Rings and Modules

Trishan Mondal

Assignment-4

Problem 1

> (a) Discuss whether the abelian group $\mathbb{Z}/m\mathbb{Z}$ can be written as the direct sum of two proper sub groups, where $m = p^2q^3r^4$ are p, q, r are distinct primes.
> (b) Determine the number of non-isomorphic abelian groups of order 360.

Solution. **(a)** We know for any m, n with $\gcd(m, n) = 1$ We can write $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/mn\mathbb{Z}$. Since, $m\mathbb{Z}+n\mathbb{Z} = \mathbb{Z}$ to get the above result. We know if there is finite number of summand in direct sum then direct sum is isomorphic to direct product. So, we can conclude that $\mathbb{Z}/mn\mathbb{Z} = \mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$.

In the given problem since $m = p^2q^3r^4$ where p, q, r are distinc prime we can say that $\mathbb{Z}/m\mathbb{Z} = \mathbb{Z}/p^2\mathbb{Z} \oplus \mathbb{Z}/q^3r^4\mathbb{Z}$. We can decompose the given group into direct sum of two proper subgroup.

(b) Let us denote $N = 360 = 2^3 \times 3^2 \times 5$. So the total number of non iso-morphic abelian group of order 360 is $P(3) \times P(2)$ which is product of total number of partition of 3 and 2 respectively. It's not hard to see that $P(3) = 3$ and $P(2) = 2$. So, there is 6 non-isomorphic abelian groups of order 360.

Problem 2

> (a)Find the base for the submodule M of $\mathbb{Z}^3$ generated by $(1, 0, -1), (2, -3, 1), (0, 3, 1), (3, 1, 5)$.
> (b) Let R be a PID. Prove that a vector $(a_1, a_2, \cdots, a_n)$ in R^n can be completed to a basis if, and only if, the ideal $(a_1, a_2, \cdots, a_n) = (1)$.

Solution. **(a)** We will consider a 4×3 matrix whose rows are the given vectors. Now we will look onto the row echelon form of that matrix to decide the rank and base for the submodule M generated by the given elements.

$$\begin{pmatrix} 1 & 0 & -1 \\ 2 & -3 & 1 \\ 0 & 3 & 1 \\ 3 & 1 & 5 \end{pmatrix} \xrightarrow{R_2 \mapsto R_2 - 2R_1, R_4 \mapsto R_4 - 3R_1} \begin{pmatrix} 1 & 0 & -1 \\ 0 & -3 & 3 \\ 0 & 3 & 1 \\ 0 & 1 & 7 \end{pmatrix} \xrightarrow{R_2 \mapsto R_2 + 3R_4, R_3 \mapsto R_3 - 3R_4} \begin{pmatrix} 1 & 0 & -1 \\ 0 & 0 & 24 \\ 0 & 0 & -20 \\ 0 & 1 & 7 \end{pmatrix}$$
$$\xrightarrow{R_2 \mapsto R_2 + R_3} \begin{pmatrix} 1 & 0 & -1 \\ 0 & 0 & 4 \\ 0 & 0 & -20 \\ 0 & 1 & 7 \end{pmatrix} \xrightarrow{R_3 \mapsto R_3 + 5R_2} \begin{pmatrix} 1 & 0 & -1 \\ 0 & 0 & 4 \\ 0 & 0 & 0 \\ 0 & 1 & 7 \end{pmatrix}$$

So, $(1,0,-1),(0,0,4),(0,1,7)$ generates M. Consiser a linear combination of these vectors which is zero.

$$\begin{aligned} a(1,0,-1)+b(0,0,4)+c(0,1,7) &= (a,c,4b-a+7c) \\ \implies (a,b,c) &= (0,0,0) \end{aligned}$$

So these vectors are linearly independent. Now these vectors can't generate $(3,1,5)$. So we can take $(0,0,1)$ in place of $(0,0,4)$. $\mathcal{B}' = \{(1,0,-1),(0,0,1),(0,1,7)\}$ forms a base for module M.

(b) If we can extend $a = (a_1,\cdots,a_n)$ to a basis of R^n then let, $\mathcal{B} = \{a, v_1, \cdots, v_n\}$ be the basis of R^n. Consider the matirix $A = \begin{pmatrix} a & v_1 & \cdots & v_{n-1} \end{pmatrix}^T$. Clearly it is invertible, hence $\det(A)$ will be unit of R. We can see that, $\det(A) = a_1x_1 + \cdots + a_nx_n$ (for some $x_1,\cdots,x_n$) which is unit in R. So,$\det(A) \in (a_1,\cdots,a_n)$. Which means $(a_1,\cdots,a_n) = R$.

If we assume $(a_1,\cdots,a_n) = R$, there exist elements of R, $c_1,\ldots,c_n$ such that $\sum_{i=1}^n c_ia_i = 1$. Define the linear map $\varphi : R^n \to R$ by $\varphi(r_1,\ldots,r_n) = \sum_{i=1}^n c_ir_i$. Let $x \in R^n$ as $\varphi(a_1,\ldots,a_n) = 1$, there exists an element y of $R(a_1,\ldots,a_n)$ such that $\varphi(x) = \varphi(y)$. Then $\varphi(x-y) = 0 \implies x-y \in \ker\varphi$. So $R^n \cong R(a_1,\ldots,a_n) + \ker\varphi$. We can also see that, $R(a_1,\ldots,a_n) \cap \ker\varphi = \phi$, as $\varphi(r(a_1,\ldots,a_n)) = 0 \implies r = 0$ where $r \in R$. Now $(a_1,\ldots,a_n)$ is a basis for $R(a_1,\ldots,a_n)$ as $r(a_1,\ldots,a_n) = 0 \implies r = 0$, this is because at least one of the a_i must be non-zero otherwise $\sum_{i=1}^n c_ia_i = 1$ would not be possible. So, we can write $R^n = R(a_1,\cdots,a_n) \oplus \ker\varphi$. Here, $\ker\varphi$ is submodule of a finitely generated free module over R(PID),which means $\ker\varphi$ is also finitely generated free module. Let $v_1,\cdots v_m$ be the basis of it then, $a, v_1, \cdots, v_m$ is basis of R^n. ■

Problem 3

(a) Find the invariant factors (that is, the Smith normal form) of

$$A = \begin{pmatrix} X-17 & 8 & 12 & -14 \\ -46 & X+22 & 35 & -41 \\ 2 & -1 & X-4 & 4 \\ -4 & 2 & 2 & X-3 \end{pmatrix}$$

(b) Find all possible Jordan forms of a matrix whose characteristic polynomial is $(X+2)^2(X-5)^3$.

Solution.
(a) We can consider the the matrix $A = xI - B$. Now rational cannonical form of B will give us smith normal form of A. We need to find characteristic polynomial of B which is $\det A$. We can see that $\det(A) = (X-1)^3(X+1)$. Also we can check that $B^3 - B^2 - B + I$ is 0 and $(B^2 - I), (B-I)^2 \neq 0$ which means $X^3 - X^2 - X + 1$ is minimal polynomial of B. So, $(X-1)^2(X+1)$ is minimal polynomial of B. We can write, $\mathbf{diag}[1,1,X-1,(X-1)^2(X+1)]$ is the rational cannonical form of A and hence $(X-1)$ and $(X-1)^2(X+1)$ are invariant factors of A.

(b) From invariant factor theorem we know If A is the matirix whose characteristic polynomial is $(X+2)^2(X-5)^3$, then the possible rational cannonical forms are,

- $\mathbf{diag}[1,1,1,X+2,(X+2)(X-5)^3]$
- $\mathbf{diag}[1,1,1,(X+2)(X-5),(X+2)(X-5)^2]$
- $\mathbf{diag}[1,1,1,(X-5),(X-5)^2(X+2)^2]$
- $\mathbf{diag}[1,1,(X-5),(X-5),(X-5)(X+2)^2]$
- $\mathbf{diag}[1,1,(X-5),(X-5)(X+2),(X-5)(X+2)]$
- $\mathbf{diag}[1,1,1,1,(X+2)^2(X-5)^3]$

Corresponding possible Jordon-cannonical forms are(respectively),

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

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

Problem 4

> Let $A \in M_n(\mathbb{Z})$ and consider the group homomorphism T_A from $\mathbb{Z}^n$ to itself given by $v \mapsto Av$ (where v is written as a column). Find necessary and sufficient conditions for the image of T_A to have finite index in $\mathbb{Z}^n$. When that condition holds, determine the index.

Solution. Since $\mathbb{Z}$ is PID we can get smith normal form of a matrix $A \in M_n(\mathbb{Z})$. which means there is invertible matrix P, Q such that $PAQ = D$ where, D is the diagonal matrix. Let, T_D be the homomorphism corresponding to the matirix D. Since P and Q are invertible matirix it will induce isomorphisms between $\mathbb{Z}^n$. PAQ is basically changing basis of T_A, So, T_A and T_D will have same image in $\mathbb{Z}^n$, $\operatorname{Im}\{T_A\} = \operatorname{Im}\{T_D\}$. If $D = \mathbf{diag}(d_1, d_2, \cdots, d_n)$ then $\mathbb{Z}^n/\operatorname{Im}\{T_D\} = \mathbb{Z}^n/\operatorname{Im}\{T_A\} = \mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_n\mathbb{Z}$.

Clearly index of Image is same as the cardinality of, $\mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_n\mathbb{Z}$. This is finite iff an only if $d_i \neq 0$ for all i (otherwise direct sum will consist some $\mathbb{Z}$ as its summand) Which means $\det A \neq 0$. On that case index is $|d_1 \cdots d_n|$ which is $|\det P \det A \det Q|$, since,P, Q is invertible over $\mathbb{Z}$, they can have determinent ± 1. Which means index is $|\det A|$. ■

Problem 5

Let $A \subset B \subset C$ be commutative rings. If C is finitely generated as a B-module and B is finitely generated as an A-module, then prove that C is finitely generated as an A-module.

Solution. Since, C is finitely generated $B-$module and B is finitely generated $A-$module we can assume, $B = Ax_1 + \cdots + Ax_n$ and $C = By_1 + \cdots + By_m$. We can write any arbitrary $c \in C$ as $c = \sum b_i y_i$ and $b_i = \sum a_{ij} x_j$, so we can write c linear combination of $\{x_i y_j\}$. We can do this for any arbitrary c so, C is finitely generated as $A-$module. More specifically we can say, $C = Ax_1y_1 + \cdots + Ax_ny_m$. ■

Problem 6

Let k be a field. Prove that two matrices $A, B \in M_n(k)$ are similar if, and only if, $XI - A$ and $XI - B$ have the same invariant factors as elements of $M_n(k[X])$.

Solution. If A and B are similar over k , i.e $A = PBP^{-1}$ for some invertible P, then $XI_n - A$ can be written as $P(XI_n - B)P^{-1}$. Which means $XI_n - A$ and $XI_n - B$ are similar and hence they must have same smith-normal form i.e. same invariant factors.

Now we want to show if $XI_n - A$ and $XI_n - B$ has same invariant factors then A and B are similar.

Claim: If f is a monic polynomial of degree n over $K[X]$ then $XI_n - C(f)$ is similar to **diag**$[1, 1, \cdots, f(X)]$. Here, $C(f)$ is companion matrix of $f(X)$.

Proof. Let,$f(x) = X^n + \sum_{i=0}^{n-1} a_i X^i$ be the polynomial then, $XI_n - C(f)$ is written as following,

$$XI_n - C(f) = \begin{pmatrix} X & 0 & 0 & \cdots & a_0 \\ -1 & X & 0 & \cdots & a_1 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & -1 & X + a_{n-1} \end{pmatrix}$$

We will do invertible row and oparation to get the desired diagonal matrix. Now we will do the following operations step by step,

- Multiply X with the last row and add it with second last row. $R_{n-1} \mapsto XR_n + R_{n-1}$.
- Multiply X with the second last row and add it with third last row. $R_{n-2} \mapsto XR_{n-1} + R_{n-2}$.
- Repeat these steps untill we reach the first row.
- Then multiply each i-th column with suitable thing and add that with last column so that the last column turns to $(f(X), 0, 0, \cdots, 0)^t$.
- them multiply -1 in each column except the last one and multiply with a proper permutation matrix

$$\begin{pmatrix} X & 0 & 0 & \cdots & a_0 \\ -1 & X & 0 & \cdots & a_1 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & -1 & X + a_{n-1} \end{pmatrix} \longrightarrow \begin{pmatrix} 0 & 0 & 0 & \cdots & a_0 + X^n + \sum_{i=1}^{n-1} a_i X^i \\ -1 & 0 & 0 & \cdots & a_1 + X^{n-1} + \sum_{i=2}^{n-1} a_i X^{i-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & -1 & X + a_{n-1} \end{pmatrix}$$

$$\longrightarrow \begin{pmatrix} 0 & 0 & 0 & \cdots & a_0 + X^n + \sum_{i=1}^{n-1} a_i X^i \\ -1 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & -1 & 0 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & f(X) \end{pmatrix}$$

■

Now we can see that, A is similar to $\oplus_{i=1}^{p} C(f_i)$ and B is similar to $\oplus_{i=1}^{q} C(g_i)$. Here, $f_i \mid f_{i+1}$ and $g_i \mid g_{i+1}$. $XI - A$ is similar to $XI - \oplus_{i=1}^{p} C(f_i)$ and $XI - B$ is similar to $XI - \oplus_{i=1}^{q} C(g_i)$. So they must have same invariant factors. Since $X - IA$ and $X - IB$ has same invariant factors we can say that, $p = q$ and $g_i = f_i$ upto multiplication of some unit. This is because,

$$\begin{aligned} XI - \oplus_{i=1}^{p} C(f_i) &= \oplus_{i=1}^{p} XI - C(f_i) \\ &\sim \oplus_{i=1}^{p} \mathbf{diag}(1, 1, .., f_i(x)) \\ &\sim \mathbf{diag}(1, 1, 1, \cdots, f_1, \cdots, f_p) \end{aligned}$$

we can do similar calculatioon for B so the number of 1 in invariant factors of $XI - A$ and $XI - B$ are same. So, $n - p = n - q \implies p = q$ and $f_i = g_i$.

It is clear that $\oplus_{i=1}^{p} C(f_i) \sim \oplus_{i=1}^{q} C(g_i)$ which means A, B are similar. ■

Problem 7

In this problem, comments about fundamental groups are made for interest; they may safely be ignored and the relevant problem on the structure of the finitely generated abelian group can be solved.

The Klein bottle is a 'surface' whose fundamental group G has a presentation $< a, b \mid ab = b^{-1}a >$. Show that $G/[G, G] \cong \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. The braid group B_n for $n \geq 3$ is the group with a presentation $< g_1, g_2, \cdots, g_{n-1} \mid g_i g_{i+1} g_i = g_{i+1} g_i g_{i+1}, g_i g_j = g_j g_i$ if `i-j` $\geq 2 >$. That is, the latter relations hold only for i, j such that `i-j` > 1.

(It is an interesting fact that the fundamental group of the complement of the trefoil knot (see figure below) is B_3. Knots are embeddings of S^1 in S^3 and are distinguished usually by the fundamental group of their complements). Show that the abelianization $B_n/[B_n, B_n]$ of B_n is isomorphic to $\mathbb{Z}$.

Solution.

• **Klein bottle** (K) has fundamental group,

$$\pi_1(K) = \langle a, b \mid ab = b^{-1}a \rangle$$

Abelianization of $\pi_1(K)$ is dependent on two generators. We know there exist a surjective map $\varphi : F_2 \to \pi_1(K)/[\pi_1(K), \pi_1(K)]$ where F_2 is free abelian group with two generators. We can say $F_2 = \mathbb{Z}^2$. Let, $\{e_1, e_2\}$ generates $\mathbb{Z}^2$ and φ takes e_1 to a and e_2 to b. The kernal of φ is generated by the following relations,

$$\begin{aligned} &e_1 + e_2 = e_2 - e_1 \\ \implies &2e_1 = 0 \end{aligned}$$

we get, $\ker\varphi = 2\mathbb{Z}$ and hence $\pi_1(K)/[\pi_1(K), \pi_1(K)] = \mathbb{Z}^2/2\mathbb{Z} = \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

• **Braid group** has presentation,

$$B_n = \langle g_1, \cdots, g_{n-1} \mid g_i g_{i+1} g_i = g_{i+1} g_i g_{i+1}, g_i g_j = g_j g_i |i - j| \geq 2\rangle$$

Just like the previous case we can see that the abelianization of B_n depends on $n-1$ generators. So, we will get a surjective map $\varphi : \mathbb{Z}^{n-1} \to B_n/[B_n, B_n]$. Let, $\{e_1, \cdots, e_{n-1}\}$ is basis of $\mathbb{Z}^{n-1}$ which maps to the generators $\{g_i\}$ by φ. Now the kernal of φ will be genarated by $\{e_i\}$ with the following relations,

$$\begin{aligned} &e_i + e_{i+1} + e_i = e_{i+1} + e_i + e_{i+1} \text{ for } i = \{1, \cdots, n-2\} \\ \implies &e_i - e_{i+1} = 0 \\ \implies &\underbrace{\begin{pmatrix} 1 & -1 & 0 & \cdots & 0 \\ 0 & 1 & -1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \\ 0 & \cdots & \cdots & 1 & -1 \\ 0 & \cdots & \cdots & 0 & 0 \end{pmatrix}}_{\text{call this matrix } A} \begin{pmatrix} e_1 \\ e_2 \\ \vdots \\ e_{n-1} \end{pmatrix} = 0 \end{aligned}$$

A is the relation matrix for the kernel. Since $\mathbb{Z}$ is PID, we can get smith normal form of A. We can see that A can be easily diagonalized to $\mathbf{diag}(1, 1, \cdots, 1, 0) = PAQ$. Where, P, Q are invertible matrix.So, transformathion by P, Q will induce an isomorphisms. So, Image of A and $\mathbf{diag}(1, 1, ..., 1, 0)$ will be same and hence, $\ker\varphi \cong \mathbb{Z}^{n-1}$. From here we get, $B_n/[B_n, B_n] = \mathbb{Z}$. ■