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 $k \mapsto k + \mathrm{Im}(H)$. 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 $\mathbb{Z}/\mathbb{Z} \cong 0$.
-

□

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. Solve this!
- Abelian group = $\mathbb{Z}$ module.
- $\mathbb{Z}^2 \xrightarrow{h} \mathbb{Z}^3 \xrightarrow{q} M \xrightarrow{0} 0$
- M is an abelian group generated by a, b, c with some relations.
- $\ker(q)$ is the module of relations, and $\ker(q) = \langle 6a - 10b + 4c, 8a - 20c\rangle$.
- $h = \begin{bmatrix} 6 & 8 \\ -10 & 0 \\ 2 & -20 \end{bmatrix}$
- $q(1,0,0) = a, q(0,1,0) = b, q(0,0,1) = c$.
- $M = \langle a, b, c \mid 6a - 10b + 4c, 8a - 20c\rangle$.
- Is the answer just $\mathbb{Z}^3/\langle(6,-10,4),(8,0,-20)\rangle$? I'm certainly not familiar with that abelian group. If I mod $\mathbb{Z}^3$ by two independent vectors, does that leave $\mathbb{Z}$?

□

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 $k \in \mathbb{N}$. 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.

Prime?

□

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. By Problem 19, $x^2 - 2y^2 = p$ has a solution if and only if p is not irreducible in $\mathbb{Z}[\sqrt{2}]$. By Problem 21, 2 is not a square in $\mathbb{Z}/(p)$ if and only if $\mathbb{Z}[\sqrt{2}]/(p)$ is an integral domain. Therefore, $x^2 - 2y^2 = p$ has a solution if and only if 2 is a square in $\mathbb{Z}/(p)$. By Quadratic reciprocity, 2 is a square in $\mathbb{Z}/(p)$ if and only if $p \equiv \pm 1 \pmod 8$.
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 2) Let $p(x) \in k[x]$ be a nonzero polynomial such that $p(T) = 0 \in \mathrm{End}_k(V)$. Show that if $p(x) \in k[x]$ is a product of linear polynomials, then there is a k-basis for V with respect to which the matrix for T is in Jordan normal form.

Proof.

Since k is just a field, I can't assume that k is algebraically closed.

- $p(x) = (x - a_1)^{m_1} \cdots (x - a_n)^{m_n}$.
- Let $N = \dim(V)$.
- Let $q(\lambda) = \det(T - \lambda \,\mathrm{Id})$ be the characteristic polynomial of T.
- Let $v_1, \cdots, v_N$ be a basis of V.

For each i, $(p(T))(v_i) = 0$. In other words, there exists a j such that $(T - a_j \,\mathrm{Id})(v) = 0$ for some nonzero v. This can be found by applying each linear factor to v_i and figure out the point where it turns into 0. In other words, $\det(T - a_j \,\mathrm{Id}) = 0$. This implies that a_j is a root of the characteristic polynomial $q(\lambda)$ of T. Thus $\lambda - a_j$ divides $q(\lambda)$.
But I'm not sure what to do next. We want to find the largest number r_j such that $(\lambda - a_j)^{r_j}$ divides $q(\lambda)$. What happens next?

□

Exercise. (Problem 3) Suppose that the field k contains m distinct m-th roots of 1. Suppose that $T^m = \mathrm{Id}_V \in \mathrm{End}_k(V)$. Show that there is a basis of V with respect to which, the matrix for T is diagonal. What can you say about the diagonal entries?

Proof.

- Let $r_i, \cdots, r_m$ denote the m distinct mth roots of 1.
- Then each $x - r_i$ divides $x^m - 1$. Thus $x^m - 1 = (x - r_1) \cdots (x - r_m)$. This means that $p(x) = x^m - 1$ is a polynomial such that $p(T) = 0$ and it is a product of linear polynomials. Then I think that we can use an approach similar to the previous problem.
- Let M denote the diagonal matrix for T. Then M^m must be the identity matrix. Moreover, the ith diagonal entry of M^m is simply the m-th power of the ith diagonal entry of M. Thus each of the diagonal entries in M must be an m-th root of 1. On the other hand, any diagonal matrix where each entry is an m-th root of 1 becomes the identity when raised to the mth power.

□

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.

For any $a, b \in \{0,1\}$,

$$\begin{bmatrix} 1 & 0 & \cdots & & & \\ a & 1 & 0 & \cdots & & \\ 0 & b & 1 & 0 & \cdots & \\ 0 & 0 & 0 & 0 & 0 & \cdots \\ \vdots & \vdots & & & & \ddots \end{bmatrix}$$

satisfies $x^2(x-1)^3$.

$\square$