Notes

- All rings are assumed to be commutative with 1.
- You may use your notes, but no other resources.
- Each problem is worth 25 points.

1 Let $S \subset R$ be a multiplicative subset of a ring R. Consider the set

$$A = \{\text{all ideals } I \subset R \text{ with } I \cap S = \varnothing\}.$$

Show that if I is a maximal element in A, then I is a prime ideal.

Proof. Assume—for contradiction—that $I \in A$ is maximal with respect to inclusion, but is not a prime ideal. Then there are some elements $a, b \in R \setminus I$ such that $ab \in I$. Then the ideals $I + (a)$ and $I + (b)$ strictly contain I, and therefore are not elements of A. That is, we can find elements

$$x \in (I + (a)) \cap S \quad \text{and} \quad y \in (I + (b)) \cap S.$$

With S multiplicatively closed, we know $xy \in S$. However, since $ab \in I$, we also have

$$xy \in (I + (a))(I + (b)) \subseteq I^2 + I(a) + I(b) + (ab) \subseteq I + (ab) = I.$$

This contradicts the fact that $I \in A$ requires $I \cap S = \varnothing$, hence I is indeed prime. $\square$

2 Give a justified counterexample to the following *false* statement: If R is a ring with the property that $R_\mathfrak{p}$ is an integral domain for all prime ideals $\mathfrak{p} \subset R$, then R is an integral domain.

(*Hint:* Consider e.g. $R = \mathbb{Z}/n\mathbb{Z}$ for suitable n.)

For distinct primes $p, q \in \mathbb{Z}$ take $R = \mathbb{Z}/pq\mathbb{Z}$, which has the prime ideals

$$\mathfrak{p} = p\mathbb{Z}/pq\mathbb{Z} \quad \text{and} \quad \mathfrak{q} = q\mathbb{Z}/pq\mathbb{Z}.$$

As a set, we have the localization

$$R_\mathfrak{p} = \{\tfrac{a}{b} \mid a, b \in R \text{ with } p \nmid b\},$$

where $\frac{a}{b} = 0 \in R_\mathfrak{p}$ if and only if there is some $t \in R \setminus \mathfrak{p}$ such that $ta = 0 \in R = \mathbb{Z}/pq\mathbb{Z}$. Equivalently, if we consider representatives in $\mathbb{Z}$, this means $pq \mid ta$. But since $p \nmid t$, we must have $p \mid a$. In fact this is a sufficient conditions as if $p \mid a$, then we can take $t = q$ to obtain $ta = 0 \in \mathbb{Z}/pq\mathbb{Z} = R$. In summary, $\frac{a}{b} = 0 \in R_\mathfrak{p}$ if and only if $p \mid a$, i.e., if and only if $a \in \mathfrak{p}$.

With $\mathfrak{p}$ a prime ideal of R, we conclude that $\frac{ac}{bd} = 0 \in R_\mathfrak{p}$ if and only if $ac \in \mathfrak{p}$, which requires $a \in \mathfrak{p}$ or $c \in \mathfrak{p}$. Hence, $\frac{a}{b} \cdot \frac{c}{d} = 0 \in R_\mathfrak{p}$ if and only if $\frac{a}{b} = 0$ or $\frac{c}{d} = 0$, so in fact $R_\mathfrak{p}$ is an integral domain.

By the same argument, $R_\mathfrak{q}$ is also an integral domain. However, $R = \mathbb{Z}/pq\mathbb{Z}$ is not an integral domain since $p, q \in R$ are nonzero but $pq = 0$.

3 Let

$$0 \longrightarrow A \xrightarrow{f} M \xrightarrow{g} B \longrightarrow 0$$

be an R-module exact sequence. Show that the following are equivalent:

(i) $M \cong A \oplus B$, with $f : A \to M$ the natural inclusion and $g : M \to B$ the natural projection.

(ii) There exists an R-homomorphism $p : M \to A$ such that $p \circ f = \mathrm{id}_A$.

(iii) There exists an R-homomorphism $q : B \to M$ such that $g \circ q = \mathrm{id}_B$.

Proof. Assume (i) holds, with $\varphi : M \to A \oplus B$ an R-module isomorphism such that

$$\iota_A = \varphi \circ f : A \longrightarrow A \oplus B$$

is the natural inclusion and

$$\pi_B = g \circ \varphi^{-1} : A \oplus B \longrightarrow B$$

is the natural projection. Denote the natural projection $\pi_A : A \oplus B \to A$ and inclusion $\iota_B : B \to A \oplus B$. Then define the maps $p = \pi_A \circ \varphi : M \to A$ and $q = \varphi^{-1} \circ \iota_B : B \to M$. Then by construction, we have

$$p \circ f = (\pi_A \circ \varphi) \circ f = \pi_A \circ \iota_A = \mathrm{id}_A$$

and

$$g \circ q = q \circ (\varphi^{-1} \circ \iota_B) = \pi_B \circ \iota_B = \mathrm{id}_B\,.$$

Hence, both (ii) and (iii) hold. It remains to prove that (i) holds in the case of (ii) or (iii).

Assume (ii) holds. Define the following homomorphism of R-modules:

$$\begin{aligned} \varphi = p \oplus g : M &\longrightarrow A \oplus B \\ m &\longmapsto p(m) \oplus g(m). \end{aligned}$$

We claim that φ is an isomorphism.

First, φ is surjective. For any $a \in A$ we have $f(a) \in M$ with

$$\varphi(f(a)) = p(f(a)) \oplus g(f(a)) = a \oplus 0.$$

That is, $A \oplus 0 \subseteq \operatorname{im} \varphi$. And for any $b \in B$ there is some $m \in M$ such that $g(m) = b$. Then we have an element $m - f(p(m)) \in M$ with

$$\begin{aligned} \varphi(m - f(p(m))) &= (p(m) - p(f(p(m))) \oplus (g(m) - g(f(p(m)))) \\ &= (p(m) - p(m)) \oplus (b - 0) \\ &= 0 \oplus b. \end{aligned}$$

That is $0 \oplus B \subseteq \operatorname{im} \varphi$. So for any $a \oplus b \in A \oplus B$ we can choose $m, n \in M$ such that $\varphi(m) = a \oplus 0$ and $\varphi(n) = 0 \oplus b$. Then $m + n \in M$ with

$$\varphi(m+n) = \varphi(m) + \varphi(n) = (a \oplus 0) + (0 \oplus b) = a \oplus b.$$

Hence, φ is surjective.

Next, φ is injective. If $m \in \ker \varphi$, then we must have $p(m) = 0 \in A$ and $g(m) = 0 \in B$. That is, $m \in \ker g = \operatorname{im} f$, so there is some $a \in A$ such that $f(a) = m$. Then

$$0 = p(m) = p(f(a)) = a,$$

so in fact $m = f(a) = f(0) = 0$. Hence $\ker \varphi = 0$, i.e., φ is injective.

We conclude that $\varphi : M \to A \oplus B$ is an isomorphism. Moreover, for all $a \in A$ we have

$$\varphi(f(a)) = p(f(a)) \oplus g(f(a)) = a \oplus 0,$$

which means $\varphi \circ f : A \to A \oplus B$ is the inclusion map. And given $a \oplus b \in A \oplus B$, there is a unique $m \in M$ such that $p(m) = a$ and $g(m) = b$. Then

$$g(\varphi^{-1}(a \oplus b)) = g(m) = b,$$

which means $g \circ \varphi^{-1} : A \oplus B \to B$ is the projection map. Hence, (i) holds.

Assume (iii) holds. Define the following homomorphism of R-modules:

$$\begin{aligned} \psi : A \oplus B &\longrightarrow M \\ a \oplus b &\longmapsto f(a) + q(b). \end{aligned}$$

We claim that ψ is an isomorphism.

First, ψ is surjective. Given $m \in M$, take $b = g(m) \in B$ and consider $m - q(b) \in M$. Mapping under g, we find

$$g(m - q(b)) = g(m) - g(q(b)) = b - b = 0,$$

so $m - q(b) \in \ker g = \operatorname{im} f$. Choose $a \in A$ such that $f(a) = m - q(b)$. Then $a \oplus b \in A \oplus B$ with

$$\psi(a \oplus b) = f(a) + q(b) = m - q(b) + q(b) = m,$$

hence ψ is surjective.

Next, ψ is injective. Suppose $a \oplus b \in \ker \psi$, which means

$$q(b) = -f(a) = f(-a) \in \operatorname{im} f = \ker g,$$

implying $b = g(q(b)) = 0$. It follows that $0 = \varphi(a \oplus b) = f(a)$, but f being injective tells us that $a = 0$. So in fact $a \oplus b = 0$, hence ψ is injective.

We conclude that $\psi : A \oplus B \to M$ is an isomorphism. Moreover, for all $a \oplus b \in A \oplus B$ we have

$$g(\psi(a \oplus b)) = g(f(a)) + g(q(b)) = 0 + b = b,$$

which means $g \circ \psi : A \oplus B \to B$ is the projection map. And given $a \in A$, there are unique $a' \in A$ and $b \in B$ such that $\psi(a' \oplus b) = f(a)$. But $\psi(a \oplus 0) = f(a)$, so $\psi^{-1}(f(a)) = a \oplus 0$, which means that $\psi^{-1} \circ f : A \to A \oplus B$ is the inclusion map. Hence, (i) holds. $\square$

4 Let

$$0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$$

be an R-module exact sequence. Show that if M' and M'' are finitely generated, then M is also finitely generated.

Proof. Suppose M' is generated by $x_1, \ldots, x_n \in M'$ and M'' is generated by $y_1, \ldots, y_k \in M''$. Define $z_i = f(x_i) \in M$ for $i = 1, \ldots, n$ and choose $z_{n+i} \in g^{-1}(y_i) \subseteq M$ for $i = 1, \ldots, k$. We claim that M is generated by $z_1, \ldots, z_{n+k} \in M$.

For a given $m \in M$, we have

$$g(m) = \sum_{i=1}^{k} b_i y_i,$$

for some $b_i \in R$. Define $m' = m - \sum_{i=1}^{k} b_i z_{n+i}$, then

$$g(m') = g(m) - \sum_{i=1}^{k} b_i g(z_{n+i}) = g(m) - \sum_{i=1}^{k} b_i y_i = g(m) - g(m) = 0.$$

This means $m' \in \ker g = \operatorname{im} f$, so there is some $n \in M'$ such that $f(n) = m'$. Then

$$n = \sum_{i=1}^{n} a_i x_i,$$

for some $a_i \in R$, so

$$m' = f(n) = \sum_{i=1}^{n} a_i f(x_i) = \sum_{i=1}^{n} a_i z_i.$$

We conclude that

$$m = \sum_{i=1}^{n} a_i z_i + \sum_{i=1}^{k} b_i z_{n+i}.$$

Hence, M is generated by $z_1, \ldots, z_{n+k} \in M$; in particular, M is finitely generated. $\square$