MATH 601 HOMEWORK (DUE 10/16)

HIDENORI SHINOHARA

Contents

1. Modules

Exercise. (Problem 2) Consider the $m \times n$ matrices given below as presentation matrices for $\mathbb{Z}$-modules. That is think of the given matrix, H, as giving a linear transformation, $\mathbb{Z}^n \to \mathbb{Z}^m$, $x \mapsto Hx$ and thus giving a presentation of $\operatorname{Coker}(H) = \mathbb{Z}^m / \operatorname{Im}(H)$. Give in each case a familiar finitely generated $\mathbb{Z}$-module which is isomorphic to the $\mathbb{Z}$-module which H presents.

- $H = 6$.
- $H = \begin{bmatrix} 2 & 1 \end{bmatrix}$.
- $H = \begin{bmatrix} 2 & 3 \\ 4 & 5 \end{bmatrix}$.
- $H = \begin{bmatrix} 4 & 12 \\ 6 & 2 \end{bmatrix}$.
- $H = \begin{bmatrix} 3 & 6 \\ 8 & 4 \\ 10 & 5 \end{bmatrix}$.
- $H = \begin{bmatrix} 36 & 12 & 24 \\ 30 & 18 & 24 \\ 15 & -6 & 12 \end{bmatrix}$.

Proof. In each case, we will compute a Smith normal form because a smith normal form allows us to find invariant factors easily. Moreover, elementary row and column operations over integers of H correspond to a change of basis of $\mathbb{Z}^m$ and $\mathbb{Z}^n$. Therefore, it does not change the module represented by the matrix.

- This H generates the exact sequence
$$\mathbb{Z}^1 \xrightarrow{H} \mathbb{Z}^1 \xrightarrow{p} \mathbb{Z}^1/6\mathbb{Z} \xrightarrow{0} 0$$
where p is the map $k \mapsto k + 6\mathbb{Z}$. Thus $\mathbb{Z}/6\mathbb{Z}$ is what H represents.
- This H generates the exact sequence
$$\mathbb{Z}^2 \xrightarrow{H} \mathbb{Z}^1 \xrightarrow{p} \mathbb{Z}^1/\operatorname{Im}(H) \xrightarrow{0} 0$$

where p is the map $k \mapsto k + \operatorname{Im}(H)$. The Smith normal form of H is $\begin{bmatrix} 1 & 0 \end{bmatrix}$ since

$$\begin{aligned} \begin{bmatrix} 2 & 1 \end{bmatrix} &\sim \begin{bmatrix} 1 & 2 \end{bmatrix} \\ &\sim \begin{bmatrix} 1 & 0 \end{bmatrix} \end{aligned}$$

Thus H represents $\mathbb{Z}/\mathbb{Z} \cong 0$.

- This H generates the exact sequence

$$\mathbb{Z}^2 \xrightarrow{H} \mathbb{Z}^2 \xrightarrow{p} \mathbb{Z}^2/\operatorname{Im}(H) \xrightarrow{0} 0$$

where p is the map $k \mapsto k + \operatorname{Im}(H)$. The Smith normal form of H is $\begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}$ since

$$\begin{aligned} \begin{bmatrix} 2 & 3 \\ 4 & 5 \end{bmatrix} &\sim \begin{bmatrix} 3 & 2 \\ 5 & 4 \end{bmatrix} \\ &\sim \begin{bmatrix} 1 & 2 \\ 1 & 4 \end{bmatrix} \\ &\sim \begin{bmatrix} 1 & 2 \\ 0 & 2 \end{bmatrix} \\ &\sim \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}. \end{aligned}$$

Consider the basis $\{(1,0),(0,1)\}$. Then for any k, $k(1,0) = 0$ in $\operatorname{Coker} H$ and $k(0,1) = 0$ in $\operatorname{Coker} H$ if and only if $k \equiv 0 \pmod 2$.

Thus H represents $\mathbb{Z}^2/\langle (1,0),(0,2)\rangle \cong \mathbb{Z}/\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z}$.

- This H generates the exact sequence

$$\mathbb{Z}^2 \xrightarrow{H} \mathbb{Z}^2 \xrightarrow{p} \mathbb{Z}^2/\operatorname{Im}(H) \xrightarrow{0} 0$$

where p is the map $k \mapsto k + \operatorname{Im}(H)$. The Smith normal form of H is $\begin{bmatrix} 2 & 0 \\ 0 & 32 \end{bmatrix}$. Thus H represents $\mathbb{Z}^2/\langle (2,0),(0,32)\rangle \cong \mathbb{Z}/\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}/32\mathbb{Z}$.

- This H generates the exact sequence

$$\mathbb{Z}^2 \xrightarrow{H} \mathbb{Z}^3 \xrightarrow{p} \mathbb{Z}^3/\operatorname{Im}(H) \xrightarrow{0} 0$$

Finish this part!

where p is the map $k \mapsto k + \operatorname{Im}(H)$. The Smith normal form of H is $\begin{bmatrix} 2 & 0 \\ 0 & 32 \end{bmatrix}$. Thus H represents $\mathbb{Z}^2/\langle (2,0),(0,32)\rangle \cong \mathbb{Z}/\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}/32\mathbb{Z}$.

-

□

Exercise. (Problem 3) To what familiar abelian group is the following abelian group isomorphic to? The group generated by a, b, c for which the module of relations is generated by the following relations, $6a - 10b + 4c = 0$ and $8a - 20c = 0$.

Proof. We claim that the following exact sequence represents the group.

$$\mathbb{Z}^2 \xrightarrow{H} \mathbb{Z}^3 \xrightarrow{q} \mathrm{Coker}(H) \xrightarrow{0} 0$$

where $H = \begin{bmatrix} 6 & 8 \\ -10 & 0 \\ 4 & -20 \end{bmatrix}$. Let $\{(1,0),(0,1)\}$ be a basis of $\mathbb{Z}^2$. Then $H(1,0) = \begin{bmatrix} 6 \\ -10 \\ 4 \end{bmatrix}$, and $H(0,1) = \begin{bmatrix} 8 \\ 0 \\ -20 \end{bmatrix}$. Thus $\mathrm{Im}(H)$ is spanned by $H(1,0), H(0,1)$. This is exactly what we want because $\mathrm{Coker}(H) = \mathbb{Z}^3/\langle (6,-10,4),(8,0,-20)\rangle$.

We will take the same approach as Problem 2. The Smith normal form of H is $S = \begin{bmatrix} 2 & 0 \\ 0 & 8 \\ 0 & 0 \end{bmatrix}$. Thus $\mathrm{Coker}(S) = \mathbb{Z}^3/\langle (2,0,0),(0,8,0)\rangle \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}$. □

Exercise. (Problem 4) How many isomorphism classes of abelian groups with $27783 = 3^4 7^3$ elements are there?

Proof. Let M be an abelian group with 27783 elements. Then M is a $\mathbb{Z}$-module with 27783 elements. By the theorem on PP.8-9 of the Module handout, $M \simeq \mathbb{Z}/(d_1) \times \cdots \times \mathbb{Z}/(d_n) \times \mathbb{Z}^{m-s}$. Since M only contains finitely many elements and $\mathbb{Z}$ contains infinitely many elements, $M \simeq \mathbb{Z}/(d_1) \times \cdots \times \mathbb{Z}/(d_n)$. $\gcd(a,b) = 1$ if and only if $\mathbb{Z}/(a)$ is isomorphic to $\mathbb{Z}/(b)$.

- $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$, $\mathbb{Z}_9 \times \mathbb{Z}_3 \times \mathbb{Z}_3$, $\mathbb{Z}_9 \times \mathbb{Z}_9$, $\mathbb{Z}_{27} \times \mathbb{Z}_3$, $\mathbb{Z}_{81}$.
- $\mathbb{Z}_7 \times \mathbb{Z}_7 \times \mathbb{Z}_7$, $\mathbb{Z}_{49} \times \mathbb{Z}_7$, $\mathbb{Z}_{343}$.

Thus the combinations of the above are exactly all the distinct classes of abelian groups with 27783 elements, so there are exactly $3 \times 5 = 15$ classes. □

2. The Quadratic Equation

Exercise. (Problem 23) Show that if $x^2 - 2y^2 = n$, $n \neq 0$ has one solution, then it has infinitely many. If n is prime in $\mathbb{Z}$, describe all the solutions.

Proof. Let $n \in \mathbb{Z}$ be given. Suppose $x^2 - 2y^2 = n$ for some $x, y \in \mathbb{Z}$. For each $k \in \mathbb{N}$, pick $a_k, b_k \in \mathbb{Z}$ such that $a_k + b_k\sqrt{2} = u_0^{2k}$ where $u_0 = 1 + \sqrt{2}$. We showed that u_0^{2k} is a unit element for each $k \in \mathbb{Z}$. Since $(a_k + b_k\sqrt{2})(a_k - b_k\sqrt{2}) = N(a_k + b_k\sqrt{2}) = N(u_0)^{2k} = 1$ by Problem 2 and 3. Moreover, $u_0^k \neq u_0^{k'}$ whenever $k \neq k'$ since $u_0 \neq 0$ and $|u_0| \neq 1$.

$n = x^2 - 2y^2 = (x + \sqrt{2}y)(x - \sqrt{2}y)$. Then $(x + \sqrt{2}y)(a_k - b_k\sqrt{2}) = (a_k x - 2b_k y) + (b_k x - a_k y)\sqrt{2}$, and $(x - \sqrt{2}y)(a_k + b_k\sqrt{2}) = (a_k x - 2b_k y) - (b_k x - a_k y)\sqrt{2}$.

$$\begin{aligned}
(a_k x - 2b_k y)^2 - 2(xb_k - a_k y)^2 &= N((a_k x - 2b_k y) + (xb_k - a_k y)\sqrt{2}) \\
&= N(x + \sqrt{2}y)N(a_k - b_k\sqrt{2}) \\
&= N(x + \sqrt{2}y)(a_k - b_k\sqrt{2})\gamma(a_k + b_k\sqrt{2}) \\
&= N(x + \sqrt{2}y)(a_k + b_k\sqrt{2})\gamma(a_k - b_k\sqrt{2}) \\
&= N(x + \sqrt{2}y)N(a_k + b_k\sqrt{2}) \\
&= N(x + \sqrt{2}y) \cdot 1 \\
&= N(x + \sqrt{2}y) \\
&= x^2 - 2y^2 = n.
\end{aligned}$$

If $k \neq k'$, then $a_k - b_k\sqrt{2} \neq a_{k'} - b_{k'}\sqrt{2}$. Thus $(x+\sqrt{2}y)(a_k - b_k\sqrt{2}) \neq (x+\sqrt{2}y)(a_k - b_k\sqrt{2})$, so $(a_k x - 2b_k y, xb_k - a_k y) \neq (a_{k'} x - 2b_{k'} y, xb_{k'} - a_{k'} y)$. Thus we get different solutions for different values of k.

Sketch: (Prove each step!)

- $N(u_0^k) = 1$ if and only if it is even.
- Let x, y be a solution.
- Claim: $(x + \sqrt{2}y)u_0^{2k}$ for $k \in \mathbb{Z}$ are all the solutions.
- If there's a solution, there exists α such that $\alpha^2 \equiv 2 \pmod{p}$.
- Since $x^2 - 2y^2 = p$, $x \equiv \pm\alpha y$.
- Guess: If (x, y) is a solution, then $(x + \sqrt{2}y)/(3 + \sqrt{2})$ gives another solution with the sign of x flipped.
- Without loss of generality, $x \equiv \alpha y$.
- Let (a, b) be another solution. Assume $a = -\alpha b$.
- Then $N(x + \sqrt{2}y), N(a + b\sqrt{2}y)$ are p or $-p$.
- Claim: $f = (x + \sqrt{2}y)/(a + \sqrt{2}b) \in \mathbb{Z}[\sqrt{2}]$.
- This is possible because $ax + 2by \equiv 0 \pmod{p}$.
- Since $N(x + \sqrt{2}y) = N(f)N(a + \sqrt{2}b)$, $N(f) = 1$.
- Thus $f = u_0^{2k}$ for some k.

□

Exercise. (Problem 24) For which $\overline{n} \in \mathbb{Z}/(8)$ does $\overline{x}^2 - \overline{2}\overline{y}^2 = \overline{n}$ have solutions?

Proof.

- $0^2 - 2 \cdot 0^2 = 0$
- $1^2 - 2 \cdot 0^2 = 1$
- $2^2 - 2 \cdot 1^2 = 2$
- $2^2 - 2 \cdot 0^2 = 4$
- $0^2 - 2 \cdot 1^2 = 6$
- $1^2 - 2 \cdot 1^2 = 7$

By Problem 25 below, there exist no solutions to $\overline{x}^2 - \overline{2}\overline{y}^2 = \overline{n}$ when $\overline{n} = 3, 5$.

□

Exercise. (Problem 25) Show that if $n \equiv \pm 3 \pmod 8$, then $x^2 - 2y^2 = n$ has no solutions.

Proof. We consider $x \mapsto x^2 \pmod 8$ for each x. $0 \mapsto 0, 1 \mapsto 1, 2 \mapsto 4, 3 \mapsto 1, 4 \mapsto 0, 5 \mapsto 1, 6 \mapsto 4, 7 \mapsto 1$. It suffices to check $x = 0, \cdots, 7$ because every integer is equivalent to one of these 8 numbers $\pmod 8$. Thus $x^2 - 2y^2 \equiv a - 2b \pmod 8$ where $a, b \in \{0, 1, 4\}$ for any $x, y \in \mathbb{Z}$. By checking those $3 \times 3 = 9$ possibilities, we can conclude that there exists no x, y such that $x^2 - 2y^2 \equiv \pm 3 \pmod 8$.

- $0 - 2 \cdot 0 \equiv 0$
- $0 - 2 \cdot 1 \equiv 6$
- $0 - 2 \cdot 4 \equiv 0$
- $1 - 2 \cdot 0 \equiv 1$
- $1 - 2 \cdot 1 \equiv 7$
- $1 - 2 \cdot 4 \equiv 1$
- $4 - 2 \cdot 0 \equiv 4$
- $4 - 2 \cdot 1 \equiv 2$
- $4 - 2 \cdot 4 \equiv 4$

□

Exercise. (Problem 26) Let $p \in \mathbb{Z}$ be an odd prime. Quadratic reciprocity says that 2 is a square mod p if and only if $p \equiv \pm 1 \pmod 8$. Conclude that $x^2 - 2y^2 = p$ has a solution if and only if $p \equiv \pm 1 \pmod 8$.

Proof. We are given that that $p \equiv \pm 1 \pmod 8$ if and only if 2 is a square mod p. By Problem 21, 2 is a square in $\mathbb{Z}/(p)$ if and only if $\mathbb{Z}[\sqrt{2}]/(p)$ is not an integral domain. $\mathbb{Z}[\sqrt{2}]/(p)$ is not an integral domain if and only if (p) is not a prime ideal. (Proposition 13, P.255)

By Problem 14, $\mathbb{Z}[\sqrt{2}]$ is a principal ideal domain. By Proposition 11 on P.284, (p) is not a prime ideal if and only if p is not irreducible. By Problem 19, p is not irreducible in $\mathbb{Z}[\sqrt{2}]$ if and only if $x^2 - 2y^2 = p$ has a solution.

Thus $x^2 - 2y^2 = p$ has a solution if and only if $p \equiv \pm 1 \pmod 8$. □

3. Jordan Canonical Form

Let k be a field, V a finite dimensional k-vector space, and $T \in \mathrm{End}_k(V)$ a linear transformation.

Exercise. (Problem 1) Show that the set $\{p(x) \in k[x] \mid p(T) = 0 \in \mathrm{End}_k(V)\}$ is an ideal, $I \subset k[x]$. Also, show that $I \neq 0$.

Proof.

- Claim 1: I is nonempty. Let $v_1, \cdots, v_n$ be a basis of V. Such a basis must exist since the dimension of V is finite. Let M be the $n \times n$ matrix associated to V with respect to the basis $\{v_1, \cdots, v_n\}$. In other words, for any $v \in V$, $Mv = T(v)$ where Mv is the product. Since M is an $n \times n$ matrix, the set $\{M^0, \cdots, M^{n^2}\}$ is linearly dependent. Thus there exist $a_{n^2}, \cdots, a_0 \in k$ such that
  - $a_{n^2} M^{n^2} + \cdots + a_0 M^0 = 0$.
  - $a_{n^2}, \cdots, a_0$ are not all zero.

Then for any $v \in V$,

$$\begin{aligned} 0 &= (a_{n^2} M^{n^2} + \cdots + a_0 M^0)v \\ &= a_{n^2} M^{n^2} v + \cdots + a_0 M^0 v \\ &= a_{n^2} T^{n^2}(v) + \cdots + a_0 T^0(v) \\ &= (a_{n^2} T^{n^2} + \cdots + a_0 T^0)(v). \end{aligned}$$

Therefore, $p(x) = a_{n^2} x^{n^2} + \cdots + a_0 x^0 \neq 0$ and $p(T) = 0$. Thus $p(x) \in I$, so I is nonempty.

- Claim 2: I is closed under subtraction. Let $p(x), q(x) \in I$. Then $p(x) - q(x) \in I$ because $p(T) - q(T) = 0 - 0 = 0$.
- Claim 3: I is closed under multiplication by elements in $k[x]$. Let $p(x) \in I, r(x) \in k[x]$. Then $p(T)r(T) = 0r(T) = 0$, so $r(x)p(x) \in I$.

By Claim 1 and 2, I is a subgroup of $k[x]$ under addition. Then Claim 3 implies that I is an ideal. By Claim 1, $I \neq 0$. □

Exercise. (Problem 4) Let V be a 9 dimensional k-vector space. Let $T \in \mathrm{End}_k(V)$ have minimal polynomial, $x^2(x-1)^3$. What are the possible Jordan canonical forms for T?

Proof. A Jordan canonical form for T must satisfy the following:

- The size of the largest block for the eigenvalue 0 must be 2.
  - If the size is bigger than 2, then it will not satisfy $x^2(x-1)^3$.
  - If the size of the largest block is less than or equal to 1, then it will satisfy $x(x-1)^3$. however, $x^2(x-1)^3$ is the minimal polynomial, so T cannot satisfy $x(x-1)^3$.
- Similarly, the size of the largest block for the eigenvalue 1 must be 3.
- It cannot have any other eigenvalues. If it does, it will not satisfy $x^2(x-1)^3$.

Since we know the existence of a block of size 2 with the eigenvalue 0, a block of size 3 with eigenvalue 1, it suffices to find what the rest should be. With the limitations on the size and eigenvalue, the remaining diagonal entries must be filled with blocks with size ≤ 2 with the eigenvalue 0 or blocks with the size ≤ 3 and the eigenvalue 1. Thus $[0], [0,0], [1], [1,1], [1,1,1]$ are the only 5 possibilities. (e.g., $[1,1]$ denotes a block of size 2 with the eigenvalue 1) By listing all the possibilities in lexicographical order while making sure that the sum of the sizes is 4, we obtain the following 16 possibilities.

- $[[0], [0], [0], [0]]$
- $[[0], [0], [0], [1]]$
- $[[0], [0], [0,0]]$
- $[[0], [0], [1], [1]]$
- $[[0], [0], [1,1]]$
- $[[0], [0,0], [1]]$
- $[[0], [1], [1], [1]]$
- $[[0], [1], [1,1]]$
- $[[0], [1,1,1]]$
- $[[0,0], [0,0]]$
- $[[0,0], [1], [1]]$

- $[[0,0],[1,1]]$
- $[[1],[1],[1],[1]]$
- $[[1],[1],[1,1]]$
- $[[1],[1,1,1]]$
- $[[1,1],[1,1]]$

(For instance, $[[0,0],[1],[1]]$ means a block of size 2 with the eigenvalue 0, two blocks of size 1 with the eigenvalue 1.)

Therefore, a Jordan canonical form of T consists of a block of size 2 with the eigenvalue 0, a block of size 3 with the eigenvalue 1, and one of the 16 possibilities above with some permutation. $\square$