Math 110BH Homework Solutions – Winter 2017

Alexander J. Wertheim
Last Updated: March 6, 2017

Contents

1 Problem 1.1

Suppose R is a ring such that $1 = 0$. For any $r \in R$, we have

$$r \cdot 0 = r \cdot (0 + 0) = r \cdot 0 + r \cdot 0$$

which implies $r \cdot 0 = 0$ by cancellation. Hence, since $r \cdot 1 = r$ for all $r \in R$, we have $r = r \cdot 1 = r \cdot 0 = 0$ for all $r \in R$, i.e R is the zero ring.

2 Problem 1.2

Let $A = \{p/2^k \in \mathbb{Q} \mid k \in \mathbb{N}, p \in \mathbb{Z}\}$. We claim that A is a subring of $\mathbb{Q}$ which is not equal to $\mathbb{Z}$ or $\mathbb{Q}$. Indeed, for any $p/2^k, q/2^l$, we have

$$\frac{p}{2^k} + \frac{q}{2^l} = \frac{2^l p + 2^k q}{2^{k+l}} \in A$$

$$\frac{p}{2^k} \cdot \frac{q}{2^l} = \frac{pq}{2^{k+l}} \in A$$

and $1/2^0 = 1 \in A$, so A is a subring of $\mathbb{Q}$. However, $A \neq \mathbb{Z}$, since $1/2 \in A$, but $1/2 \notin \mathbb{Z}$. On the other hand, $A \neq \mathbb{Q}$, since $1/3 \in \mathbb{Q}$, but $1/3 \notin A$; indeed, if $1/3 = p/2^k$ for some $k \in \mathbb{N}, p \in \mathbb{Z}$, then $2^k = 3p$, a contradiction since 3 divides the RHS but not the LHS.

3 Problem 1.3

Suppose $[x]_m \in \mathbb{Z}/m\mathbb{Z}$ is a zero divisor, and put $\gcd(x, m) = d$ with $x = kd$ for some $k \in \mathbb{Z}$. Then there is some nonzero $[y]_m \in \mathbb{Z}/m\mathbb{Z}$ such that $[x]_m[y]_m = [xy]_m = 0$, i.e. m divides xy. Since $[x]_m$ and $[y]_m$ are nonzero, m does not divide x or y, yet divides xy, so $1 < d < m$. On the other hand, if $1 < d < m$, then $m = df$ for some $1 < f < m$, so

$$[x]_m[f]_m = [xf]_m = [kdf]_m = [k]_m[m]_m = 0$$

whence $[x]_m$ is a zero divisor, since $[x]_m$ and $[f]_m$ are both nonzero. Hence, $[x]_m$ is a zero divisor in $\mathbb{Z}/m\mathbb{Z}$ if and only if $1 < \gcd(x, m) < m$. (Of course, in this description, we are implicitly using $\gcd(x + km, m) = \gcd(x, m)$ for any $k \in \mathbb{Z}$.)

4 Problem 1.4

For any $f \in \mathrm{End}(\mathbb{Z})$, f is completely determined by $f(1)$, since $\mathbb{Z}$ is additively generated by 1 and f is a group homomorphism; one can express this property as $f(n) = nf(1)$. Hence, if $f, g \in \mathrm{End}(\mathbb{Z})$ satisfy $f(1) = g(1)$, then $f = g$. Furthermore, for any $z \in \mathbb{Z}$, there is $f \in \mathrm{End}(\mathbb{Z})$ such that $f(1) = \mathrm{End}(\mathbb{Z})$; indeed, if we let $f(q) = qz$ for any $q \in \mathbb{Z}$, then it is easy to verify that f is a group homomorphism (one can think of f as the extension of the assignment $f(1) = z$ to a well-defined group endomorphism).
Thus, define $\Phi\colon \mathrm{End}(\mathbb{Z}) \to \mathbb{Z}$ by $\Phi(f) = f(1)$. The above considerations prove that Φ

is a bijection, so it remains to show that Φ is a ring homomorphism. Indeed, for any $f, g \in \mathrm{End}(\mathbb{Z})$,

$$\Phi(f+g) = (f+g)(1) = f(1) + g(1) = \Phi(f) + \Phi(g)$$
$$\Phi(f \circ g) = (f \circ g)(1) = f(g(1)) = g(1) \cdot f(1) = \Phi(f) \cdot \Phi(g)$$
$$\Phi(\mathrm{Id}_{\mathbb{Z}}) = \mathrm{Id}_{\mathbb{Z}}(1) = 1$$

so this completes the proof.

5 Problem 1.5

Let R be an integral domain, and let $S \subset R$ be a subring. For any nonzero $x, y \in S$, the product xy is nonzero, since x, y also belong to R, which is an integral domain; hence, S is an integral domain as well. However, it is not true that if R is a field, then S is a field. Indeed, a counterexample is given by $\mathbb{Z} \subset \mathbb{Q}$.

6 Problem 1.6

This is a classical problem, which admits several classical solutions: I'll present two here.
The first, which is perhaps more common, goes like this: let R be a finite integral domain, and let $x \in R$ be a nonzero element. Consider the map $l_x \colon R \to R$ given by $l_x(r) = rx$. Since R is a domain, l_x must be injective; indeed if $l_x(r) = l_x(s)$, then $rx - sx = (r-s)x = 0$, whence $r - s = 0$ since $x \neq 0$. Since R is finite, l_x must also be surjective, whence there is some $r \in R$ such that $l_x(r) = rx = 1$, so $x \in R^{\times}$. Thus, every nonzero element of R is a unit, whence R is a field. This reasoning actually holds in more general settings: see Rings, Problem 1(a) as an example, if curious.
Alternatively, one can reason as follows. Let R be an integral domain and x be a nonzero element of R. Then consider the set

$$S = \{x, x^2, x^3, \ldots\}$$

Since R is finite, S must also be finite. Hence, it follows that $x^i = x^j$ for some $i > j$ (without loss of generality). But this means that $x^j(x^{i-j} - 1) = 0$, and since R is an integral domain, this means that $x^j = 0$ or $x^{i-j} - 1 = 0$. But $x^j \neq 0$ since $x \neq 0$, so we must have $x^{i-j} = 1$. Since $i > j, i - j \geqslant 1$, so $x(x^{i-j-1}) = 1$, i.e. $x^{-1} = x^k$ for some $k \geqslant 0$. This proof actually shows something stronger: namely, the inverse to x is some power of x!

7 Problem 1.7

(a) We claim that for any ring R, $\mathrm{Mor}_{\mathrm{Rings}}(\mathbb{Z}, R)$ contains one element, i.e. $\mathbb{Z}$ is initial in the category of rings. Note that any homomorphism $\varphi \colon \mathbb{Z} \to R$ must satisfy $\varphi(1_{\mathbb{Z}}) = 1_R$. For any $n \in \mathbb{Z}$,

$$\varphi(n) = \varphi(n(1_{\mathbb{Z}})) = n\varphi(1_{\mathbb{Z}}) = n(1_R)$$

Hence, every homomorphism $\varphi\colon \mathbb{Z} \to R$ is determined by $\varphi(1_\mathbb{Z})$, which must be 1_R, so $|\operatorname{Mor}_{\text{Rings}}(\mathbb{Z}, R)| \leqslant 1$. The formula above shows that the map $\varphi\colon \mathbb{Z} \to R$ defined by $\varphi(n) = n(1_R)$ is indeed a homomorphism, i.e. $|\operatorname{Mor}_{\text{Rings}}(\mathbb{Z}, R)| = 1$.

(b) Let T be the zero ring. We claim that for any ring R, $\operatorname{Mor}_{\text{Rings}}(R, T)$ contains one element, i.e. T is terminal in the category of rings. Since T consists of one element, any homomorphism $\varphi\colon R \to T$ must map every element of R to 0_T, so $|\operatorname{Mor}_{\text{Rings}}(R, T)| \leqslant 1$. Any such φ satisfies

$$\varphi(1_R) = 0_T = 1_T$$
$$\varphi(r_1 + r_2) = 0_T = 0_T + 0_T = \varphi(r_1) + \varphi(r_2)$$
$$\varphi(r_1 r_2) = 0_T = 0_T \cdot 0_T = \varphi(r_1) \cdot \varphi(r_2)$$

for each $r_1, r_2 \in R$, so in fact $|\operatorname{Mor}_{\text{Rings}}(R, T)| = 1$.

8 Problem 1.8

Let $f\colon R \to S$ be a ring homomorphism, I be an ideal of R, and J be an ideal of S.

(a) Note $f^{-1}(J) \supseteq f^{-1}(0) = \ker(f)$. Suppose $x, y \in f^{-1}(J)$. Then $f(x + y) = f(x) + f(y) \in J$, since $f(x) \in J$ and $f(y) \in J$ and J is an ideal. Likewise, if $r \in R$, then $f(rx) = f(r)f(x) \in J$, since $f(r) \in S, f(x) \in J$ and (again) J is an ideal. Hence, $f^{-1}(J)$ is an ideal of R containing $\ker(f)$.

(b) Suppose f is surjective. For any $x, y \in I$, $f(x) + f(y) = f(x + y) \in f(I)$, since $x + y \in I$. Further, for any $s \in S$, there is some $r \in R$ such that $f(r) = s$, so $sf(x) = f(r)f(x) = f(rx) \in f(I)$, since $rx \in I$. Thus, $f(I)$ is an ideal of S. If f is not surjective, then $f(I)$ need not be an ideal of S. Taking $R = \mathbb{Z}, S = \mathbb{Q}$, f to be the inclusion map and $I = \mathbb{Z}$, $f(I) = \mathbb{Z}$ is not an ideal of $\mathbb{Q}$, since the only ideals of $\mathbb{Q}$ are $\{0\}$ and $\mathbb{Q}$.

9 Problem 1.9

(a) Let $x \in \operatorname{Nil}(A)$ such that $x^n = 0$. Then for all $a \in A, (ax)^n = a^n x^n = 0$, so $\mathfrak{R}$ is closed under multiplication by A. There is a standard trick to show $\operatorname{Nil}(A)$ is closed under addition. Let $x, y \in \operatorname{Nil}(A)$. Then by the binomial theorem, which holds in any commutative ring,

$$(x + y)^{m+n} = \sum_{k=0}^{m+n} \binom{m+n}{k} x^k y^{m+n-k}$$

If $k < n$, then $m + n - k > m$, so $y^{m+n-k} = 0$. If $k \geq n$, then $x^k = 0$, so we see each term of the sum vanishes.
Now let $x \in A$ and suppose $\bar{x} \in A/\operatorname{Nil}(A)$ is nilpotent. Then $\bar{x}^n = 0$, i.e. $x^n \in \operatorname{Nil}(A)$ for some $n \in \mathbb{N}$. Then for some $k \in \mathbb{N}, (x^n)^k = x^{nk} = 0$, so $x \in \operatorname{Nil}(A)$ and $\bar{x} = 0$.

There is another approach here to the first part. Let $\rho_n : A \to A$ be the n^{th} power map defined by $\rho_n(x) = x^n$. Since A is commutative, ρ_n is a homomorphism and $\ker \rho_n$ is an ideal of A. It is clear that

$$\text{Nil}(A) = \bigcup_{n=1}^{\infty} \ker \rho_n$$

The proof then proceeds similarly to the proof that the union of a chain of ideals is an ideal, since $\ker \rho_{n_1}$ and $\ker \rho_{n_2}$ are both contained in $\ker \rho_{n_1 n_2}$, which is again an ideal.

(b) ($\implies$) Suppose $f(X) = a_0 + a_1 X + \cdots + a_n X^n \in R[X]$ is nilpotent. Then so is Xf, so by Problem 1.10(a), $1 + Xf$ is a unit of $R[X]$. By Problem 1.10(b), $a_0, \ldots, a_n$ must thus be nilpotent.
($\impliedby$) Suppose $a_0, a_1, \ldots, a_n$ are nilpotent, i.e. $a_i \in \text{Nil}(R)$ for each $i = 0, \ldots, n$. Then $a_i \in \text{Nil}(R[X])$ for each $i = 0, \ldots, n$. Since $\text{Nil}(R[X])$ is an ideal of $R[X]$ by 9(a), $\sum_{i=0}^{n} a_i g_i(X) \in \text{Nil}(R[X])$ for all $g_i(X) \in R[X]$. Taking $g_i(X) = X^i$ establishes $f \in \text{Nil}(R[X])$.

10 Problem 1.10

(a) Suppose $a^n = 0$ for some $n \in \mathbb{N}$. We prove by induction that for all $n \geqslant 1, x \in R$, we have:

$$(1+x)\left(\sum_{i=0}^{n}(-1)^i x^i\right) = (1+x)(1 - x + x^2 - \ldots - x^n) = 1 + (-1)^n x^{n+1}$$

It is clearly true for $n = 1$, as

$$(1+x)(1-x^1) = 1 - x + x - x^2 = 1 - x^2 = 1 + (-1)^1 x^2$$

Suppose it is true for some $n > 1$. Then

$$\begin{aligned}(1+x)\left(\sum_{i=0}^{n+1}(-1)^i x^i\right) =& (1+x)\left(\sum_{i=0}^{n}(-1)^i x^i\right) + (1+x)(-1)^{n+1}x^{n+1} \\ =& 1 + (-1)^n x^{n+1} + (-1)^{n+1}x^{n+1} + (-1)^{n+1}x^{n+2} \\ =& 1 + (-1)^{n+1}x^{n+2}\end{aligned}$$

Thus,

$$(1+a)\left(\sum_{i=0}^{n-1}(-1)^i a^i\right) = 1 + (-1)^{n-1}a^n = 1$$

So $1 + a$ is a unit. If $y \in R$ is a unit, then $y + a$ is also a unit, since $y + a = y(1 + y^{-1}a)$, and hence is a product of units ($y^{-1}a$ is also nilpotent).

(b) ($\implies$) We proceed by induction on n. The case $n = 0$ is clear. Suppose $n > 0$, and f is a unit, with inverse $g(X) = b_0 + b_1 X + \cdots + b_m X^m$. We show $a_n^{r+1} b_{m-r} = 0$ by induction on r, starting with the case $r = 0$. Since $f(X)g(X) = 1$, each coefficient of the nonzero

powers of X in the product must vanish. Hence, since $a_n b_m$ is the coefficient of the term X^{n+m}, it follows that $a_n b_m = a_n^{1+0} b_{m-0} = 0$.
Now suppose $r > 0$. The coefficient of X^{n+m-r} is given by

$$\alpha = \sum_{i=0}^{r} a_{n-i} b_{m-r+i} = a_n b_{m-r} + \sum_{i=1}^{r} a_{n-i} b_{m-r+i}$$

which must vanish as per the argument above. Then

$$a_n^r \cdot \alpha = a_n^{r+1} b_{m-r} + \sum_{i=1}^{r} a_{n-i} a_n^r b_{m-r+i} = 0$$

By the induction hypothesis, $a_n^r b_{m-r+i} = a_n^{i-1} \left(a_n^{(r-i)+1} b_{m-(r-i)} \right) = 0$, so all of the terms of

$$\sum_{i=1}^{r} a_{n-i} a_n^r b_{m-r+i}$$

vanish, whence $a_n^{r+1} b_{m-r} = 0$. Since $a_n^{r+1} b_{m-r} = 0$ for all $0 \leq r \leq m$, it follows that $a_n^{m+1} g(x) = 0$. Since $g(X)$ is a unit in $R[X]$ and thus cannot be a zero divisor, we must have $a_n^{m+1} = 0$, so a_n is nilpotent. Hence, $-a_n X^n$ is nilpotent, so $h(X) = f(X) + (-a_n X^n)$ is a unit by 10(a), and since $\deg h(X) < \deg f(X) = n$, by the induction hypothesis, a_0 is a unit and $a_1, \ldots, a_{n-1}$ are nilpotent, whence the nilpotence of a_n completes the proof.
($\Longleftarrow$) Suppose a_0 is a unit and $a_1, \ldots, a_n$ are nilpotent. Let $g(X) = a_1 X + \cdots + a_n X^n$; note that $g(X)$ is nilpotent by 9(b). Then $f(X) = a_0 + g(X)$, so f is a unit in $R[X]$ by 10(a).

11 Problem 2.1

We prove a more general fact.

Lemma 11.0.1. *Let $R = \prod_{k=1}^{n} R_k$ be a finite product of rings. Then every (left) ideal I of R is a product of (left) ideals $\prod_{k=1}^{n} I_k$ such that I_k is a (left) ideal of R_k for each $k = 1, \ldots, n$.*

Proof. Let $\{e_k\}_{k=1}^{n}$ be the "standard basis" of idempotents for R, and let $\pi_k \colon R \to R_k$ be the canonical projection homomoprhism onto the kth component for each $k = 1, 2, \ldots, n$. Let I be an ideal of R. Note that π_k is trivially a surjective ring homomorphism, and therefore $\pi_k(I) =: I_k$ is an ideal of R_k for each k by Problem 1.8(b). For any $x := (x_1, \ldots, x_n) \in I$, $\pi_j(x) = x_j \in I_j$, so $I \subseteq I_1 \times I_2 \times \cdots \times I_n$. On the other hand, $e_k I \subseteq I$ for each I, so $\sum_{k=1}^{n} e_k I \subseteq I$. But clearly $I_1 \times I_2 \times \cdots \times I_n = \sum_{k=1}^{n} e_k I$, since $e_k I = \{0\} \times \cdots \times \{0\} \times I_k \times \{0\} \times \cdots \times \{0\}$, so we have $I = I_1 \times I_2 \times \cdots \times I_n$. □

12 Problem 2.2

(a) Note that $105 = 3 \cdot 5 \cdot 7$, so $\mathbb{Z}/105\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$ by the Chinese Remainder theorem. If $(x, y, z) \in \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$ is idempotent, then $x^2 = x, y^2 = y, z^2 = z$,

i.e. x, y and z are idempotent in $\mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/5\mathbb{Z}$ and $\mathbb{Z}/7\mathbb{Z}$ respectively. By Problem 2.2(b), this implies that x, y and z must be trivial idempotents, and it is clear that $(\varepsilon_1, \varepsilon_2, \varepsilon_3) \in \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$ where $\varepsilon_i \in \{0, 1\}$ is idempotent, so these are all idempotents of $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$. Hence, there are 8 idempotents in $\mathbb{Z}/105\mathbb{Z}$ formed by gluing the various triples $(\varepsilon_1, \varepsilon_2, \varepsilon_3)$ together: we list them here.

$$[0], [1], [15], [21], [36], [70], [85], [91]$$

This calculation can be sped up by using the result of Problem 2.3(b), since e an idempotent implies $1 - e$ is also an idempotent.

(b) Suppose $[x] \in \mathbb{Z}/p^n\mathbb{Z}$ is idempotent. Then $[x]^2 - [x] = [x^2 - x] = [0]$, i.e. $x^2 - x = x(x-1)$ is divisible by p^n. But the prime factors of x and $x - 1$ are distinct, so either p^n divides x, or p^n divides $x - 1$, whence $[x] = [0]$ or $[x] = [1]$.
N.B.: this is immediate by Problem 3.4 and Problem 2.6: $\mathbb{Z}/p^n\mathbb{Z}$ is a local ring with unique maximal ideal $\langle [p] \rangle$.

13 Problem 2.3

Let R be a ring, and let e be a central idempotent of R.

(a) Equip $Re = \{re \mid r \in R\}$ with the same addition and multiplication operations of R. We claim that this gives Re the structure of a ring with identity $e = 1 \cdot e$ and additive identity $0 = 0 \cdot e$. Indeed, for any $re, se \in Re$, we have

$$re + se = (r + s)e \in Re$$
$$(re)(se) = rse^2 = (rs)e \in Re$$

and

$$0 + re = re = re + 0$$
$$e \cdot re = re \cdot e = re^2 = re$$

However, Re is not a subring of R unless $e = 1$, or $e = 0$ and R is the zero ring, since otherwise the identity elements of Re and R are not equal.

(b) Let $f = 1 - e$; then $f^2 = (1 - e)(1 - e) = 1 - 2e + e^2 = 1 - 2e + e = 1 - e$, so f is also idempotent; f is also central, since it is the sum of central elements of R. Further, note that $fe = ef = e(1 - e) = e - e^2 = 0$. Define $\Phi \colon R \to Re \times Rf$ by $\Phi(r) = (re, rf)$; we claim that Φ is a ring isomorphism. Note $\Phi(1) = (e, f)$, which by (a) is the identity element of $Re \times Rf$. Further, for any $r, s \in R$,

$$\Phi(r + s) = ((r + s)e, (r + s)f) = (re + se, rf + sf) = (re, rf) + (se, sf) = \Phi(r) + \Phi(s)$$
$$\Phi(rs) = (rse, rsf) = (rse^2, rsf^2) = (rese, rfsf) = (re, rf)(se, sf) = \Phi(r)\Phi(s)$$

Hence, Φ is a ring homomorphism. Suppose $\Phi(r) = (0, 0)$. Then $re = rf = 0$, so $0 = 0 = 0 = re + rf = r(e + f) = r \cdot 1 = r$, whence Φ is injective. Let $(re, sf) \in Re \times Rf$. Then

$$\Phi(re + sf) = ((re + sf)e, (re + sf)f = (re^2 + sfe, ref + sf^2) = (re, sf)$$

so Φ is surjective, which completes the proof.

14 Problem 2.4

Let $f\colon \mathbb{Z}\times\mathbb{Z}\to\mathbb{Z}$ be a ring homomorphism. Since $f(1,1)=1$, f must be surjective, since 1 generates $\mathbb{Z}$ additively and f is a homomorphism (more explicitly, $f(z,z)=zf(1,1)=z$ for any $z\in\mathbb{Z}$). If $f(1,0)=x, f(0,1)=y$, then

$$f(a,b)=f(a(1,0)+b(0,1))=af(1,0)+bf(0,1)=ax+by$$

where we are (inductively) using that f is a ring homomorphism. Of course, we must then have $f(1,1)=x+y=1$, and since $(1,0)(0,1)=(0,0)\in\mathbb{Z}\times\mathbb{Z}$, this enforces the condition

$$xy=f(1,0)f(0,1)=f((1,0)(0,1))=f(0,0)=0$$

so $xy=0$, meaning $x=0$ or $y=0$. Hence, we must have either $x=1,y=0$ or $x=0,y=1$. In the first case, f is the projection $\pi_1\colon\mathbb{Z}\times\mathbb{Z}\to\mathbb{Z}$ sending (a,b) to a, and in the second, f is the projection $\pi_2\colon\mathbb{Z}\times\mathbb{Z}\to\mathbb{Z}$ sending (a,b) to b. It is easy to see that π_1 and π_2 are distinct homomorphisms, and hence constitute all homomorphisms from $\mathbb{Z}\times\mathbb{Z}$ to $\mathbb{Z}$.
As noted above, both π_1 and π_2 are surjective. The kernel of π_1 is $\{0\}\times\mathbb{Z}$, and the kernel of π_2 is $\mathbb{Z}\times\{0\}$.

15 Problem 2.5

Let R be an integral domain (hence commutative) and $a,b\in R$ such that $Ra=Rb$. Then $a=rb$ for some $r\in R$, and likewise $b=sa$ for some $s\in R$, so $a=rb=rsa$. Since R is an integral domain, cancellation implies $rs=1$, i.e. $r\in R^\times$.

16 Problem 2.6

Let R be a commutative ring. Suppose $a\in R$ is invertible. Then $aR=R$, so any maximal ideal containing a must be all of R, which is absurd; hence, a does not belong to any maximal ideal of R. Conversely, suppose $a\in R$ is not invertible. Let Ω be the set of proper ideals of R containing a, ordered by inclusion; Ω is nonempty, since aR is a proper ideal of R containing a. For any chain of ideals $\{I_j\}_{j\in J}$ in Ω, $I:=\bigcup_{j\in J}I_j$ is a proper ideal of R containing a. That I contains a is obvious; I must be proper, since $I=R$ if and only if $I_j=R$ for some $j\in J$. If $x\in I$, then $x\in I_j$ for some $j\in J$, hence $rx\in I_j$ for any $r\in R$, whence $rx\in I$. Further, suppose $x\in I_j, y\in I_k$ for some $j,k\in J$. Then either $I_k\supseteq I_j$ or $I_j\supseteq I_k$, so WLOG $x,y\in I_j$ and hence $x+y\in I_j$, and therefore belongs to I. Thus, $I\in\Omega$ and is an upper bound for the chain $\{I_j\}_{j\in J}$, so by Zorn's lemma, Ω has a maximal element with respect to inclusion, whence a belongs to some maximal ideal.
Alternatively, if one already knows the usual Zorn's lemma argument for existence of maximal ideals, then one can apply this statement to R/aR; the conclusion above is then immediate.

17 Problem 2.7

Since $\mathbb{Z}$ is a principal ideal domain, every ideal of $\mathbb{Z}/n\mathbb{Z}$ is principal, generated by the class of a divisor of n. Indeed, by the correspondence theorem for ideals of a quotient ring, the

ideals of $\mathbb{Z}/n\mathbb{Z}$ are in a bijective correspondence with the ideals of $\mathbb{Z}$ containing $n\mathbb{Z}$ via the canonical projection map $\pi\colon \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$. The ideals of $\mathbb{Z}$ containing $n\mathbb{Z}$ are the ideals $d\mathbb{Z}$ for d dividing n, so the ideals of $\mathbb{Z}/n\mathbb{Z}$ are principal generated by $[d]_n$ for each divisor d of n. For each such ideal, we have an isomorphism

$$(\mathbb{Z}/n\mathbb{Z})/\langle [d]_n \rangle \cong \mathbb{Z}/\langle n, d \rangle \cong \mathbb{Z}/\gcd(n,d)\mathbb{Z} \cong \mathbb{Z}/d\mathbb{Z}$$

which is an integral domain (in fact, a field) if and only if d is prime. Hence, every prime ideal of $\mathbb{Z}/n\mathbb{Z}$ is maximal of the form $\langle [p]_n \rangle$ for some prime divisor p of n.

18 Problem 2.8

(a) Every maximal ideal of $\mathbb{Z}$ is of the form $p\mathbb{Z}$ for some prime p; hence,

$$\mathrm{Rad}(\mathbb{Z}) = \bigcap_{p \text{ prime}} p\mathbb{Z}$$

A nonzero element $z \in \mathbb{Z}$ belongs to $p\mathbb{Z}$ for every prime p if and only if z is divisible by every prime p; since no integer is divisible by every prime, $\mathrm{Rad}(\mathbb{Z}) = \{0\}$.
By Problem 2.7, the maximal ideals of $\mathbb{Z}/12\mathbb{Z}$ are $\langle [2]_{12} \rangle, \langle [3]_{12} \rangle$, whose intersection is $\langle [6]_{12} \rangle$, so $\mathrm{Rad}(\mathbb{Z}/12\mathbb{Z}) = \langle [6]_{12} \rangle = \{[0]_{12}, [6]_{12}\}$.

(b) Suppose $x \in \mathrm{Rad}(R)$, i.e. $x \in \mathfrak{m}$ for every maximal ideal $\mathfrak{m}$ of R. If there is some $y \in R$ such that $1 + xy$ is not a unit, then $1 + xy$ is contained in some maximal ideal $\mathfrak{m}$ of R. Since $x \in \mathfrak{m}$, so is xy, whence $1 \in \mathfrak{m}$, a contradiction. Hence, $1 + xy$ is a unit for each $y \in R$.
Conversely, suppose $x \in R$ such that $1 + xy$ is a unit for each $y \in R$. Suppose there is some maximal ideal $\mathfrak{m}$ which does not contain x; then together, $\mathfrak{m}$ and x generate the unit ideal, i.e. $1 = m + xy$ for some $m \in \mathfrak{m}, y \in R$. Then $1 - xy \in \mathfrak{m}$, but $1 - xy$ is a unit by hypothesis, which is absurd. Hence, x belongs to every maximal ideal of R, i.e. $x \in \mathrm{Rad}(R)$.

19 Problem 2.9

(a) Let $x \in \mathrm{Nil}(R)$. Then there exists $n \in \mathbb{N}$ such that $x^n = 0$. Since 0 belongs to every prime ideal $\mathfrak{p}$, so does x^n. Hence, $x \in \mathfrak{p}$ or $x^{n-1} \in \mathfrak{p}$ by the primality of $\mathfrak{p}$. By induction, one sees that $x \in \mathfrak{p}$, so $\mathrm{Nil}(R)$ belongs to every prime ideal of R.

(b) By Problem 2.9(a), $\mathrm{Nil}(R)$ belongs to every prime ideal of R, hence every maximal ideal of R, and so is a subset of the intersection of all maximal ideals of R, namely $\mathrm{Rad}(R)$.

20 Problem 2.10

This problem is quite tricky. Define a multiplication operation on the abelian group $R := \mathbb{Z} \oplus A$ by $(n, a) \cdot (m, b) = (nm, ma + nb)$. To check that R is a ring, we need to verify

associativity of $\cdot$ and distributivity of $\cdot$ over addition, and determine the unit element. First, note that $\cdot$ is clearly commutative. Then it is easy to check that $(1,0)$ is unit element, since

$$(1,0)\cdot(n,a) = (1\cdot n, 1\cdot a + n\cdot 0) = (n,a)$$

for any $(n,a) \in R$. Further, suppose $(n,a),(m,b),(o,c) \in R$. Then

$$\begin{aligned}((n,a)+(m,b))\cdot(o,c) =& (n+m, a+b)\cdot(o,c)\\ =&((n+m)o, (n+m)c + o(a+b))\\ =&(no+mo, (nc+oa)+(mc+ob))\\ =&(no, nc+oa)+(mo, mc+ob)\\ =&(n,a)\cdot(o,c)+(m,b)\cdot(o,c)\end{aligned}$$

and

$$\begin{aligned}((n,a)\cdot(m,b))\cdot(o,c) =& (nm, ma+nb)\cdot(o,c)\\ =&((nm)o, o(ma+nb)+(nm)c)\\ =&(n(mo), n(ob+mc)+(mo)a)\\ =&(n,a)\cdot(mo, ob+mc)\\ =&(n,a)\cdot((m,b)\cdot(o,c))\end{aligned}$$

This completes the tedious verification that R is indeed a ring. Now, the more interesting question: what are the prime/maximal ideals of R?

A clue is given in Problem 2.9(a). Consider any element $(0,a) \in \{0\}\oplus A \subset R$. Then note that $(0,a)\cdot(0,a) = (0, 0\cdot a + 0\cdot a) = (0,0)$. Hence, $(0,a) \in \mathrm{Nil}(R)$, and as proved in Problem 2.9(a), $\mathrm{Nil}(R)$ is contained in every prime ideal of R. Hence, every prime ideal of R contains $\{0\}\oplus A$. For each $n \in \mathbb{Z}$, put $I_n := n\mathbb{Z}\oplus A$. Each I_n is the kernel of the surjective ring homomorphism $\rho_n\colon R \to \mathbb{Z}/n\mathbb{Z}$ sending (x,a) to $[x]_n$. Hence, I_n is a prime ideal if and only if $n = 0$ or $n = p$ for some prime p; in the latter case, I_n is maximal. We claim that these are all prime (hence maximal) ideals of R.

Indeed, suppose $\mathfrak{p} \subset R$ is a prime ideal. As reasoned above, $I_0 \subseteq \mathfrak{p}$, so if $(n,a) \in \mathfrak{p}$, then $(n,0) \in \mathfrak{p}$ as well because $(0,a) \in \mathfrak{p}$, whence $n\mathbb{Z}\oplus A \subseteq \mathfrak{p}$. Let $S = \{n \in \mathbb{Z} \mid n\mathbb{Z}\oplus A \subseteq \mathfrak{p}\}$, and let $x\mathbb{Z}$ be the (principal) ideal of $\mathbb{Z}$ generated by S. We claim that $\mathfrak{p} = x\mathbb{Z}\oplus A$. Note that x can be expressed as a finite sum $z_1n_1 + \cdots + z_kn_k$ for elements $n_1,\ldots,n_k \in S$ and $z_1,\ldots,z_k \in \mathbb{Z}$, so

$$(x,a) = (z_1,0)(n_1,0) + \cdots + (z_k,0)(n_k,0) + (0,a)$$

Since $n_i\mathbb{Z}\oplus A \subseteq \mathfrak{p}$, the containment $x\mathbb{Z}\oplus A \subseteq \mathfrak{p}$ is clear. Suppose $(n,a) \in \mathfrak{p}$. Then as noted above, $n\mathbb{Z}\oplus A \subseteq \mathfrak{p}$, so $n \in S \subseteq x\mathbb{Z}$, i.e. $n = kx$ for some $k \in \mathbb{Z}$, so $(n,a) = (k,0)(x,0) + (0,a) \in x\mathbb{Z}\oplus A$, whence $\mathfrak{p} = x\mathbb{Z}\oplus A = I_x$. This establishes the claim.

21 Problem 3.1

Let R be the ring of continuous functions on $\mathbb{R}$, and let I be the subset of all functions in R such that $f(0) = f(1) = 0$. For any $f,g \in I$,

$$(f+g)(0) = f(0)+g(0) = 0 = f(1)+g(1) = (f+g)(1)$$

so $f + g \in I$. Further, for any $h \in R$,

$$(hf)(0) = h(0)f(0) = 0 = h(1)f(1) = (hf)(1)$$

so $hf \in I$, whence I is an ideal of R. However, note that I is not a prime ideal. Indeed, take $f(x) = x, g(x) = x - 1$. Since $f(1) = 1$ and $g(0) = -1$, neither f nor g belong to I. However, $fg = x(x - 1)$ does belong to I.

22 Problem 3.2

Let R be a commutative ring, and I and J be ideals of R, and P a prime ideal of R containing $I \cap J$. Then $IJ \subseteq I \cap J \subseteq P$. Suppose there is some $x \in I$ such that $x \notin P$. Then for every $y \in J$, $xy \in IJ \subset P$, so $x \in P$ or $y \in P$ by the primality of P, whence $y \in P$, so $J \subset P$. Otherwise, $x \in P$ for all $x \in I$, so $I \subset P$.

23 Problem 3.3

Let R be a finite commutative ring, and let $\mathfrak{p}$ be a prime ideal of R. Then $R/\mathfrak{p}$ is a finite integral domain, hence a field by Problem 1.6, so $\mathfrak{p}$ is a maximal ideal.

24 Problem 3.4

Let R be a local ring with unique maximal ideal M.

(a) This follows immediately from Problem 2.6.

(b) Suppose R has a nontrivial idempotent e. Then both e and $1 - e$ are nontrivial idempotents, which must belong to M since they are zero divisors and $R^\times = R \setminus M$ by (a). But then $e + (1 - e) = 1 \in M$, a contradiction.

(c) Let $R = \{n/m \mid n, m \in \mathbb{Z}, m \in \mathbb{Z} \setminus 2\mathbb{Z}\}$. Then R contains $1 = 1/1$, and for any $n/m, p/q \in R$,

$$\frac{n}{m} + \frac{p}{q} = \frac{nq + mp}{mq} \in R$$
$$\frac{n}{m} \cdot \frac{p}{q} = \frac{np}{mq} \in R$$

since mq is odd. Hence, R is a subring of $\mathbb{Q}$. Let $I = 2R$; we claim that I is the unique maximal ideal of R. Indeed, if $x \in R \setminus I$, then $x = n/m$ for some $n, m \in \mathbb{Z}$ both odd. Since $m/n \in R$, $x \cdot m/n = 1$, $x \in R^\times$. Hence, if J is an ideal of R such that $J \cap I$ is not contained in I, then J contains some element of $R \setminus I$, i.e. $J = R$. Hence, if $J \supseteq I$, then $J = I$ or $J = R$, whence I is maximal; and if M is a maximal ideal of R, then $M \subseteq I$ since $M \neq R$, whence $M = I$ by maximality, so I is the unique maximal ideal of R.

(d) If $\mathbb{Z}/n\mathbb{Z}$ is a local ring, then by Problem 2.7, n has exactly one prime divisor, so $n = p^k$ for some prime p and integer $k > 0$.

25 Problem 3.5

Let F be a field, and let K be the field of fractions of F. We claim that the map $\rho\colon F \to K$ defined by $\rho(x) = (x, 1)$ is a ring isomorphism. Indeed, for any $x, y \in F$, we have

$$\rho(x + y) = (x + y, 1) = (x, 1) + (y, 1) = \rho(x) + \rho(y)$$

$$\rho(xy) = (xy, 1) = (x, 1)(y, 1) = \rho(x)\rho(y)$$

$$\rho(1) = (1, 1)$$

so ρ is a ring homomorphism. Furthermore, let $(k, j) \in K$. Then $(k, j) = (kj^{-1}, 1) = \rho(kj^{-1})$, so ρ is surjective. Suppose $\rho(x) = (x, 1) = (0, 1)$. Then $x \cdot 1 = 1 \cdot 0 = 0$, so ρ has trivial kernel. Hence, ρ is an isomorphism.

26 Problem 3.6

Any subfield of $\mathbb{R}$ must contain 1, hence $\mathbb{Z}$ by additive closure, hence $\mathbb{Q}$ by multiplicative closure. The same argument shows that any field F contains the so-called "prime subfield", which is the multiplicative closure of the characteristic subring, i.e. the image of the unique ring homomorphism $\mathbb{Z} \to F$.

27 Problem 3.7

Let $R = \mathbb{Z}[i]$, $I = 2R, J = (3 + i)R$. We factor 2 and $(3 + i)$ into irreducible as follows:

$$2 = (1 - i)(1 + i)$$

$$(3 + i) = (1 - i)(1 + 2i)$$

To see that $1 - i, 1 + i, 1 + 2i$ are irreducible, note that their norms (see Problem 3.8) are prime: $N(1 - i) = N(1 + i) = 2, N(1 + 2i) = 5$, and any element of $\mathbb{Z}[i]$ with prime norm is irreducible. Indeed, let γ be an element of prime norm p; since N is multiplicative, if there were $\alpha, \beta \in R$ such that $\gamma = \alpha\beta$, then $N(\alpha)N(\beta) = N(\gamma) = p$, whence $N(\alpha)$ or $N(\beta)$ must be 1. Since the elements of norm 1 are all units in $\mathbb{Z}[i]$ (see Problem 3.8),
If $\alpha \in I \cap J$, then α is divisible by both 2 and $(3 + i)$. By unique factorization in R, it is necessary that α be divisible by each of $1 - i, 1 + i, 1 + 2i$, hence divisible by their product $2 + 4i$; thus, $I \cap J \subseteq (2 + 4i)R$. Since $2 + 4i = 2(1 + 2i) = (1 + i)(3 + i)$, $2 + 4i \in I \cap J$, whence $(2 + 4i) = I \cap J$.

28 Problem 3.8

Consider the norm $N\colon \mathbb{Z}[i] \to \mathbb{N}$ defined by $N(\alpha) = \alpha\overline{\alpha}$, where $\overline{\alpha}$ is the complex conjugate of α. Explicitly, if $\alpha = a + bi$, then $N(\alpha) = a^2 + b^2$. It is straightforward to see that N is multiplicative, i.e. $N(\alpha\beta) = N(\alpha)N(\beta)$ for any $\alpha, \beta \in \mathbb{Z}[i]$. If $\alpha \in \mathbb{Z}[i]^\times$, then there exists $\beta \in \mathbb{Z}[i]$ such that $\alpha\beta = 1$, so $1 = N(1) = N(\alpha\beta) = N(\alpha)N(\beta)$, so $N(\alpha) \in \mathbb{Z}^\times = \{-1, 1\}$.

Since $N(\alpha) \geqslant 0$, we must have $N(\alpha) = 1$, i.e. any unit of $\mathbb{Z}[i]$ must belong to the list of elements of norm 1. It is straightforward to see that any element $a + bi \in \mathbb{Z}[i]$ with norm 1 must have $a = \pm 1, b = 0$ or $a = 0, b = \pm 1$, so the units of $\mathbb{Z}[i]$ are a subset of $\{1, -1, i, -i\}$. However, it is clear that each of these elements are units (i has inverse $-i$), so $\mathbb{Z}[i]^\times = \{1, -1, i, -i\}$.

29 Problem 3.9

We prove a more general fact: namely, if R is an integral domain such that $R[X]$ is a PID, then R is a field. We give two proofs.

Let R be an integral domain, and suppose $R[X]$ is a principal ideal domain. Let $r \neq 0 \in R$, and consider the ideal $\langle r, X\rangle$. Since $R[X]$ is a PID, $\langle r, X\rangle = \langle \alpha(X)\rangle$ for some $\alpha(X) \in R$. In particular, we have $\alpha(X)f(X) = r$ for some $f(X) \in R[X]$. Since R is an integral domain, so is $R[X]$, so a simple degree argument shows that $\deg(\alpha(X)) = 0$, i.e. $\alpha(X) = s$ for some $s \in R$. Further, we also have $\alpha(X)g(X) = s \cdot g(X) = X$ for some $g(X) \in R[X]$. A similar degree argument shows that $\deg(g(X)) = 1$, i.e. $g(X) = r'X + s'$, whence $s \cdot (r'X + s') = sr'X + ss' = X$. We thus obtain that $sr' = 1$, i.e. s is a unit. Thus, $\langle r, X\rangle = \langle s\rangle = R[X]$, so in particular there exists $p(X), q(X)$ such that $rp(X) + Xq(X) = 1$ for some $p(X), q(X) \in R[X]$. Since $\deg(Xq(X)) \geqslant 1$ if $q(X) \neq 0$, we must have $q(X) = 0$, whence $rp(X) = 1$. Similarly, we must have $\deg(p(X)) = 0$, i.e. $p(X) = t$ for some $t \in R$, so r is a unit in R. Since r was an arbitrary nonzero element of R, this means R is a field.

A second approach is more elegant. Note that $I := \langle X\rangle$ is a prime ideal of $R[X]$, since $R[X]/I \cong R$ (see Problem 6.1, though you can do this now), which is an integral domain. But in a PID, every prime ideal is maximal (See Problem 4.3), so $R/I \cong R$ must be a field. Applying the above to $R = \mathbb{Z}$, we see by the contrapositive the $\mathbb{Z}[X]$ is not a PID.

30 Problem 3.10

Let $R = \mathbb{Z}[\sqrt{2}]$, and let $N\colon R \setminus \{0\} \to \mathbb{Z}_{\geqslant 0}$ be the map defined by

$$a + b\sqrt{2} \mapsto |a^2 - 2b^2|$$

We claim that R is a Euclidean domain with Euclidean map N, i.e for every $u, v \in R$ with $v \neq 0$, there exist $q, r \in R$ such that $u = vq + r$, and either $r = 0$ or $N(r) < N(v)$. It is clear that $N(xy) = N(x)N(y)$ for any $x = a + b\sqrt{2}, y = c + d\sqrt{2} \in R$, since

$$xy = (ac + 2bd) + (bc + ad)\sqrt{2}$$

so

$$\begin{aligned} N(xy) =& |a^2c^2 + 4acbd + 4b^2d^2 - 2(b^2c^2 + 2abcd + a^2d^2)| \\ =& |a^2(c^2 - 2d^2) - 2b^2(c^2 - 2d^2)| \\ =& |a^2 - 2b^2| \cdot |c^2 - 2d^2| \\ =& N(x)N(y) \end{aligned}$$

Now, let $u, v \in R$ such that $v \neq 0$. Let $u/v = \alpha + \beta\sqrt{2}$ with $\alpha, \beta \in \mathbb{Q}$. There exist $a, b \in \mathbb{Z}$ such that $|\alpha - a| \leqslant 1/2, |\beta - b| \leqslant 1/2$. Put

$$w = \frac{u}{v} - (a + b\sqrt{2}) = (\alpha - a) + (\beta - b)\sqrt{2}$$

Then by the triangle inequality,

$$N(w) = |(\alpha - a)^2 - 2(\beta - b)^2| \leqslant |\alpha - a|^2 + 2|\beta - b|^2 \leqslant \frac{1}{4} + 2 \cdot \frac{1}{4} = \frac{3}{4} < 1$$

Now, put $q = a + b\sqrt{2} \in R, r = vw$. Then $u/v = q + w$, so $u = vq + vw = vq + r$; note $r \in R$, since $r = u - vq$. Then if $r \neq 0$,

$$N(r) = N(vw) = N(v)N(w) < N(v) \cdot 1 = N(v)$$

so R is a Euclidean domain.

31 Problem 4.1

Let F be a field, and define a function $N \colon F \setminus \{0\} \to \mathbb{Z}_{\geqslant 0}$ by $N(x) = 0$ for all $x \in F$. Let $u, v \in F$ with v nonzero. We need to show that there exist $q, r \in F$ such that $u = vq + r$ with $N(r) < N(v)$ or $r = 0$. Since $u = v(v^{-1}u) + 0$, we may take $q = v^{-1}u, r = 0$ always, so F is a Euclidean domain. Note that any choice of N would have worked here.

32 Problem 4.2

First, some preliminaries. We claim that $\mathbb{Z}[\sqrt{-5}] \cong \mathbb{Z}[X]/\langle X^2 + 5\rangle$. Indeed, there is a (surjective) ring homomorphism $\Phi \colon \mathbb{Z}[X] \to \mathbb{Z}[\sqrt{-5}]$ which sends $p(X)$ to $p(\sqrt{-5})$ (namely, the evaluation homomorphism at $\sqrt{-5}$). It is clear that $\langle X^2 + 5\rangle \subseteq \ker(\Phi)$. On the other hand, say $p(X) \in \ker(\Phi)$. Since $X^2 + 5$ is monic, we can perform Euclidean division by $X^2 + 5$ on $p(X)$ to write $p(X) = q(X)(X^2 + 5) + r(X)$ for some $q(X), r(X) \in \mathbb{Z}[X]$ such that $\deg(r(X)) < deg(X^2 + 5) = 2$ or $r(X) = 0$. Since $p(X) \in \ker(\Phi)$, we have

$$0 = p(\sqrt{-5}) = q(\sqrt{-5})(0) + r(\sqrt{-5}) = r(\sqrt{-5})$$

But if r is nonzero, then r must be linear, whence $\sqrt{-5} \in \mathbb{Z}$, a contradiction; hence $r = 0$, and $p(X) \in \langle X^2 + 5\rangle$, so $\ker(\varphi) = \langle X^2 + 5\rangle$. By the first isomorphism theorem, $\mathbb{Z}[X]/\langle X^2 - 5\rangle \cong \mathbb{Z}[\sqrt{-5}]$, as desired.
Let $R = \mathbb{Z}[\sqrt{-5}]$, and let $N \colon R \to \mathbb{Z}_{\geqslant 0}$ be the map defined by

$$a + b\sqrt{-5} \mapsto a^2 + 5b^2$$

As in Problem 3.8, it is clear that $N(xy) = N(x)N(y)$ for any $x, y \in R$, since N is the restriction to R of the map on $\mathbb{C}$ which sends a complex number to its (complex) norm.
Suppose that $I := \langle 2, 1 + \sqrt{-5}\rangle = xR$ for some $x \in R$. Then x divides 2 and $1 + \sqrt{-5}$, whence $N(x)$ divides $N(2) = 4$ and $N(1 + \sqrt{-5}) = 6$. Hence, $N(x) = 2$ or $N(x) = 1$. The

only solution to $a^2 + 5b^2 = 1$ for $a, b \in \mathbb{Z}$ is $a = \pm 1, b = 0$, and there are no solutions to $a^2 + 5b^2 = 2$ for $a, b \in \mathbb{Z}$, so $x = \pm 1$. Hence, $I = xR = R$. However,

$$R/I \cong \mathbb{Z}[X]/\langle X^2 + 5, 1 + X, 2\rangle \cong \mathbb{Z}/\langle 2, 6\rangle \cong \mathbb{Z}/2\mathbb{Z} \neq 0$$

so $I \neq R$, a contradiction. (See problem 5.7 for a more detailed explanation of this isomorphism.)

33 Problem 4.3

Note that $\mathbb{Z}[i]$ is a UFD, so by Problem 4.5, all instances of "prime" in this problem can be replaced by "irreducible". We also recall the definition of the norm function $N\colon \mathbb{Z}[i] \to \mathbb{N}$ from the solution to Problem 3.8.

(a) Suppose $3 = \alpha\beta$ for some $\alpha, \beta \in \mathbb{Z}[i]$. Then $9 = N(3) = N(\alpha)N(\beta)$, whence $N(\alpha) = 1, 3$ or 9. If $N(\alpha) = 1$, then by Problem 3.8, $\alpha \in (\mathbb{Z}[i])^\times$; likewise, if $N(\alpha) = 9$, then $N(\beta) = 1$, so $\beta \in (\mathbb{Z}[i])^\times$. We can see that $N(\alpha) \neq 3$ for any $\alpha \in \mathbb{Z}[i]$, since 3 is not a sum of squares of integers (this is easy to show by enumeration of the possibilities). Thus, 3 is irreducible in $\mathbb{Z}[i]$, hence prime.

(b) We proved that $2 = (1-i)(1+i)$ is a factorization of 2 into irreducibles in Problem 3.8.

34 Problem 4.4

Let R be a PID, and let $a \in R$ be a *nonzero* prime element. It suffices to prove that aR is a maximal ideal, whence R/aR is a field. Indeed, suppose $aR \subseteq xR$ for some $x \in R$. Then $x \mid a$, i.e. $a = xb$ for some $b \in R$. Since a is prime, either $a \mid x$ or $a \mid b$. If $a \mid x$, then $xR \subseteq aR$, so $aR = xR$. If $a \mid b$, then $b = ac$ for some $c \in R$, so $a = axc$. Hence, $xc = 1$ by cancellation, since R is a domain and $a \neq 0$, so $x \in R^\times$ and thus $xR = R$. Thus, aR is maximal, as desired.

35 Problem 4.5

Let R be a UFD. Suppose $x \in R$ is prime. Since R is a UFD, we can factor x as a product of irreducibles $x = x_1 \cdots x_n$. Since x is prime, $x \mid x_k$ for some $k \in \{1, \ldots, n\}$; since $x_k \mid x$, $Rx = Rx_k$, whence $x = ux_k$ for some $u \in R^\times$ by Problem 2.5, and therefore x is irreducible. On the other hand, suppose x is irreducible, and $x \mid ab$ for some $a, b \in R$. Since R is a UFD, we can factor $a = a_1 \cdots a_n, b = b_1 \cdots b_m$, where a_i, b_j are irreducible. If $ab = xk$, then by unique factorization, x must appear in the unique factorization of ab into irreducibles, which is necessarily given (up to units) by $a_1 \cdots a_n b_1 \cdots b_m$ using unique factorization again. Thus, x must be (up to multiplication by a unit) one of a_i, b_j, so $x \mid a$ or $x \mid b$, whence x is prime.

36 Problem 4.6

Let $R = \mathbb{Z}[\sqrt{-13}]$, and let $N\colon R \to \mathbb{Z}_{\geqslant 0}$ be the map defined by

$$a + b\sqrt{-13} \mapsto a^2 + 13b^2$$

As in Problems 3.8 and 4.3, N is multiplicative, i.e. $N(xy) = N(x)N(y)$ for any $x, y \in R$. Note that

$$14 = 2 \cdot 7 = (1 + \sqrt{-13})(1 - \sqrt{-13})$$

so if $2, 7, 1 + \sqrt{-13}, 1 - \sqrt{-13}$ are all irreducible and nonassociate, then 14 has two distinct factorizations into irreducibles in R, whence R is not a UFD. As in previous problems, the standard argument is to use the norm N.

First, let $x = a + b\sqrt{-13} \in R$. If $N(x) = 1$, then $a^2 + 13b^2 = 1$, which clearly only admits the solutions $a = \pm 1, b = 0$, so $x = \pm 1$. Suppose $2 = \alpha\beta$ for some $\alpha, \beta \in R$. Then $N(\alpha)N(\beta) = N(2) = 4$, so $N(\alpha) = 1, 2$ or 4. If $N(\alpha) = 1$, then $\alpha = \pm 1$, and if $N(\alpha) = 4$, then $N(\beta) = 1$, so $\beta = \pm 1$. Note that $N(\alpha)$ cannot be 2, since there are no solutions to $a^2 + 13b^2 = 2$ for $a, b \in \mathbb{Z}$, so 2 is irreducible. The arguments that $7, 1 + \sqrt{-13}, 1 - \sqrt{-13}$ are irreducible proceed identically.

Now, since every unit of R has norm 1 (see Problem 3.8 if this is not clear), two associate elements of R must have the same norm. Since $N(2) = 4, N(7) = 49, N(1 + \sqrt{-13}) = 14, N(1 - \sqrt{-13}) = 14$, none of these elements are associate, so this concludes the proof. Of course, since R is not a UFD, it cannot be a PID, since every PID is a UFD.

37 Problem 4.7

Let $R = S \times T$ where S, T are Noetherian rings. By Problem 2.1, every ideal of R is of the form $I \times J$ for some ideal I of S and some ideal J of T. Since S and T are Noetherian, I is generated by some $s_1, \ldots, s_k \in S$, and likewise J is generated by some $t_1, \ldots, t_j \in T_2$ where $k, j \in \mathbb{N}$. Hence, $I \times J$ is finitely generated by the pairs $(s_1, 0), \ldots, (s_k, 0), (0, t_1), \ldots, (0, t_j)$. Alternatively, suppose $I_1 \times J_1 \subseteq I_2 \times J_2 \subseteq \cdots$ is an ascending chain of ideals in R. Then $I_1 \subseteq I_2 \subseteq \cdots$ is an ascending chain of ideals in S, whence S Noetherian implies $I_n = I_{n+1} = \cdots$ for some $n \in NN$. Likewise, $J_1 \subseteq J_2 \subseteq \cdots$ is an ascending chain of ideals in T, so $J_m = J_{m+1} = \cdots$ for some $m \in NN$. Taking $k = \max(m, n)$, $I_k \times J_k = I_{k+1} \times J_{k+1} = \cdots$, so every ascending chain in R stabilizes.

38 Problem 4.8

Suppose R is a PID. Then every ideal is principal, so R is trivially a Bezout domain. Further, every PID is Noetherian, since every ideal is finitely generated, namely by one element. Conversely, suppose R is a Noetherian Bezout domain. We claim that every ideal generated by n elements is principal, proceeding by induction on n. The case $n = 1$ is clear, and the case $n = 2$ is immediate since R is a Noetherian Bezout domain. Suppose $n > 1$, and $I = a_1R + a_2 + \cdots + a_{n-1}R + a_nR$ for some $a_1, \ldots, a_n \in R$. Since addition of ideals is associative, $I = (a_1R + a_2 + \cdots + a_{n-1}R) + a_nR$, and the induction hypothesis implies

$a_1R + a_2 + \cdots + a_{n-1}R = aR$ for some $a \in R$. Then $I = aR + a_nR$, and since R is a Bezout domain, there is some $b \in R$ such that $I = bR$, which completes the induction. Hence, every finitely generated ideal of R is principal; but R is Noetherian, so every ideal of R is finitely generated, i.e. R is a PID.

39 Problem 4.9

Let $R_1 = \mathbb{Q}$, and $R_{n+1} = R_n[X_n]$ for $n \geqslant 1$. Put $R = \bigcup_{n\in\mathbb{N}} R_n$. We claim that R is a commutative ring that is not Noetherian. There is a standard embedding of R_k into R_l for any $k \leqslant l$, so that we can regard R_k as a subring of R_l for $k \leqslant l$. Then R has the structure of a commutative ring as follows. For any $f, g \in R$, we have $f \in R_k, g \in R_l$ for some $k, l \in \mathbb{N}$. If (WLOG) $k \leqslant l$, then we can regard f as an element of R_l, so that we add/multiply f, g as elements of R_l; since R_l is a ring, the result belongs to $R_l \subset R$. All of the necessary properties (including commutativity) of these addition/multiplication operations defined this way are inherited from the ring structure on R_l, so R is indeed a commutative ring.
However, R is not Noetherian, as the ideal $\langle X_1, X_2, \ldots\rangle$ is not finitely generated. (Alternatively, the ascending chain of ideals $\langle X_1\rangle \subset \langle X_1, X_2\rangle \subset \langle X_1, X_2, X_3\rangle \subset \cdots$ does not stabilize, so R is not Noetherian by an equivalent characterization.)

40 Problem 4.10

Let $R = \mathbb{Z}[\sqrt{-5}]$, and let $I = 2R + (1 + \sqrt{-5})R, J = 3R + (1 + \sqrt{-5})R$. Every element $x \in I$ is of the form $2\alpha + (1 + \sqrt{-5})\beta$ for some $\alpha, \beta \in R$, and likewise every element $y \in J$ is of the form $3\alpha' + (1 + \sqrt{-5})\beta'$ for some $\alpha', \beta' \in R$. Then

$$(2\alpha + (1 + \sqrt{-5})\beta)(3\alpha' + (1 + \sqrt{-5})\beta') = 6\alpha\beta + (3\alpha'\beta + 2\alpha\beta' + (1 + \sqrt{-5})\beta\beta')(1 + \sqrt{-5})$$

Since $6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$, we see that $xy \in (1 + \sqrt{-5})R$, whence $IJ \subseteq (1 + \sqrt{-5})R$. To show that $(1 + \sqrt{-5})R \subset IJ$, it suffices to show that $(1 + \sqrt{-5})R \in IJ$. Indeed, $2, 2 + (1 + \sqrt{-5}) \in I$ and $3, 3 + (1 + \sqrt{-5}) \in J$, so $2(3 + (1 + \sqrt{-5})), 3(2 + (1 + \sqrt{-5})) \in IJ$, whence

$$3(2 + (1 + \sqrt{-5})) - 2(3 + (1 + \sqrt{-5})) = 1 + \sqrt{-5} \in IJ$$

41 Problem 5.1

This is an old classic, which admits the standard Euclidean proof (note that the proof below can easily be converted to a direct proof.)
Recall that $F[X]$ is a UFD (in fact, $F[X]$ is a Euclidean domain). Suppose $F[X]$ has only finitely many (nonassociate) irreducible polynomials $p_1(X), \ldots, p_n(X) \in F[X]$. Then $g(X) = \prod_{i=1}^{n} p_i(X) + 1$ is not divisible by any of the polynomials $p_1, \ldots, p_n$, and so must be divisible by an irreducible polynomial $k(X) \neq p_i(X)$ for each $i = 1, \ldots, n$. Since the factorization of $g(X)$ is unique up to units, it is clear that $k(X)$ is nonassociate to any $p_i(X)$, so this is a contradiction. Hence, $F[X]$ has infinitely many nonassociate irreducible polynomials, which completes the proof.

42 Problem 5.2

Let p be a prime integer such that $p \equiv 3 \pmod 4$. Since $\mathbb{Z}[i]$ is a UFD, p is prime if and only if p is irreducible by Problem 4.5, so it suffices to show that p is irreducible. Suppose $p = \alpha\beta$ for some $\alpha, \beta \in \mathbb{Z}[i]$. Recalling the norm N on $\mathbb{Z}[i]$ introduced in Problem 3.8, note that $p^2 = N(p) = N(\alpha)N(\beta)$. Thus, it suffices to show (WLOG) that there is no $\alpha \in \mathbb{Z}[i]$ such that $N(\alpha) = p$, as then we must have either $N(\alpha) = 1$ or $N(\beta) = 1$, whence one of α, β belongs to $(\mathbb{Z}[i])^\times$. Suppose $\alpha = a + bi \in \mathbb{Z}[i]$ such that $N(\alpha) = a^2 + b^2 = p$. Then $a^2 + b^2 \equiv 3 \mod 4$, which is a contradiction as the only squares mod 4 are 0 and 1.

43 Problem 5.3

Let F be a field, and let R be the subset of $F(X)$ of Laurent polynomials.

(a) Clearly, $1 \in R$. Suppose $f(X)/X^n, g(X)/X^m \in R$. Then

$$\frac{f(X)}{X^n} + \frac{g(X)}{X^m} = \frac{X^m f(X) + X^n g(X)}{X^{n+m}} \in R$$

$$\frac{f(X)}{X^n} \cdot \frac{g(X)}{X^m} = \frac{f(X)g(X)}{X^{n+m}} \in R$$

since $n + m \in \mathbb{N}$ and $X^k f(X)$ is a polynomial for any $k \in \mathbb{N}, f(X) \in F[X]$. Hence, R is indeed a subring of $F(X)$.
This argument should feel fairly standard at this point. In fact, most of these "elements of ring with denominators form a ring" problems are a special case of a more general phenomenon, known as localization. We'll talk about this in discussion.

(b) Let I be an ideal of R, and let $S = \{f(X) \in F[X] \mid f(X)/X^k \in I \text{ for some } k \in \mathbb{N}\}$; that is, S is the set of "numerators" in I. Note that if $f(X) \in S$, then $f(X) \in I$, since $f(X)/X^k \in I$ implies $X^k \cdot f(X)/X^k = f(X) \in I$. Further, since $F[X]$ is a PID, the ideal generated by S can be generated by one element $p(X) \in F[X]$. We claim $I = \langle p(X) \rangle$. Indeed, for any $f(X)/X^k \in I$, $f(X) = p(X)q(X)$ for some $q(X) \in F[X]$, so $f(X) = \frac{q(X)}{X^k} \cdot p(X) \in \langle p(X) \rangle \subset R$. On the other hand, since the ideal generated by S in $F[X]$ contains $p(X)$, it follows that $p(X) = f_1(X)q_1(X) + \cdots + f_n(X)q_n(X)$ for some $n \in \mathbb{N}$ and $f_1, \ldots, f_n \in S, q_1, \ldots, q_n \in F[X]$. As noted above, $f_1, \ldots, f_n \in I$, so $p(X) \in I$, whence $I = \langle p(X) \rangle \subset R$.

44 Problem 5.4

Since $\mathbb{Z}$ is a UFD, $\mathbb{Z}[X]$ is a UFD by results proved in class. Using the isomorphism $R[X, Y] \cong (R[X])[Y]$, a simple induction argument then shows that $\mathbb{Z}[X_1, X_2, \ldots, X_k]$ is a UFD for each $k \in \mathbb{N}$. Let $R := \mathbb{Z}[X_1, X_2, \ldots]$, and $f \in R$. Since $R = \bigcup_{k=1}^{\infty} \mathbb{Z}[X_1, X_2, \ldots, X_k]$, $f \in \mathbb{Z}[X_1, X_2, \ldots, X_n]$ for some $n \in \mathbb{N}$. Since $\mathbb{Z}[X_1, \ldots, X_n]$ is a UFD, f admits a unique factorization into a product of irreducible elements $f_1, \ldots, f_k$ of $\mathbb{Z}[X_1, X_2, \ldots, X_n] \subset R$. If $f = gh$ for some $g, h \in R$, then $g, h \in \mathbb{Z}[X_1, \ldots, X_n]$; if not, then WLOG g contains some

monomial containing X_k for some $k > n$, and therefore so does f (since $\mathbb{Z}$ is a domain), a contradiction. Hence, factorization of f in R is the same as factorization of f in $\mathbb{Z}[X_1, \ldots, X_n]$; in particular, the elements f_i remain irreducible as elements of R, and the factorization $f = f_1 \cdots f_k$ is a unique among factorizations of f into irreducibles in R, so R is a UFD.

45 Problem 5.5

Let R be a PID, $a, b \in R$, and $d = \gcd(a, b)$. Let $y = ar + br' \in aR + bR$. Since $a = ds, b = ds'$, we have $y = dsr + ds'r' = d(sr + s'r') \in dR$, so $aR + bR \subseteq dR$. On the other hand, since R is a PID, $aR + bR = xR$ for some $x \in R$. Since $aR \subseteq xR$, $x \mid a$, and likewise $x \mid b$, so $x \mid \gcd(a, b) = d$. But then $dR \subseteq xR = aR + bR$, so $dR = aR + bR$.

46 Problem 5.6

To compute $\gcd(2, 5 + i)$, we can use the Euclidean algorithm with the standard norm N on $\mathbb{Z}[i]$ (see Problem 3.8). First, note

$$5 + i = 2(2 + i) + (1 - i)$$

Since $N(-1 - i) = 2 < 4 = N(2)$, we continue to the next step:

$$2 = (1 - i)(1 + i) + 0$$

so $\gcd(2, 5 + i) = 1 - i$. (Of course, this is really only well-defined up to multiplication by a unit: a better way to say this would be $\gcd(2, 5 + i)\mathbb{Z}[i] = (i - 1)\mathbb{Z}[i]$). One can additionally check $(5 + i) = (1 - i)(2 + 3i)$; since $N(2 + 3i) = 13$ is prime, $(2 + 3i)$ is irreducible in $\mathbb{Z}[i]$.

47 Problem 5.7

The ideas used in the solution to Problem 4.2 present one way to solve this problem. By a proof identical to the one given in Problem 4.2, $\mathbb{Z}[i] \cong \mathbb{Z}[X]/\langle X^2+1\rangle$. Under the isomorphism $\mathbb{Z}[X]/\langle 1 + X\rangle \cong \mathbb{Z}$ sending the equivalence class $\overline{X}$ to -1, $\overline{X^2 + 1}$ maps to $(-1)^2 + 1 = 2$, so

$$\mathbb{Z}[i]/(1 + i)\mathbb{Z}[i] \cong \mathbb{Z}[X]/\langle X^2 + 1, 1 + X\rangle \cong (\mathbb{Z}[X]/\langle 1 + X\rangle)/\langle\overline{X^2 + 1}\rangle \cong \mathbb{Z}/2\mathbb{Z}$$

48 Problem 5.8

Let $f, g \in \mathbb{Q}[X]$ such that $fg \in \mathbb{Z}[X]$. Since $\mathbb{Z}[X]$ is a UFD, we can factor fg as a product of irreducible polynomials $h_1 \cdots h_m$, $h_i \in \mathbb{Z}[X]$. Let d be the product of all h_i which are constant, and let $h_1, \ldots, h_n$ be the nonconstant irreducible factors of fg, so that $fg = d(h_1 \cdots h_n)$. By Gauss' lemma, each h_i is irreducible in $\mathbb{Q}[X]$ as well, and $d \in \mathbb{Q}^\times$, so $fg = d(h_1 \cdots h_n)$ is a factorization of fg into irreducibles over $\mathbb{Q}[X]$. In particular, we can redefine h_1 as dh_1, which remains irreducible over $\mathbb{Q}[X]$ since $d \in \mathbb{Q}^\times$, and $dh_1 \in \mathbb{Z}[X]$. Let $f = p_1 \cdots p_i, g = q_1 \cdots q_j$ be irreducible factorizations of f, g over $\mathbb{Q}[X]$. Then $fg =$

$p_1 \cdots p_i \cdot q_1 \cdots q_k$ is a factorization of fg into irreducibles over $\mathbb{Q}$, so by unique factorization, these factorizations must be the same up to units: that is, $i + j = n$, and WLOG, we may assume

$$p_1 = u_1 h_1, \ldots, p_i = u_i h_i, q_1 = u_{i+1} h_{i+1}, \ldots, q_j = u_n h_n$$

for some $u_1, \ldots, u_n \in \mathbb{Q}^\times$. Put $a = u_1^{-1} \cdots u_i^{-1} = (u_1 \cdots u_i)^{-1} \in \mathbb{Q}^\times$. Since

$$fg = h_1 \cdots h_n = p_1 \cdots p_i \cdot q_1 \cdots q_k$$

we must have $u_1 \cdots u_n = 1$, so $(u_1 \cdots u_i)^{-1} = u_{i+1} \cdots u_n$. Hence,

$$f = p_1 \cdots p_i = (u_1 h_1) \cdots (u_i h_i) = a^{-1}(h_1 \cdots h_i)$$

$$g = q_1 \cdots q_j = (u_{i+1} h_{i+1}) \cdots (u_n h_n) = a(h_{i+1} \cdots h_n)$$

whence $af \in \mathbb{Z}[X], a^{-1}g \in \mathbb{Z}[X]$.

49 Problem 5.9

Let S be a set of prime integers, and let R be the set of all rational numbers a/b such that the prime divisors of b belong to S.

(a) Note that $1 = 1/1 \in R$, since the prime divisors of 1 (the empty set!) always belong to S. Further, suppose $a/b, c/d \in R$. Then

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \in R$$

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd} \in R$$

since the prime divisors of b, d belong to S and therefore so do the prime divisors of bd by unique factorization in $\mathbb{Z}$. Hence, R is a subring of $\mathbb{Q}$.

(b) Let $I \subset R$ be an ideal, and let $Q = \{a \in I \mid a \in \mathbb{Z} \subset R\}$. The set Q is actually an ideal of $\mathbb{Z}$, since I is an ideal of R, and R contains $\mathbb{Z}$, whence $Q = x\mathbb{Z}$ for some $x \in \mathbb{Z}$; we claim $I = xR$. Suppose $a/b \in I$; then $b \cdot a/b = a \in I$, so $a \in S \subseteq x\mathbb{Z}$, whence $a = xk$ for some $k \in \mathbb{Z}$. Hence, $a/b = x(k/b) \in xR$, so $I \subseteq xR$. On the other hand, $x \in Q \subseteq I$, so $xR \subseteq I$, whence $I = xR$. Hence, R is a PID.
Note that a/b is irreducible if and only if a is irreducible; indeed, a and a/b are associates by the unit b. Hence, it suffices to classify all irreducible integer elements of R. Certainly, this is a subset of the irreducible elements of $\mathbb{Z}$, i.e. the prime elements of $\mathbb{Z}$. Let P be the set of all primes in $\mathbb{Z}$; we claim that the irreducible integer elements of R are $P \setminus S$. Indeed, every element of S is a unit of R, hence not irreducible. Further, let $p \in P \setminus S$. Note that p is not a unit, as if $p \cdot a/b = 1$ for some $a/b \in R$, then $pa = b$. This is a contradiction, since $p \mid b$, but every prime divisor of b belongs to S, which does not include p. Further, suppose $p = a/b \cdot c/d$. Then $pbd = ac$; by unique factorization in $\mathbb{Z}$, every prime divisor of ac belongs to S except p, and since p appears in the prime factorization of pbd with exponent 1, p may only divide one of a, c. Hence, every prime divisor of (WLOG) c must belong to S, whence c/d is a unit with inverse d/c. Hence, p is irreducible in R, as claimed. We have thus proven that the irreducible elements of R are of the form p/b for $p \in P \setminus S$.

50 Problem 5.10

Let F be a field, and let R be the subset of $F[X]$ of polynomials whose X-coefficient is 0. Let $f(X) = a_0 + a_2X^2 + \cdots + a_nX^n, g(X) = b_0 + \cdots + b_2X^2 + \cdots + b_mX^m \in R$. Then

$$f + g = (a_0 + b_0) + (a_2 + b_2)X^2 + \cdots$$

$$fg = a_0b_0 + (a_0b_2 + a_2b_0)X^2 + \cdots$$

Thus, $fg, f + g$ have X-coefficient 0, so $fg, f + g \in R$. Since $1 \in R$, R is a subring of F.
We claim that R is not a UFD. Indeed, note that X^2 and X^3 are irreducible elements of R. For any $f, g \in F[X]$ nonzero, $\deg(fg) = \deg(f) + \deg(g)$, so the only way $X^2 = fg$ for $f, g \in F[X]$ is if one of f, g has degree 0 or f and g both have degree 1. Since R contains no degree one polynomials, this implies that one of f, g must have degree 0, i.e. (WLOG) $f \in F[X]^\times$, so X^2 is irreducible. Likewise, X^3 is irreducible by similar degree considerations. Finally, note that X^2 and X^3 are not associate in R, since $R^\times \subset (F[X])^\times = F^\times$ by Problem 1.10(b). Since $X^6 = (X^2)^3 = (X^3)^2$ can be factored into two distinct product of irreducible elements of R whose factors are not associate, R is not a UFD.

51 Problem 6.1

Consider the evaluation morphism $\varphi\colon R[X] \to R$ given by $f \mapsto f(0)$. This is a surjective ring homomorphism, and $X \cdot R[X] \subset \ker(\varphi)$, since $\varphi(X \cdot p(X)) = 0 \cdot p(0) = 0$. If $p(X) \in \ker(\varphi)$, then $p(0) = 0$, i.e. p has constant term zero, so $p \in X \cdot R[X]$, whence $\ker(\varphi) = X \cdot R[X]$. By the first isomorphism theorem, $R[X]/(X \cdot R[X]) \cong R$.

52 Problem 6.2

(a) Let $f(X) = X^2 + X + 1 \in (\mathbb{Z}/2\mathbb{Z})[X]$. Then $f(0) = 0 + 0 + 1 \neq 0 \in \mathbb{Z}/2\mathbb{Z}$ and $f(1) = 1 + 1 + 1 = 1 \neq 0 \in \mathbb{Z}/2\mathbb{Z}$, so f has no roots over $\mathbb{Z}/2\mathbb{Z}$, whence it is irreducible over $\mathbb{Z}/2\mathbb{Z}$.

(b) Let $f(X) = X^3 + X + 1 \in (\mathbb{Z}/3\mathbb{Z})[X]$. Then $f(1) = 1 + 1 + 1 = 0 \in \mathbb{Z}/3\mathbb{Z}$, so $X + 1$ divides f. Then we can write f as $f(X) = (X + 2)(X^2 + X + 2)$, and $X^2 + X + 2$ has no roots over $\mathbb{Z}/3\mathbb{Z}$, so this is a factorization of f into irreducibles over $\mathbb{Z}/3\mathbb{Z}$.

(c) Let $f(X) = X^4 + 1 \in (\mathbb{Z}/5\mathbb{Z})[X]$. Then $f(0) = 1, f(1) = 2, f(2) = 2, f(3) = 2, f(4) = 2$, so f has no roots over $(\mathbb{Z}/5\mathbb{Z})[X]$. Thus, if f is reducible over $(\mathbb{Z}/5\mathbb{Z})[X]$, it must be as a product of irreducible quadratics, and since f is monic, these quadratics can be taken to be monic after normalizing each factor.
If f is a reducible quadratic in $(\mathbb{Z}/5\mathbb{Z})[X]$, then it is a product of linear factors, so we can compute all reducible quadratics over $\mathbb{Z}/5\mathbb{Z}$ by computing $(X - a)(X - b)$ for all $a, b \in \mathbb{Z}/5\mathbb{Z}$. Doing so, we find that the following polynomials are *irreducible* over $\mathbb{Z}/5\mathbb{Z}$:

$$X^2 + 2, X^2 + 3, X^2 + X + 1, X^2 + X + 2, X^2 + 2X + 3$$

$$X^2+2X+4, X^2+3X+3, X^2+3X+4, X^2+4X+1, X^2+4X+2$$

Now, we can see that $(X^2+2)(X^2+3) = X^4+5X^2+6 = X^4+1$, so this is the irreducible factorization of X^4+1 in $(\mathbb{Z}/5\mathbb{Z})[X]$. Of course, if we did not notice this, we could do long division on X^4+1 by each of the irreducible polynomials above until we found the factorization (or concluded that there isn't one).

N.B.: it would probably be less computationally intensive for the purposes of this problem to write $X^4+1 = (X^2+aX+b)(X^2+cX+d)$, find constraints on a, b, c, d, and simply check that X^2+2, X^2+3 are irreducible once we found a, b, c, d. However, this technique is not helpful for polynomials of higher degree, whereas the above procedure generalizes well. When we know more about finite fields (110 C?), we can discuss more sophisticated factorization techniques, e.g. Berlekamp's algorithm.

53 Problem 6.3

Clearly, $1, X, X+1$ are irreducible by degree considerations. Since any reducible polynomial of degree $\leqslant 3$ over $(\mathbb{Z}/2\mathbb{Z})[X]$ must have a root over $\mathbb{Z}/2\mathbb{Z}$, we can recursively build all reducible quadratics and cubics; first, we build the quadratics. All reducible quadratics are given by $X^2, X(X+1), (X+1)^2$, so the lone irreducible quadratic over $\mathbb{Z}/2\mathbb{Z}$ is X^2+X+1 (see 6.2(a) if you want extra verification!). Now, all *reducible* cubics are given by

$$X^3, X^2(X+1), X(X+1)^2, (X+1)^3, X(X^2+X+1), (X+1)(X^2+X+1)$$

so the *irreducible* cubics over $\mathbb{Z}/2\mathbb{Z}$ are: X^3+X^2+1, X^3+X+1.

54 Problem 6.4

Let $f(X) = c_0 + c_1X + \cdots + c_nX^n \in \mathbb{Z}[X]$. Then for any $a, b \in \mathbb{Z}$, $f(b) - f(a) = (c_0 + c_1b + \cdots + c_nb^n) - (c_0 + c_1a + \cdots + c_na^n) = c_1(b-a) + c_2(b^2-a^2) + \cdots + c_n(b^n-a^n)$. We claim $b-a \mid b^n-a^n$ for all $n \in \mathbb{N}$, so that $b-a \mid f(b)-f(a)$. We proceed by induction. It is clear for the cases $n = 0, 1$, so suppose $n > 1$. Then note that

$$b^n - a^n = (b-a)(b^{n-1}+a^{n-1}) + ab^{n-1} - ba^{n-1} = (b-a)(b^{n-1}+a^{n-1}) + ab(b^{n-2}-a^{n-2})$$

The first term is clearly divisible by $b-a$, and the second term is as well by the induction hypothesis, since $n \geqslant 2$. This completes the proof.

55 Problem 6.5

Let $f(X) = X^n - 13 \in \mathbb{Z}[i][X]$ for some $n \in \mathbb{N}$. Let N be the norm as defined in the solution to Problem 3.8, and recall that (as shown in the solution to Problem 3.7), any element of prime norm in $\mathbb{Z}[i]$ is irreducible (hence prime). Since $13 = (3+2i)(3-2i) = N(3+2i)$, $3+2i$ is a prime element of $\mathbb{Z}[i]$, so $\mathfrak{p} = (3+2i)\mathbb{Z}[i]$ is a prime ideal. Further, since $(\mathbb{Z}[i])^\times = \{\pm 1, \pm i\}$ by Problem 3.8, $3+2i$ and $3-2i$ are not associate, whence $13 \in \mathfrak{p}$ but not in $\mathfrak{p}^2$, so f is irreducible by Eisenstein at $\mathfrak{p}$.

N.B.: does a similar Eisenstein argument work for $f(X) = X^n - 2$? If not, where does it go wrong? (For those interested, this touches on the issue of ramification of prime ideals in algebraic number fields - see also splitting of prime ideals in Galois extensions.)

56 Problem 6.6

Let $f(X, Y) = X^2 + Y^2 - 1 \in \mathbb{Z}[X, Y]$. Via the isomorphism $\mathbb{Z}[X, Y] \cong (\mathbb{Z}[X])[Y]$, we can view f as a polynomial in Y with coefficients in X, and rewrite $f(X, Y)$ as $Y^2+(X-1)(X+1)$. Since $\mathbb{Z}[X]/\langle X-1\rangle \cong \mathbb{Z}$, $\langle X-1\rangle$ is a prime ideal of $\mathbb{Z}[X]$. Further, $(X-1)^2$ does not divide $(X-1)(X+1)$ (i.e. $(X-1)(X+1)$ does not belong to $\langle X-1\rangle^2 = \langle (X-1)^2\rangle$), so by Eisenstein's criterion at $X - 1 \in \mathbb{Z}[X]$, f is irreducible over $(\mathbb{Z}[X])[Y]$ and therefore is also irreducible over $\mathbb{Z}[X, Y]$.

57 Problem 6.7

Let $f = X^n + c_{n-1}X^{n-1} + \cdots + c_0 \in \mathbb{Z}[X]$ be a monic polynomial with root $a \in \mathbb{Q}$. Write $a = p/q$ with $p, q \in \mathbb{Z}$ such that $\gcd(p, q) = 1$. Then

$$f\left(\frac{p}{q}\right) = \left(\frac{p}{q}\right)^n + c_{n-1}\left(\frac{p}{q}\right)^{n-1} + \cdots + c_0 = 0$$

so multiplying both sides by q^n (which is nonzero),

$$p^n + c_{n-1}p^{n-1}q + \cdots + c_1pq^{n-1} + c_0q^n = 0$$

For any prime z dividing q, taking both sides mod z gives $p^n \equiv 0 \pmod{z}$, i.e. $z \mid p^n$, so $z \mid p$ by Euclid's lemma. Since $\gcd(p, q) = 1$, this means the list of primes dividing q must be empty, i.e. $q = \pm 1$, so $a \in \mathbb{Z}$.
N.B.: this problem shows that the ring of algebraic integers in $\mathbb{Q}$ is $\mathbb{Z}$. Large swaths of algebraic number theory and commutative algebra are dedicated to understanding so-called questions of integrality. In particular, one is often interested in the ring of integers in some number field; in general, these are very difficult problems! For an interesting yet tractable challenge, you might try computing the ring of integers in $\mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}$.

58 Problem 6.8

Let $f(X) = X^3 - 3X + 1$. Since f is monic (hence primitive), f is irreducible over $\mathbb{Q}$ if and only if it is irreducible over $\mathbb{Z}$ by Gauss' Lemma, so it suffices to show that f is irreducible over $\mathbb{Q}$. Since $\deg(f) = 3$, f is reducible if and only if it has a root over $\mathbb{Q}$. By the rational root theorem, the only possible roots of f over $\mathbb{Q}$ are ± 1, and we can se that $f(1) = -1, f(-1) = 1$, so f has no roots over $\mathbb{Q}$ and is therefore irreducible over $\mathbb{Q}$.

59 Problem 6.9

Let $f(X) = X^p - X \in (\mathbb{Z}/p\mathbb{Z})[X]$. By Fermat's little theorem, $a^{p-1} \equiv 1 \pmod{p}$ for all $a \notin p\mathbb{Z}$, i.e. $q^{p-1} = 1$ for all nonzero $q \in \mathbb{Z}/p\mathbb{Z}$. Hence, $q^p = q$ for all $q \in \mathbb{Z}/p\mathbb{Z}$ (this clearly holds for $q = 0 \in \mathbb{Z}/p\mathbb{Z}$ as well), so every $q \in \mathbb{Z}/p\mathbb{Z}$ is a root of f. Since $\mathbb{Z}/p\mathbb{Z}$ is a field, this means f splits into linear factors over $\mathbb{Z}/p\mathbb{Z}$, so a factorization of f into a product of irreducibles is

$$f(X) = \prod_{q \in \mathbb{Z}/p\mathbb{Z}} (X - q)$$

60 Problem 6.10

No, it isn't: $X^4 + 64 = (X^2 - 4X + 8)(X^2 + 4X + 8)$.

61 Problem 7.1

(a) Let M be an R-module. Let $\varphi\colon R \to \mathrm{End}(M)$ be given by $\varphi(a) = f_a$. Then $\varphi(1)(m) = 1 \cdot m = m$ for all $m \in M$, so $\varphi(1) = \mathrm{Id}_M$. Further, let $r, s \in R$. Then for all $m \in M$,

$$\varphi(r+s)(m) = (r+s) \cdot m = r \cdot m + s \cdot m = \varphi(r)(m) + \varphi(s)(m) = (\varphi(r) + \varphi(s))(m)$$

$$\varphi(rs)(m) = (rs) \cdot m = r \cdot (s \cdot m) = \varphi(r)(s \cdot m) = \varphi(r)(\varphi(s)(m)) = (\varphi(r) \circ \varphi(s))(m)$$

i.e. $\varphi(r+s) = \varphi(r) + \varphi(s)$ and $\varphi(rs) = \varphi(r) \circ \varphi(s)$, so φ is a ring homomorphism.

(b) Let $f\colon R \to \mathrm{End}(M)$ be a ring homomorphism, and define the formula $a \cdot m = f(a)(m)$. Then for all $r, s \in R$ and $m, n \in M$,

(1) $(r+s) \cdot m = f(r+s)(m) = f(r)(m) + f(s)(m) = r \cdot m + s \cdot m$

(2) $r \cdot (s \cdot m) = f(r)(f(s)(m)) = (f(r) \circ f(s))(m) = f(rs)(m) = rs \cdot m$

(3) $r \cdot (m + m') = f(r)(m + m') = f(r)(m) + f(r)(m')$

(4) $1 \cdot m = f(1)(m) = \mathrm{Id}_M(m) = m$.

where (1), (2) and (4) hold because f is a ring homomorphism, and (3) holds because $f(r) \in \mathrm{End}(M)$ is a group homomorphism.

62 Problem 7.2

Let M be a (left) R-module generated by $m \in M$. Define an R-module homomorphism $f\colon R \to M$ by $r \mapsto r \cdot m$. Then f is surjective, since M is generated by m, and so $R/\ker(f) \cong M$. Since $\ker(f)$ is a (left) R-submodule of R, it is an ideal of R.

63 Problem 7.3

Let R be a commutative ring, and let M, N be R-modules. Define an R-module structure $\cdot\colon R \times \mathrm{Hom}_R(M,N) \to \mathrm{Hom}_R(M,N)$ by $(r \cdot f)(m) = r \cdot f(m)$ for $f \in \mathrm{Hom}_R(M,N)$. Then for any $r, s \in R$, $f, g \in \mathrm{Hom}_R(M,N)$ and $m \in M$,

(1) $((r+s)\cdot f)(m) = (r+s)\cdot f(m) = r\cdot f(m) + s\cdot f(m) = (r\cdot f)(m) + (s\cdot f)(m)$

(2) $(r\cdot(s\cdot f))(m) = r\cdot(s\cdot f(m)) = (rs)\cdot f(m) = (rs\cdot f)(m)$

(3) $(r\cdot(f+g))(m) = r\cdot((f+g)(m)) = r\cdot(f(m)+g(m)) = r\cdot f(m) + r\cdot g(m) = (r\cdot f)(m) + (r\cdot g)(m)$

(4) $(1\cdot f)(m) = 1\cdot f(m) = f(m)$.

so

$$(r+s)\cdot f = r\cdot f + s\cdot f$$
$$r\cdot(s\cdot f) = (rs)\cdot f$$
$$r\cdot(f+g) = r\cdot f + r\cdot g$$
$$1\cdot f = f$$

Note that $(1)-(4)$ follow from the R-module structure on N.

64 Problem 7.4

Let M be a (left) R-module, and $N \subset M$ be a (left) R-submodule. Suppose that both N and M/N are finitely generated. Let $n_1, \ldots, n_k$ be generators for N, and let M/N be generated by $m_1 + N, \ldots, m_j + N$. Let $m \in M$. Then $m + N = r_1(m_1+N) + \cdots + r_j(m_j+N) = (r_1m_1 + r_2m_2 + \cdots + r_jm_j) + N$ for some $r_1, \ldots, r_j \in R$. Then $m - r_1m_1 + r_2m_2 + \cdots + r_jm_j \in N$, and hence can be written as $s_1n_1 + \cdots + s_kn_k$ for some $s_1, \ldots, s_k \in R$. Thus,

$$m = r_1m_1 + r_2m_2 + \cdots + r_jm_j + s_1n_1 + \cdots + s_kn_k$$

and so M is finitely generated by $n_1, \ldots, n_k, m_1 \ldots, m_j$.

65 Problem 7.5

Let R be a ring, and M a (left) R-module. For any $m \in M$, note that there is an R-module homomorphism $f_m\colon R \to M$ defined by $f_m(r) = r\cdot m$, and in particular, $f_m(1) = 1\cdot m = m$. Further, suppose $f\colon R \to M$ is an R-module homomorphism. Then $f(r) = f(r\cdot 1) = r\cdot f(1)$, so f is completely determine by $f(1)$; in particular, if $f, g \in \mathrm{Hom}_R(R,M)$ such that $f(1) = g(1)$, then $f = g$. Hence, define a map $\Phi\colon \mathrm{Hom}_R(R,M) \to M$ by $\Phi(f) = f(1)$. The considerations above show that Φ is a bijection, and Φ is a homomorphism of groups, since for any $f, g \in \mathrm{Hom}_R(M)$,

$$\Phi(f+g) = (f+g)(1) = f(1) + g(1) = \Phi(f) + \Phi(g)$$

so Φ is a group isomorphism.

66 Problem 7.6

The proof proceeds exactly as one does in linear algebra (although we must be a bit more careful with commutativity considerations here). Let $g\colon R^n \to R^m$ be a right R-module homomorphism. Let $e_1, \ldots, e_n$ be the standard (central) idempotents in R^n, e.g. $e_1 = (1, 0, \ldots, 0)$, and let $f_i = g(e_i) \in R^m$ for each $i = 1, \ldots, n$. Since every $x := (r_1, \ldots, r_n) \in R^n$ can be written as $e_1 r_1 + \cdots + e_n r_n$ and g is a right R-module homomorphism,

$$g(x) = g(e_1 r_1 + \cdots + e_n r_n) = g(e_1) r_n + \cdots + g(e_n) r_n = f_1 r_1 + \cdots f_n r_n$$

Letting A be the $m \times n$ matrix whose columns are given by $f_1, \ldots, f_n$, we see that this formula exactly specifies $g(x) = Ax$, as desired.

67 Problem 7.7

Suppose $\mathbb{Q}$ is a free abelian group ($\mathbb{Z}$-module) with generating set $S := \{x_i\}_{i \in I}$ with $x_i = p_i/q_i$ for some $p_i, q_i \in \mathbb{Z}$. Suppose $|I| \geqslant 2$; then there exist distinct $x_i, x_j \in S$, and $-q_i pj(x_i) + q_j p_i(x_j) = 0$. Since $q_i, q_j \neq 0$ and $x_i \neq x_j$, at most one of $q_i p_j, q_j p_i$ is 0, so x_i, x_j are linearly dependent, a contradiction. Hence, we must have $|I| = 1$, i.e. $\mathbb{Q}$ is a cyclic abelian group.
There are a great number of ways to proceed from here, but all routes boil down to the fact that $\mathbb{Q}$ is not isomorphic to $\mathbb{Z}$ (as abelian groups), since $\mathbb{Z}$ is the unique infinite cyclic group up to isomorphism. In fact, every group homomorphism $\mathbb{Q} \to \mathbb{Z}$ is trivial! One way to see this is a consequence of the fact that $\mathbb{Q}$ is divisible, and $\mathbb{Z}$ is not. The following proof, mutatis mutandi, shows that for any divisible group G, every group homomorphism $\varphi\colon G \to \mathbb{Z}$ is trivial.
Suppose $\varphi\colon \mathbb{Q} \to \mathbb{Z}$ were a nontrivial group homomorphism. Then $\varphi(1) = z$ for some nonzero $z \in \mathbb{Z}$. But then $n\varphi(1/n) = \varphi(1) = z$ for every $n \in \mathbb{N}$, i.e. z has infinitely many divisors, which is impossible.

68 Problem 7.8

Let M be a free R-module which is finitely generated by $m_1, \ldots, m_k$ for some $k \in \mathbb{N}$ with basis $B := \{x_i\}_{i \in I}$. Any subset of B is R-linearly independent, so it suffices to find a finite spanning subset of B. Indeed, let B' be the finite subset of B which spans $\{m_1, \ldots, m_k\}$. Since $m_1, \ldots, m_k$ is a generating set for R, B' also spans R, hence is a finite basis for R.

69 Problem 7.9

(a) Define an R/I-module structure on M by setting $(r + I) \cdot m = rm$ for each $r + I \in R/I$. First, note that this operation is well-defined; suppose $r' + I = r + I$, i.e. $r' = r + i$ for some $i \in I$. Then since $IM = 0$,

$$(r' + I)m = r'm = (r + i)m = rm + im = rm = (r + I)m$$

Further, this R/I-scalar multiplication possesses the four properties specifying a module structure, which follows from the R-module structure on M:

(i) $(1+I)\cdot m = 1m = m$ for all $m \in M$

(ii) For all $r, r' \in R$ and $m \in M$

$$((r+I)(r'+I))\cdot m = (rr'+I)m = (rr')m = r(r'm) = (r+I)\cdot((r'+I)\cdot m)$$

(iii) For all $r, r' \in R$ and $m \in M$,

$$((r+I)+(r'+I))\cdot m = (r+r'+I)\cdot m = (r+r')m = rm+r'm = (r+I)\cdot m+(r'+I)\cdot m$$

(iv) For all $r \in R$ and $m, m' \in M$

$$(r+I)\cdot(m+m') = r(m+m') = rm+rm' = (r+I)\cdot m+(r+I)\cdot m'$$

(b) If M is an R-module, then M/IM is clearly I-torsion, and hence admits the R/I-module structure described in (a).

(c) Suppose M is a free R-module, and let $X \subset M$ be a basis. Let $I \subseteq R$ be an ideal, and let $\pi\colon M \to M/IM$ be the canonical projection homomorphism. We claim

$$\overline{X} = \{\pi(x) \mid x \in X \setminus IM\} \subseteq M/IM$$

is an R/I-basis for M. (Note that we must require $x \notin IM$, since any subset containing 0 cannot be linearly independent.)
First, we show $\overline{X}$ spans M/IM. Let $\overline{m} \in M/IM$ represent the equivalence class $\pi(m) = m+IM$, and let $\overline{r} \in R/I$ represent the equivalence class $r+I$. Since X is a basis for M over R, expand m as an R-linear combination of basis elements:

$$m = \sum_{x\in X} r_x \cdot x$$

Since π is an R-module homomorphism,

$$\overline{m} = \pi(m) = \pi\left(\sum_{x\in X} r_x \cdot x\right) = \sum_{x\in X} r_x\pi(x) = \sum_{x\in X} \overline{r_x}\cdot\overline{x}$$

where the last equality follows by the definition of the R/I-module structure on M/IM. Thus, $\overline{X}$ spans M/IM over R/I.
Now, we show that the elements of $\overline{X}$ are R/I-linearly independent. Let $\{\overline{x_i}\}_{i=1}^n$ be a finite subset of $\overline{X}$, and let $\{\overline{r_i}\}_{i=1}^n \subset R/I$ such that

$$\sum_{i=1}^n \overline{r_i}\cdot\overline{x_i} = \sum_{i=1}^n r_i\cdot\overline{x_i} = \overline{0}$$

Then $\sum_{i=1}^{n} r_i x_i \in IM$, so

$$\sum_{i=1}^{n} r_i x_i = \sum_{j=1}^{l} \alpha_j m_j$$

where $\alpha_j \in I, m_j \in M$ for each $j = 1, \ldots, l$. Since X is a basis for M, we may write

$$m_j = \sum_{x \in X} \beta_x^j \cdot x$$

whence

$$\sum_{i=1}^{n} r_i x_i = \sum_{j=1}^{l} \alpha_j \sum_{x \in X} \beta_x^j \cdot x$$

Note that every coefficient on the RHS expression is an element of I. But the expression of any element of M in terms of basis elements is unique, so we must have $r_i \in I$ for each $i = 1, \ldots, n$, whence $\overline{r_i} = \overline{0}$ for each i. This establishes the linear independence of $\overline{X}$ over R/I, so $\overline{X}$ is indeed an R/I-basis for M/IM.

(d) Let R be a commutative ring, and suppose R^n and R^m are isomorphic for some $n, m \in \mathbb{N}$. By Zorn's lemma, R has some maximal ideal I; since I is maximal, R/I is a field.
Let $k \in \mathbb{N}$. By part (a), R^k/IR^k has a natural structure of a left R/I-module (vector space). The dimension of any vector space is determined by the cardinality of any basis, so to compute $\dim_{R/I}(R^k/IR^k)$, it suffices to compute an R/I-basis for R^k/IR^k. Let $X = \{e_1, \ldots, e_n\}$ be the standard basis for R^n, i.e.

$$e_i = (0, 0, \underbrace{\ldots, 1, \ldots}_{i^{\text{th}} \text{ position}}, 0, 0)$$

We claim $e_i \notin IR^k$ for any $i = 1, \ldots, n$. To see this, suppose $e_i \in IR^k$ for some i. Then

$$e_i = \sum_{j=1}^{l} \alpha_j (r_{j,1}, r_{j,2}, \ldots, r_{j,n})$$

for some $l \in \mathbb{N}$, where $\alpha_j \in I$ for each $j = 1, \ldots, l$. We see

$$e_i = \sum_{j=1}^{l} \alpha_j (r_{j,1}, r_{j,2}, \ldots, r_{j,n}) = \left(\sum_{j=1}^{l} \alpha_j r_{j,1}, \ldots, \sum_{j=1}^{l} \alpha_j r_{j,n} \right)$$

whence

$$1 = \sum_{j=1}^{l} \alpha_j r_{j,i}$$

which implies $1 \in I$, a contradiction to the maximality of I. Hence, as defined in part (a), $\overline{X} = \{\overline{e_1}, \ldots, \overline{e_n}\}$ is an R/I-basis for R^k/IR^k. Thus, $\dim_{R/I}(R^k/IR^k) = k$.
Now, suppose $\alpha \colon R^n \to R^m$ is an R-module isomorphism, and let $\pi \colon R^m \to R^m/IR^m$

be the canonical projection homomorphism. Then $\pi \circ \alpha \colon R^n \to R^m/IR^m$ is a surjective R-module homomorphism, so $R^n/\ker(\pi \circ \alpha) \cong R^m/IR^m$ as R-modules, hence as R/I-modules (vector spaces).
Note that $\ker(\pi \circ \alpha) = \alpha^{-1}(IR^m) = I\alpha^{-1}(R^m) = IR^n$, since α^{-1} is an R-module homomorphism. Hence, if $R^n \cong R^m$, then there is an induced isomorphism of R/I-vector spaces $R^n/IR^n \cong R^m/IR^m$. Since $\dim_{R/I}(R^n/IR^n) = n, \dim_{R/I}(R^m/IR^m) = m$, we must have $n = m$.

70 Problem 7.10

We prove something more general: let R be a ring, and fix an element $r \in R$. Then there is a ring homomorphism $\mathbb{Z}[X] \to R$ with $f(X) = r$; in a (perhaps) more sophisticated formulation, the forgetful functor from Rings to Sets is represented by $\mathbb{Z}[X]$, i.e. there is a bijection of sets $\mathrm{Hom}(\mathbb{Z}[X], R) \cong R$. Define a map $\Phi \colon \mathbb{Z}[X] \to R$ by $\Phi(p(X)) = p(r)$, where if $p(X) = a_0 + a_1X + \cdots + a_nX^n$, then $p(r) = a_0 \cdot 1_R + a_1r + a_2r^2 + \cdots + a_nr^n$. Let $f(X) = a_0 + a_1X + \cdots + a_nX^n, g(X) = b_0 + b_1X + \cdots + b_mX^m \in \mathbb{Z}[X]$, and WLOG assume $n < m$. Then

$$\begin{aligned}\Phi(f+g) =& (a_0+b_0)\cdot 1_R + (a_1+b_1)r + \cdots + (a_n+b_n)r^n + b_{n+1}r^{n+1} + \cdots + b_mX^m \\ =& (a_0 \cdot 1_R + a_1r + \cdots + a_nr^n) + (b_0 \cdot 1_R + b_1r + \cdots + b_mr^m) \\ =& \Phi(f) + \Phi(g)\end{aligned}$$

$$\begin{aligned}\Phi(fg) =& \Phi\left(\sum_{1 \leqslant i \leqslant n, 1 \leqslant j \leqslant m} a_ib_jX^{i+j}\right) \\ =& \sum_{1 \leqslant i \leqslant n, 1 \leqslant j \leqslant m} a_ib_jr^{i+j} \\ =& (a_0 \cdot 1_R + a_1r + \cdots + a_nr^n)(b_0 \cdot 1_R + b_1r + \cdots + b_mr^m) \\ =& \Phi(f)\Phi(g)\end{aligned}$$

Finally, since $\Phi(1) = 1 \cdot 1_R = 1_R$, so Φ is a ring homomorphism satisfying $\Phi(X) = r$.
N.B.: There is a natural homomorphism of (cyclic) $\mathbb{Z}$-algebras $\mathbb{Z}[X] \to \mathbb{Z}[r]$; the map Φ defined above is the composition of this morphism with the inclusion $\mathbb{Z}[r] \hookrightarrow R$.
Now the problem is a simple consequence of the lemma we just proved. Let A be an abelian group, $f \in \mathrm{End}(A)$. By the result above, there is a ring homomorphism $\Phi \colon \mathbb{Z}[X] \to \mathrm{End}(A)$ with $\Phi(X) = f$. By problem 7.1(b), there is a $\mathbb{Z}[X]$-module structure on A with $p(X) \cdot a = \Phi(p(X))(a) = (p(f))(a)$, so in particular, $X \cdot a = f(a)$.

71 Problem 8.1

Let R be a PID, and let M be a torsion finitely generated R-module with invariant factors $d_1 \mid d_2 \mid \cdots \mid d_k$. By the structure theorem for finitely generated modules over a PID,

$$M \cong R/d_1R \oplus R/d_2R \oplus \cdots \oplus R/d_kR$$

as R-modules. Put $I = \{a \in R \mid aM = 0\}$. Since $d_i \mid d_k$ for each $i = 1, \ldots, k$, $d_k R \subseteq d_i R$ for each i, so $d_k(R/d_i R) = 0$ for each i. Hence, $d_k R \subseteq I$. On the other hand, since R is a PID, $I = xR$ for some $x \in R$. Since $xM = 0$, in particular $x(R/d_k R) = 0$, i.e. $xR \subseteq d_k R$, whence $I = xR = d_k R$.

72 Problem 8.2

Let A be an abelian group of order $300 = 2^2 \cdot 3 \cdot 5^2$. By the structure theorem for finitely generated modules over a PID, A can be expressed as the direct sum

$$A \cong \left(\bigoplus_{i=1}^{2} \mathbb{Z}/2^{r_i}\mathbb{Z}\right) \oplus \mathbb{Z}/3\mathbb{Z} \oplus \left(\bigoplus_{i=1}^{2} \mathbb{Z}/5^{q_i}\mathbb{Z}\right)$$

where $r_i, q_i \in \mathbb{N}$ such that $r_1 + r_2 = 2 = q_1 + q_2$. Hence, there are 4 abelian groups of order 300 up to isomorphism, listed below as:

$$\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/25\mathbb{Z}$$

$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/25\mathbb{Z}$$

$$\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}$$

$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}$$

73 Problem 8.3

Let N be the subgroup in $\mathbb{Z}^3$ generated by $(2, -2, 0), (0, 4, -4), (5, 0, -5)$. We want to compute the rank of N. Note that

$$\operatorname{rank}(N) = \operatorname{rank}(\mathbb{Z}^3) - \operatorname{rank}(\mathbb{Z}^3/N) = 3 - \operatorname{rank}(\mathbb{Z}^3/N)$$

since there is a short exact sequence $0 \to N \to \mathbb{Z}^3 \to \mathbb{Z}^3/N \to 0$, and rank of abelian groups is additive over short exact sequences. Thus, by the classification theorem for finitely generated modules over a PID, it suffices to compute the isomorphism type of $\mathbb{Z}^3/N$ by computing the Smith normal form of the matrix

$$\begin{pmatrix} 2 & 0 & 5 \\ -2 & 4 & 0 \\ 0 & -4 & -5 \end{pmatrix}$$

using elementary row and column operations. This will uniquely classify the free part of $\mathbb{Z}^3/N$, and thus the rank of $\mathbb{Z}^3/N$, whence we have determined the rank of N. We compute

$$\begin{pmatrix} 2 & 0 & 5 \\ -2 & 4 & 0 \\ 0 & -4 & -5 \end{pmatrix} \xrightarrow{R_2+R_1} \begin{pmatrix} 2 & 0 & 5 \\ 0 & 4 & 5 \\ 0 & -4 & -5 \end{pmatrix} \xrightarrow{R_3+R_2} \begin{pmatrix} 2 & 0 & 5 \\ 0 & 4 & 5 \\ 0 & 0 & 0 \end{pmatrix} \xrightarrow{R_2-R_1} \begin{pmatrix} 2 & -4 & 0 \\ 0 & 4 & 5 \\ 0 & 0 & 0 \end{pmatrix}$$

$$\xrightarrow{C_2+2C_1} \begin{pmatrix} 2 & 0 & 0 \\ 0 & 4 & 5 \\ 0 & 0 & 0 \end{pmatrix} \xrightarrow{C_3-C_2} \begin{pmatrix} 2 & 0 & 0 \\ 0 & 4 & 1 \\ 0 & 0 & 0 \end{pmatrix} \xrightarrow{C_2-4C_3} \begin{pmatrix} 2 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} \xrightarrow{C_2 \leftrightarrow C_3} \begin{pmatrix} 2 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

Thus, $\mathbb{Z}^3/N \cong \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, whence $\operatorname{rank}(\mathbb{Z}^3/N) = 1$, so $\operatorname{rank}(N) = 2$.

74 Problem 8.4

Let N be the subgroup in $\mathbb{Z}^3$ generated by $(3,-3,3),(0,6,-12),(9,0,-9)$. We want to compute the invariants factors of $\mathbb{Z}^3/N$. This amounts to computing the Smith normal form of the matrix

$$\begin{pmatrix} 3 & 0 & 9 \\ -3 & 6 & 0 \\ 3 & -12 & -9 \end{pmatrix}$$

using elementary row and column operations. We compute

$$\begin{pmatrix} 3 & 0 & 9 \\ -3 & 6 & 0 \\ 3 & -12 & -9 \end{pmatrix} \xrightarrow{R_2+R_1} \begin{pmatrix} 3 & 0 & 9 \\ 0 & 6 & 9 \\ 3 & -12 & -9 \end{pmatrix} \xrightarrow{R_3-R_2} \begin{pmatrix} 3 & 0 & 9 \\ 0 & 6 & 9 \\ 0 & -12 & -18 \end{pmatrix} \xrightarrow{C_3-3C_1} \begin{pmatrix} 3 & 0 & 0 \\ 0 & 6 & 9 \\ 0 & -12 & -18 \end{pmatrix}$$

$$\xrightarrow{R_3+2R_2} \begin{pmatrix} 3 & 0 & 0 \\ 0 & 6 & 9 \\ 0 & 0 & 0 \end{pmatrix} \xrightarrow{C_3-C_2} \begin{pmatrix} 3 & 0 & 0 \\ 0 & 6 & 3 \\ 0 & 0 & 0 \end{pmatrix} \xrightarrow{C_2-2C_3} \begin{pmatrix} 3 & 0 & 0 \\ 0 & 0 & 3 \\ 0 & 0 & 0 \end{pmatrix} \xrightarrow{C_2\leftrightarrow C_3} \begin{pmatrix} 3 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

Thus, the invariant factors of $\mathbb{Z}^3/N$ are given by $\mathrm{IF}(A) = \{3,3\}$.

75 Problem 8.5

Suppose M is a finitely generated torsion R-module. By the structure theorem for finitely generated modules over a PID, M is a finite direct sum of cyclic R-modules $R/p_i^{\alpha_i}R$ for some primes $p_1,\dots,p_n \in R$ and $\alpha_1,\dots,\alpha_n \in \mathbb{N}$. Put $p = \prod_i p_i^{\alpha_i}$.
Suppose that the elementary divisors of M are pairwise relatively prime; then the ideals $p_i^{\alpha_i}R$ and $p_j^{\alpha_j}R$ are comaximal for any $i \neq j$. By the Chinese Remainder Theorem,

$$\bigoplus_{i=1}^{n} R/p_i^{\alpha_i}R \cong R/pR$$

as both rings and R-modules, whence $M \cong R/pR$ is cyclic. On the other hand, suppose M is cyclic. By problem 7.2, $M \cong R/qR$ for some $q \in R$. Since R is a PID, we can factor qR uniquely as a product of ideals $(p_1^{\alpha_1}R)\cdots(p_k^{\alpha_k}R)$ for distinct prime elements $p_1,\dots,p_k$. The ideals $p_i^{\alpha_i}R, p_k^{\alpha_k}R$ are pairwise comaximal for $i \neq j$, so by the Chinese Remainder Theorem,

$$R/qR \cong \bigoplus_{i=1}^{n} R/p_i^{\alpha_i}R$$

as both rings and R-modules. By the uniqueness of the elementary divisor decomposition of M, we see that the factors $p_1^{\alpha_1},\dots,p_k^{\alpha_k}$ are the elementary divisors of M, and as already mentioned above, they are coprime.

76 Problem 8.6

Let R be a commutative ring, and consider R as a module over itself. Clearly, R is a free R-module. Let I be an ideal of R; then it is straightforward to see that I is a submodule of R. Suppose I is not principal; we claim that I is not free. Indeed, if I were free, then any basis for I over R must consist of at least two (nonzero) elements $x, y \in I$, since I is not principal. But then $yx + (-x)y = 0$ exhibits a nontrivial R-linear dependence between x and y, a contradiction.
Now take M to be your favorite commutative ring which is not a PID, and I to be some nonprincipal ideal, e.g. $R = \mathbb{Z}[X], I = \langle 2, X \rangle$ (see Problem 3.9).

77 Problem 8.7

Since an abelian group is a $\mathbb{Z}$-module, this follows immediately from 7.9(a) with $R = \mathbb{Z}, I = n\mathbb{Z}, M = A$.

78 Problem 8.8

Fix $n \in \mathbb{N}$, and let $I = n\mathbb{Z}$. If M is a finitely generated $\mathbb{Z}$-module such that $IM = 0$, then M is a (finitely generated) $\mathbb{Z}/n\mathbb{Z}$-module by Problem 8.7. On the other hand, if M is a finitely generated $\mathbb{Z}/n\mathbb{Z}$-module, then M is an I-torsion $\mathbb{Z}$-module; indeed, for any $m \in M$, $[1]_n \cdot m = m$, so

$$nm = \underbrace{1m + 1m + \cdots + 1m}_{n \text{ times}} = \underbrace{[1]_n \cdot m + [1]_n \cdot m + \cdots + [1]_n \cdot m}_{n \text{ times}} = [n]_n \cdot m = 0$$

Hence, every finitely generated I-torsion $\mathbb{Z}$-module is a finitely generated $\mathbb{Z}/n\mathbb{Z}$-module, and likewise every finitely generated $\mathbb{Z}/n\mathbb{Z}$-module is a finitely generated I-torsion $\mathbb{Z}$-module. Hence, it suffices to classify finitely generated I-torsion $\mathbb{Z}$-modules.
Let M be a finitely generated $\mathbb{Z}$-module. If M is I-torsion, then $\operatorname{rank}(M) = 0$, i.e. $M = M_{\text{tors}}$. Then

$$M \cong \mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \oplus \mathbb{Z}/p_2^{\alpha_2}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p_k^{\alpha_k}\mathbb{Z}$$

where $p_1, \ldots, p_k$ are (not necessarily distinct) primes, and $\alpha_1, \ldots, \alpha_k \in \mathbb{N}$. Since M is I-torsion, it is necessary that $p_i^{\alpha_i} \mid n$ for each $i = 1, \ldots, k$; equivalently, p_i must divide n for each i, and α_i must not exceed the highest power of p_i dividing n. This is also a sufficient condition for M to be I-torsion, so this concludes the classification of finitely generated I-torsion $\mathbb{Z}$-modules, and by the above thus classifies all finitely generated $\mathbb{Z}/n\mathbb{Z}$-modules.

79 Problem 8.9

Let $M = \mathbb{Z}/3\mathbb{Z}$, $N = \mathbb{Z}/2\mathbb{Z}$. Then M, N are $\mathbb{Z}$-modules such that $6M = 6N = 0$, whence M, N inherit the structure of $\mathbb{Z}/6\mathbb{Z}$-modules by Problem 8.7. By the Chinese Remainder Theorem, there is an isomorphism of $\mathbb{Z}$-modules $\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, and it is straightforward to see that this descends to an isomorphism of $\mathbb{Z}/6\mathbb{Z}$-modules. Hence, $M \oplus N$ is a free

$\mathbb{Z}/6\mathbb{Z}$-module; it remains to show that neither M nor N is free. This is clear, since every element of M is annihilated by $[3]_6$, so any nonempty basis for M is linearly dependent. Likewise, N is torsion, as every element is annihilated by $[2]_6$.

80 Problem 8.10

Let R be a PID, and let M be an R-module finitely generated by n elements. We claim that any submodule $N \subset M$ can be generated by at most n elements. Indeed, let $F = R^n$; consider the surjection $\rho\colon F \to M$ sending the standard idempotents of R^n to the generating elements of M. The preimage $G := \rho^{-1}(N) \subset F$ is a submodule of F, hence free on at most n generators (say) $x_1, \ldots, x_n$. Then $\rho|_G\colon G \to N$ is a surjection, so N is finitely generated by (at most) n elements, namely by the images $\rho(x_1), \ldots, \rho(x_n)$.

81 Problem 9.1

This is the case $n = 1$ of Problem 8.10. In any event, here is a direct argument: by Problem 7.2, every cyclic R-module M is isomorphic to R/I for some ideal I of R. Since R is a PID, R/I is also a PID. Indeed, every ideal J of R/I is the projection of an ideal xR of R containing I, whence $J = \overline{x}(R/I)$. Since the submodules of R/I are ideals of R/I, and every ideal of R/I is principal, every submodule of R/I is cyclic.

82 Problem 9.2

Let R be a PID, and let $a, b \in R$; put $M = R/aR \oplus R/bR$. Let $\{p_i\}_{i=1}^k$ be the set of primes dividing at least one of a, b, such that

$$a = \prod_{i=1}^k p_i^{\alpha_i} \qquad b = \prod_{i=1}^k p_i^{\beta_i}$$

where α_i, β_i are nonnegative integers for each $i = 1, \ldots, k$. Then the elementary divisors of M are given by

$$\mathrm{ED}(M) = \{p_i^{\alpha_i}, p_i^{\beta_i} \mid \alpha_i \neq 0, \beta_i \neq 0\}$$

whence M has two invariant factors given respectively by

$$c = \prod_{i=1}^k p_i^{\max(\alpha_i, \beta_i)} \qquad d = \prod_{i=1}^k p_i^{\min(\alpha_i, \beta_i)}$$

Thus, by the classification theorem for finitely generated modules over a PID, we have

$$R/aR \oplus R/bR \cong R/cR \oplus R/dR$$

But it is clear that c is the least common multiple of a and b, and d is the greatest common divisor of a and b, so we are done.

83 Problem 9.3

Let N be the subgroup in $\mathbb{Z}^3$ generated by $(-4,4,2),(16,-4,-8),(8,4,2),(12,0,-6)$. Using the classification theorem for finitely generated modules over a PID, we compute the invariant factors of $M = \mathbb{Z}^3/N$ by computing the Smith normal form of the matrix

$$\begin{pmatrix} -4 & 16 & 8 & 12 \\ 4 & -4 & 4 & 0 \\ 2 & -8 & 2 & -6 \end{pmatrix}$$

using elementary row and column operations. The nonunit diagonal entries will be the invariant factors of M. We compute

$$\begin{pmatrix} -4 & 16 & 8 & 12 \\ 4 & -4 & 4 & 0 \\ 2 & -8 & 2 & -6 \end{pmatrix} \xrightarrow{R_1 \leftrightarrow R_3} \begin{pmatrix} 2 & -8 & 2 & -6 \\ 4 & -4 & 4 & 0 \\ -4 & 16 & 8 & 12 \end{pmatrix} \xrightarrow{R_2 - 2R_1} \begin{pmatrix} 2 & -8 & 2 & -6 \\ 0 & 12 & 0 & 12 \\ -4 & 16 & 8 & 12 \end{pmatrix}$$

$$\xrightarrow{R_3+2R_1} \begin{pmatrix} 2 & -8 & 2 & -6 \\ 0 & 12 & 0 & 12 \\ 0 & 0 & 12 & 0 \end{pmatrix} \xrightarrow{C_2+4C_1} \begin{pmatrix} 2 & 0 & 2 & -6 \\ 0 & 12 & 0 & 12 \\ 0 & 0 & 12 & 0 \end{pmatrix} \xrightarrow{C_3-C_1} \begin{pmatrix} 2 & 0 & 0 & -6 \\ 0 & 12 & 0 & 12 \\ 0 & 0 & 12 & 0 \end{pmatrix}$$

$$\xrightarrow{C_4+3C_1} \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 12 & 0 & 12 \\ 0 & 0 & 12 & 0 \end{pmatrix} \xrightarrow{C_4-C_2} \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 12 & 0 & 0 \\ 0 & 0 & 12 & 0 \end{pmatrix}$$

Thus, the invariant factors of M are

$$\mathrm{IF}(M) = \{2, 12, 12\}$$

84 Problem 9.4

Let A be the matrix

$$\begin{pmatrix} -2 & 0 & 0 \\ -1 & -4 & -1 \\ 2 & 4 & 0 \end{pmatrix}$$

We want to compute the rational canonical form of A. To do so, it suffices to compute the Smith normal form of the associated matrix $X \cdot I_3 - A$. The rational canonical form of A is then given by the block diagonal matrix whose block diagonal entries are the companion matrices (in order) of the invariant factors of A. We compute

$$X \cdot I_3 - A = \begin{pmatrix} X+2 & 0 & 0 \\ 1 & X+4 & 1 \\ -2 & -4 & X \end{pmatrix} \xrightarrow{R_1 \leftrightarrow R_2} \begin{pmatrix} 1 & X+4 & 1 \\ X+2 & 0 & 0 \\ -2 & -4 & X \end{pmatrix}$$

$$\xrightarrow{R_2-(X+2)R_1} \begin{pmatrix} 1 & X+4 & 1 \\ 0 & (-X+2)(X+4) & -(X+2) \\ -2 & -4 & X \end{pmatrix} \xrightarrow{R_3+2R_1} \begin{pmatrix} 1 & X+4 & 1 \\ 0 & -(X+2)(X+4) & -(X+2) \\ 0 & 2X+4 & X+2 \end{pmatrix}$$

$$\xrightarrow{C_3-C_1} \begin{pmatrix} 1 & X+4 & 0 \\ 0 & -(X+2)(X+4) & -(X+2) \\ 0 & 2(X+2) & X+2 \end{pmatrix} \xrightarrow{C_2-(X+4)C_1} \begin{pmatrix} 1 & 0 & 0 \\ 0 & (-X+2)(X+4) & -(X+2) \\ 0 & 2(X+2) & X+2 \end{pmatrix}$$

$$\xrightarrow{C_2 \leftrightarrow C_3} \begin{pmatrix} 1 & 0 & 0 \\ 0 & -(X+2) & -(X+2)(X+4) \\ 0 & X+2 & 2(X+2) \end{pmatrix} \xrightarrow{R_2+R_3} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -(X+2)(X+4)+2(X+2) \\ 0 & X+2 & 2(X+2) \end{pmatrix}$$

$$\xrightarrow{C_3-2C_2} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -(X+2)(X+2) \\ 0 & X+2 & 0 \end{pmatrix} \xrightarrow{R_3 \leftrightarrow R_2} \begin{pmatrix} 1 & 0 & 0 \\ 0 & X+2 & 0 \\ 0 & 0 & -(X+2)(X+2) \end{pmatrix}$$

$$\xrightarrow{-1 \cdot R_3} \begin{pmatrix} 1 & 0 & 0 \\ 0 & X+2 & 0 \\ 0 & 0 & (X+2)(X+2) \end{pmatrix}$$

Hence, the invariant factors of A are $\{X+2, (X+2)^2\}$. The companion matrices for these factors are given by

$$C(x+2) = (-2)$$

$$C((x+2)^2) = C(x^2+4x+4) = \begin{pmatrix} 0 & -4 \\ 1 & -4 \end{pmatrix}$$

So the rational canonical form of A is given by

$$\mathrm{RCF}(A) = \begin{pmatrix} -2 & 0 & 0 \\ 0 & 0 & -4 \\ 0 & 1 & -4 \end{pmatrix}$$

85 Problem 9.5

Let

$$A = \begin{pmatrix} 2i & 1 \\ 1 & 0 \end{pmatrix}$$

We want to find the Jordan canonical form of A over $\mathbb{C}$. To do so, we must compute the elementary divisors of A, which will uniquely determine the Jordan blocks in the Jordan canonical form of A up to permutation. To find the elementary divisors of A, we will compute the invariant factors of A by reducing $X \cdot I_2 - A$ to Smith normal form, as follows:

$$X \cdot I_2 - A = \begin{pmatrix} X-2i & -1 \\ -1 & X \end{pmatrix} \xrightarrow{C_1 \leftrightarrow C_2} \begin{pmatrix} -1 & X-2i \\ X & -1 \end{pmatrix} \xrightarrow{R_2+XR_1} \begin{pmatrix} -1 & X-2i \\ 0 & X(X-2i)-1 \end{pmatrix}$$

$$\xrightarrow{C_2+(X-2i)C_1} \begin{pmatrix} 1 & 0 \\ 0 & (X-i)^2 \end{pmatrix}$$

Thus, the invariant factors of A are given by $\mathrm{IF}(A) = \{(X-i)^2\}$. Since A has only one invariant factor, the elementary divisors of A are given by $\mathrm{ED}(A) = \{(X-i)^2\}$, whence the Jordan canonical form of A is composed of one Jordan block $J(i,i)$, i.e.

$$\mathrm{JCF}(A) = \begin{pmatrix} i & 1 \\ 0 & i \end{pmatrix}$$

86 Problem 9.6

Throughout this problem, for any matrix A, let $P_A(X)$ denote the characteristic polynomial of A, and $m_A(X)$ the minimal polynomial of A.

(a) Let A, B be 2×2 matrices which are not multiples of the identity. Suppose A and B are similar, i.e. there is an (invertible) 2×2 matrix P such that $A = PBP^{-1}$. Then

$$\begin{aligned} P_B(X) &= \det(X \cdot I_2 - B) \\ &= \det(P)\det(X \cdot I_2 - B)\det(P^{-1}) \\ &= \det(P(X \cdot I_2 - B)P^{-1}) \\ &= \det(X \cdot I_2 - PBP^{-1}) \\ &= \det(X \cdot I_2 - A) \\ &= P_A(X) \end{aligned}$$

Now instead suppose that $P_A(X) = P_B(X)$. It suffices to show that A and B must have the same rational canonical form, i.e. that A and B have the same invariant factors, since A and B are both similar to their respective rational canonical forms. Let $f_1, f_2, \ldots, f_r$ be the invariant factors of A, where we recall that $f_r = m_A(X)$. Since A is not a scalar matrix, $m_A(X)$ has degree at least 2; since $m_A(X)$ divides $P_A(X)$ and both are monic, $m_A(X) = P_A(X)$. By the product condition $P_A(X) = f_1 f_2 \cdots f_r$, this forces $r = 1$ with $\mathrm{IF}(A) = \{m_A(X)\} = \{P_A(X)\}$; likewise, by identical reasoning, $\mathrm{IF}(B) = \{P_B(X)\}$, so A and B have the same invariant factors, and are therefore similar.

(b) Let A and B be 3×3 matrices. If A and B are similar with $A = PBP^{-1}$, the same proof above shows $P_A(X) = P_B(X)$. Note that

$$m_B(A) = m_B(PBP^{-1}) = Pm_B(B)P^{-1} = 0$$

so $m_A(X) \mid m_B(X)$. Likewise, $m_A(B) = 0$, so $m_B(X) \mid m_A(X)$, whence $m_A(X)$ and $m_B(X)$ agree up to some unit; $m_A(X)$ and $m_B(X)$ forces $m_A(X) = m_B(X)$.
Suppose A and B have the same characteristic and the same minimal polynomials. As above, it suffices to prove that the invariant factors of A and B agree. Let $f_1, f_2, \ldots, f_r$ be the invariant factors of A, with $f_r = m_A(X)$. Since $\deg(P_A(X)) = 3$, $\deg(m_A(X)) \leqslant 3$. Suppose $\deg(m_A(X)) = 1$; since $f_1 \mid f_2 \mid \cdots \mid f_r$ and $P_A(X) = f_1 f_2 \cdots f_r$, degree considerations show that $\mathrm{IF}(A) = \{m_A(X), m_A(X), m_A(X)\}$. Similarly, $m_A(X) = m_B(X)$ forces $\mathrm{IF}(B) = \{m_B(X), m_B(X), m_B(X)\} = \mathrm{IF}(A)$, so this proves the claim. If $\deg(m_A(X)) = 3$, then as above, $P_A(X) = m_A(X) = m_B(X) = P_B(X)$ and $\mathrm{IF}(A) = \{m_A(X)\} = \{m_B(X)\} = \mathrm{IF}(B)$, so we again have $\mathrm{IF}(A) = \mathrm{IF}(B)$.
Hence, it remains to demonstrate our claim in the case $\deg(m_A(X)) = 2$. In this case, degree considerations from the condition $P_A(X) = f_1 f_2 \cdots f_r$ show that A has two invariant factors $f_1, f_2 = m_A(X)$, and likewise B has invariant factors $g_1, g_2 = m_B(X)$. Since $f_1 f_2 = P_A(X) = P_B(X) = g_1 g_2$ and $f_2 = m_A(X) = m_B(X) = g_2$, we have by cancellation $f_1 = g_1$, so once again $\mathrm{IF}(A) = \mathrm{IF}(B)$.

87 Problem 9.7

Let $P_A(X)$ be the characteristic polynomial of A, and let $m_A(X)$ be the characteristic polynomial of A. By the Cayley-Hamilton theorem, $P_A(X) = 0$, whence $m_A(X) \mid P_A(X)$. Thus, every irreducible divisor of $m_A(X)$ must also be an irreducible divisor of $P_A(X)$.
Let $f_1, f_2, \ldots, f_r$ be the invariant factors of A, where we recall that $f_r = m_A(X)$. We additionally recall that $P_A(X) = f_1 f_2 \cdots f_r$. Let $q(x)$ be an irreducible divisor of $P_A(X)$. Then $q(x)$ divides $f_i(X)$ for some $i = 1, \ldots, r$. If $i \neq r$, then by the divisibility condition on the invariant factors of A, $f_i \mid f_r = m_A$, so $q(x)$ also divides $m_A(X)$. Thus, $P_A(X)$ has the same irreducible divisors as $m_A(X)$.

88 Problem 9.8

Let A be a matrix with entries in a field F. Suppose the elementary divisors of A are all linear. Then every companion matrix of an elementary divisor of A is one dimensional, so the rational canonical form of A is diagonal. Thus, A is similar to a diagonal matrix.
Now suppose A is similar to a diagonal matrix $D = \operatorname{diag}(d_1, \ldots, d_n)$. Then the elementary divisors of A are the equal (up to rearrangement) to the elementary divisors of D. Note for any polynomial $p \in F[X]$, $p(D) = \operatorname{diag}(p(d_1), \ldots, p(d_n))$. Hence, let $\{e_1, \ldots, e_k\}$ be the distinct elements of $\{d_1, \ldots, d_n\}$. Then $p(X) = (X - e_1)(X - e_2) \cdots (X - e_k)$ annihilates D, so the minimal polynomial $m_D(X)$ of D divides p. Every elementary divisor of D is of the form $q_i(x)^{k_i}$, where $q_i(x)$ is a monic irreducible, $k_i \in \mathbb{N}$ and $q_i(x)^{k_i} \mid m_D(X)$. Since $m_D(x)$ is a product of distinct linear polynomials, every such $q_i(x)$ must be linear with $k_i = 1$, so the elementary divisors of D are linear polynomials, whence the elementary divisors of A are all linear.

89 Problem 9.9

Let $P_A(X)$ be the characteristic polynomial of A, and $m_A(X)$ be the minimal polynomial of A. Since $A^N = 0$ for some $N \in \mathbb{N}$, the polynomial $f(X) = X^N$ annihilates A, so $m_A \mid f$. Since $m_A(X) \mid P_A(X)$, $\deg(m_A(X)) \leqslant \deg(P_A(X)) = n$, so X^k annihilates A and therefore so does X^n. Further, since every invariant factor of A divides $m_A(X)$, the invariant factors of A are powers of X.

90 Problem 9.10

Let A be a matrix with entries in a field. Then the invariant factors of A are determined by the Smith normal form D of $X \cdot I_n - A$, which can be obtained by applying elementary row and column operations to $X \cdot I_n - A$. These elementary operations can be written as invertible matrices P and P' such that $D = P(X \cdot I_n - A)P'$. Now, since D is a diagonal matrix, $D^t = D$, so

$$D = D^t = (P')^t (X \cdot I_n - A)^t P^t = (P')^t (X \cdot I_n - A^t) P^t$$

Hence, $X \cdot I_n - A^t$ has the same Smith normal form as $X \cdot I_n - A$, whence A and A^t have the same invariant factors and are therefore similar. Put another way, by applying the elementary row and column operations which reduce $X \cdot I_n - A$ to its Smith normal form D to $X \cdot I_n - A^t$ as elementary column and row operations respectively, we reduce $X \cdot I_n - A^t$ to D.