MATH 100B: Homework #9

Due on Mar 14, 2023 at 12:00pm

Professor McKernan

Section A02 6:00PM - 6:50PM
Section Leader: Castellano-Macías

Source Consulted: Textbook, Lecture, Discussion, Office Hour

Ray Tsai
A16848188

Problem 1

Let R be an integral domain and let M be an R-module. We say that $m \in M$ is torsion if there is a non-zero element $r \in R$ such that $r \cdot m = 0$.

(i) Show that the subset T of all elements of M which are torsion is a submodule of M.

Proof. Let $a, b \in T$. There exists $r, s, t \in R$ such that $ra = sb = 0$. But then $rs(a+b) = s(ra)+r(sb) = 0$ and $s(ta) = t(sa) = 0$, so T is closed under addition and scalar multiplication, so T is a submodule of M. □

(ii) What are the torsion elements in

(a) $\mathbb{Q}/\mathbb{Z}$?

Proof. Note that $\mathbb{Q}/\mathbb{Z} = \{a + \mathbb{Z} \mid a \in \mathbb{Q}, 0 \le a < 1\}$. Let $[a] \in \mathbb{Q}/\mathbb{Z}$. If $a \in \mathbb{Z}$, then $[a] = [0]$ and there is nothing to prove. Otherwise, since $\mathbb{Q}$ is closed under taking inverses, there eixsts nonzero $b = \frac{1}{a} \in \mathbb{Q}$ such that $[a][b] = [ab] = [1] = [0]$. Hence, all elements in $\mathbb{Q}/\mathbb{Z}$ are torsion elements. □

(b) $\mathbb{R}/\mathbb{Z}$?

Proof. Note that $\mathbb{R}/\mathbb{Z} = \{a + \mathbb{Z} \mid 0 \le a < 1\}$. Let $[a] \in \mathbb{R}/\mathbb{Z}$. If $a \in \mathbb{Z}$, then $[a] = [0]$ and there is nothing to prove. Otherwise, there eixsts nonzero $b = \frac{1}{a} \in \mathbb{R}$ such that $[a][b] = [ab] = [1] = [0]$. Hence, all elements in $\mathbb{R}/\mathbb{Z}$ are torsion elements. □

(c) $\mathbb{R}/\mathbb{Q}$?

Proof. Note that $\mathbb{R}/\mathbb{Q} = \{a + \mathbb{Q} \mid a \text{ is irrational}\}$. Let $[a] \in \mathbb{R}/\mathbb{Q}$. If $a \in \mathbb{Q}$, then $[a] = [0]$ and there is nothing to prove. Otherwise, there eixsts nonzero $b = \frac{1}{a} \in \mathbb{R}$ such that $[a][b] = [ab] = [1] = [0]$. Hence, all elements in $\mathbb{R}/\mathbb{Q}$ are torsion elements. □

(iii) Is the $\mathbb{Z}$-module $\mathbb{Q}$

(a) torsion-free?

Proof. Yes. Since $\mathbb{Q}$ is an integral domain and $\mathbb{Q} \supset \mathbb{Z}$, $\mathbb{Q}$ does not contain $r \in \mathbb{Z}$ such that $rq = 0$, for $q, r \neq 0$. □

(b) free?

Proof. No. Suppose for the sake of contradiction that the collection $B = \{x_i\}$ is a basis of $\mathbb{Q}$. Let $x, y \in \mathbb{Q}$, say $x = \frac{p}{q}$ and $y = \frac{m}{n}$. But then there exists $a = mq, b = -np \in \mathbb{Z}$ such that $ax + by = 0$. This implies any two elements in $\mathbb{Q}$ are linearly dependent, and thus B contains at most one element. However, elements in $\mathbb{Q}$ cannot be written as a fixed rational scaled by integers, and thus B is not a basis of $\mathbb{Q}$, contradiction. □

(c) finitely generated?

Proof. No. Suppose for the sake of contradiction that $\mathbb{Q}$ is finitely generated by $B = \{x_i\}_{i=1}^n$, say $x_i = \frac{p_i}{q_i}$. Since there are infinitely any primes, let p be a prime such that p does not divide q_i, for any i. Let $d = \prod q_i$. Since B generates $\mathbb{Q}$,

$$\frac{1}{p} = \sum r_i \cdot \frac{p_i}{q_i} = \frac{k}{d},$$

for some $r_i, k \in \mathbb{Z}$. But then p does not divide d, so $\frac{k}{d} \neq \frac{1}{p}$, contradiction. □

Problem 2

Let R be a PID and let M be a finitely generated module over R.

(i) Show that there is a free module F which is a quotient of M and which is maximal with respect to this property.

Proof. By Corollary 14.6, $M = F \oplus T$, where F is a free module and T is the torsion module. F is obvisouly a quotient of M and the maximal free module in M, as T is not free. $\square$

(ii) Show that there is an injective R-linear map $F \to M$.

Proof. Take $\phi : F \to F \oplus T \simeq M$ that simply sends a to $(a, 0)$. ϕ is obvisouly an injective R-linear map. $\square$

(iii) Show that the image of F is not always unique.

Proof. Consider $R = \mathbb{Z}$ and $M = \mathbb{Z} \oplus \mathbb{Z}_2$. Since there exists two injective linear maps $R \to M$, one sends n to $(n, 0)$ and the other sends n to (n, n), the result follows. $\square$

Problem 3

Let

$$A = \begin{pmatrix} -4 & -6 & 7 \\ 2 & 2 & 4 \\ 6 & 6 & 15 \end{pmatrix} \in M_{3,3}(\mathbb{Z}).$$

(i) Put A into Smith normal form D using elementary operations.

Proof. Note that the *gcd* of all entries of A is 1. We first replace the thrid column by the sum of the last two column, and then we swap the first column with the thrid and get

$$\begin{pmatrix} 1 & -6 & -4 \\ 6 & 2 & 2 \\ 21 & 6 & 6 \end{pmatrix}$$

We then eliminate the entries of first rows and columns

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 38 & 26 \\ 0 & 132 & 90 \end{pmatrix}$$

Now perform the euclidean algorithm on 38 and 26 to cancel the entry on 2nd row 3rd column

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 2 \\ 0 & 6 & 6 \end{pmatrix}$$

Finally, we eliminate the bottom right entry and swap the last two column and get the smith noraml form of A.

$$D = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 6 \end{pmatrix}$$

$\square$

(ii) Check your answer using minors.

Proof. Note that $d_1(A) = 1$, $d_2(A) = \gcd(4, -30, -38, 12, -102, -132, 0, 0, 6) = 2$, $d_3(A) = \det(A) = 12$. It follows that $\frac{d_1(A)}{d_0(A)} = 1$, $\frac{d_2(A)}{d_1(A)} = 2$, and $\frac{d_3(A)}{d_2(A)} = 6$, so we didn't make any dumb mistakes. $\square$

(iii) Explain how to find invertible matrices P and Q such that $D = QAP$.

Proof. Note that every elementary matrix operation can be converted into an elementary matrix multiplication, with pre-multiplication for row manipulations and post-multiplication for column manipulations. Note that elementary matrices are invertible. Hence, we may follow our process in (i) and multiply all elementary matrix in each step. At the end, the product of the elementary matrix in each step would be our Q and P. $\square$

Problem 4

Find the Smith normal form of

$$\begin{pmatrix} 2x-1 & x & x-1 & 1 \\ x & 0 & 1 & 0 \\ 0 & 1 & x & x \\ 1 & x^2 & 0 & 2x-2 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} x^2+2x & 0 & 0 & 0 \\ 0 & x^2+3x+2 & 0 & 0 \\ 0 & 0 & x^3+2x^2 & 0 \\ 0 & 0 & 0 & x^4+x^3 \end{pmatrix}$$

over the ring $\mathbb{R}[x]$.

Proof. Let the left matrix be A and the right one be B. For A, we first move the 1 at the 2nd column 3rd row to the top right and eliminate the first row and first column

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

We now swap the second and thrid columns, then eliminate the second row and column

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & x^3-x^2+3x-1 & -x^2+1 \\ 0 & 0 & x^4+1 & -x^3+2x-2 \end{pmatrix}$$

Since the gcd for the bottom right 2x2 submatrix is 1, we may put the third diagonal as 1 and the last diagonal entry as the determinant of the 2x2 submatrix, and we are done with A.

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & x^5-2x^4-3x^3+9x^2-8x+1 \end{pmatrix}$$

For B we calculate the gcd's of minors of all sizes

$$d_1(B) = 1$$

$$d_2(B) = \gcd(x(x+1)(x+2)^2, x^2(x+1)(x+2)^2, x^5(x+1)(x+2), x^2(x+2)^2, x^4(x+2)(x+1), x^3(x+1)^2(x+2)) = x(x+2)$$

$$d_3(B) = \gcd(x^3(x+1)(x+2)^3, x^6(x+1)(x+2)^2, x^4(x+1)^2(x+2)^2, x^5(x+1)^2(x+2)^2) = x^3(x+1)(x+2)^2$$

$$d_4(B) = x^6(x+1)^2(x+2)^3.$$

Thus, the Smith normal form of B is

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & x(x+2) & 0 & 0 \\ 0 & 0 & x^2(x+1)(x+2) & 0 \\ 0 & 0 & 0 & x^3(x+1)(x+2) \end{pmatrix}$$

$\square$

Problem 5

Let G be the abelian group with presentation given by generators a, b and c, and relations $6a + 10b = 0$, $6a + 15c = 0$ and $10b + 15c = 0$. Determine the structure of G as a product of cyclic groups.

Proof. Since G is a module over $\mathbb{Z}$ generated by three elements, G is a quotient of $\mathbb{Z}^3$. In other words, $G \simeq \mathbb{Z}^3/K$, for some kernel K. We wish to find a map $\mathbb{Z}^3 \to \mathbb{Z}^3$ whose image is K. Define linear map $\phi : \mathbb{Z}^3 \to \mathbb{Z}^3$, whose transformation matrix is

$$\begin{pmatrix} 6 & 10 & 0 \\ 6 & 0 & 15 \\ 0 & 10 & 15 \end{pmatrix}.$$

Note that ϕ obvisouly encodes the relations of the generators, and thus it's image is K. The smith normal form of ϕ can be calculated by the minors, and we get

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 30 & 0 \\ 0 & 0 & 60 \end{pmatrix},$$

and thus G is isomorphic to $\mathbb{Z}^3/(\mathbb{Z} \oplus 30\mathbb{Z} \oplus 60\mathbb{Z}) \simeq \mathbb{Z}_{30} \oplus \mathbb{Z}_{60}$. $\square$

Problem 6

Let A be a complex square matrix with characteristic polynomial $(x+1)^6(x-2)^3$ and minimal polynomial $(x+1)^3(x-2)^2$. What are all of the possible Jordan normal forms for A?

Proof. Since the characteristic polynomial is $(x+1)^6(x-2)^3$, there are six -1's on the diagonal and three 2's on the diagonal. Since the minimal polynomial is $(x+1)^3(x-2)^2$, the largest Jordan block of eigenvalue -1 is of size 3×3, and the largest Jordan block of eigenvalue 2 is of size 2×2. Let J_i^n be the Jordan block of eigenvalue i of size $n \times n$. The possible configurations, up to reordering, of the Jordan normal form of A are

$$diag(J_{-1}^3, J_{-1}^3, J_2^2, J_2), \quad diag(J_{-1}^3, J_{-1}^2, J_{-1}, J_2^2, J_2), \quad diag(J_{-1}^3, J_{-1}, J_{-1}, J_{-1}, J_2^2, J_2),$$

where *diag* represents a matrix whose diagonals are specified Jordan blocks. $\square$

Problem 7

Describe all conjugacy classes of the following finite groups. For each conjugacy class give the order and the minimal polynomial of an element.

(i) $GL_2(\mathbb{F}_2)$

Proof. Note that there are 6 elements in $GL_2(\mathbb{F}_2)$, and so we list out all conjugacy classes:

$$\left\{\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\right\}, \quad \text{order: } 1, \text{ minimal polynomial: } x-1,$$

$$\left\{\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}, \begin{pmatrix}0 & 1\\ 1 & 1\end{pmatrix}, \begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix}\right\}, \quad \text{order: } 2, \text{ minimal polynomial: } x^2+x+1,$$

$$\left\{\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}, \begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix}\right\}, \quad \text{order: } 3, \text{ minimal polynomial: } x^2+1,$$

□

(ii) $GL_3(\mathbb{F}_2)$

Proof. Note that if two matrices are similar, they have the same characteristic polynomials. Hence, we may count the number of normal forms each characteristic polynomial have to obtain the size of each conjugacy class. By example 8.11, we get all irreducible polynomials of order at most 3, and the rest is left as an exercise for the grader. □