Honors Algebra **Spring 2025**
HW 3: Rings **2/11/2025**

Abstract Algebra: An Integrated Approach by J.H. Silverman.
Page 79-90: 3.2, 3.8, 3.14, 3.15, 3.22, 3.25, 3.26, 3.29, 3.49, 3.51

Problem 1 (3.2)**.** Let R be a commutative ring.

(a) Suppose that the map

$$f : R \longrightarrow R, \quad f(a) = a^3,$$

is a ring homomorphism. Prove that $1_R + 1_R = 0_R$. In less fancy notation, prove that $2 = 0$ in the ring R.

Since $f : R \longrightarrow R$ is a ring homomorphism, we know it preserve addition and multiplication. For all $a, b \in R$:

$$f(a + b) = f(a) + f(b), \quad f(ab) = f(a)f(b), \quad \text{and} \quad f(1_R) = 1_R.$$

Given that $f(a) = a^3$, we analyze its behavior on 1_R:

$$f(1_R) = 1_R^3 = 1_R.$$

Since f is a homomorphism, we also have:

$$f(1_R + 1_R) = f(1_R) + f(1_R).$$

Expanding both sides using $f(a) = a^3$:

$$\begin{aligned}
(1_R + 1_R)^3 &= 1_R^3 + 1_R^3 \\
(1_R + 1_R)^3 &= 1_R + 1_R \\
1_R^3 + 3(1_R^2)(1_R) + 3(1_R)(1_R^2) + 1_R^3 &= 1_R + 1_R \\
1_R + 3(1_R) + 3(1_R) + 1_R &= 1_R + 1_R \\
1_R + 6(1_R) + 1_R &= 1_R + 1_R \\
8(1_R) &= 2(1_R) \\
6(1_R) &= 0_R
\end{aligned}$$

The characteristic must divide 6 thus,

$$2(1_R) = 0_R.$$

Therefore, $2 = 0$ in the ring R.

(b) Conversely, if $2 = 0$ in the ring R, prove that $f(a) = a^2$ is a homomorphism from $R \longrightarrow R$.

To show that $f(a) = a^2$ is a ring homomorphism, we need to verify that it preserves addition and multiplication. That is, we must check:

1. Additivity: $f(a+b) = f(a) + f(b)$
2. Multiplicativity: $f(ab) = f(a)f(b)$

Step 1: Check Additivity

$$f(a+b) = (a+b)^2$$

Expanding using the distributive property:

$$(a+b)^2 = a^2 + 2ab + b^2$$

Since $2 = 0$ in R, we have:

$$(a+b)^2 = a^2 + 0 \cdot ab + b^2 = a^2 + b^2$$

Thus, $f(a+b) = f(a) + f(b)$, satisfying additivity.

Step 2: Check Multiplicativity

$$f(ab) = (ab)^2 = a^2b^2 = f(a)f(b)$$

This confirms that f preserves multiplication.

Since both conditions hold, $f(a) = a^2$ is a ring homomorphism.

(c) Suppose that the map

$$f : R \longrightarrow R, \quad f(a) = a^3$$

is a ring homomorphism. Prove that $6 = 0$ in the ring R.

Since $f(a) = a^3$ is a ring homomorphism, it must satisfy the additivity condition:

$$f(a+b) = f(a) + f(b)$$

Expanding the left-hand side:

$$(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$$

Since $f(a+b) = f(a) + f(b)$, we equate:

$$a^3 + 3a^2b + 3ab^2 + b^3 = a^3 + b^3$$

Canceling $a^3 + b^3$ from both sides:

$$3a^2b + 3ab^2 = 0$$

Factoring:

$$3ab(a+b) = 0$$

This must hold for all $a, b \in R$. Setting $a = 1, b = 1$, we get:

$$3(1)(1+1) = 3(2) = 6 = 0$$

Thus, we conclude that $6 = 0$ in R.

Problem 2 (3.8). Let R be a commutative ring, let $c \in R$, and let $E_c : R[x] \longrightarrow R$ be the evaluation map $E_c(f) = f(c)$.

(a) Prove that E_c is a ring homomorphism

To show that E_c is a ring homomorphism, we must verify that it preserves addition and multiplication, i.e., for all polynomials $f, g \in R[x]$,

1. Additivity: $E_c(f + g) = E_c(f) + E_c(g)$
2. Multiplicativity: $E_c(fg) = E_c(f)E_c(g)$

Step 1: Additivity

$$E_c(f + g) = (f + g)(c) = f(c) + g(c) = E_c(f) + E_c(g)$$

This confirms that E_c preserves addition.

Step 2: Multiplicativity

$$E_c(fg) = (fg)(c) = f(c)g(c) = E_c(f)E_c(g)$$

Thus, E_c also preserves multiplication.

Since both conditions hold, E_c is a ring homomorphism.

(b) Prove that $E_c(f) = 0$ if and only if there is a polynomial $g(x) \in R[x]$ satisfying $f(x) = (x - c)g(x)$; i.e., prove that $\ker(E_c)$ is the principle ideal generated by $x - c$.

First, if $f(x) = (x - c)g(x)$, then $f(c) = 0$
Substituting $x = c$ into $f(x)$,

$$f(c) = (c - c)g(c) = 0.$$

Thus, $f(x)$ is in $\ker(E_c)$

For the second part, if $f(c) = 0$, then $f(x)$ is a multiple of $x - c$
Since $f(c) = 0$, we use the polynomial division algorithm to divide $f(x)$ by $x - c$:

$$f(x) = (x - c)g(x) + r,$$

where $g(x) \in R[x]$ is the quotient and r is a remainder that is a constant in R, say $r \in R$.

Evaluating at $x = c$,

$$f(c) = (c - c)g(c) + r = 0 + r = 0.$$

Thus, $r = 0$, meaning that $f(x)$ is exactly $(x - c)g(x)$, proving that every polynomial in $\ker(E_c)$ is a multiple of $x - c$.

Problem 3 (3.14). Let $R[x, y]$ be the ring of polynomials in two variables with coefficients in R, as described in Exercise 3.13. In this exercise we will look at polynomials that don't change if we swap x and y. For example, the polynomials

$$x + y, \quad xy, \quad x^2 + y^2$$

are invariant under an $x \leftrightarrow y$ swap. We observe that our third example can be expressed using the first two examples,

$$x^2 + y^2 = (x+y)^2 - 2xy$$

In other words, if we let $g_2(u,v) = u^2 - 2v$, then $x^2 + y^2 = g_2(x+y, xy)$.

(a) Do the same for $x^3 + y^3$ and $x^4 + y^4$; i.e., find polynomials $g_3(u,v), g_4(u,v) \in R[u,v]$ such that

$$x^3 + y^3 = g_3(x+y, xy) \quad \text{and} \quad x^4 + y^4 = g_4(x+y, xy)$$

We express $x^3 + y^3$ and $x^4 + y^4$ in terms of $x + y$ and xy.

Expressing $x^3 + y^3$

$$\begin{aligned}
x^3 + y^3 &= (x+y)(x^2 - xy + y^2) && \text{Using identity} \\
x^3 + y^3 &= (x+y)((x+y)^2 - 3xy) && \text{Substituting } x^2 + y^2 = (x+y)^2 - 2xy \\
g_3(u,v) &= u(u^2 - 3v) \\
x^3 + y^3 &= g_3(x+y, xy)
\end{aligned}$$

Expressing $x^4 + y^4$

$$\begin{aligned}
x^4 + y^4 &= (x^2 + y^2)^2 - 2x^2y^2 && \text{using identity} \\
x^4 + y^4 &= ((x+y)^2 - 2xy)^2 - 2(xy)^2 && \text{substituting } x^2 + y^2 = (x+y)^2 - 2xy \\
x^4 + y^4 &= (x+y)^4 - 4(x+y)^2xy + 4(xy)^2 - 2(xy)^2 \\
x^4 + y^4 &= (x+y)^4 - 4(x+y)^2xy + 2(xy)^2 \\
g_4(u,v) &= u^4 - 4u^2v + 2v^2 \\
x^4 + y^4 &= g_4(x+y, xy)
\end{aligned}$$

(b) More generally, prove that for every $n \geq 1$ there is a polynomial $g_n(u,v) \in R[u,v]$ such that

$$x^n + y^n = g_n(x+y, xy)$$

Hint: Use induction on n.

Base Case:
We already established the cases for $n = 2, 3, 4$.

Inductive Step:
Assume that for some $k \geq 1$, there exists a polynomial $g_k(u,v)$ such that:

$$x^k + y^k = g_k(x+y, xy).$$

We show that the statement holds for $k+1$. Using the recurrence relation:

$$x^{k+1} + y^{k+1} = (x+y)(x^k + y^k) - xy(x^{k-1} + y^{k-1}),$$

and applying the inductive hypothesis:

$$x^k + y^k = g_k(x+y, xy) \quad \text{and} \quad x^{k-1} + y^{k-1} = g_{k-1}(x+y, xy),$$

we obtain:

$$x^{k+1} + y^{k+1} = (x+y)g_k(x+y, xy) - xyg_{k-1}(x+y, xy).$$

Defining:

$$g_{k+1}(u, v) = ug_k(u, v) - vg_{k-1}(u, v),$$

Thus we can conclude that $g_n(u, v)$ exists for all n.

(c) Even more generally, suppose that $f(x, y) \in R[x, y]$ is any polynomial with the symmetry property

$$f(x, y) = f(y, x)$$

Pove that there is a polynomial $g(u, v) \in R[u, v]$ such that

$$f(x, y) = g(x+y, xy)$$

We prove this by expressing any symmetric polynomial in terms of elementary symmetric polynomials.

The elementary symmetric polynomials in two variables are:

$$s_1 = x + y, \quad s_2 = xy.$$

The fundamental theorem of symmetric polynomials states that any symmetric polynomial $f(x, y)$ can be written as a polynomial in s_1 and s_2, meaning that there exists some $g(u, v) \in R[u, v]$ such that:

$$f(x, y) = g(s_1, s_2) = g(x+y, xy).$$

Problem 4 (3.15). Let R be a continous ring, and let $f(x) \in R[x]$ be a polynomial with coefficients in R. We define the *formal derivative* $f'(x)$ of $f(x)$ by writing $f(x)$ as

$$f(x) = \sum_{k=0}^{n} a_k x^k \quad \text{and setting} \quad f'(x) = \sum_{k=0}^{n} k a_k x^{k-1}$$

Note that there is no limit being taken, so the formal derivative makes sense even if, for example, R is a ring such that as $\mathbb{Z}/m\mathbb{Z}$. It also means that when doing this exercise, you'll need to directly use the definition of $f'(x)$, since you can't rely on the proofs from calculus.

(a) Let $f(x), g(x) \in R[x]$. Prove that $(f+g)'(x) = f'(x) + g'(x)$

Let

$$f(x) = \sum_{k=0}^{n} a_k x^k, \quad g(x) = \sum_{k=0}^{m} b_k x^k.$$

Then their sum is:

$$(f+g)(x) = \sum_{k=0}^{\max(n,m)} (a_k + b_k)x^k.$$

Taking the formal derivative, we apply the definition:

$$(f+g)'(x) = \sum_{k=1}^{\max(n,m)} k(a_k + b_k)x^{k-1}.$$

By the distributive property in R:

$$(f+g)'(x) = \sum_{k=1}^{n} k a_k x^{k-1} + \sum_{k=1}^{m} k b_k x^{k-1} = f'(x) + g'(x).$$

Thus, we have proved that:

$$(f+g)'(x) = f'(x) + g'(x).$$

(b) Let $f(x), g(x) \in R[x]$. Prove that $(f \cdot g)'(x) = f(x)g'(x) + g(x)f'(x)$

Let

$$f(x) = \sum_{i=0}^{n} a_i x^i, \quad g(x) = \sum_{j=0}^{m} b_j x^j.$$

Their product is given by:

$$(f \cdot g)(x) = \sum_{i=0}^{n} \sum_{j=0}^{m} a_i b_j x^{i+j}.$$

Taking the formal derivative, we apply the definition:

$$(f \cdot g)'(x) = \sum_{i=0}^{n} \sum_{j=0}^{m} a_i b_j (i+j) x^{i+j-1}.$$

We split the sum into two parts:

$$(f \cdot g)'(x) = \sum_{i=0}^{n} \sum_{j=0}^{m} i a_i b_j x^{i-1} x^j + \sum_{i=0}^{n} \sum_{j=0}^{m} j a_i b_j x^i x^{j-1}.$$

Factoring out terms:

$$(f \cdot g)'(x) = \left(\sum_{i=1}^{n} i a_i x^{i-1} \right) \left(\sum_{j=0}^{m} b_j x^j \right) + \left(\sum_{j=1}^{m} j b_j x^{j-1} \right) \left(\sum_{i=0}^{n} a_i x^i \right).$$

Recognizing these as $f'(x)$ and $g'(x)$, we can conclude that

$$(f \cdot g)'(x) = f(x)g'(x) + g(x)f'(x).$$

(c) Let $f(x), g(x) \in R[x]$. Prove that the formal derivative of $f(g(x))$ is $f'(g(x))g'(x)$. (*Hint:* First prove it is true for $f(x) = x^i$ using induction on i and (b). Then write $f(g(x))$ as a sum of powers of $g(x)$ and use (a).)

Base Case
For $i = 1$, we have $f(x) = x$

$$\begin{aligned} f(g(x)) &= g(x) \\ (f(g(x)))' &= g'(x) \\ f'(g(x))g'(x) &= g'(x) \quad \text{Since } f'(x) = 1 \end{aligned}$$

Inductive Step
Assume the result holds for $i = k$:

$$((g(x))^k)' = k(g(x))^{k-1}g'(x).$$

Now consider $i = k + 1$:

$$f(x) = x^{k+1} \quad \Rightarrow \quad f(g(x)) = (g(x))^{k+1}$$

$$\begin{aligned} (g(x))^{k+1} &= g(x) \cdot (g(x))^k && \text{product rule from part (b)} \\ ((g(x))^{k+1})' &= g(x)(g(x)^k)' + g'(x)(g(x))^k && \text{taking derivative} \\ ((g(x))^{k+1})' &= g(x) \cdot k(g(x))^{k-1}g'(x) + g'(x)(g(x))^k && \text{by inductive hyp.} \\ ((g(x))^{k+1})' &= (k(g(x))^k + (g(x))^k)g'(x) = (k+1)(g(x))^k g'(x) \end{aligned}$$

$$f'(x) = (k+1)x^k \quad \Rightarrow \quad f'(g(x)) = (k+1)(g(x))^k$$

Thus, $(f(g(x)))' = f'(g(x))g'(x)$

General Case
Suppose $f(x)$ is a general polynomial:

$$f(x) = \sum_{i=0}^{n} a_i x^i.$$

Then,

$$\begin{aligned} f(g(x)) &= \sum_{i=0}^{n} a_i (g(x))^i. \\ (f(g(x)))' &= \sum_{i=0}^{n} a_i ((g(x))^i)' && \text{by linearity (a)} \\ (f(g(x)))' &= \sum_{i=0}^{n} a_i f_i'(g(x))g'(x) && \text{by result for powers} \\ (f(g(x)))' &= f'(g(x))g'(x) && \text{factoring out } g'(x) \end{aligned}$$

□

Problem 5 (3.22)**.** Let R be a finite integral domain; i.e., R is an integral domain and it has finitely many elements. Prove that R is a field. (*Hint:* Let $a \in R$ with $a \neq 0$. First prove that the map

$$R \longrightarrow R, \quad b \longmapsto ab$$

is injective. Use this to decide that the map is also surjective.)

Given that the given map is injective, define the function $\varphi : R \to R$ by $\varphi(b) = ab$ for all $b \in R$. Suppose $\varphi(b_1) = \varphi(b_2)$, i.e., $ab_1 = ab_2$. Since R is an integral domain, it has no zero divisors, meaning that if $a \neq 0$ and $ab_1 = ab_2$, then we must have: $b_1 = b_2$. And this proves that φ is injective.

Since R is finite, an injective function from R to itself must also be surjective. That is, for every $c \in R$, there exists some $b \in R$ such that $ab = c$. In particular, setting $c = 1$, we find some $b \in R$ such that $ab = 1$. Thus, b is the multiplicative inverse of a, meaning every nonzero element of R has an inverse and decides that this map is also surjective.

Since every nonzero element of R has a multiplicative inverse, R is a field.

Problem 6 (3.25)**.** Let R be a commutative ring.

(a) Prove that there is exactly one integral domain R such that the map

$$f : R \longrightarrow R, \quad f(a) = a^6$$

is a ring homomorphism. (You'll need to use the fact that $1_R \neq 0_R$.)

To verify that f is a ring homomorphism, we must check:

$$f(a+b) = f(a) + f(b) \quad \text{and} \quad f(ab) = f(a)f(b), \quad \text{for all } a, b \in R.$$

For $f(ab) = f(a)f(b)$:

$$f(ab) = (ab)^6 = a^6b^6 = f(a)f(b).$$

This holds since R is commutative.

For $f(a+b) = f(a) + f(b)$:

$$f(a+b) = (a+b)^6 \neq a^6 + b^6,$$

in general. The equality holds if and only if $(a+b)^6 = a^6 + b^6$, which expands to:

$$a^6 + b^6 + 6a^5b + 15a^4b^2 + 20a^3b^3 + 15a^2b^4 + 6ab^5 = a^6 + b^6.$$

This implies:

$$6a^5b + 15a^4b^2 + 20a^3b^3 + 15a^2b^4 + 6ab^5 = 0.$$

Since R is an integral domain and has no zero divisors, the above equation holds if and only if $a = 0$ or $b = 0$. Thus, the only integral domain where $f(a+b) = f(a) + f(b)$ for all $a, b \in R$ is $R = \mathbb{Z}/6\mathbb{Z}$. However, $\mathbb{Z}/6\mathbb{Z}$ is not an integral domain. Therefore, the only integral domain where this map is a homomorphism is $R = \mathbb{F}_2$ (the field with two elements), where $1 + 1 = 0$.

(b) Find at least two different integral domains R such that the map

$$f : R \longrightarrow R, \quad f(a) = a^15$$

is a ring homomorphism. Are there any others?

As in part (a), $f(ab) = f(a)f(b)$ holds in any commutative ring, but $f(a+b) = f(a)+f(b)$ only holds in specific cases.

Expanding $(a+b)^{15}$ using the binomial theorem, we get:

$$(a+b)^{15} = a^{15} + b^{15} + \sum_{k=1}^{14} \binom{15}{k} a^{15-k} b^k.$$

For $f(a+b) = f(a) + f(b)$ to hold, the terms involving $a^{15-k}b^k$ must vanish. This occurs in characteristic 15 or any characteristic dividing 15 (i.e., 3 or 5).

Two different integral domains for which f is a ring homomorphism are:
1. $R = \mathbb{F}_3$ (field with 3 elements).
2. $R = \mathbb{F}_5$ (field with 5 elements).

In characteristic 15, there are no integral domains since 15 is not a prime power, so there are no others.

(c) For each of parts (a) and (b), find at least one ring that is not an integral domain for which the indicated map is a ring homomorphism.

For part (a), an example of a ring that is not an integral domain where $f(a) = a^6$ is a homomorphism is $R = \mathbb{Z}/6\mathbb{Z}$, where the characteristic ensures that $(a+b)^6 = a^6 + b^6$.

For part (b), an example of a ring that is not an integral domain where $f(a) = a^{15}$ is a homomorphism is $R = \mathbb{Z}/15\mathbb{Z}$. In this case, the characteristic 15 ensures the desired property holds.

(d) Let p and q be distinct primes. Characterize all integral domains R for which the map $f(a) = a^{pq}$ is a ring homomorphism. (This is a difficult problem with the tools that you have at your disposal, but it's a fun problem, so give it a whirl!)

Let $f(a) = a^{pq}$, where p and q are distinct primes. For f to be a ring homomorphism, we require:

$$f(a+b) = f(a) + f(b).$$

Expanding $(a+b)^{pq}$ using the binomial theorem:

$$(a+b)^{pq} = a^{pq} + b^{pq} + \sum_{k=1}^{pq-1} \binom{pq}{k} a^{pq-k} b^k.$$

For $f(a+b) = f(a) + f(b)$, the cross terms must vanish. This occurs if the characteristic of R is a common divisor of all the binomial coefficients $\binom{pq}{k}$ for $1 \leq k \leq pq - 1$.

Since p and q are distinct primes, the characteristic of R must divide pq but not p or q individually. The only integral domain where this is true is $R = \mathbb{F}_p$ or $R = \mathbb{F}_q$, the fields with p or q elements, respectively. Thus, the integral domains R for which $f(a) = a^{pq}$ is a homomorphism are those of characteristic p or q.

Problem 7 (3.26)**.** Let R be a ring. We define three properties that an element $a \in R$ may posses.

- a is nilpotent if $a^n = 0$ for some $n \geq 1$
- a is unipotent if $a - 1$ is nilpotent; i.e., if $(a-1)^n = 0$ for some $n \geq 1$
- a is idempotent if $a^2 = a$

(a) If R is an integral domain, describe all of the nilpotent elements of R, all of the unipotent elements, and all of the idempotent elements. In particular, how many are there of each?

Nilpotent elements: An element $a \in R$ is nilpotent if $a^n = 0$ for some $n \geq 1$. In an integral domain, the only nilpotent element is $a = 0$. This is because if $a^n = 0$ and R has no zero divisors, then $a = 0$ must hold. Hence, there is exactly 1 nilpotent element.

Unipotent elements: An element $a \in R$ is unipotent if $a - 1$ is nilpotent, i.e., $(a-1)^n = 0$ for some $n \geq 1$. Since the only nilpotent element in an integral domain is 0, we must have $a - 1 = 0$, or $a = 1$. Thus, there is exactly 1 unipotent element.

Idempotent elements: An element $a \in R$ is idempotent if $a^2 = a$. Factoring, we have $a(a-1) = 0$. In an integral domain, this implies $a = 0$ or $a = 1$. Therefore, there are exactly 2 idempotent elements: 0 and 1.

(b) Let $p \in \mathbb{Z}$ be a prime and let $k \geq 1$. Describe all of the nilpotent elements in $\mathbb{Z}/p^k\mathbb{Z}$. In particular, how many are there?

Nilpotent elements: An element $a \in \mathbb{Z}/p^k\mathbb{Z}$ is nilpotent if $a^n = 0$ for some $n \geq 1$. In this ring, $a^n = 0$ if and only if $a = mp^j$ for some $1 \leq j < k$ and $m \in \mathbb{Z}$ such that $1 \leq m \leq p^{k-j} - 1$. The powers of p determine the values of j, and m determines the number of distinct elements for each j.

Lets count the total number of nilpotent elements:
For each j from 1 to $k-1$, the number of elements is $p^{k-j} - 1$.
Summing over all j, the total number of nilpotent elements is:

$$\sum_{j=1}^{k-1} (p^{k-j} - 1) = (p^{k-1} - 1) + (p^{k-2} - 1) + \cdots + (p - 1).$$

This can be written as:

$$\text{Total nilpotent elements} = (p-1) + (p^2 - 1) + \cdots + (p^{k-1} - 1) = \frac{p^k - p}{p - 1} - (k-1).$$

Thus, there are $\frac{p^k - p}{p-1} - (k-1)$ nilpotent elements in $\mathbb{Z}/p^k\mathbb{Z}$.

Problem 8 (3.29). (a) Let R be a commutative ring, and suppose that its unit group R^* is finite, say $n = \#R^*$. Prove that every element $a \in R^*$ satisfies

$$a^n = 1$$

(*Hint:* Use Lagrange's Theorem, more specifically Corollary 2.50.)

Since $a \in R^*$, a is a unit, meaning there exists $b \in R$ such that $ab = 1$. The unit group R^* forms a finite group under multiplication. By Corollary 2.50, the order of any element $a \in R^*$ divides the order of the group, n.

Let m denote the order of a in R^*. Then m is the smallest positive integer such that $a^m = 1$. Since m divides n, we can write $n = km$ for some integer k. Thus,

$$a^n = a^{km} = (a^m)^k = 1^k = 1.$$

Therefore, every $a \in R^*$ satisfies $a^n = 1$.

(b) Let p be a prime, and let $a \in \mathbb{Z}$, be an integer with $p \nmid a$. Use (a) to prove:

Fermat's Last Theorem: $a^{p-1} \equiv 1 (\mathrm{mod}\ p)$

(*Hint:* Consider the unit group of $\mathbb{Z}/p\mathbb{Z}$.)

Since $p \nmid a$, the element a is coprime to p, and its residue class modulo p lies in the unit group $(\mathbb{Z}/p\mathbb{Z})^*$. The set $(\mathbb{Z}/p\mathbb{Z})^*$ is the group of units of the ring $\mathbb{Z}/p\mathbb{Z}$ under multiplication. This group has order $p-1$, since there are exactly $p-1$ integers in $\mathbb{Z}/p\mathbb{Z}$ that are coprime to p.

By part (a), every element $b \in (\mathbb{Z}/p\mathbb{Z})^*$ satisfies $b^{p-1} = 1$ in $(\mathbb{Z}/p\mathbb{Z})^*$. In particular, this holds for the residue class of a, so:

$$a^{p-1} \equiv 1 \pmod{p}.$$

This is Fermat's Little Theorem.

Problem 9 (3.49). Let R be a ring, let I be an ideal of R, and for any other ideal J of R, let $\bar{J}$ be the following subset of the qotient ring R/I:

$$\bar{J} = \{a + I : a \in J\}$$

(a) Prove that $\bar{J}$ is an ideal of R/I. (If we assume further that $I \subseteq J$, then the ideal $\bar{J}$ is typically denoted J/I.)

We must check the two conditions for $\bar{J}$ to be an ideal.

Additive closure:
Take any two elements $x + I, y + I \in \bar{J}$. Then $x, y \in J$ because $\bar{J}$ is defined as $\{a + I : a \in J\}$. Since J is an ideal of R, $x + y \in J$. Therefore:

$$(x + I) + (y + I) = (x + y) + I \in \bar{J}.$$

Closed under multiplication by R/I:
Take $r+I \in R/I$ and $x+I \in \bar{J}$. Then $x \in J$, and since J is an ideal of R, $rx \in J$. Therefore:

$$(r+I)(x+I) = rx + I \in \bar{J}.$$

Hence, $\bar{J}$ satisfies both conditions and is an ideal of R/I.

(b) Let $\bar{K}$ be an ideal of R/I. Prove that the set

$$\bigcup_{a+I\in\bar{K}} (a+I)$$

is an ideal of R that contains I.

Let $\bar{K}$ be an ideal of R/I. Define the set:

$$K = \bigcup_{a+I\in\bar{K}} (a+I) = \{a \in R : a+I \in \bar{K}\}.$$

We want to prove that K is an ideal of R and that $I \subseteq K$.

Additive closure:
Let $a, b \in K$. Then $a+I, b+I \in \bar{K}$ since $a, b \in K$ implies $a+I, b+I \in \bar{K}$. Since $\bar{K}$ is an ideal of R/I, it is closed under addition, so:

$$(a+I) + (b+I) = (a+b) + I \in \bar{K}.$$

Thus, $a+b \in K$.

Closed under multiplication by R:
Let $r \in R$ and $a \in K$. Then $a+I \in \bar{K}$. Since $\bar{K}$ is an ideal of R/I, we have:

$$(r+I)(a+I) = (ra) + I \in \bar{K}.$$

Thus, $ra \in K$.

Containment of I:
For any $i \in I$, $i + I = 0 + I \in \bar{K}$ since $\bar{K}$ is an ideal of R/I and contains $0+I$. Therefore, $i \in K$, so $I \subseteq K$.

Hence, K is an ideal of R that contains I.

(c) Conclude that there is a bijective map

$$\{\text{ideals of } R \text{ that contain } I\} \longrightarrow \{\text{ideals of } R/I\}, \quad J \longmapsto J/I$$

We want to show this where $J/I = \{a+I : a \in J\}$.

Injectivity:
Let J_1 and J_2 be ideals of R that contain I, and suppose $J_1/I = J_2/I$. Then:

$$\{a+I : a \in J_1\} = \{a+I : a \in J_2\}.$$

This implies $J_1 = J_2$, since the cosets uniquely determine their representatives modulo I. Thus, the map is injective.

Surjectivity:
Let $\bar{K}$ be an ideal of R/I. By part (b), the set:

$$K = \{a \in R : a + I \in \bar{K}\}$$

is an ideal of R that contains I, and $K/I = \{a + I : a \in K\} = \bar{K}$. Thus, every ideal of R/I arises as J/I for some ideal J of R that contains I. Hence, the map is surjective.

Since the map is both injective and surjective, thus it is bijective.

Problem 10 (3.51)**.** Let I be the following subset of the ring $\mathbb{Z}[x]$ of polynomials having integer coefficients:

$$I = \{2a(x) + xb(x) : a(x), b(x) \in \mathbb{Z}[x]\}$$

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

We check the two conditions for I to be an ideal:

Additive closure:
Let $f(x) = 2a_1(x)+xb_1(x)$ and $g(x) = 2a_2(x)+xb_2(x)$, where $a_1(x), a_2(x), b_1(x), b_2(x) \in \mathbb{Z}[x]$. Then:

$$f(x)+g(x) = [2a_1(x)+xb_1(x)]+[2a_2(x)+xb_2(x)] = 2(a_1(x)+a_2(x))+x(b_1(x)+b_2(x)).$$

Since $a_1(x) + a_2(x), b_1(x) + b_2(x) \in \mathbb{Z}[x]$, it follows that $f(x) + g(x) \in I$.

Closed under multiplication by elements of $\mathbb{Z}[x]$:
Let $f(x) = 2a(x) + xb(x) \in I$ and $c(x) \in \mathbb{Z}[x]$. Then:

$$c(x)f(x) = c(x)[2a(x) + xb(x)] = 2c(x)a(x) + xc(x)b(x).$$

Since $c(x)a(x), c(x)b(x) \in \mathbb{Z}[x]$, it follows that $c(x)f(x) \in I$.

Thus, I is an ideal of $\mathbb{Z}[x]$.

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

To prove that $I \neq \mathbb{Z}[x]$, note that if $I = \mathbb{Z}[x]$, then $1 \in I$. This would mean there exist $a(x), b(x) \in \mathbb{Z}[x]$ such that:

$$1 = 2a(x) + xb(x).$$

However, this is impossible because $2a(x)$ is always an even polynomial (its coefficients are all even), and $xb(x)$ is divisible by x. Since 1 is neither even nor divisible by x, $1 \notin I$. Therefore, $I \neq \mathbb{Z}[x]$.

(c) Prove that I is not a principal ideal; i.e., prove that there does not exist a polynomial $c(x) \in \mathbb{Z}[x]$ such that $I = c(x)\mathbb{Z}[x]$.

To prove that I is not a principal ideal, suppose for contradiction that there exists $c(x) \in \mathbb{Z}[x]$ such that $I = c(x)\mathbb{Z}[x]$. This means every element of I can be written as $c(x)q(x)$ for some $q(x) \in \mathbb{Z}[x]$. In particular, the generators of I, 2 and x, must both belong to $c(x)\mathbb{Z}[x]$. Therefore, there exist $q_1(x), q_2(x) \in \mathbb{Z}[x]$ such that:

$$2 = c(x)q_1(x), \quad x = c(x)q_2(x).$$

The first equation implies that $c(x)$ divides 2, so $c(x)$ must be a constant divisor of 2, i.e., $c(x) \in \{\pm 1, \pm 2\}$. However, if $c(x)$ is a constant, it cannot generate both 2 and x because x is not a multiple of any constant polynomial. This is a contradiction. Hence, I is not a principal ideal.

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

We must show that the quotient ring $\mathbb{Z}[x]/I$ is a field.

Note that $I = \{2a(x) + xb(x) : a(x), b(x) \in \mathbb{Z}[x]\}$. Consider the homomorphism $\phi : \mathbb{Z}[x] \to \mathbb{Z}/2\mathbb{Z}[x]$ defined by reducing coefficients modulo 2 and sending x to x. The kernel of ϕ is exactly I, and thus:

$$\mathbb{Z}[x]/I \cong \mathbb{Z}/2\mathbb{Z}[x]/(x),$$

where (x) is the ideal generated by x in $\mathbb{Z}/2\mathbb{Z}[x]$. The quotient $\mathbb{Z}/2\mathbb{Z}[x]/(x)$ is isomorphic to $\mathbb{Z}/2\mathbb{Z}$, which is a field.

Since the quotient ring $\mathbb{Z}[x]/I$ is a field, I is a maximal ideal of $\mathbb{Z}[x]$.