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

■

3

■

4

∎

4

∎

4

■

4

∎

4

■