Problem §1 (3.40) Let R be a commutative ring.

(a) Let I be an ideal of R. Prove that the map

$$\pi : R \longrightarrow R/I, a \longmapsto a + I$$

is a surjective ring homomorphism.

(b) Let I, J be ideals of R. Prove that the map

$$\phi : R \longrightarrow R/I \times R/J, a \longmapsto (a + I, a + J)$$

is a homomorphism. What is its kernel? Give an example where it is surjective, and give an example where it is not.

Solution:

(a) Let I be an ideal of R, with π as defined above.

- $\pi(1_R) = 1 + I = 1_{R/I}$ (since for any $a + I \in R/I$, we have $(a + I)(1 + I) = (a \cdot 1 + I) = a + I$).
- Let $a, b \in R$. Then $\pi(a + b) = (a + b) + I = (a + I) + (b + I) = \pi(a) + \pi(b)$, by the definition of coset addition.
- $\pi(ab) = ab + I = (a + I)(b + I) = \pi(a)\pi(b)$, by the definition of coset multiplication.

Hence π is a ring homomorphism. Surjectivity is almost trivial: let $a + I \in R/I$. Since $a \in R$, we have $\pi(a) = a + I$.

(b) Let I, J be ideals of R, with ϕ as defined above.

- $\phi(1_R) = (1+I, 1+J) = 1_{R/I\times R/J}$ (since $(a+I, a+J)(1+I, 1+J) = (a\cdot1+I, a\cdot1+J) = (a+I, a+J)$).
- $\phi(a+b) = ((a+b)+I, (a+b)+J) = ((a+I)+(b+I), (a+J)+(b+J)) = (a+I, a+J)+(b+I, b+J) = \phi(a) + \phi(b)$ by the definition of coset addition and addition in product rings.
- $\phi(ab) = (ab + I, ab + J) = ((a + I)(b + I), (a + J)(b + J)) = (a + I, a + J)(b + I, b + J) = \phi(a)\phi(b)$ by the definition of coset multiplication and multiplication in product rings.

Hence ϕ is a ring homomorphism. Suppose $\phi(a) = 0_{R/I\times R/J} = (0 + I, 0 + J)$. $a + I = 0 + I$ whenever $a \in I$, and $a + J = 0 + J$ whenever $a \in J$. Thus a must be in both I and J, and so $\ker(\phi) = I \cap J$ (and thus $I \cap J$ is also an ideal of R, since the kernel of any ring homomorphism $\phi : R \to R'$ is an ideal of R).

Consider $\phi : \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. Then

$$\phi(0) = (0, 0),\ \phi(1) = (1, 1),\ \phi(2) = (0, 2),\ \phi(3) = (1, 0),\ \phi(4) = (0, 1),\ \phi(5) = (1, 2),$$

so ϕ is surjective. Now consider $\phi : \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. Clearly, $\phi(n) \neq (1, 2)$ for any $n \in \mathbb{Z}$; similarly with $(1, 0)$ (since no number is both odd and even); thus ϕ is not surjective.

Problem §2 (3.41) Let I be the principal ideal $(x^2 + 1)\mathbb{R}[x]$ of $\mathbb{R}[x]$. Prove that the map

$$\phi : \mathbb{R}[x]/I \longrightarrow \mathbb{C},\ \phi(f(x) + I) = f(i)$$

is a well-defined isomorphism.

Solution: Consider the evaluation map $E_i : \mathbb{R}[x] \to \mathbb{C},\ E_i(f(x)) = f(i)$. We first show that E_i is a ring homomorphism:

- $E_i(1) = 1$

- $E_i(a(x)+b(x)) = a(i)+b(i) = E_i(a(x))+E_i(b(x))$
- $E_i(a(x)b(x)) = a(i)b(i) = E_i(a(x))E_i(b(x))$

Next, consider $E_i(a(x)) = 0$. For $a(i) = 0$, $a(x)$ must have i as a root; in other words, $a(x) = (x^2+1)b(x)$ for some $b(x) \in \mathbb{R}[x]$. Thus $\ker(E_i) = (x^2+1)\mathbb{R}[x] = I$, and so by Proposition 3.31b, $\overline{E_i} : \mathbb{R}[x]/I \to \mathbb{C}$ is a well-defined, injective ring homomorphism. It remains to show that E_i is surjective; but that's easy, since for any $a+bi \in \mathbb{C}$, we can construct a polynomial $f(x) = a+bx \in \mathbb{R}[x]$ such that $f(i) = a+bi$. Hence E_i is surjective, and so $\overline{E_i} = \phi : \mathbb{R}[x]/I \to \mathbb{C}$ is a well-defined isomorphism.

Problem §3 (3.42) Let R be a commutative ring and let I, J be ideals of R.

(a) Prove that the intersection $I \cap J$ is an ideal of R.

(b) Prove that the *ideal sum*

$$I + J = \{a+b \mid a \in I, b \in J\}$$

is an ideal of R.

(c) The *ideal product* of two ideals

$$IJ = \{\sum_{i=1}^{n} a_i b_i \mid n \geq 1,\ a_i \in I,\ b_i \in J\}.$$

Prove that IJ is an ideal of R.

(d) Let $R = \mathbb{Z}[x]$, and let $I = 2\mathbb{Z}[x] + x\mathbb{Z}[x],\ J = 3\mathbb{Z}[x] + x\mathbb{Z}[x]$. Prove that the set of products $\{ab \mid a \in I, b \in J\}$ is not an ideal.

(e) On the other hand, prove in general that if either I or J is a principal ideal, then the set of products $\{ab \mid a \in I,\ b \in J\}$ is an ideal.

Solution:

(a) (Proven in 3.40b) Let $\phi : R \to R/I \times R/J$, $\phi(a) = (a+I, a+J)$. From 3.40b, we get that $\ker(\phi) = I \cap J$, and since any kernel of a ring homomorphism $\phi : R \to R'$ is an ideal of R, $I \cap J$ is an ideal of R.

Alternatively, let $a, b \in I \cap J$. Since $a, b \in I$, $a+b \in I$; similarly, $a, b \in J$ implies $a+b \in J$. Hence $a+b \in I \cap J$. Additionally, $a \in I$ implies $ra \in I$ for any $r \in R$, and analogously for J; hence $ra \in I \cap J$, and so $I \cap J$ is an ideal of R.

(b) Let $\alpha = a_1 + b_1,\ \beta = a_2 + b_2 \in I + J$. Thus by the commutativity of addition in R,

$$\alpha + \beta = (a_1 + b_1) + (a_2 + b_2) = (a_1 + a_2) + (b_1 + b_2),$$

and since $a_1 + a_2 \in I,\ b_1 + b2 \in J$, we get $(a_1 + a_2) + (b_1 + b_2) = \alpha + \beta \in I + J$. For $\alpha = a + b \in I + J$, $a \in I, b \in J$ implies $ra \in I,\ rb \in J$ for any $r \in R$. Thus

$$r\alpha = r(a+b) = ra + rb \in I + J,$$

and so $I + J$ is an ideal.

(c) Let $\alpha, \beta \in IJ$, where $\alpha = \sum_{i=1}^{n} a_i b_i,\ \beta = \sum_{j=1}^{m} a'_j b'_j$. Then

$$\alpha + \beta = \sum_{i=1}^{n} a_i b_i + \sum_{j=1}^{m} a'_j b'_j = \sum_{i=1}^{n+m} a_i b_i \in IJ,$$

since each individual summand $a_i b_i$ has $a_i \in I,\ b_i \in J$ (pardon my slight abuse of notation). Moreover, for any $r \in R$, $ra \in I$; thus $r\alpha = r\sum_{i=1}^{n} a_i b_i = \sum_{i=1}^{n} (ra_i) b_i \in IJ$. Thus IJ is an ideal of R.

(d) First, consider $2 \in I,\ 3 \in J$. Then $6 \in \{ab \mid a \in I, b \in J\}$. Similarly, $x \in I,\ x \in J$, so $x^2 \in \{ab \mid a \in I, b \in J\}$. But clearly $x^2 + 6$ has no integer (or, for that matter, real) roots, and so no such $a(x) \in \mathbb{Z}[x],\ b(x) \in \mathbb{Z}[x]$ satisfies $a(x)b(x) = x^2 + 6$; thus $x^2 + 6 \notin \{ab \mid a \in I, b \in J\}$, and so $\{ab \mid a \in I, b \in J\}$ is not an ideal.

(e) Suppose without loss of generality that I is a principal ideal. Then for some $c \in R$, $I = cR$, and so any $a_\in I$ can be rewritten as $a = cr$ for some $r \in R$. Consider $\{ab \mid a \in I, b \in J\}$. For any $a_1, a_2 \in I,\ b_1, b_2 \in J$, we have

$$a_1b_1 + a_2b_2 = cr_1b_1 + cr_2b_2 = cb_1' + cb_2' = c(b_1' + b_2') \in IJ,$$

where $b_i' = rb_i$, since $b_1', b_2' \in J$ and ideals are closed under addition. Moreover, for any $r \in R$,

$$rab = r(r_1c)b = (rr_1c)b \in IJ,$$

since $rr_1 \in R$ by closure of multiplication, and for any $r \in R$, $rc \in I$; and so $rr_1c \in I,\ b \in J$. Hence $\{ab \mid a \in I,\ b \in J\}$ is an ideal (and commutativity implies $ab = ba$, so the proof with J as the principal ideal follows analogously).

Problem §4 (3.45) Let $I = 2\mathbb{Z}[x] + x\mathbb{Z}[x]$ be a subset of $\mathbb{Z}[x]$.

(a) Prove that I is an ideal of $\mathbb{Z}[x]$.

(b) Prove that $I \neq \mathbb{Z}[x]$.

(c) Prove that I is not a principal ideal.

(d) Prove that I is a maximal ideal of $\mathbb{Z}[x]$.

Solution:

(a) Let $I = 2\mathbb{Z}[x] + x\mathbb{Z}[x]$. Let $2a_1(x) + xb_1(x),\ 2a_2(x) + xb_2(x) \in I$. Then $2a_1(x) + xb_1(x) + 2a_2(x) + xb_2(x) = 2(a_1(x) + a_2(x)) + x(b_1(x) + b_2(x)) = 2a'(x) + xb'(x) \in I$, since $a'(x), b'(x) \in \mathbb{Z}[x]$ by closure of addition.

Let $c(x) \in \mathbb{Z}[x]$. Then $c(x)(2a(x) + xb(x)) = 2c(x)a(x) + xc(x)b(x) \in I$ by closure of multiplication. Thus I is an ideal.

(b) Consider $1 \in \mathbb{Z}[x]$. $1 \notin I$, since we need $a(x) = a_0,\ b(x) = 0 \in \mathbb{Z}[x]$; but all coefficients of $\mathbb{Z}[x]$ are integers, so no such $a_0 \in \mathbb{Z}$ yields $2a_0 = 1$.

(c) Consider $x^2+2, x^2+4 \in I$ (select $a_1(x) = 1,\ a_2(x) = 2; b(x) = x$ for $a_1(x), a_2(x), b(x) \in \mathbb{Z}[x]$). Suppose there exists some $c(x) \in \mathbb{Z}[x]$ such that $I = c(x)\mathbb{Z}[x]$; that is, for any $a(x) \in I$, $a(x) = c(x)d(x)$ for some $d(x) \in \mathbb{Z}[x]$. In particular, we have

$$x^2 + 2 = c(x)d(x)$$
$$x^2 + 4 = c(x)d'(x).$$

Since x^2+2 has no real roots, we need either $c(x) = 1, d(x) = x^2+2$ or $c(x) = x^2+2, d(x) = 1$. Clearly, $c(x) \neq 1$, since $I \neq \mathbb{Z}[x]$, so suppose $c(x) = x^2 + 2$. Then for some $d'(x) \in \mathbb{Z}[x]$, $x^2 + 4 = (x^2+2)d'(x)$. Clearly, no such $d'(x)$ exists (since both have same degrees, we need $d'(x) = a_0$ and $a_0x^2 = x^2,\ 2a_0 = 4$; but no such a_0 satisfies both $a_0 = 1$ and $a_0 = 2$). Hence no $c(x) \in \mathbb{Z}[x]$ successfully generates both $x^2 + 2$ and $xsr + 4$, and so I is not a principal ideal.

(d) Suppose $I \subsetneq J \subseteq R = \mathbb{Z}[x]$ for some ideal J of R. Let $a(x) \in J,\ a(x) \notin I$.

If $a(x) = a_0 \in \mathbb{Z}[x]$ is a constant, then we must have $a_0 \notin 2\mathbb{Z}$ (if $a_0 \in 2\mathbb{Z}$, then we can take $a'(x) = \frac{a_0}{2}$, and so $a(x) = \frac{2a_0}{2} = 2a'(x) \in I$, a contradiction). Thus a_0 must be odd; i.e. $a_0 = 2n + 1 \in 1 + 2\mathbb{Z}$. But then, note that $2n \in I$ (since we can set $a(x) = n,\ b(x) = 0$ to get $2n \in I$); and since J is an ideal, and $a_0 = 2n+1 \in J$, $2n \in I \subset J$, we have $2n+1-2n = 1 \in J$. Hence $1 \in J$, but then for every $r \in R$, we have $r = r \cdot 1 \in J$ (by ideal properties); hence $J = R$.

If $a(x)$ is a polynomial of degree ≥ 1 (that is, $a(x)$ has at least 1 "x" variable), then $a(x) = a_0 + a_1 x + \ldots + a_n x^n$. But then $a(x) = a_0 + x(a_1 + \ldots + a_n x^{n-1}) = a_0 + xa'(x)$, where $a'(x) = a_1 + \ldots + a_n x^{n-1} \in \mathbb{Z}[x]$. Thus, if $a(x) \notin I$, we must have a_0 odd; but then, from above, if a_0 odd, then $J = R$.

Thus, in either case, if $I \subsetneq J \subseteq R$, then $J = R$. Thus I is a maximal ideal.

Remark 1. It seems that for any $a(x) \in J$, there are really only two cases: either a_0 even, or a_0 odd. $a(x)$ being a polynomial is pretty much irrelevant, since if its degree ≥ 1, then we can always factor out x to achieve a new polynomial of the form $a_0 + xb(x)$; which again is dependent on the parity of a_0. Thus, it seems that $\mathbb{Z}[x]/(2\mathbb{Z}[x] + x\mathbb{Z}[x])$ is isomorphic to $\mathbb{Z}/2\mathbb{Z}$. Indeed, since $\mathbb{Z}[x]/(2\mathbb{Z}[x] + x\mathbb{Z}[x])$ only has two elements (all elements of J with a_0 the same parity are in the same congruence class, and there are only two parities), $0 + I$ and $1 + I$ depending on the parity of a_0, we can easily construct an isomorphism between $\mathbb{Z}[x]/(2\mathbb{Z}[x] + x\mathbb{Z}[x])$ and $\mathbb{Z}/2\mathbb{Z}$.

Moreover, I suspect this could be generalized to any $I = p\mathbb{Z}[x] + x\mathbb{Z}[x]$, where $p \in \mathbb{Z}$ is a prime. Let $I \subsetneq J \subseteq R$, if $a(x) \in J, a(x) \notin I$, then we need $a_0 \not\equiv 0 \mod p$. The $x\mathbb{Z}[x]$ essentially causes any x^n to vanish, so we only really need to focus on a_0; and by Fermat's Little Theorem, since p is prime, if $a_0 \not\equiv 0 \mod p$, then $a_0^{p-1} \equiv 1 \mod p$, so $1 \in J$, and so $J = R$. Moreover, any $a_0 \equiv a_0'$ mod p are in the same congruence class $\mod I$. Thus, any $I = p\mathbb{Z}[x] + x\mathbb{Z}[x]$ is a maximal ideal, and $\mathbb{Z}[x]/(p\mathbb{Z}[x] + x\mathbb{Z}[x]) \cong \mathbb{Z}/p\mathbb{Z}$.

Problem §5 (3.46)

(a) Let $m \neq 0$ be an integer. Prove that the ideal $m\mathbb{Z}$ is a maximal ideal (and hence also a prime ideal) if and only if $|m|$ is a prime number in the usual sense of primes in $\mathbb{Z}$.

(b) Let F be a field, and let $a, b \in F$ with $a \neq 0$. Prove that the principal ideal $(ax+b)F[x]$ is a maximal ideal of the polynomial ring $F[x]$.

(c) Let F be a field with characteristic not equal to 2, and let $c \in F$ be an element with the property that c is not the square of any element in F. Prove that the ideal $(x^2 - c)F[x]$ is a maximal ideal of the polynomial ring $F[x]$.

Solution:

(a) Suppose $|m| \in \mathbb{Z}$ is a prime. Then by Proposition 3.17, $\mathbb{Z}/m\mathbb{Z}$ is a field, and thus, by Theorem 3.40, $m\mathbb{Z}$ is a maximal (and prime) ideal.

Conversely, suppose $m\mathbb{Z}$ is a maximal ideal, and suppose m is composite. Then $ab = m$ for some $a, b \in \mathbb{Z}, 1 < a, b < m$. But then $m\mathbb{Z} \subset a\mathbb{Z} \subset \mathbb{Z}$ (since $a \notin m\mathbb{Z}$, but $m = ab \in a\mathbb{Z}$; moreover, $a - 1 \notin a\mathbb{Z}$, but $a - 1 \in \mathbb{Z}$), and so $m\mathbb{Z}$ is not maximal, a contradiction. Thus m must be prime.

Alternatively, suppose $m\mathbb{Z}$ is a prime ideal. Then for any $a, b \in \mathbb{Z}$, if $ab \in m\mathbb{Z}$, then $a \in m\mathbb{Z}$ or $b \in m\mathbb{Z}$. Suppose m is composite. Then $m = ab$ for some $a, b \in \mathbb{Z}$, $1 < a, b < m$; but then $ab = m \in m\mathbb{Z}$, so either $a \in \mathbb{Z}$ or $b \in \mathbb{Z}$. But that's not possible, since $a \not\equiv 0 \mod m$ and $b \not\equiv 0 \mod m$ (neither a nor b are multiples of m, by construction); thus m must be prime.

(b) Let $I = (ax+b)F[x]$, and let $a(x) \in F[x]$. If $a(x) \notin I$, then $a(x)$ is not a multiple of $ax+b$; that is,

$$a(x) = q(x)(ax+b) + r(x),$$

where $q(x),\ r(x) \in F[x]$, and $0 \leq$ the degree of $r(x) <$ the degree of $ax+b$ by the Division Algorithm. But the degree of $ax+b = 1$, so $r(x)$ has degree 0. In other words, all cosets of I in $F[x]/I$ are of the form $\{b_0 + I \mid b_0 \in F\}$. $b_0 \neq 0$, since otherwise $b_0 + I = I$, a contradiction of not being a multiple; but since $b_0 \in F$, and F is a field, all non-zero elements have a multiplicative inverse, so for some $b_0^{-1} \in F$, we have $(b_0 + I)(b_0^{-1} + I) = 1 + I = 1_{F[x]/I}$. Hence every non-zero coset has an inverse, and so $F[x]/(ax+b)F[x]$ is a field. By Theorem 3.40, $(ax+b)F[x]$ is therefore a maximal ideal.

(c) Let $I = (x^2 - c)F[x]$. For some $a(x) \in F[x]$, let $a(x) + I \in F[x]/I$ be a non-zero coset of I; then $a(x) \notin I$, so $a(x)$ is not a multiple of $x^2 - c$; in other words, for any $q(x) \in F[x]$, $q(x)(x^2 - c) \neq a(x)$.

We then make one observation:

- If $p(x)$ divides $x^2 - c$ for some $p(x) \in F[x]$, then either $p(x) = k$ or $p(x) = k(x^2 - c)$ for some $k \in F$. Clearly, these two work:

$$\frac{x^2 - c}{k} = \frac{1}{k}(x^2 - c) \in F[x], \text{ and } \frac{x^2 - c}{k(x^2 - c)} = \frac{1}{k} \in F[x].$$

We claim that only these two polynomials work. Clearly, any $p(x)$ with degree ≥ 2 doesn't work, so consider $a_1x + b_1 \in F[x]$. Then

$$\frac{x^2 - c}{a_1x + b_1}.$$

implies

$$(a_1x + b_1)(a_2x + b_2) = a_1a_2x^2 + (a_1b_2 + a_2b_1)x + b_1b_2 = x^2 - c;$$

hence

$$a_1a_2 = 1 \implies a_1 = \frac{1}{a_2},\ b_1b_2 = -c \implies b_1 = -\frac{c}{b_2}.$$

Moreover, we have $(a_1b_2 + a_2b_1) = 0$, so

$$a_1b_2 + a_2b_1 = \frac{b_2}{a_2} - \frac{a_2c}{b_2} = \frac{b_2^2 - a_2^2c}{a_2b_2} = 0,$$

so $b_2^2 = a_2^2c$, or $c = \left(\frac{b_2}{a_2}\right)^2$; but c is not the square of any number, so this is a contradiction. Thus if $p(x)$ divides $x^2 - c$, then either $p(x) = k$ or $p(x) = k(x^2 - c)$ for some $k \in F$.

Let $\gcd(a(x), x^2 - c) = r(x)$ for some $r(x) \in F[x]$. From the observation, $r(x) = k(x^2 - c)$ or $r(x) = k$. Suppose $r(x) = k(x^2 - c)$. Since $r(x)$ is a divisor of $a(x)$, we have $a(x) = kq(x)(x^2 - c)$ for some $q(x) \in F[x]$; but $a(x) \neq (kq(x))(x^2 - c)$ for any $q(x) \in F[x]$, a contradiction. Hence $r(x) = k$ for some $k \in F$.

By the Euclidean Algorithm, for some $u(x),\ v(x) \in F[x]$, we have

$$u(x)a(x) + v(x)(x^2 - c) = k = \gcd(a(x), (x^2 - c)).$$

Then $\frac{1}{k}u(x)a(x) + \frac{1}{k}v(x)(x^2 - c) = 1$. But $\frac{1}{k}v(x)(x^2 - c) \equiv 0 \mod (x^2 - c)$, so

$$\frac{1}{k}u(x)a(x) + \frac{1}{k}v(x)(x^2 - c) \equiv \frac{1}{k}u(x)a(x) \equiv 1 \mod (x^2 - c).$$

Clearly, $\frac{1}{k}u(x) \in F[x]$, and so $(a(x) + I)(\frac{1}{k}u(x) + I) = 1 + I$; hence for any $a(x) + I \in F[x]/I$, we have $a^{-1}(x) + I \in F[x]/I$. Thus any non-zero coset $a(x) + I \in F[x]/I$ has an inverse, and so $F[x]/I$ is a field. By Theorem 3.40, $I = (x^2 - c)F[x]$ is a maximal ideal.