CATEGORY THEORY
TOPIC 35: RINGS
(DRAFT)

PAUL L. BAILEY

Abstract. Rings are generalization of the integers $\mathbb{Z}$, and fields are generalization of the rational number $\mathbb{Q}$.

Ring theory gives us insight into the algebra of these sets, but also readily applies to polynomial rings, which gives us deeper insight into the structure of the reals and the complex numbers. This is the aspect of ring theory we wish to pursue.

1. Rings

Definition 1. A *ring* is a set R together with a pair of binary operations

$$+ : R \times R \to R \text{ and } \cdot : R \times R \to R$$

such that

(R1) $a + b = b + a$ for every $a, b \in R$;
(R2) $(a + b) + c = a + (b + c)$ for every $a, b, c \in R$;
(R3) there exists $0 \in R$ such that $a + 0 = a$ for every $a \in R$;
(R4) for every $a \in R$ there exists $-a \in R$ such that $a + (-a) = 0$;
(R5) $(ab)c = a(bc)$ for every $a, b, c \in R$;
(R6) there exists $1 \in R$ such that $a \cdot 1 = 1 \cdot a = a$ for every $a \in R$;
(R7) $a(b + c) = ab + ac$ for every $a, b, c \in R$;
(R8) $(a + b)c = ac + bc$ for every $a, b, c \in R$.

A *commutative ring* is a ring R which additionally satifies

(R9) $ab = ba$ or every $a, b \in R$.

The standard rules for additive and multiplicative notation are in force.

The additive identity is denoted by 0 and the additive inverse of a is denoted $-a$. If $n \in \mathbb{Z}$, then $na = 0$ if $n = 0$, $na = a + \cdots + a$ (n times) if $n > 0$, and $na = (-a) + \cdots + (-a)$ (n times) if $n < 0$.

The multiplicative identity is denoted by 1 and the multiplicative inverse of a (if it exists) is denoted by a^{-1}. If $n \in \mathbb{N}$, then $a^n = 1$ if $n = 0$ and $a^n = a \cdot \cdots \cdot a$ (n times) if $n > 0$. If a has a multiplicative inverse and $n < 0$, then $a^n = (a^{-1})^{-n}$. The notation 0^0 is undefined. The product symbol $\cdot$ may be dropped, so that multiplication is denoted by juxtaposition.

From the theory of binary operations that has been studied prior to groups, we know that the identities are unique, as are inverses when they exist. It should be noted that a ring is an abelian group under addition.

Date: April 28, 2018.

Problem 1. Let R be a ring and let $a \in R$. Show that $a \cdot 0 = 0 \cdot a = 0$.

Solution. First this first problem, we write all the details. As we proceed, we leave more details to the reader.

$$\begin{aligned} a \cdot 0 &= a \cdot (0+0) && \text{by } \textbf{(R3)} \\ &= a \cdot 0 + a \cdot 0 && \text{by } \textbf{(R7)}. \end{aligned}$$

By **(R4)**, $-a \cdot 0$ exists, so

$$\begin{aligned} 0 &= a \cdot 0 + -(a \cdot 0)) && \text{by } \textbf{(R4)} \\ &= (a \cdot 0 + a \cdot 0) + -(a \cdot 0) && \text{adding } -a \cdot 0 \text{ to both sides} \\ &= a \cdot 0 + (a \cdot 0 - a \cdot 0) && \text{by } \textbf{(R2)} \\ &= a \cdot 0 + 0 && \text{by } \textbf{(R4)} \\ &= a \cdot 0 && \text{by } \textbf{(R3)} \end{aligned}$$

That is, $a \cdot 0 = 0$. □

Problem 2. Let R be a ring and let $a, b \in R$. Show that $(-a)b = a(-b) = -(ab)$.

Solution. By Problem 1, zero times anything is zero. Now we use uniqueness of inverses: add ab to $(-a)b$ to get 0:

$$ab + (-a)b = (a + (-a))b = 0 \cdot b = 0,$$

so since the inverse of ab is unique, it must be $(-a)b$. That is, $(-a)b = -(ab)$. The second equality is similar. □

2. Examples of Rings

Example 1. Let $R = \{0\}$. Define $0 + 0 = 0$ and $0 \cdot 0 = 0$. Then R is a ring, called the *zero ring* .

Example 2. The following sets of numbers are rings under their standard addition and multiplication: **(a)** $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$, the integers;
(b) $\mathbb{Q} = \{\frac{a}{b} \mid a, b \in \mathbb{Z}\}$, the rational numbers;
(c) $\mathbb{R}$, the real numbers;
(d) $\mathbb{C} = \{a + ib \mid a, b \in \mathbb{R} \text{ and } i^2 = -1\}$, the complex numbers.

Example 3. Let R and S be rings. Define addition and multiplication on their cartesian product $R \times S$ componentwise by

- $(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2)$;
- $(r_1, s_1) \cdot (r_2, s_2) = (r_1 s_1, r_2 s_2)$.

Then $R \times S$ is a ring, called the *product ring* of R and S.

Example 4. Let X be a set and let R be a commutative ring. Let $\mathcal{F}(X, R)$ denote the set of all functions from X to R. Define addition and multiplication of functions in $\mathcal{F}(X, R)$ pointwise by

- $(f + g)(x) = f(x) + g(x)$;
- $(f \cdot g)(x) = f(x)g(x)$.

Then $\mathcal{F}(X, R)$ is a ring, called the *ring of functions* from X to R.

Example 5. Let R be a commutative ring, and let $\mathcal{M}_n(R)$ denote the set of all $n \times n$ matrices with entries from R, together with matrix addition and multiplication. Then $\mathcal{M}_n(R)$ is a ring. This is the main example of a noncommutative ring.

3. Entire and Invertible Elements

Definition 2. Let R be a commutative ring and let $a \in R$.

We say that a is *entire* if $ab = 0 \Rightarrow b = 0$ for every $b \in R$.

We say that a is *cancellable* if $ab = ac \Rightarrow b = c$ for every $b, c \in R$.

We say that a is *invertible* if there exists an element $a^{-1} \in R$ such that $aa^{-1} = 1$.

Nonentire, nonzero elements are often called *zero divisors*.

Problem 3. Let R be a commutative ring and let $a \in R$. Show that a is entire if and only if a is cancellable.

Solution. To show an if and only if statement, it is often best to show each direction independently.

($\Rightarrow$) Suppose that a is entire. Let $b, c \in R$ and suppose that $ab = ac$. We wish to show that $b = c$. Subtract ac from both sides to get $ab - ac = 0$. By the distributive law, $a(b - c) = 0$. Since a is entire, this implies that $b - c = 0$, so $b = c$. Thus a is cancellable

($\Leftarrow$) Suppose that a is cancellable. Let $b \in R$ and suppose that $ab = 0$. Then $ab = a \cdot 0$, so by cancellation, $b = 0$. Thus a is entire. □

Problem 4. Let R be a commutative ring and let $a \in R$. Show that if a is invertible, then a is entire.

Solution. Suppose that a is invertible. Let $b \in R$ and suppose that $ab = 0$. Then $a^{-1}ab = a^{-1} \cdot 0$, that is, $b = 0$. □

Definition 3. Let R be a nonzero commutative ring. Set

$$R^* = \{x \in R \mid x \text{ is invertible } \}$$

and

$$R^\bullet = \{x \in R \mid x \text{ is entire } \}.$$

Problem 5. Let R be a nonzero commutative ring. Show that R^* is an abelian group under multiplication.

Solution. By **(R5)**, R^* is associative. Since 1 is invertible, $1 \in \mathbb{R}^*$. Since $(a^{-1})^{-1} = a$, a is closed under inverses. Finally, $(ab)^{-1} = b^{-1}a^{-1}$, which shows that R^* is closed under multiplication. □

Definition 4. Let R be a nonzero commutative ring.

We say that R is an *integral domain* if every nonzero element of R is entire.

We say that R is a *field* if every nonzero element of R is invertible.

Problem 6. Let R be a commutative ring. Show that if R is a field, then R is an integral domain.

Solution. Let $a \in R$ be nonzero. Then a is invertible, so a is entire by Problem 4. Thus R is a domain. □

Problem 7. Let R be a finite integral domain. Show that R is a field.

Solution. Let $a \in R \setminus \{0\}$ and define a function

$$\mu_a : R \to R \quad \text{given by } \mu_a(x) = ax.$$

We claim that μ_a is surjective. To see this, suppose that $\mu_a(x_1) = \mu_a(x_2)$. By definition of μ_a, we have $ax_1 2 = ax_2$. Since a is entire, it is cancellable, so $x_1 = x_2$. Thus μ_a is injective. An injective function from a finite set to itself is necessarily surjective, so μ_a is surjective. Thus there exists $b \in R$ such that $\mu_a(b) = 1$; that is, $ab = 1$. Thus b is the inverse of a, and a is invertible. There, R is a field. □

4. Divisibility

Definition 5. Let R be a commutative ring and let $a, b \in R$.

We say that a *divides* b, and write $a \mid b$, if there exists $c \in R$ such that $b = ac$. Otherwise we write $a \nmid b$.

Definition 6. Let R be a commutative ring and let $a, b \in R^\bullet$.

We say that a and b are *associates*, and write $a \sim b$, if $a \mid b$ and $b \mid a$.

Problem 8. Let R be a commutative ring and let $a, b \in R^\bullet$. Show that $a \sim b$ if and only if there exists an invertible element $u \in R$ such that $b = ua$.

Solution. Suppose that $a \sim b$. Then $a \mid b$ and $b \mid a$, which says that $b = ax$ and $a = by$ for some $x, y \in R$. Substitute to get $b = bax$. Since b is entire, $1 = ax$, so a is invertible. Let $u = a$ and commute to get $ua = 1$.

On the other hand, suppose that $b = ua$ for some $u \in R^*$. Then $a \mid b$, and since $a = u^{-1}b$, we also have that $b \mid a$. Thus $a \sim b$. □

Problem 9. Let R be a commutative ring. Show that $\sim$ is an equivalence relation on $R^\bullet$.

Solution. We use Problem 8.

Reflexive: Since $a = 1 \cdot a$, $b \sim b$.

Symmetric: Suppose $a \sim b$. Then $b = ua$ for some $u \in R^*$. Then $u^{-1} \in R^*$, and $a = u^{-1}b$. Thus $b \sim a$.

Transitive: Suppose $a \sim b$ and $b \sim c$. Then $b = ua$ and $c = vb$ for some $u, v \in R^*$. Substitution gives $c = vua$. Since $vu \in R^*$, $a \sim c$. □

Problem 10. Let R be a commutative ring and let $a, b \in R^\bullet$.

(a) Show that $bR \subset aR$ if and only if $a \mid b$.
(b) Show that $bR = aR$ if and only if $a \sim b$.
(c) Show that $abR \subset aR \cap bR$.
(d) Give an example where $abR \neq aR \cap bR$.

Solution. We prove four parts.

(a) Suppose $bR \subset aR$. Since $1 \in R$, $b = b \cdot 1 \in bR$. Thus $b \in aR$, so $b = ar$ for some $r \in R$. Thus $a \mid b$.

One the other hand, suppose that $a \mid b$, and let $z \in bR$. Then $z = by$ for some $y \in R$. Since $a \mid b$, $b = ax$ for some $x \in R$. Substitution gives $z = axy$, so $z \in aR$. Thus $bR \subset aR$.

(b) Clearly,

$$bR = aR \Leftrightarrow bR \subset aR \text{ and } aR \subset bR \Leftrightarrow a \mid b \text{ and } b \mid a \Leftrightarrow a \sim b.$$

(c) Let $z \in abR$. Then $z = abr$ for some $r \in R$. Thus $z = a(br) \in aR$ and $z = b(ar) \in bR$, so $z \in aR \cap bR$.

(d) Note that $12\mathbb{Z}$ is a proper subset of $2\mathbb{Z} \cap 3\mathbb{Z}$. □

Definition 7. Let R be a commutative ring and let $p \in R^\bullet \smallsetminus R^*$.

We say that p is *irreducible* if whenever $p = ab$, then either a is invertible or b is invertible.

We say that p is *prime* if whenever $p \mid ab$, then either $p \mid a$ or $p \mid b$.

Problem 11. Let D an integral domain and let $p \in D$.
Show that if p is prime, then p is irreducible.

Solution. Suppose that p is prime, and that $p = ab$ for some $a, b \in R$. We see that $p \mid ab$, and since p is prime, $p \mid a$ or $p \mid b$.

Suppose that $p \mid a$. Then $a = px$ for some $x \in R$, so $p = pxb$. By cancellation, $1 = xb$, so b is invertible. Similarly, if $p \mid b$, we will get that a is invertible. □

5. Subrings

Definition 8. Let R be a ring. A *subring* of R is a subset $S \subset R$ such that

(S0) $1 \in S$;
(S1) $a, b \in S \Rightarrow a + b \in S$;
(S2) $a \in S \Rightarrow -a \in S$;
(S3) $a, b \in S \Rightarrow ab \in S$.

If S is a subring of R, we write $S \leq R$.

Problem 12. Let F be a field and let $R \leq F$. Show that R is an integral domain.

Solution. Let $a \in R$, and suppose that $ab = 0$ for some $b \in R$. Then $b = a^{-1} \cdot 0 = 0$, so b is entire. Thus R is an integral domain. □

6. Ring Homomorphisms

Definition 9. Let R and S be rings. A *ring homomorphism* from R to S is a function $\phi : R \to S$ such that

(H0) $\phi(1_R) = 1_S$;
(H1) $\phi(a + b) = \phi(a) + \phi(b)$ for all $a, b \in R$;
(H2) $\phi(ab) = \phi(a)\phi(b)$ for all $a, b \in R$.

A bijective ring homomorphism is called a *ring isomorphism*. If there exists a ring isomorphism from R to S we say that R and S are *isomorphic*, and write $R \cong S$.

An isomorphism from a ring onto itself is called a *ring automorphism*.

Note that property **(H1)** says that ϕ is an additive group homomorphism.

Problem 13. Let $\phi : R \to S$ be a ring homomorphism.
(a) Show that $\phi(0_R) = 0_S$.
(b) Show that $\phi(-r) = -\phi(r)$ for every $r \in R$.

Solution. For part **(a)**, we write $\phi(0_R) = \phi(0_R + 0_R) = \phi(0_R) + \phi(0_R)$. Subtract $\phi(0_R)$ from both sides, and switch the sides, to get $\phi(0_R) + \phi(0_R) - \phi(0_R) = \phi(0_R) - \phi(0_R)$, whence $\phi(0_R) + 0_S = 0_S$, so $\phi(0_R) = 0_S$.

For part **(b)**, we note that $\phi(r) + \phi(-r) = \phi(r - r) = \phi(0_R) = 0_S$; thus, $\phi(-r)$ is the unique additive inverse of $\phi(r)$, that is to say, $\phi(-r) = -\phi(r)$. □

Problem 14. Let $\phi : R \to S$ be a ring homomorphism with S nonzero.
Show that if $r \in R$ is invertible, then $\phi(r)$ is invertible and $\phi(r^{-1}) = \phi(r)^{-1}$.

Solution. Suppose that r is invertible. Now $\phi(r) \cdot \phi(r^{-1}) = \phi(rr^{-1}) = \phi(1_R) = 1_S$ by **(H0)**; thus $\phi(r^{-1})$ is the multiplicative inverse of $\phi(r)$ in S; that is to say, $\phi(r^{-1}) = \phi(r)^{-1}$. □

Problem 15. Let $\phi : R \to S$ be a ring homomorphism and let $T \leq R$.
Show that $\phi(T) \leq S$.

Solution. To prove that something is a subring, we show properties **(S0)**, **(S1)**, **(S2)**, and **(S3)**.

(S0) By **(S0)**, $1_R \in T$. By **(H0)**, $\phi(1_R) = 1_S$, so $1_S \in \phi(T)$.

(S1) Let $s_1, s_2 \in \phi(T)$. Then $s_1 = t_1$ and $s_2 = t_2$ for some $t_1, t_2 \in T$. Since T is a subring, $t_1 + t_2 \in T$, so $s_1 + s_2 = \phi(t_1) + \phi(t_2) = \phi(t_1 + t_2) \in \phi(T)$.

(S2) Let $s \in \phi(T)$. Then $s = \phi(t)$ for some $t \in T$. Since T is a subring, $-t \in T$, so $-s = -\phi(t) = \phi(-t) \in \phi(T)$.

(S3) Let $s_1, s_2 \in \phi(T)$. Then $s_1 = t_1$ and $s_2 = t_2$ for some $t_1, t_2 \in T$. Since T is a subring, $t_1 t_2 \in T$, so $s_1 s_2 = \phi(t_1) \cdot \phi(t_2) = \phi(t_1 t_2) \in \phi(T)$. □

Problem 16. Let $\phi : R \to S$ and $\psi : S \to T$ be ring homomorphisms.
Show that $\psi \circ \phi : R \to T$ is a ring homomorphism.

Proof. To show that something is a ring homomorphism, we show **(H0)**, **(H1)**, and **(H2)**.

(H0) $\psi \circ \phi(1_R) = \psi(\phi(1_R)) = \psi(1_S) = 1_T$.

(H1) Let $r_1, r_2 \in R$. Then

$$\psi\circ\phi(r_1+r_2) = \psi(\phi(r_1+r_2)) = \psi(\phi(r_1)+\phi(r_2)) = \phi(\phi(r_1))+\phi(\psi(r_2)) = \phi\circ\psi(r_1)+\phi\circ\psi(r_2).$$

(H2) Let $r_1, r_2 \in R$. Then

$$\psi \circ \phi(r_1 r_2) = \psi(\phi(r_1 r_2)) = \psi(\phi(r_1) \cdot \phi(r_2)) = \phi(\phi(r_1)) \cdot \phi(\psi(r_2)) = \phi \circ \psi(r_1) \cdot \phi \circ \psi(r_2).$$

□

Problem 17. Let $\phi : F \to S$ be a ring homomorphism, where F is a field and S is nonzero. Show that ϕ is injective.

Solution. Let $x \in F$ be nonzero. By Problem , $\phi(x)$ is invertible in S. Since S is nonzero, $x \neq 0$. So the only member of F which maps to zero is zero.

Let $x_1, x_2 \in F$, and suppose that $\phi(x_1) = \phi(x_2)$. Then $\phi(x_1) - \phi(x_2) = 0$, so $\phi(x_1 - x_2) = 0$, which indicates that $x_1 - x_2 = 0$; hence, $x_1 = x_2$. Therefore, ϕ is injective. □

Thus the image of F in S is a subfield of S which is isomorphic to F.

7. Ideals

Definition 10. Let R be a commutative ring. An *ideal* of R is a subset $I \subset R$ such that

(I1) $a, b \in I \Rightarrow a + b \in I$;
(I2) $a \in I \Rightarrow ar \in I$.

If I is an ideal of R, we write $I \lhd R$.

Since $-1 \in R$, properties **(I1)** and **(I2)** say that I is an additive subgroup of R. It is easy to see that $\{0\} \lhd R$ and $R \lhd R$.

Definition 11. Let R be a ring and let $I \lhd R$.
We say that I is *improper* if $I = R$; otherwise I is *proper*.
We say that I is *trivial* if $I = \{0\}$; otherwise I is *nontrivial*.
We say that R is *simple* if $I \lhd R \Rightarrow I = \{0\}$ or $I = R$.

Problem 18. Let R be a ring and $I \lhd R$. Show that if I contains an invertible element, then I is improper.

Problem 19. Let R be a commutative ring. Show that R is simple if and only if R is a field.

Problem 20. Let R be a ring and let $I, J \lhd R$. Show that $I \cap J \lhd R$.

Problem 21. Let R be a ring and let $I, J \lhd R$. Set

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

Show that $I + J \lhd R$.

Definition 12. Let $\phi : R \to S$ be a ring homomorphism. The *kernel* of ϕ is denoted by $\ker(\phi)$ and is defined to be the subset of R given by

$$\ker(\phi) = \{r \in R \mid \phi(r) = 0_S\}.$$

Problem 22. Let $\phi : R \to S$ be a ring homomorphism.
Show that $\ker(\phi) \lhd R$.

Problem 23. Let $\phi : R \to S$ be a ring homomorphism.
Show that ϕ is injective if and only if $\ker(\phi) = \{0\}$.

Problem 24. Let $\phi : R \to S$ be a surjective ring homomorphism and let $I \lhd R$.
Show that $\phi(I) \lhd R$.

Problem 25. Give an example of a nonsurjective ring homomophism $\phi : R \to S$ and an ideal $I \lhd R$ such that $\phi(I)$ is not an ideal in S.

8. Factor Rings

Definition 13. Let R be a ring and let $I \triangleleft R$. Let $x \in R$. The *coset* for x of I in R is the set

$$x + I = \{x + a \mid a \in I\}.$$

Let $x, y \in R$. We say that x and y are *congruent modulo* I, and write $x \equiv y \mod I$, if $x - y \in I$.

Let R/I denote the set of all cosets of I in R. The *index* of I in R is $[R : I] = |R/I|$.

Ideals are additive normal subgroups. Thus cosets in ring theory are a special case of cosets for groups under addition.

Let R be a commutative ring and let $I \triangleleft R$. From the theory of groups, we know that an equivalent condition for congruence is $x + I = y + I \Leftrightarrow x - y \in I$, and that congruence modulo I is an equivalence relation on R. The cosets partition R into blocks of equal size. If R is finite, then $|R| = |R/I|[R : I]$. Moreover, we know that addition on R/I, given by

$$(x + I) + (y + I) = (x + y) + I,$$

is well-defined, and endows R/I with the structure of an additive group. The ideal condition **(I2)** is the necessary extra condition which ensures that multiplication, defined by

$$(x + I) \cdot (y + I) = xy + I,$$

is also well-defined, and produces a ring structure on R/I. We call R/I a *factor ring* of R by I.

Define a function $\beta : R \to R/I$ by $\beta(x) = x + I$. Show that β is a surjective ring homomorphism whose kernel is I. We call β the *canonical* homomorphism from R to R/I. Thus every kernel is an ideal and every ideal is a kernel.

9. Isomorphism Theorem

Problem 26. (Isomorphism Theorem)
Let $\phi : R \to S$ be a ring homomorphism and let $K = \ker(\phi)$. Let $\beta : R \to R/K$ be the canonical homomorphism. Define a function $\overline{\phi} : R/K \to S$ by $\overline{\phi}(x+K) = \phi(x)$.

- **(a)** Show that $\overline{\phi}$ is well-defined.
- **(b)** Show that $\overline{\phi}$ is an injective ring homomorphism.
- **(c)** Show that $\phi = \overline{\phi} \circ \beta$.
- **(d)** Show that if ϕ is surjective, then $\overline{\phi}$ is a ring isomorphism.

Remark 1. Thus every homomorphic image of R is isomorphic to a quotient of R, and every quotient of R is a homomorphic image of R.

Problem 27. Let R be a ring and let $I, J \triangleleft R$ such that $I \subset J$. Let $\beta : R \to R/I$ and $\alpha : R \to R/J$ be the canonical homomorphisms. Set $J/I = \{a + I \in R/I \mid a \in J\}$. Define $\gamma : R/I \to R/J$ by $\gamma(a + I) = a + J$.

- **(a)** Show that γ is a well-defined surjective ring homomorphism.
- **(b)** Show that $\alpha = \gamma \circ \beta$.
- **(c)** Show that $J/I \triangleleft R/I$.
- **(d)** Show that

$$\frac{R}{J} \cong \frac{R/I}{J/I}.$$

Problem 28. (Correspondence Theorem)
Let $\phi : R \to S$ be a surjective ring homomorphism and let $K = \ker(\phi)$. Set

$$\mathcal{I} = \{I \triangleleft R \mid K \subset I\} \quad \text{and} \quad \mathcal{J} = \{J \triangleleft S\}.$$

Define a function

$$\Phi : \mathcal{I} \to \mathcal{J} \quad \text{by} \quad \Phi(I) = \phi(I).$$

- **(a)** Show that Φ is bijective.
- **(b)** Show that $I_1 \subset I_2 \Leftrightarrow \Phi(I_1) \subset \Phi(I_2)$.

Remark 2. Thus the ideals in the range of a ring homomorphism correspond to the ideals in the domain which contain the kernel. This correspondence is inclusion preserving. Via the isomormorphism theorem, this is equivalent to the fact that the ideals in R which contain I correspond to the ideals in R/I.

Problem 29. (Chinese Remainder Theorem)
Let R be a commutative ring and let $I, J \triangleleft R$ such that $I + J = R$.
Define a function $\phi : R \to R/I \times R/J$ by $\phi(r) = (r + I, r + J)$.

- **(a)** Show that for every $a \in R$ there exist $x, y \in R$ such that $x \equiv a \mod I$ and $y \equiv a \mod J$.
- **(b)** Show the ϕ is a surjective homomorphism with kernel $I \cap J$.
- **(c)** Conclude that

$$R/(I \cap J) \cong R/I \times R/J.$$

10. Polynomial Rings

Definition 14. Let R be a commutative ring. A *polynomial over R with indeterminate X* is an expression of the form

$$f(X) = a_0 + a_1X + \cdots + a_nX^n = \sum_{i=0}^{n} a_iX^i,$$

where $a_i \in R$ for $i = 0, 1, \ldots, n$, and $a_n \neq 0$. The *degree* of f is n. The a_i's are called *coefficients*. The *leading coefficient* is a_n. The *constant coefficient* is a_0.

Let f and g be polynomials over R.

Define *polynomial addition* by

$$(f+g)(X) = \sum_{i=0}^{d}(a_i + b_i)X^i,$$

where $a_i = 0$ if $i > m$, $b_i = 0$ if $i > n$, and d is the largest integer i less than or equal to $\max\{m, n\}$ such that $a_i + b_i \neq 0$.

Define *polynomial multiplication* by

$$(fg)(X) = \sum_{i=0}^{d} c_iX^i,$$

where $a_i = 0$ if $i > m$, $b_i = 0$ if $i > n$,

$$c_i = \sum_{j=0}^{i} a_jb_{i-j},$$

and d is the largest integer less than or equal to $m + n$ such that $c_i \neq 0$.

Problem 30. Let R be a commutative ring, and let $R[X]$ denote the set of all polynomials over R. Verify that $R[X]$, together with polynomial addition and multiplication as defined above, is a ring.

Definition 15. Let R be a commutative ring and let $f \in R[X]$. Then

$$f(X) = \sum_{i=0}^{n} a_iX^i$$

for some $a_i \in R$.

Let $x \in R$. The *evaluation* of f at x is

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

This induces a function, which we also denote by f, defined by

$$f : R \to R \quad \text{given by} \quad f(x) = \sum_{i=0}^{n} a_ix^i.$$

Let $r \in R$. The *evaluation map* induced by r is

$$\psi_r : R[X] \to R \quad \text{given by} \quad \psi_r(f) = f(r).$$

Problem 31. Let R be a commutative ring and let $r \in R$. Let $f, g \in R[X]$.

(a) Show that $\psi_r(f + g) = \psi_r(f) + \psi_r(g)$.

(b) Show that $\psi_r(fg) = \psi_r(f) \cdot \psi_r(g)$.

11. Polynomial Division

Proposition 1. (The Division Algorithm for Polynomial)
Let F be a field and let $f, g \in F[X]$. Then there exist $q, r \in F[X]$ such that

$$g = fq + r \quad \text{and} \quad \deg(r) < \deg(f).$$

Reason. We call r the *remainder*, q the *quotient*, f the *divisor*, and g the *dividend*.

Use long division to divide f into g. This process stops when the remainder is of degree less than that of f. Let q be the quotient and let r be the remainder. □

We divide by a linear polynomial and use the division algorithm to show that remainders are values of the dividend.

Proposition 2. (Remainder Theorem)
Let F be a field and let $g \in F[X]$. Let $a \in F$ and set $f(x) = x - a$. Write $g = fq + r$ with $\deg(r) < \deg(f)$. Then $r \in F$, and $g(a) = r$.

Proof. A polynomial of degree 0 is a constant, and since $\deg(r) < \deg(f) = 1$, we see that $\deg(r) = 0$, so $r \in F$. Thus $g(x) = f(x)q(x) + r$ for every $x \in F$. Plug in $x = a$ to see that

$$\begin{aligned} g(a) &= f(a)q(a) + r \\ &= (a - a)q(a) + r && \text{because } f(x) = (x - a) \\ &= 0 \cdot q(a) + r \\ &= r \end{aligned}$$

□

We provide the precise condition under which a linear polynomial is a factor of another polynomial.

Proposition 3. (Factor Theorem)
Let F be a field and let $g \in F[X]$. Let $a \in F$ and set $f(x) = x - a$. Then $g(a) = 0$ if and only if $f \mid g$.

Proof. We prove both directions of the implication.

($\Rightarrow$) Suppose that $g(a) = 0$. Write $g = fq + r$ with $\deg(r) < \deg(f)$. By the Remainder Theorem, $r = g(a) = 0$, so $g = fq$. Thus $f \mid g$.

($\Leftarrow$) Suppose that $f \mid g$. Then $g = fq$ for some $q \in F[X]$, so $g(a) = f(a)q(a) = (a - a)q(a) = 0 \cdot q(a) = 0$. □

The Factor Theorem says that the zeros of g produce linear factors of g, and vice versa. Thus in order to find the x-intercepts of a polynomial g, we factor it.

12. Polynomial Quotient Rings

Definition 16. Let F be a field and let $f, g, h \in F[X]$. We say that g *is congruent to* h *modulo* f, and write $g \equiv h \pmod{f}$, if f divides $g - h$; that is,

$$g \equiv h \pmod{f} \quad \Leftrightarrow \quad f \mid (g - h).$$

Proposition 4. *Let F be a field and let $f \in F[x]$ with $\deg(f) > 0$. Then congruence modulo f is an equivalence relation.*

Proof. We wish to show that the relation is reflexive, symmetric, and transitive.

(*Reflexive*) Let $g \in F[X]$. Then $(g-g) \cdot 0 = 0 = f \cdot 0$, so $f \mid (g-g)$. Thus $g \equiv g$.

(*Symmetric*) Let $g, h \in F[X]$ such that $g \equiv h$. Then $f \mid h - g$, so $g - h = fq$ for some $q \in F[X]$. So $h - g = f(-q)$, which shows that $f \mid g - h$, so $h \equiv g$.

(*Transitive*) Let $g, h, k \in F[X]$ such that $g \equiv h$ and $h \equiv k$. Then $f \mid h - g$ and $f \mid k - h$. Thus $h - g = fq_1$ and $k - h = fq_2$ for some $q_1, q_1 \in F[X]$. But then $h = g + fq_1$, and plugging this into the second equation gives $k - (g + fq_1) = fq_2$. After some algebra, $k - g = f(q_1 + q_2)$, so $f \mid (k - g)$. Therefore, $g \equiv k$.f □

Since congruence is an equivalence relation on $F[X]$, it partition $F[X]$ into equivalence classes. For $g \in F[X]$, let $\overline{g}$ denote the equivalence class of g, and let $\overline{F[X]}$ denote the set of all equivalence classes. Define addition and multiplication on $\overline{F[X]}$ by

$$\overline{g} + \overline{h} = \overline{g + h} \quad \text{and} \quad \overline{g} \cdot \overline{h} = \overline{gh}.$$

One can show that these operations are well defined, and satisfy the properties that promote $\overline{F[X]}$ to a commutative ring.

Definition 17. Let F be a field and let $f \in F[X]$. The *ring of polynomials over F modulo f* is $\overline{F[X]}$.

Department of Mathematics and CSci, BASIS Scottsdale
E-mail address: paul.bailey@basised.com