Algorithms HW

1

■

2. Express each of the following as a direct sum of cyclic modules.

- The quotient of $\mathbb{Z}^2$ by the $\mathbb{Z}$-submodule spanned by the vector $\begin{pmatrix} 18 \\ 30 \end{pmatrix}$.
- The quotient of $\mathbb{Z}[i]^3$ by the $\mathbb{Z}[i]$-submodule spanned by the vectors $\begin{pmatrix} 2+2i \\ 8+6i \\ 6 \end{pmatrix}$ and $\begin{pmatrix} 1+i \\ 7+3i \\ 3-3i \end{pmatrix}$.
- The quotient of $\mathbb{Q}[x]^2$ by the $\mathbb{Q}[x]$-submodule spanned by the vectors $\begin{pmatrix} x^2-1 \\ x^3-x^2 \end{pmatrix}$, $\begin{pmatrix} x^3+x^2-2x \\ x^4-2x^2+x \end{pmatrix}$ and $\begin{pmatrix} x^4+x^3-x^2-1 \\ x^5-x^3 \end{pmatrix}$.

I will outline the general procedure for how we decompose M a finitely generated module over a PID R into it's direct sum of cyclic modules.

Since M is finitely generated, say by n generators, then we have a surjection from the free module R^n into M, $f : R^n \twoheadrightarrow M$. Moreover, $\ker(f)$ is also finitely generated as a submodule of a finitely generated module over a Noetherian ring (since R is a PID). Let $m := rank \ker(f)$ and then, by similar reasoning, we have another map given by the composition $g : R^m \twoheadrightarrow \ker f \hookrightarrow R^n$. Moreover, by the first isomorphism theorem of modules, we have that $M \cong R^n/\text{im }(g) = \text{coker}(g)$. And so, if we determine the $\text{coker}(g)$ we have a representation of M.

Since $g : R^m \to R^n$ we can represent it by a $m \times n$ matrix A. Then, if we put A into Smith Normal Form (SNF) (which amounts to representing the same transformation under a change of basis of R^m and R^n) then we can write $M \cong \langle e_1, \cdots, e_n \rangle / \langle d_1 e_1, \cdots, d_k e_k \rangle$ where d_i are the Smith Normal Form entries, and where $k \leq n$.

With this procedure outlined, let me now actually answer the given questions lol.

- We have $M = \mathbb{Z}^2/\langle (18, 30) \rangle$ and the surjection $f : \mathbb{Z}^2 \twoheadrightarrow M$ via the quotient map. Moreover, manifestly, we have $\ker(f) = \langle (18, 30) \rangle$ and so we have a map $g : \mathbb{Z} \to \mathbb{Z}^2$ via $g(a) = a \cdot (18, 30)$. We can represent g as the 2×1 matrix $A = [18, 30]^T$. Let us now put A into Smith Normal Form. The SNF of A is of the form $[d_1, 0]^T$ and we have that generally the first Smith factor d_1 is the greatest common divisor of all the entires of A. That is $A \sim [gcd(18, 30), 0]^T = [6, 0]^T$. And now we can write our

decomposition
$$M \cong \frac{\langle e_1, e_2 \rangle}{\langle 6e_1 \rangle} \cong \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}.$$

- Following in a similar fashion to part (a), we have a surjective map $f : \mathbb{Z}[i]^3 \hookrightarrow M$ given by the quotient map. We have $\ker f \cong \langle (2+2i, 8+6i, 6), (1+i, 7+3i, 3-3i) \rangle$ and then the matrix representing $g : \mathbb{Z}[i]^2 \to \mathbb{Z}[i]^3$ is given by
$$A = \begin{bmatrix} 2+2i & 1+i \\ 8+6i & 7+3i \\ 6 & 3-3i \end{bmatrix}.$$
Whose SNF will be of the form
$$A \sim \begin{bmatrix} d_1 & 0 \\ 0 & d_2 \\ 0 & 0 \end{bmatrix}.$$
Once, again we can compute $d_1 = gcd(1+i, 2+2i, 8+6i, 7+3i, 6, 3-3i)$. Notice that $1+i$ is a Gaussian Prime (it has norm 2, and so it is straightforward to verify by enumeration of elements with smaller norm that it has no divisors other than 1 and itself). And so, if $1+i$ divides every element in A then $d_1 = 1+i$ otherwise $d_1 = 1$.

  It turns out that $1+i$ divides every element in A. I will only outline how I attempted to divides one element by $1+i$, because I am curious if there's a better method. But I will not write out the details of every check. Consider $7+3i$, we want to know if there's some Gaussian integer a such that $a(1+i) = 7+3i$. Notice that $\|1+i\| = 2$ and $\|7+3i\| = 58$. And so any such $a = x+yi$ must satisfy $\|a\| = 29$. Enumerating all the squares up to 100 gives us that we must have $\|x\| = 4$ and $\|y\| = 25$ or vice versa. Then, checking the four possibilities for x, y gives $7+3i = (1+i)\cdot(5-2i)$. And so, $1+i$ is a divisor of $7+3i$. Using a similar method gives that $1+i$ is a divisor of every element in A and so $d_1 = 1+i$. oh, shit, what if there's a greater common divisor. nooo, since $1+i$ is a Gaussian prime, the gcd of the whole list is already "bounded above" by this number.

Now to compute d_2 we have that the 2nd invariant factor of A, given by the gcd of all the 2×2 minors of A, is equal to $d_1 d_2$. Computing all the 2×2 minors of A gives

$$d_2 = \gcd(-24i, 6 - 6i, 6 + 6i).$$

Given the computations I already did for d_1, it is easy to write down a unique (up to units) factorization of each of the elements

$$\begin{aligned} 6 + 6i &= 6(1+i) = 3(1+i)^2(1-i) \\ 6 - 6i &= 6(1-i) = 3(1-i)^2(1+i) \\ -24i &= -12(1+i)^2, \end{aligned}$$

And then we can inspect that $d_2 = 1 + i$. Quick question, I noticed that we can also write $-24i = 12(1-i)(-1+i)$, which would then imply that the gcd of these elements is $(1-i)$. Although, of course, $1 + i = i(1-i)$, and so is the gcd only unique up to units? (I suppose even in $\mathbb{Z}$ it is true that the gcd is unique only up to ± 1.)

To summarize, the SNF of A is given by

$$A \sim \begin{bmatrix} 1+i & 0 \\ 0 & 1+i \\ 0 & 0. \end{bmatrix}$$

And hence, our decomposition of M is given by

$$M \cong \frac{\langle e_1, e_2, e_3 \rangle}{\langle (1+i)e_1, (1+i)e_2 \rangle} \cong \mathbb{Z}[i]/(1+i) \oplus \mathbb{Z}[i]/(1+i) \oplus \mathbb{Z}[i].$$

Question for self, how can we tell that each of these factors is in fact cyclic? Is $\mathbb{Z}[i]/(1+i) \cong \mathbb{Z}$?

come back and do part 3 later

■

■

4. (Aluffi Exercise VI.7.3) Show that two 3×3 matrices are similar if and only if they have the same characteristic and minimal polynomials. Is this true for 4×4 matrices?

Suppose we have two matrices A, B over a field (so that $k[x]$ is a PID) have the same characteristic and minimal polynomials. To show that $A \sim B$ we can show that they have the same rational canonical forms. Recall that the rational canonical form of a matrix is of the form

$$\begin{bmatrix} C_{f_1} & & \\ & C_{f_2} & \\ & & C_{f_3} \end{bmatrix},$$

where the C_{f_i} are companion matrices to the f_i. And the f_i are the invariant factors for the cyclic decomposition of the finitely generated $k[x]$-module induced by the k-linear transformation A, say. That is, we can show that $A \sim B$ if we can show that they have the same invariant polynomials. In generality, since A and B are 3×3 matrices, let us say that their characteristic polynomials are of degree 3. Let f_1, f_2, f_3 be the invariant factors for A and let g_1, g_2, g_3 be the invariant factors for B, where $f_1|f_2|f_3$ and $g_1|g_2|g_3$.

Recall from Aluffi that the characteristic and minimal polynomials are related to the invariant factors by $P_A = f_1 f_2 f_3$ and, since the minimal polynomial is defined to be the minimal degree polynomial dividing P_A, $m_A = f_1$.

Since $m_A = m_B$ we have $f_1 = g_1 := k$. Since k is in particular an integral domain we then have $k(f_2 f_3 - g_2 g_3) = 0$, and since $k \neq 0$, $f_2 f_3 = g_2 g_3$. Now how, from here, do we show that $f_2 = g_2$ and $f_3 = g_3$? probably also need to discuss the cases of the different degrees also

The following is the if direction. On the other hand, suppose that $A \sim B$. Then $A = CBC^{-1}$ for some invertable matrix $C \in GL_3(k)$. Note that conjugation by an invertible matrix amounts to a change of basis of the original transformation. Then CBC^{-1} has the same eigenvalues as B counted with multiplicity (although, it's eigenvectors must change under this change of basis). And so, since the characteristic polynomial of a linear transformation is determined by its eigenvalues with multiplicity, $A = CBC^{-1}$ has the same characteristic polynomial as B.

Now we cliam that A and B also have the same minimal polynoimal. i think i might need to think about their jordan normal forms to understand this one

∎

4

■

4

■

7. Let p be a prime number. How many conjugacy classes are there in $\mathrm{GL}_4(\mathbb{F}_p)$?
[Hint: rational canonical form]

Recall that the conjugacy classes of $GL_4(\mathbb{F}_p)$ are those matrices which are related to each other by conjugation. That is, the classes of similar matrices over $GL_4(\mathbb{F}_p)$. Recall that every similarity class of matrices has a unique rational canonical form. And so, if we can enumerate the different possible rational canonical forms we will have found the number of conjugacy classes $GL_4(\mathbb{F}_p)$.

Recall that the rational canonical form of a matrix is of the form

$$A = \begin{bmatrix} C_{f_1} & & & \\ & C_{f_2} & & \\ & & \cdots & \\ & & & C_{f_k} \end{bmatrix},$$

where the C_{f_i} are the companion matrices of the invariant factors f_i. Recall that the invariant factors satisfy $f_1|f_2|\cdots|f_k$. And so, we have cases given by increasing integer partitions of 4, which will correspond to the possible degrees of the f_i: $1,1,1,1$, $1,1,2$, $2,2$,$1,3$, 4. This follows a degree n polynomial has an $n \times n$ companion matrix and we have A is 4×4.

1,1,1,1: Let us start with the case where we have four invariant factors, all of which are degree 1. Since each f_i is degree 1 and monic, it follows that we must in fact have $f_1 = f_2 = f_3 = f_4 =: f = x + a_0$. In this case A takes the form

$$A = \begin{bmatrix} -a_0 & & & \\ & -a_0 & & \\ & & -a_0 & \\ & & & -a_0 \end{bmatrix}.$$

In principle, we have one such distinct rational canonical form matrix for each element of $\mathbb{F}_p$. However, A should be an element of $GL_4(\mathbb{F}_p)$ we should restrict to those A which are invertible. In particular, we have $det(A) = (a_0)^4$ which is zero exactly when $a_0 = 0$ since $\mathbb{F}_p$ is in particular an integral domain. And so we have $p - 1$ such rational canonical matrices of the above form.

1,1,2: We have three invariant factors $f_1|f_2|f_3$. However, since $f_1|f_2$ and both are monic, we must have $f_1 = f_2 = x + a_0$. Moreover, since $f_2|f_3$ we have $f_3 = (x + a_0)(x + b_0) = x^2 + (a_0 + b_0) + a_0 b_0$. Then rational canonical form matrix is given by

$$A = \begin{bmatrix} -a_0 & & & \\ & -a_0 & & \\ & & 0 & -a_0 b_0 \\ & & 1 & -(a_0 + b_0) \end{bmatrix}.$$

In principle we have p choices for a_0 and p choices for b_0, but we should restrict our choices to those which give invertible A. We have $det A = (-a_0)(-a_0)(a_0 b_0) = -(a_0)^3 b_0$. And so we should exclude those choices with $a_0 = 0$ or $b_0 = 0$. This gives $(p-1)(p-1)$ rational canonical matrices of this form.

2,2: We consider two invariant factors f_1, f_2 each of degree two. Since $f_1|f_2$ and both are monic and of equal degree, we have $f_1 = f_2 := f = x^2 + a_1 x + a_0$. We then have

$$A = \begin{bmatrix} 0 & -a_0 & 0 & 0 \\ 1 & -a_1 & 0 & 0 \\ 0 & 0 & 0 & -a_0 \\ 0 & 0 & 1 & -a_1 \end{bmatrix}.$$

Now we exclude those A which are non-invertible. We have $det(A) = (a_0)^2$, and so we need to exclude the choices with $a_0 = 0$. Thus, we have $p(p-1)$ rational canonical matrices of this form.

1,3: We have two invariant factors f_1, f_3 degree 1 and degree 3 respectively and with $f_1|f_3$. If we write $f_1 = x + a_0$ then we must have $f_3 = (x + a_0)(x^2 + b_1 x + b_0) = x^3 + (b_1 + a_0)x^2 + (b_0 + b_1 a_0)x + a_0 b_0$. Then our rational canonical form in this case is given by

$$A = \begin{bmatrix} -a_0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -a_0 b_0 \\ 0 & 1 & 0 & -(b_0 + b_1 a_0) \\ 0 & 0 & 1 & -(b_1 + a_0) \end{bmatrix},$$

this matrix has determinant $det(A) = (a_0)^2 b_0$. And so, we need to restrict our choices to $a_0 \neq 0$ and $b_0 \neq 0$. This gives at most $p(p-1)^2$ possible such rational canonical forms. we should double check how much degeneracy there is in these choices.

4: Lastly, we consider a single invariant factor $f = x^4 + a_3x^3 + b_2x^2 + b_1x + b_0$ which has companion matrix

$$A = \begin{bmatrix} 0 & 0 & 0 & -a_0 \\ 1 & 0 & 0 & -a_1 \\ 0 & 1 & 0 & -a_2 \\ 0 & 0 & 1 & -a_3 \end{bmatrix}.$$

This matrix has determinant $det(A) = a_0$. And so we should restrict our choices to $a_0 \neq 0$. This leaves us with $(p-1)p^3$ different such matrices A. Each one of these choices manifestly gives different matrices, and so we get exactly $(p-1)p^3$ different rational canonical matrices of this form.

Overall, counting up all the cases gives us less than or equal to

$$p - 1 + (p-1)^2 + p(p-1) + p(p-1)^2 + (p-1)p^3$$

distinct conjugacy classes in $GL_4(\mathbb{F}_p)$.

■

4

■