

# Problem Set 8

D. Zack Garza

November 18, 2019

## Contents

<b>1</b>	<b>Regular Problems</b>	<b>1</b>
1.1	Problem 1 . . . . .	1
1.1.1	Part a . . . . .	1
1.1.2	Part 2 . . . . .	2
1.1.3	Part 3 . . . . .	3
1.1.4	Part 4 . . . . .	3
1.2	Problem 2 . . . . .	5
1.3	Problem 3 . . . . .	6
1.4	Problem 4 . . . . .	6
1.5	Problem 5 . . . . .	7
1.6	Problem 6 . . . . .	8
1.6.1	Part 1 . . . . .	8
1.6.2	Part 2 . . . . .	9
1.7	Problem 7 . . . . .	11
<b>2</b>	<b>Qual Problems</b>	<b>12</b>
2.1	Problem 8 . . . . .	12
2.1.1	Part 1 . . . . .	12
2.1.2	Part 2 . . . . .	13
2.2	Problem 9 . . . . .	14
2.2.1	Part 1 . . . . .	14
2.2.2	Part 2 . . . . .	14
2.3	Problem 10 . . . . .	15
2.3.1	Part 1 . . . . .	15
2.3.2	Part 2 . . . . .	15
2.3.3	Part 3 . . . . .	15

## 1 Regular Problems

### 1.1 Problem 1

#### 1.1.1 Part a

Define a map

$$\begin{aligned}\phi_{\text{ev}} : \text{hom}_{\mathbb{Z}}(\mathbb{Z}_m, A) &\rightarrow A \\ (f : \mathbb{Z}_m \rightarrow A) &\mapsto f(1)\end{aligned}$$

Then  $\phi_{\text{ev}}$  is a  $\mathbb{Z}$ -module homomorphism, since

$$\begin{aligned}\phi_{\text{ev}}(nf + g) &= (nf + g)(1) \\ &= nf(1) + g(1) \\ &= n\phi_{\text{ev}}(f) + \phi_{\text{ev}}(g)\end{aligned}$$

But this forces  $f(\bar{0}) = 0_A$  (where  $\bar{0} : \mathbb{Z}_m \rightarrow A$  is the zero map), we have

$$0 = f(0) = f(m) = mf(1),$$

we must have  $mf(1) = 0$  in  $A$ . So

$$\text{im } \phi_{\text{ev}} = \{a \in A \mid ma = 0\} := A[m].$$

It is also the case that

$$\ker \phi_{\text{ev}} = \{f \in \text{hom}_{\mathbb{Z}}(\mathbb{Z}_m, A) \mid f(1) = 0\} = \{\bar{0}\},$$

which follows from the fact that  $\mathbb{Z}_m = \langle 1 \bmod m \rangle$  and  $A = \langle 1_A \rangle$  as  $\mathbb{Z}$ -modules, so if  $f(1 \bmod m) = 0_A$  then

$$f(n \bmod m) = nf(1 \bmod m) = 0$$

and so  $f$  is necessarily the zero map. So  $\ker \phi = \bar{0}$ .

We can then apply the first isomorphism theorem,

$$\frac{\text{hom}_{\mathbb{Z}}(\mathbb{Z}_m, A)}{\ker \phi_{\text{ev}}} \cong \text{im } \phi_{\text{ev}} \implies \text{hom}_{\mathbb{Z}}(\mathbb{Z}_m, A) \cong A[m].$$

### 1.1.2 Part 2

**Lemma:** If  $x \mid n$  and  $x \mid m$  then  $x \mid \gcd(m, n)$

*Proof:* We have  $x \mid km + \ell n$  for any integers  $k, \ell$ . So let  $d = \gcd(m, n)$ , then there exist integers  $a, b$  such that  $am + bn = d$ . But we can now just take  $k = a$  and  $\ell = b$ .  $\square$

We claim that  $\mathbb{Z}_n[m] \cong \mathbb{Z}_{(m,n)}$ , from which the result immediately follows by part 1.

Define a map

$$\begin{aligned}\phi : \mathbb{Z} &\rightarrow \mathbb{Z}_n[m] \\ 1 &\mapsto [1] \pmod{n},\end{aligned}$$

which we claim is an isomorphism.  $\phi$  is clearly surjective since  $\mathbb{Z} \rightarrow \mathbb{Z}_n$  is a quotient map and  $\mathbb{Z}_n[m]$  is a subgroup of  $\mathbb{Z}_n$ , and if we let  $d := \gcd(m, n)$ , we have

$$\begin{aligned}\ker \phi &= \{x \in \mathbb{Z}_n \mid mx = 0\} \\ &= \{x \in \mathbb{Z}_n \mid x \mid m\} \\ &= \{x \in \mathbb{Z} \mid x \mid n \text{ and } x \mid m\} \\ &= \{x \in \mathbb{Z} \mid x \mid d\} \quad \text{by the lemma} \\ &= d\mathbb{Z}.\end{aligned}$$

Then by the first isomorphism theorem, we have

$$\frac{\mathbb{Z}}{\ker \phi} \cong \text{im } \phi \implies \frac{\mathbb{Z}}{d\mathbb{Z}} \cong \mathbb{Z}_n[m].$$

### 1.1.3 Part 3

Let  $f \in \mathbb{Z}^* = \text{hom}_{\mathbb{Z}}(\mathbb{Z}_m, \mathbb{Z})$ , so  $f : \mathbb{Z}_m \rightarrow \mathbb{Z}$ . These are both  $\mathbb{Z}$ -modules generated by their identity elements, so such a map is determined by where it send  $[1] \pmod{m}$ .

So let  $f([1] \pmod{m}) = n \in \mathbb{Z}$ . Since  $f$  is a module homomorphism, we have  $f([0] \pmod{m}) = 0$ , and in particular we have

$$\begin{aligned}0 &= f([0] \pmod{m}) \\ &= f([m] \pmod{m}) \\ &= f([1m] \pmod{m}) \\ &= mf([1] \pmod{m}),\end{aligned}$$

which forces  $f([1]) \in \mathbb{Z}[m] = \{0\}$ , so  $f$  must be the zero map and  $\mathbb{Z}^* = 0$ .

Note:  $\mathbb{Z}[m] = 0$  because  $\mathbb{Z}$  is an integral domain, so  $mx = 0$  forces  $m = 0$  or  $x = 0$ .

### 1.1.4 Part 4

To see that  $\mathbb{Z}_m$  is a  $\mathbb{Z}_{mk}$  module, we define an action

$$\begin{aligned}\mathbb{Z}_{mk} &\curvearrowright \mathbb{Z}_m \\ [x]_{mk} \curvearrowright [y]_m &:= [xy]_m\end{aligned}$$

**This is a well-defined action:**

If  $[x_1]_{mk} = [x_2]_{mk}$  are two representatives of the same equivalence class, then

$$[x_1]_{mk} - [x_2]_{mk} = [x_1 - x_2]_{mk} = [0]_{mk} \implies m \mid x_1 - x_2.$$

But then

$$\begin{aligned} ([x_1]_{mk} \curvearrowright [y]_m) - ([x_2]_{mk} \curvearrowright [y]_m) &= [x_1 y]_m - [x_2 y]_m \\ &= [(x_1 - x_2)y]_m \\ &= [0]_m, \end{aligned}$$

which shows that their resulting actions on  $\mathbb{Z}_m$  are equal.

**This action yields a module structure:**

- $r.(x + y) = r.x + r.y$ :

$$[r]_{mk} \curvearrowright ([x]_m + [y]_m) = [r]_{mk} \curvearrowright [x + y]_m = [r(x + y)]_m = [rx]_m + [ry]_m.$$

- $(r + s).x = r.x + s.x$ :

$$[r]_{mk} + [s]_{mk} \curvearrowright [x]_m = [r + s]_{mk} \curvearrowright [x]_m = [(r + s)x]_m = [rx]_m + [sx]_m.$$

- $(rs).x = r.s.x$ :

$$\begin{aligned} [r]_{mk} \cdot [s]_{mk} \curvearrowright [x]_m &= [rs]_{mk} \curvearrowright [x]_m \\ &= [(rs)x]_m \\ &= [r]_{mk} \curvearrowright [sx]_m \\ &= [r]_{mk} \curvearrowright ([s]_{mk} \curvearrowright [x]_m). \end{aligned}$$

- $1.x = x$ :

$$[1]_{mk} \curvearrowright [x]_m = [1x]_m = [x]_m.$$

$$\mathbb{Z}_m^* := \text{hom}_{\mathbb{Z}_{mk}}(\mathbb{Z}_m, \mathbb{Z}_{mk}) \cong \mathbb{Z}_m:$$

Define a map

$$\begin{aligned} \phi : \text{hom}_{\mathbb{Z}_{mk}}(\mathbb{Z}_m, \mathbb{Z}_{mk}) &\rightarrow \mathbb{Z}_m \\ f &\mapsto [f([1]_m)]_m \end{aligned}$$

$\phi$  is a homomorphism, as

$$\begin{aligned}\phi(f + g) &= [(f + g)([1]_m)]_m = [f([1]_m) + g([1]_m)]_m = [f([1]_m)]_m + [g([1]_m)]_m, \\ \phi([r]_{mk} \curvearrowright f) &= [[r]_{mk}f([1]_m)]_m = [r]_m \cdot [f([1]_m)]_m = [r]_{mk} \curvearrowright \phi(f).\end{aligned}$$

$\phi$  is **injective**, as  $[f([1]_m)]_m = [0]_m$ , then for any  $1 \leq \ell \leq m$ , we have

$$[f([\ell]_m)]_m = [\ell f([1]_m)]_m = \ell [f([1]_m)]_m = \ell [0]_m = [0]_m,$$

so  $f$  must be the zero map.

$\phi$  is **surjective**, since if  $[\ell]_m \in \mathbb{Z}_m$ , we can define

$$\begin{aligned}f_\ell : \mathbb{Z}_m &\rightarrow \mathbb{Z}_{mk} \\ [1]_m &\mapsto [\ell]_{mk}\end{aligned}$$

which makes sense and is well-defined because  $\mathbb{Z}_m \hookrightarrow \mathbb{Z}_{mk}$ , and the map is defined on the generator.

So we have the desired bijection.  $\square$

## 1.2 Problem 2

We have the map

$$\begin{aligned}\pi : \mathbb{Z} &\rightarrow \mathbb{Z}_2 \\ x &\mapsto [x]_2\end{aligned}$$

which is a surjection and thus an epimorphism in the category  $\mathbb{Z}\text{-Mod}$ , and if we apply the functor  $\text{hom}_{\mathbb{Z}}(\mathbb{Z}_2, \cdot)$  to  $\pi$  we obtain an induced map

$$\begin{aligned}\bar{\pi} : \text{hom}_{\mathbb{Z}}(\mathbb{Z}_2, \mathbb{Z}) &\rightarrow \text{hom}_{\mathbb{Z}}(\mathbb{Z}_2, \mathbb{Z}_2) \\ f &\mapsto \pi \circ f.\end{aligned}$$

The claim is that  $\bar{\pi}$  is *not* a surjection, and thus not an epimorphism (in the same category).

To see that this is the case, we can simply note that  $\text{hom}_{\mathbb{Z}}(\mathbb{Z}_2, \mathbb{Z}) = 0$  by part 3 of Problem 1, whereas  $\text{hom}_{\mathbb{Z}}(\mathbb{Z}_2, \mathbb{Z}_2) \neq 0$ .

For example, one can define  $\text{id}_{\mathbb{Z}_2} : \mathbb{Z}_2 \rightarrow \mathbb{Z}_2$ ,  $[x]_2 \mapsto [x]_2$ , which is a nontrivial module homomorphism.

So any such  $f$  appearing must be the zero map, and thus  $\bar{\pi}$  is also the zero map.  $\square$

### 1.3 Problem 3

Let  $f : R \rightarrow R$  be an endomorphism of  $R$  in the category of rings. We can then check that for any  $r \in R$ , we have  $f(r) = f(r1_R) = rf(1_R)$ , which says that  $f$  is given by right-multiplication by some fixed element  $x_f := f(1_R)$ , i.e.

$$\begin{aligned} f : R &\rightarrow R \\ r &\mapsto r \cdot x_f \end{aligned}$$

and so we can attempt to define

$$\begin{aligned} \phi_1 : \text{hom}_R(R, R) &\rightarrow R \\ f &\mapsto x_f := f(1_R) \end{aligned}$$

We can check that

$$(g \circ f)(r) = g(f(r)) = g(r \cdot x_f) = r \cdot x_f \cdot x_g,$$

which shows that in fact

$$\phi(g \circ f) = x_f \cdot x_g,$$

which reverses the multiplication. So the correct codomain is  $R^{op}$ , and we amend the definition:

$$\begin{aligned} \phi_2 : \text{hom}_R(R, R) &\rightarrow R^{op} \\ f &\mapsto x_f := f(1_R) \end{aligned}$$

By construction,  $\phi_s$  **is a ring homomorphism**. If  $R$  is commutative, then  $x_f \cdot x_g = x_g \cdot x_f$ , which makes  $\phi_1$  a ring homomorphism as well. It remains to check that it is an isomorphism/

**$\phi_1$  is injective:** We can check that  $\ker \phi_1 = 0$  as a ring. To that end, suppose  $\phi_1(f) = x_f = 0$ . Then  $f(r) = r \cdot 0 = 0$ , so  $f$  can only be the zero map.

**$\phi_1$  is surjective:** Let  $x \in R$  be arbitrary, then we can define  $f : R \rightarrow R$  by  $f(1_R) = x$ , so  $f(r) = r \cdot x$ . This is an endomorphism of  $R$ , and thus an element of  $\text{hom}_R(R, R)$ .

By the first isomorphism theorem for rings, we thus have  $\text{hom}_R(R, R) \cong R$ .  $\square$

### 1.4 Problem 4

We have maps

$$\begin{aligned} \theta_A : A &\rightarrow (A^\vee)^\vee \\ a &\mapsto (\text{ev}_a : f \mapsto f(a)) \end{aligned}$$

$$\begin{aligned}\theta_B : B &\rightarrow (B^\vee)^\vee \\ b &\mapsto (\text{ev}_b : g \mapsto g(b))\end{aligned}$$

$$\begin{aligned}f : A &\rightarrow B \\ a &\mapsto f(a)\end{aligned}$$

$$\begin{aligned}f^\vee : B^\vee &\rightarrow A^\vee \\ g &\mapsto g \circ f\end{aligned}$$

$$\begin{aligned}f^{\vee\vee} : A^{\vee\vee} &\rightarrow B^{\vee\vee} \\ h &\mapsto h \circ f^\vee\end{aligned}$$

We can now check that  $f^{\vee\vee} \circ \theta_A = \theta_B \circ f$  as maps from  $A$  to  $B^{\vee\vee}$ . Letting  $a \in A$ , and  $h \in B^{\vee\vee}$  (so  $h : B^\vee \rightarrow R$ ), we will show that both maps act on  $h$  in the same way.

For notational convenience, write  $\phi \curvearrowright h := h \circ \phi$ . We then have

$$\begin{aligned}(f^{\vee\vee} \circ \theta_A)(a) \curvearrowright h &:= f^{\vee\vee}(\theta_A(a)) \curvearrowright h \\ &:= f^{\vee\vee}(\text{ev}_a) \curvearrowright h \\ &= (\text{ev}_a \circ f^\vee) \curvearrowright h \\ &:= h \circ (\text{ev}_a \circ f) \\ &:= h(f(a)) \\ &= \text{ev}_{f(a)} \curvearrowright h \\ &:= \theta_B(f(a)) \curvearrowright h \\ &:= (\theta_B \circ f)(a) \curvearrowright h,\end{aligned}$$

which shows that these actions agree, and thus the diagram commutes.

## 1.5 Problem 5

Let  $E$  be a free module over  $R$  an integral domain. Then  $E$  has a basis  $\{\mathbf{e}_i\} \subseteq E$ , so if  $x \neq 0 \in E$ , we have

$$x = \sum_i r_i \mathbf{e}_i$$

where each  $r_i \in R$ . Moreover, since  $x \neq 0$ , at least one  $r_i \neq 0$ , so let  $r_j$  denote one of the nonzero coefficients.

Now suppose  $x$  is a torsion element, so  $mx = 0$  for some  $m \neq 0 \in E$ . We can then write

$$mx = m \sum_i r_i \mathbf{e}_i = \sum_i mr_i \mathbf{e}_i = 0$$

But by linear independence, this forces  $mr_i = 0$  for all  $i$ . In particular,  $mr_j = 0$  where  $r_j \neq 0$ . But this exhibits either  $m$  or  $r_j$  as a zero divisor, and since the only zero divisor in an integral domain is zero, we must have  $m = 0$  or  $r_j = 0$ , a contradiction.

So  $x$  can not be a torsion element. But since  $x \in E$  was arbitrary,  $E$  must be torsion-free.

For an example of a torsion-free module over an integral domain that is *not* free, consider  $\mathbb{Q}$  as a  $\mathbb{Z}$ -module. Then  $\mathbb{Q}$  is clearly torsion-free, since it is an integral domain and the same argument as above applies.

But  $\mathbb{Q}$  is not free as  $\mathbb{Z}$ -module. Supposing that  $\mathcal{B} = \{\mathbf{b}_1, \mathbf{b}_2, \dots\} \subset \mathbb{Q}$  was a  $\mathbb{Z}$ -basis, consider  $\mathbf{b}_1 = \frac{p_1}{q_1}$  and  $\mathbf{b}_2 = \frac{p_2}{q_2}$ . Then  $\mathbf{b}_1, \mathbf{b}_2$  can not be linearly independent over  $\mathbb{Z}$ , which follows from the fact that

$$q_1 p_2 \mathbf{b}_1 + q_2 p_1 \mathbf{b}_2 = p_2 p_1 - p_1 p_2 = 0,$$

while  $q_1 p_2, q_2 p_1 \neq 0 \in \mathbb{Z}$ .  $\square$

## 1.6 Problem 6

If  $A$  is a cyclic module over a commutative ring  $R$ , so we have  $A = Ra$  for some  $a \in A$ . By Hungerford's definition, the submodule  $A$  has order  $r \iff$  the element  $a$  has order  $r \iff$  the order ideal  $\mathcal{O}_a := \{x \in R \mid xa = 0\} = (r)$ .

In particular,  $ra = 0$ .

### 1.6.1 Part 1

Since  $(r, s) = (1)$ , we can find  $t_1, t_2 \in R$  such that

$$\begin{aligned} t_1 r + t_2 s = 1 &\implies t_1 ra + t_2 sa = 1a \\ &\implies t_1(ra) + t_2 sa = a \\ &\implies t_2 sa = a && \text{since } ra = 0 \\ &\implies s(t_2 a) = a && \text{since } R \text{ is commutative,} \end{aligned}$$

which implies that  $a \in sA$  and thus  $A \subseteq sA$ . However, we always have  $sA \subseteq A$  for modules, so this shows that  $A = sA$ .

To see that  $A[s] = \{x \in A \mid sx = 0\} = 0$ , let  $x \in A[s]$ ; we will show  $x = 0$ . Since  $x \in A = Ra$ , we have  $x = r_1 a$ , and in particular

$$ra = 0 \implies rx = rr_1 a = r_1(ra) = 0.$$



So we now have  $rx = 0$  and  $sx = 0$ , and we can write

$$\begin{aligned} x &= (t_1r + t_2s)x \\ &= t_1(rx) + t_2(sx) \\ &= t_10 + t_20 \\ &= 0. \end{aligned}$$

So  $x = 0$  and thus  $A[s] = 0$ .  $\square$

### 1.6.2 Part 2

Suppose  $r = sk$ . Toward an application of the first isomorphism theorem, define a map

$$\begin{aligned} \phi : R &\rightarrow sA = sRa \\ x &\mapsto sxa. \end{aligned}$$

**$\phi$  is well-defined:**

This follows from that fact that  $a \in A \implies xA \in A$  for any  $x \in R$ , so the codomain is in fact  $sA$ .

**$\phi$  is an  $R$ -module homomorphism:**

We have

$$\begin{aligned} t \in R &\implies \phi(tx) = s(tx)a = t(sxa) = t\phi(x) \\ x, y \in R &\implies \phi(x + y) = s(x + y)a = sxa + sya = \phi(x) + \phi(y) \end{aligned}$$

$\ker \phi = (k)$ :

Suppose  $x \in \ker \phi$  so  $sxa = 0_A$ ; we'd like to show  $x \in (k)$ .

By definition  $sx \in \mathcal{O}_a$ , and by assumption  $\mathcal{O}_a = (r)$ , so  $sx = t_1r$  for some  $t_1 \in R$ .

$$\begin{aligned} sxa &= 0_A \\ \implies sx &= t_1r && \text{since } sx \in \mathcal{O}_a \\ \implies sx &= t_1(sk) && \text{since } r = sk \text{ by assumption} \\ \implies sx &= s(t_1k) && \text{since elements in } R \text{ and } A \text{ commute} \\ \implies x &= t_1k && \text{since } R \text{ is a domain, so } sm = sn, s \neq 0 \implies m = n, \end{aligned}$$

which exhibits  $x = t_1k \implies x \in (k)$  as desired.

**$\phi$  is surjective:**

Since  $A = Ra$ , we have  $sA = sRA$  and thus  $x \in sA \implies x = sra$  for some  $r \in R$ ; but then  $\phi(r) = sra = x$ .

We thus have

$$R/\ker \phi \cong \text{im } \phi \implies R/(k) \cong sA.$$

Similarly, define a map

$$\begin{aligned} \psi : R &\rightarrow A[s] \\ x &\mapsto kxa \end{aligned}$$

**$\psi$  is well-defined:**

It suffices to check that  $\text{im } \psi \subseteq A[s]$  (since we will show surjectivity shortly), i.e. that  $s$  annihilates anything in the image. This follows from

$$s(kxa) = (sk)xa = rxa = x(ra) = 0,$$

since  $ra = 0$  by assumption.

**$\psi$  is an  $R$ -module homomorphism:**

We can check

$$\psi(tr_1 + r_2) = k(tr_1 + r_2)s = tkr_1s + kr_2s = t\psi(r_1) + \psi(r_2)$$

which follows because elements of  $R$  commute with those from  $A$  under multiplication.

$\ker \psi = (s)$ :

Suppose  $x \in \ker \psi$ , so  $kxa = 0$ . Then  $kx \in \mathcal{O}_a = (r)$ , so  $kx = rt_1$ . Then

$$\begin{aligned} kxa &= 0_A \\ \implies kx &= rt_1 && \text{since } kx \in \mathcal{O}_a \\ \implies kx &= (sk)t_1 && \text{since } r = sk \\ \implies kx &= k(st_1) && \text{since } R \text{ is commutative} \\ \implies x &= st_1 && \text{since } R \text{ is a domain,} \end{aligned}$$

and so  $x \in (s)$  as desired.

**$\psi$  is surjective:**

Letting  $y \in A[s]$  be arbitrary. We have

$$\begin{aligned}
y \in A[s] &\implies x = t_1 a, \quad sx = 0 \\
&\implies s(t_1 a) = 0 \\
&\implies st_1 \in \mathcal{O}_a \implies \exists x \in R \ni st_1 = xr = x(sk) \\
&\implies st_1 = sxk \\
&\implies t_1 = xk \quad \text{since } R \text{ is a domain} \\
&\implies y = t_1 a = (xk)a = kxa,
\end{aligned}$$

so  $\psi(x) = y$ .

We can then apply the first isomorphism theorem

$$R/\ker \psi \cong \text{im } \psi \implies R/(s) \cong A[s].$$

□

## 1.7 Problem 7

**Lemma:** If  $M$  is a cyclic module over a PID, then  $M$  has exactly 1 invariant factor.

**Lemma:** Let  $A$  be a cyclic module, so  $A = Ra$ . If the order of  $A$  is  $r$ , so  $\mathcal{O}_a = (r)$ , then  $A \cong R/(r)$ .

This means that we can write  $A = R/(a)$  and  $B = R/(b)$ , and  $a, b$  are the invariant factors of  $A, B$  respectively, and  $M := A \oplus B \cong R/(ab)$ .

Since  $R$  is a PID, there is unique factorization, so we can write

$$\begin{aligned}
r &= \prod_{i=1}^n p_i^{k_i} \\
s &= \prod_{i=1}^n p_i^{\ell_i} \\
\implies rs &= \prod_{i=1}^n p_i^{k_i + \ell_i},
\end{aligned}$$

where we allow some  $k_i, \ell_i = 0$  so that we can take the product over the same set of primes.

However, means that the elementary divisors of  $M$  are given by the multiset  $L := \{p_i^{k_i}\} \cup \{p_i^{\ell_i}\}$ .

The largest invariant factor  $d_1$  of  $M$  is obtained from the elementary divisors by

- Forming the multiset  $L$  of elementary divisors,
- Selecting the highest power of each prime occurring, say  $s_i := p_i^{\max(k_i, \ell_i)}$ ,
- Removing  $s_i$  from  $L$ ,
- Then letting  $d_1 = \prod s_i$ .

However, this process yields  $d_1 = \text{lcm}(r, s)$  by construction, since

$$d_1 = \prod_{i=1}^n s_i = \prod_{i=1}^n p_i^{\max(k_i, \ell_i)} := \text{lcm}(r, s).$$

The next largest invariant factor is obtained by performing the same process on the remaining prime powers in  $L$ . However, we can note that after obtaining  $d_1$ , we have  $L = \{p_i^{\min(k_i, \ell_i)}\}$ , since **there were only two choices** for each  $p_i$  occurring and we chose the copy with the maximal exponent.

But this means when we perform step (b) to obtain  $d_2$ , **there is now only one choice**, and thus each  $s_i = p_i^{\min(k_i, \ell_i)}$  and we have

$$d_2 = \prod_{i=1}^n s_i = \prod_i p_i^{\min(k_i, \ell_i)} := \text{gcd}(r, s).$$

Note: by construction,  $d_2 \mid d_1$ , since we are choosing from the same prime powers but with smaller exponents.

Since there were only at most two copies of each prime occurring in  $L$ , where one of them was chosen for  $d_1$  and the other was chosen for  $d_2$ , this exhausts all of the elements in  $L$ . But this means  $M$  has only two invariant divisors,

$$\begin{aligned} d_1 &= \text{lcm}(r, s) \\ d_2 &= \text{gcd}(r, s), \end{aligned}$$

which is what we wanted to show.  $\square$

Note: the indexing convention for  $d_i$  is opposite the usual one here, since we are choosing the largest invariant factor first, and so we have  $d_n \mid d_{n-1} \mid \cdots \mid d_1$ .

## 2 Qual Problems

### 2.1 Problem 8

#### 2.1.1 Part 1

The claim is that every element in  $M := R^n / \text{im } A$  is torsion  $\iff$  the matrix rank of  $A$  is exactly  $n \iff$  the Smith normal form of  $A$  has exactly  $n$  nonzero invariant factors.

To see that this is the case, we can apply the structure theorem for finitely-generated modules over a PID. This gives us

$$M \cong F \oplus \bigoplus R/(r_i)$$

where  $F$  is free of finite rank,  $R/(r_i)$  is cyclic torsion, and  $r_i \mid r_{i+1} \mid \cdots$  are the invariant factors of  $M$ .

We thus have

$$M \cong R^n / \text{im } A \cong F \oplus \bigoplus R/(r_i),$$

which will be pure torsion if and only if  $F = 0$ .

But if we compute the smith normal form of  $A$ , we obtain

$$SNF(A) = \begin{bmatrix} d_1 & 0 & \cdots & 0 & \cdots & 0 \\ 0 & d_2 & & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \cdots & 0 \\ 0 & 0 & \cdots & d_n & \cdots & 0 \end{bmatrix}$$

where  $d_1 \mid d_2 \mid \cdots \mid d_n$ , and thus

$$\text{im } A \cong \text{im } SNF(A) \cong d_1 R \oplus d_2 R \oplus \cdots \oplus d_n R$$

$$\implies M = R^n / \text{im } A \cong \frac{R^n}{d_1 R \oplus d_2 R \oplus \cdots \oplus d_n R}$$

$$\cong R/(d_1) \oplus R/(d_2) \cdots \oplus R/(d_n)$$

where  $R/(d_i)$  is a cyclic torsion module precisely when  $d_i \neq 0$ . If instead some  $d_i = 0$ , we then have  $R/(d_i) \cong R$ , which is a free  $R$ -module, yielding non-torsion elements in  $M$ .

But  $\det(A) = \det(SNF(A)) = \prod_{i=1}^n d_i$ , and so if  $d_i = 0$  for some  $i$  iff  $\det A = 0$  iff  $\text{rank } A < n$ .

### 2.1.2 Part 2

Identifying

$$R \times F = F[x] \oplus F \cong F[x] \oplus \frac{F[x]}{(f)}$$

where  $f$  is any degree 1 polynomial in  $F[x]$ , by the structure theorem we can pick a matrix  $A \in M_2(F[x])$  with invariant factors  $d_1 = 0, d_2 = f$ . Then by the same argument given in part 1, we would have

$$(F[x])^2 / \text{im } A \cong \frac{F[x]}{(d_1)} \oplus \frac{F[x]}{(d_2)} = F[x] \oplus \frac{F[x]}{(f)}$$

So we can choose  $n = 2$ , and say  $f(x) = x + 1$ , and then just pick a matrix that is already in Smith normal form:

$$A = \begin{bmatrix} x+1 & 0 \\ 0 & 0 \end{bmatrix}.$$

## 2.2 Problem 9

### 2.2.1 Part 1

Let  $M$  be a finitely generated module over  $R$  a PID.

Then

$$M \cong F \oplus \bigoplus_{i=1}^n R/(d_i)$$

where  $F$  is free of finite rank and  $R/(d_i)$  are cyclic torsion modules (the *invariant factors*) satisfying  $d_1 \mid d_2 \mid \cdots \mid d_n$ .

Equivalently,

$$M \cong F \oplus \bigoplus_{i=1}^n R/(p_i^{s_i})$$

where  $F$  is free of finite rank,  $p_i \in R$  are (not necessarily distinct) prime elements (the *elementary divisors*), and  $s_i \in \mathbb{Z}^{\geq 1}$ .

### 2.2.2 Part 2

Since  $\mathbb{Z}^4$  is a finitely generated module over the PID  $\mathbb{Z}$ , the structure theorem applies, and we can write  $M \cong \mathbb{Z}^k \oplus \bigoplus \mathbb{Z}/(r_i)$  for some  $k \leq 4$  and some collection  $r_i$  of invariant factors.

If we write  $M \cong \mathbb{Z}^4/N$  where  $N$  is the submodule generated by the prescribed relations, then we can construct a homomorphism of  $\mathbb{Z}$ -modules  $L : \mathbb{Z}^4 \rightarrow N$  which is given by the matrix

$$A_L = \begin{pmatrix} 3 & 12 & 3 & 6 \\ 0 & 6 & 0 & 0 \\ -3 & 6 & -3 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Then  $\text{im } A_L \cong N$ , and we can compute the Smith normal form,

$$SNF(A_L) = \begin{pmatrix} 3 & 0 & 0 & 0 \\ 0 & 6 & 0 & 0 \\ 0 & 0 & 6 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

which shows that the invariant factors are 3, 6, 6, 0. We can thus write  $\text{im } A_L \cong 3\mathbb{Z} \oplus 6\mathbb{Z} \oplus 6\mathbb{Z}$ , and so

$$M \cong \frac{\mathbb{Z}^4}{3\mathbb{Z} \oplus 6\mathbb{Z} \oplus 6\mathbb{Z}} \cong \mathbb{Z} \oplus \mathbb{Z}/(3) \oplus \mathbb{Z}/(6) \oplus \mathbb{Z}/(6).$$

## 2.3 Problem 10

### 2.3.1 Part 1

An element  $x \in M$  is *torsion* iff there exists some nonzero  $r \in R$  such that  $rx = 0$ , or equivalently  $\text{Ann}(x) \neq 0$ .

### 2.3.2 Part 2

Let  $R = \mathbb{C}[x]$ ,  $M = \mathbb{C}^2$ , and

$$A = \begin{bmatrix} 1 & 2 \\ 2 & 1 \end{bmatrix} \in M_2(\mathbb{C}).$$

Then  $\mathbb{C}^2$  is a module over  $\mathbb{C}[x]$  with action given by

$$p(x) \curvearrowright \mathbf{v} := p(A)\mathbf{v}$$

Then  $M$  is cyclic as an  $R$ -module and generated by the basis vector  $[1, 0]^T \in \mathbb{C}^2$ , since

$$\begin{aligned} & (tA + s) \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} x \\ y \end{bmatrix} \\ \implies & \begin{bmatrix} t & 2t \\ 2t & t \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} + \begin{bmatrix} s \\ 0 \end{bmatrix} = \begin{bmatrix} x \\ y \end{bmatrix} \\ & \implies \begin{bmatrix} t+s \\ 2t \end{bmatrix} = \begin{bmatrix} x \\ y \end{bmatrix} \\ \implies & \begin{bmatrix} 1 & 1 \\ 2 & 0 \end{bmatrix} \begin{bmatrix} t \\ s \end{bmatrix} = \begin{bmatrix} x \\ y \end{bmatrix} \end{aligned}$$

which is a linear system of equations represented by an invertible matrix, which always has a solution. So every  $\mathbf{v} \in \mathbb{C}^2$  is the image of some polynomial in  $A$ .

It is then easy to see that  $\mathbb{C}^2$  is torsion as a module over  $\mathbb{C}[x]$ , since by Cayley-Hamilton we have  $\text{Ann}(A) = (\text{minpoly}(A)) = (x^2 - 2x - 3)$ , and so letting  $p(x) = x^2 - 2x - 3$ , we find that

$$\forall \mathbf{v} \in \mathbb{C}^2 \quad p(A) \curvearrowright \mathbf{v} = 0 \curvearrowright \mathbf{v} = 0.$$

### 2.3.3 Part 3

Suppose  $R$  is a domain,  $M$  an  $R$ -module, and let

$$T(M) = \{m \in M \mid rm = 0 \text{ for some } r \neq 0 \in R\}.$$

Then  $T(R)$  is a submodule iff for all  $r \in R$  and all  $m, n \in T(M)$  we have  $rm + n \in T(M)$ .

So pick annihilators  $a_m, a_n \neq 0 \in R$  where  $a_m m = 0$  and  $a_n n = 0$ .

Since  $a_m \neq 0$  and  $a_n \neq 0$ , the product  $a_m a_n \neq 0$  **because  $R$  is a domain**.

Since  $0 \in T(M)$ , we can suppose  $rm + n \neq 0$  (otherwise this is in  $T(M)$  trivially). Then

$$\begin{aligned} a_m a_n (rm + n) &= a_m a_n rm + a_m a_n n \\ &= r a_n (a_m m) + a_m (a_n n) \\ &= r a_n 0 + a_m 0 \\ &= 0. \end{aligned}$$

where the commutativity of  $r, a_n, a_m$  follows from the fact that these are all elements of  $R$ , which is a domain, and in particular is commutative.  $\square$