these two blocks on the diagonal and zeros elsewhere, is:

$$\begin{pmatrix} 0 & -1 & 0 & 0 & 0 & 0 \\ 1 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -2 \\ 0 & 0 & 1 & 0 & 0 & 7 \\ 0 & 0 & 0 & 1 & 0 & -9 \\ 0 & 0 & 0 & 0 & 1 & 5 \end{pmatrix}$$

Problem 1. For the matrix A in part (a) of question 1 of page 388 of the book, find square matrices P and Q such that PAQ is in Smith normal form.

Each row operation corresponds to multiplying the matrix on the left by a corresponding elementary matrix, as we've seen in lectures. Similarly, each column operation corresponds to multiplying the matrix on the right by a corresponding matrix. So P is the product $P = X_a \cdots X_1$ of the matrices corresponding to the row operations (in order from right to left) and Q is the product $Q = Y_1 \cdots Y_b$ of the matrices corresponding to the column operations (in order from left to right).

Multiplying the identity matrix on the left by X_1 has the same effect as the row operation corresponding to X_1. Then multiplying X_1 on the left by X_2 has the same effect as the row operation corresponding to X_2, and so on. So we can compute the product $P = X_a \cdots X_1$ by applying the same row operations that we applied to A (in the same order), starting with the identity matrix. Similarly, we can compute the product $Q = Y_1 \cdots Y_b$ by applying the column operations we applied to A to the identity matrix, in order.

Computing P, from the row operations:

$$\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix} \xrightarrow[R_3-R_1]{R_2+3R_1} \begin{pmatrix}1&0&0\\3&1&0\\-1&0&1\end{pmatrix} \xrightarrow[R_2\leftrightarrow R_3]{} \begin{pmatrix}1&0&0\\-1&0&1\\3&1&0\end{pmatrix} \xrightarrow[R_3+R_2]{} \begin{pmatrix}1&0&0\\-1&0&1\\2&1&1\end{pmatrix} \xrightarrow[R_2\leftrightarrow R_3]{}$$
$$\begin{pmatrix}1&0&0\\2&1&1\\-1&0&1\end{pmatrix} \xrightarrow[R_3+2R_2]{} \begin{pmatrix}1&0&0\\2&1&1\\3&2&3\end{pmatrix} \xrightarrow[(-1)\cdot R_2]{(-1)\cdot R_1} \begin{pmatrix}-1&0&0\\-2&-1&-1\\3&2&3\end{pmatrix}$$

Computing Q, from the column operations:

$$\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix} \xrightarrow[C_1\leftrightarrow C_3]{} \begin{pmatrix}0&0&1\\0&1&0\\1&0&0\end{pmatrix} \xrightarrow[C_2+2C_1]{} \begin{pmatrix}0&0&1\\0&1&0\\1&2&0\end{pmatrix} \xrightarrow[C_2\leftrightarrow C_3]{} \begin{pmatrix}0&1&0\\0&0&1\\1&0&2\end{pmatrix} \xrightarrow[C_3+3C_2]{} \begin{pmatrix}0&1&3\\0&0&1\\1&0&2\end{pmatrix} \xrightarrow[C_3+5C_2]{} \begin{pmatrix}0&1&8\\0&0&1\\1&0&2\end{pmatrix}$$

Hence, we have

$$P = \begin{pmatrix}-1&0&0\\-2&-1&-1\\3&2&3\end{pmatrix}, \qquad Q = \begin{pmatrix}0&1&8\\0&0&1\\1&0&2\end{pmatrix}.$$

We check:

$$\begin{aligned} PAQ &= \begin{pmatrix}-1&0&0\\-2&-1&-1\\3&2&3\end{pmatrix} \begin{pmatrix}0&2&-1\\-3&8&3\\2&-4&-1\end{pmatrix} \begin{pmatrix}0&1&8\\0&0&1\\1&0&2\end{pmatrix} \\ &= \begin{pmatrix}0&-2&1\\1&-8&0\\0&10&0\end{pmatrix} \begin{pmatrix}0&1&8\\0&0&1\\1&0&2\end{pmatrix} = \begin{pmatrix}1&0&0\\0&1&0\\0&0&10\end{pmatrix}, \end{aligned}$$

Problem 2. A ring R is said to be a *Euclidean domain* if there is a function $\varphi : R \to \mathbb{Z}$ satisfying:

(a) For all nonzero elements $a, b \in R$ satisfying $a|b$, we have $\varphi(a) \le \varphi(b)$.

(b) For all $a, b \in R$ with b nonzero, there are elements q, r in R such that $a = qb + r$ and $\varphi(r) < \varphi(b)$.

Answer Problem 1 on page 219. (Note that, in the book, $a|b$ can only hold if a, b are both nonzero. But the question is still correct with our definition).

Part (a). Suppose $b \neq 0$. By (b) in the definition, we can write $b = qb + r$ where $\varphi(r) < \varphi(b)$. If $r \neq 0$, then $b(1-q) = r$, so by (a) in the definition, $\varphi(b) \le \varphi(r)$, a contradiction. Hence $r = 0$ and $\varphi(0) < \varphi(b)$.

Part (b). Suppose $a, b \in R$ are associates. Then $a = 0$ if and only if $b = 0$, and in this case $\varphi(a) = \varphi(b)$. So assume a, b are both non-zero. Since a, b are associates, $a|b$ and $b|a$. Hence $\varphi(a) \le \varphi(b)$ and $\varphi(b) \le \varphi(a)$ by (a) in the definition. So $\varphi(a) = \varphi(b)$ as required.

Part (c). Suppose $a, b \in R$ satisfy $a|b$ and $\varphi(a) = \varphi(b)$. So $b = ca$ for some $c \in R$. If $a = 0$ then $b = 0$. If $b = 0$ and $a \neq 0$, then $\varphi(a) \neq \varphi(b)$ by part (a), a contradiction, so $a = 0$. Hence $a = 0$ if and only if $b = 0$, and in this case, a, b are associates.

We are left with the case a, b both non-zero. Write $a = qb + r$, where $\varphi(r) < \varphi(b)$. We assume first that $r \neq 0$. We have $r = a - qb = a - qca = a(1 - qc)$, so $\varphi(a) \le \varphi(r)$ by (a) in the definition. We then have:

$$\varphi(a) \le \varphi(r) < \varphi(b) = \varphi(a),$$

a contradiction. Hence $r = 0$ and $a = qb$. Therefore $a = qb = qca$. Since $a \neq 0$, $1 = qc$ and q, c are units, so a, b are associates as required.

Problem 3. It is known that every Euclidean domain is a principal ideal domain (see Theorem 3.2 on page 218 of the book). Give a technique for reducing a matrix over a Euclidean domain to its Smith normal form using only elementary row and column operations (Challenge question).

We first prove:

Lemma Let R be a Euclidean domain. Let $a \in R$.

(i) If $a \neq 0$ then $\varphi(a) \geq \varphi(1)$.

(ii) We have $\varphi(a) = \varphi(1)$ if and only if a is a unit.

Proof. Note that, by part (a) of Problem 2, $\varphi(0) < \varphi(a)$ for any element $a \in R \setminus \{0\}$. Also, for such an element a, we have $1|a$ so, by (a) in the definition of a Euclidean domain, $\varphi(1) \leq \varphi(a)$.

Suppose $a \in R$ and $\varphi(a) = \varphi(1)$. Since $1|a$, we have by part (c) from Problem 2 that a and 1 are associates, which implies that a is a unit. Conversely, if a is a unit, then a and 1 are associates so by part (b) of Problem 2, $\varphi(a) = \varphi(1)$. So an element of R is a unit if and only if $\varphi(a) = \varphi(1)$. □

Suppose we are given $A \in M_{m,n}(R)$. If every entry of A is zero, we are done. If not, we find a_{ij} with $\varphi(a_{ij})$ minimal and apply row and column exchanges to move the entry to the top left corner of A. We then try to reduce the first row of the matrix to zeros.

Step 1: If $a_{1t} \neq 0$ and $a_{11}|a_{1t}$ for some $t \neq 1$, write $a_{1t} = da_{11}$. We can apply:

$$C_t - dC_1$$

to reduce this entry to zero. We do this for all possible t.

Step 2: If there is still some non-zero entry a_{1t} in A with $t \neq 1$, we write $a_{1t} = qa_{11} + r$ where $\varphi(r) < \varphi(a_{11})$. We then apply the operations:

$$C_t - qC_1, \qquad C_1 \leftrightarrow C_t$$

which reduce the entry a_{1t} to r and swap it into the $(1, 1)$ position.

We then repeat Steps 1 and 2. Each time we apply Step 2, we reduce the value of φ applied to the $1, 1$-entry of the matrix. Suppose this process never stopped. By the Lemma, we would eventually reach the point where a_{11} was a unit, and stop, a contradiction. It follows that after finitely many steps we must have $a_{12} = \cdots = a_{1n} = 0$.

We apply the same procedure to the first column. Note that while doing this, we may swap rows so that the first row has non-zero entries again, apart from the first. We therefore repeat the first step, clearing the first row again (making $a_{12} = \cdots = a_{1n} = 0$), then the first column, and so on.

Since the value of φ applied to the $1, 1$-entry decreases each time we return to the first row, it again follows from the Lemma that this process must terminate after finitely many steps, with the first row and column cleared, i.e. with $a_{12} = \cdots = a_{1n} = 0$ and $a_{21} = \cdots = a_{m1} = 0$. The rest of the algorithm is as in the general PID case considered in lectures and the book, except that we follow the above procedure again in the last step of the proof, i.e. in order to reduce a matrix:

$$\begin{pmatrix} a_1 & & & & \\ & a_2 & & & \\ & & \ddots & & \\ & & & a_k & \\ & & & & \\ & & & & \end{pmatrix}$$

where $a_1 \nmid a_2$, we apply $R_1 + R_2$ and then repeat the whole of the above procedure: the algorithm terminates because the value of φ applied to the $1, 1$ entry decreases each time we do this (we again use the Lemma).

R. J. Marsh, 18/11/14.