CATEGORY THEORY
RING THEORY SUMMARY

PAUL L. BAILEY

1. Binary Operations

Definition 1. A *binary operation* on a set A is a function

$$* : A \times A \to A.$$

We write $a * b$ to mean $*(a, b)$.

Definition 2. Let $*$ be a binary operation on a set A.

We say that $*$ is *commutative* if $a * b = b * a$ for all $a, b \in A$.

We say that $*$ is *associative* if $(a * b) * c = a * (b * c)$ for all $a, b, c \in A$.

We say that $e \in A$ is an *identity* for $*$ if $a * e = e * a = a$ for all $a \in A$.

We say that $\widehat{a} \in A$ is an *inverse* for $a \in A$ if $a * \widehat{a} = \widehat{a} * a = e$.

If $\triangle$ is another binary operation on A, we say that $\triangle$ *distributes* over $*$ if $(a * b) \triangle c = (a \triangle c) * (b \triangle c)$ and $a \triangle (b * c) = (a \triangle b) * (a \triangle c)$ for all $a, b, c, \in A$.

Problem 1. Let $*$ be a binary operation on a set A. Let $e, f \in A$ be identities for $*$. Show that $e = f$.

Problem 2. Let $*$ be an associative binary operation on a set A with identity e. Let $a \in A$ and let that $b, c \in A$ be inverses for a. Show that $b = c$.

Definition 3. Let $*$ be a binary operation on a set A, and let $B \subset A$. We say that $*$ is *closed* on B if $b * c \in B$ for every $b, c \in B$.

Definition 4. A *magma* is a set M together with a binary operation

$$* : M \times M \to M.$$

Definition 5. A *monoid* is a set M together with a binary operation

$$* : M \times M \to M$$

satisfying

(M1) $(a * b) * c = a * (b * c)$ for all $a, b, c \in M$;

(M2) there exists $e \in G$ such that $a * e = e * a = a$ for all $a \in M$.

Thus, a monoid is an associative magma with identity.

Definition 6. A *group* is a set G together with a binary operation

$$* : G \times G \to G$$

satisfying

(G1) $(a * b) * c = a * (b * c)$ for all $a, b, c \in G$;

(G2) there exists $e \in G$ such that $a * e = e * a = a$ for all $a \in G$;

(G3) for every $a \in G$ there exists $\widehat{a} \in G$ such that $a * \widehat{a} = \widehat{a} * a = e$.

Thus, a group is a monoid with inverses.

We sat that a group G is *abelian* if $a * b = b * a$ for every $a, b \in G$.

Date: January 9, 2020.

2. Rings

Definition 7. 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 $a, b, c \in R$.

Thus, a ring an abelian group under addition and a monoid under multiplication, where the operations are intertwined by the distributive property.

We say that a ring R is *commutative* if $ab = ba$ for every $a, b \in R$.

We will focus on commutative rings for the rest of this document.

Although the operations in rings can be denoted with different symbols (as long as the axioms are satisfied), we will use standard notation for addition and multiplication in general rings.

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.

To emphasize that a certain element acts as an identity in the ring R, we may write 0_R or 1_R instead of just 0 or 1. This is useful when comparing rings.

Problem 3. Let R be a ring and let $a, b \in R$.

(a) Show that $a \cdot 0 = 0 \cdot a = 0$.
(b) Show that $(-a)b = a(-b) = -(ab)$.

Problem 4. Let R be a ring and let $a, b \in R$. Let $n \in \mathbb{N}$.

(a) Show that $n(ab) = (na)b = a(nb)$.
(b) Show that $(-n)a = -(na)$.

3. Standard Rings

The reader should verify that the following examples of rings satisfy the axioms.

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

If R is a ring in which the additive and multiplicative identities are the same element, then R is the zero ring, because if $a \in R$, then $0 = 0 \cdot a = 1 \cdot a = a$, so $a = 0$.

Example 2. The following standard sets 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 $R \times S$ coordinatewise 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 $\mathcal{P}(X)$ be the collection of all subsets of X. Define addition and multiplication on $\mathcal{P}(X)$ by

- $A + B = A \triangle B = (A \cup B) \smallsetminus (A \cap B) = (A \smallsetminus B) \cup (B \smallsetminus A)$;
- $A \cdot B = A \cap B$.

Then $\mathcal{P}(X)$ is a commutative ring, called the *power set* of X.

Example 5. Let X be a set and let R be a 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 6. Let $\mathcal{C}(I)$ denote the set of all continuous functions $I \to \mathbb{R}$, where $I \subset \mathbb{R}$ is an interval. The operations are pointwise addition and multiplication.

Example 7. Let A be an additive abelian group and set

$$\mathrm{End}(A) = \{f : A \to A \mid f(a + b) = f(a) + f(b) \text{ for all } a, b \in A\}.$$

Define addition and multiplication of functions in $\mathrm{End}(A)$ by

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

Then $\mathrm{End}(A)$ is a ring, called the *ring of endomorphisms* of A.

Example 8. Let $\mathcal{B}$ denote the set of all continuous functions $I \to I$, where $I = [0, 1] \subset \mathbb{R}$ is the closed unit interval. Addition is pointwise addition, and multiplication is composition of functions. Let us call this the *box ring*.

4. Domains and Fields

Definition 8. 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 $aa^{-1} = 1$.

Problem 5. Let R be a commutative ring and let $a \in R$. Show that a is entire if and only if a is cancellable.

Problem 6. Let R be a commutative ring and let $a \in R$. Show that if a is invertible, then a is entire.

Definition 9. Let R be a nonzero commutative ring. Set

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

Problem 7. Let R be a nonzero commutative ring. Show that R^* is an abelian group under multiplication.

Definition 10. Let R be a commutative ring and let $a \in R$.
We say that a is a *zero divisor* if $a \neq 0$ and there exists $b \in R \setminus \{0\}$ such that $ab = 0$.

Problem 8. Let R be a commutative ring and let $a \in R$.
Show that a is a zero divisor if and only if a is a nonzero nonentire element of R.

Definition 11. 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 9. Let R be a commutative ring. Show that if R is a field, then R is an integral domain.

Problem 10. Let R be a finite integral domain. Let $a \in R \setminus \{0\}$ and define a function

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

(a) Show that μ_a is injective.
(b) Show that μ_a is surjective.
(c) Show that a is invertible.
(d) Conclude that R is a field.

Example 9. Describe the invertible elements, entire elements, and zero divisors of the following rings.

(a) $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$
(b) $\mathbb{Z} \times \mathbb{Z}$, $\mathbb{Z} \times \mathbb{Q}$, $\mathbb{Q} \times \mathbb{Q}$
(c) $\mathcal{P}(X)$, where $X = \{1, 2, 3\}$
(d) $\mathcal{C}(\mathbb{R})$ from Example 6
(e) $\mathcal{B}$ from Example 8
(f) $\mathrm{End}(\mathbb{Z})$ from Example 7

5. Subrings

Definition 12. 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 $S \leq R$.

Properties **(S1)** and **(S2)** say that S is an additive subgroup of R.

The restriction of $+$ and $\cdot$ to $S \times S$ induces a ring structure on S.

Note that R is a subring of itself, but $\{0\}$ is *not* a subring of R, unless R is the zero ring. We insist the subrings contain *the same* multiplicative identity

Problem 11. Let F be a field and let $R \leq F$. Show that R is an integral domain.

Problem 12. Let R be a ring and define the *center* of R to be

$$Z(R) = \{x \in R \mid xy = yx \text{ for all } y \in R\}.$$

Show that $Z(R) \leq R$.

Definition 13. A *subfield* of R is a subring $F \leq R$ such that

(F1) $a, b \in F \Rightarrow ab = ba$;
(F2) $a \in F \setminus \{0\} \Rightarrow a$ is invertible and $a^{-1} \in F$.

The restriction of $+$ and $\cdot$ to $F \times F$ induces a field structure on F.

Problem 13. Let $\mathbb{Q}[\sqrt{5}] = \{x \in \mathbb{R} \mid x = a + b\sqrt{5} \text{ for some } a, b \in \mathbb{Q}\}$. Show that $\mathbb{Q}[\sqrt{5}] \leq \mathbb{R}$.

Definition 14. Let X be a set and let $\mathcal{C} \subset \mathcal{P}(X)$ be a collection of subsets of X. Define the *intersection* and *union* of the collection by

- $\cap\mathcal{C} = \{x \in X \mid x \in C \text{ for all } C \in \mathcal{C}\}$;
- $\cup\mathcal{C} = \{x \in X \mid x \in C \text{ for some } C \in \mathcal{C}\}$.

Problem 14. Let R be a ring and let $\mathcal{S}$ be a nonempty collection of subrings of R.
Show that $\cap\mathcal{S}$ is a subring of R.

Definition 15. Let R be a ring and let $X \subset R$. The *subring generated by* X is denoted by $\mathrm{gr}_R(X)$ and is defined to be the intersection of all subrings of R which contain X.

Definition 16. Let F be a field and let $X \subset F$. The *subfield generated by* X is denoted by $\mathrm{gf}_F(X)$ and is defined to be the intersection of all subfields of F which contain X.

Since the intersection of rings is a ring, and the intersection of fields is a field, it is clear that $\mathrm{gr}_R(X)$ is the smallest subring of R which contains X, and that $\mathrm{gf}_F(X)$ is the smallest subfield of F which contains X.

Example 10. Let $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$ denote the smallest subring of $\mathbb{R}$ which contains $\mathbb{Q}$, $\sqrt{2}$, and $\sqrt{3}$.

(a) Describe $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$ and show that your description produces a subring of $\mathbb{R}$.
(b) Is $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$ a field?

Example 11. Let $\mathbb{Q}[\sqrt[3]{5}]$ denote the smallest subring of $\mathbb{R}$ such contains $\mathbb{Q}$ and $\sqrt[3]{5}$.

(a) Describe $\mathbb{Q}[\sqrt[3]{5}]$ and show that your description produces a subring of $\mathbb{R}$.
(b) Is $\mathbb{Q}[\sqrt[3]{5}]$ a field?

Example 12. Describe some meaningful subrings of the followings rings.

(a) $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$
(b) $\mathbb{Z} \times \mathbb{Z}$, $\mathbb{Z} \times \mathbb{Q}$, $\mathbb{Q} \times \mathbb{Q}$
(c) $\mathcal{P}(X)$, where $X = \{1, 2, 3\}$
(d) $\mathcal{C}(\mathbb{R})$ from Example 6
(e) $\mathcal{B}$ from Example 8
(f) $\mathrm{End}(\mathbb{Z})$ from Example 7

6. Ring Homomorphisms

Definition 17. 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*.

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

Problem 15. 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 $r \in R$.

Problem 16. 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 $\phi(r^{-1}) = \phi(r)^{-1}$.

Problem 17. Give an example of a ring homomorphism $\phi : R \to S$ such that $\phi(r) = s$ for some $r \in R$, $s \in S$, where s is invertible but r is not.

Problem 18. Let $\phi : R \to S$ be a ring isomorphism. Then $\phi^{-1} : S \to R$ is a bijective function. Show that ϕ^{-1} is a ring isomorphism.

Problem 19. Let $\phi : R \to S$ be a ring homomorphism and let $T \leq R$.
Show that $\phi(T) \leq S$.

Problem 20. Let $\phi : R \to S$ be a ring homomorphism and let $T \leq S$.
Show that $\phi^{-1}(T) \leq R$.

Problem 21. 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.

Problem 22. Let $\phi : R \to S$ be a ring homomorphism and let $X \subset R$.
Show that $\phi(\mathrm{gr}_R(X)) = \mathrm{gr}_S(\phi(X))$.

Problem 23. Let E and F be a fields.
Let $\phi : E \to F$ be a ring homomorphism and let $X \subset E$.
Show that $\phi(\mathrm{gf}_E(X)) = \mathrm{gf}_F(\phi(X))$.

Problem 24. Let $\phi : F \to S$ be a ring homomorphism, where F is a field and S is nonzero.
Show that ϕ is injective. Thus the image of F in S is a subfield of S which is isomorphic to F.

Example 13. Describe some meaningful ring homomorphisms between the following rings.

- $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$
- $\mathbb{Z} \times \mathbb{Z}$, $\mathbb{Z} \times \mathbb{Q}$, $\mathbb{Q} \times \mathbb{Q}$
- $\mathcal{P}(X)$, where $X = \{1, 2, 3\}$
- $\mathcal{C}(\mathbb{R})$ from Example 6
- $\mathcal{B}$ from Example 8
- $\mathrm{End}(\mathbb{Z})$ from Example 7

7. Ideals

Definition 18. Let R be a ring. An *ideal* of R is a subset $I \subset R$ such that

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

(I2) $a \in I$ and $r \in R \Rightarrow ra, ar \in I$.

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

Remark 1. Since $-1 \in R$, properties **(I1)** and **(I2)** say that I is an additive subgroup of R.

Problem 25. Let R be a ring. Show that $\{0\} \lhd R$ and $R \lhd R$.

Definition 19. 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 26. Let R be a ring and $I \lhd R$. Show that if I contains an invertible element, then I is improper.

Problem 27. Let R be a commutative ring. Show that R is simple if and only if R is a field.

Problem 28. Let R be a ring and let $\mathcal{I}$ be a collection of ideals of R. Show that $\cap\mathcal{I} \lhd R$.

Problem 29. 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 20. 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 30. Let $\phi : R \to S$ be a ring homomorphism.
Show that $\ker(\phi) \lhd R$.

Problem 31. Let $\phi : R \to S$ be a ring homomorphism.
Show that ϕ is injective if and only if $\ker(\phi) = \{0\}$.

Problem 32. Let $\phi : R \to S$ be a ring homomorphism and let $J \lhd S$.
Show that $\phi^{-1}(J) \lhd R$.

Problem 33. Let $\phi : R \to S$ be a surjective ring homomorphism and let $I \lhd R$.
Show that $\phi(I) \lhd R$.

Problem 34. Give an example of a nonsurjective ring homomorphism $\phi : R \to S$ and an ideal $I \lhd R$ such that $\phi(I)$ is not an ideal in S.

Problem 35. Let R be a ring and let $\mathcal{I}$ be a nonempty collection of ideals in R. Show that $\cap\mathcal{I} \lhd R$.

Definition 21. Let R be a ring and let $X \subset R$. The *ideal generated by* X is denoted $\mathrm{gi}_R(X)$ or $\langle X \rangle$ and is defined to be the intersection of all ideals of R which contain X.

Problem 36. Let R be a ring and let $I, J \lhd R$. Show that $\mathrm{gi}_R(I \cup J) = I + J$.

Problem 37. Let $\phi : R \to S$ be a surjective ring homomorphism and let $X \subset R$.
Show that $\phi(\mathrm{gi}_R(X)) = \mathrm{gi}_S(\phi(X))$.

Example 14. Consider your homomorphisms from Example 13. In each case, describe the kernel.

8. Factor Rings

Definition 22. 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 $x - y \in I$.

Problem 38. Let R be a ring and let $I \triangleleft R$.

(a) Show that $0 \in I$.
(b) Let $x, y \in R$. Show that $x + I = y + I \Leftrightarrow x - y \in I$.
(c) Show that congruence modulo I is an equivalence relation.
(b) Show that the congruence classes modulo I are the cosets of I in R.

Problem 39. Let R be a ring and let $I \triangleleft R$. Let R/I denote the collection of cosets of I in R. Define addition and multiplication on R/I by $(x + I) + (y + I) = (x + y) + I$ and $(x + I)(y + I) = xy + I$. Show that these operations are well-defined and induce a ring structure on R/I. We call R/I a *factor ring*, or the *quotient* of R by I.

Problem 40. Let R be a ring and let $I \triangleleft R$. 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.

Problem 41. (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.

Problem 42. (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 $I_1 \subset I_2 \Leftrightarrow \Phi(I_1) \subset \Phi(I_2)$.

Problem 43. (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 $R/(I \cap J) \cong R/I \times R/J$.

Example 15. Let $C = \mathcal{C}(\mathbb{R})$ be the ring of continuous functions $\mathbb{R} \to \mathbb{R}$. Consider the function $\phi : C \to \mathbb{R}$ given by $\phi(f) = f(0)$.

(a) Show that ϕ is a ring homomorphism.
(b) Let $K = \ker(\phi)$. Describe K.
(c) Show that $C/K \cong \mathbb{R}$.

9. Polynomial Rings

Definition 23. Let R be a commutative ring. A *polynomial* over R with indeterminate X is an expression of the form

$$f(X) = \sum_{i=0}^{\infty} a_i X^i = a_0 + a_1 X + a_2 X^2 + \cdots,$$

where $a_i \in R$ and $a_i = 0$ for all but finitely many i.

The *degree* of f is

$$\deg(f) = \max\{i \in \mathbb{N} \mid a_i \neq 0\}.$$

If $\deg(f) = n$, we normally write is permissible to write

$$f(X) = \sum_{i=0}^{n} a_i X^i = a_0 + a_1 X + \cdots + a_n X^n.$$

The *coefficients* of f are the elements $a_i \in R$ for $i \leq \deg(f)$.

The *constant coefficient* of f is a_0.

The *leading coefficient* of f is a_n, where $n = \deg(f)$. We say that f is *monic* if $a_n = 1$.

We define addition and multiplication of polynomials as follows.

Let $f(X) = \sum_{i=0}^{\infty} a_i X^i$ and $g(x) = \sum_{i=0}^{\infty} b_i X^i$. Then

- $(f+g)(X) = \sum_{i=0}^{\infty} (a_i + b_i) X^i$;
- $(fg)(X) = \sum_{i=0}^{\infty} c_i X_i$, where $c_i = \sum_{j+k=i} a_j b_k$.

Let $R[X]$ denote the set of all polynomials with indeterminate X over R. Then $R[X]$ is a commutative ring, called the *ring of polynomials* over R, and R embeds in $R[X]$ via $a \mapsto (a, 0, 0, 0, \dots)$; we will consider R to be a subring of $R[X]$. The members of R in $R[X]$ are called *constants*.

Problem 44. Let R be a commutative ring and let $f, g \in R[X]$.

(a) Show that $\deg(f+g) \leq \max\{\deg(f), \deg(g)\}$;
(b) Show that $\deg(fg) \leq \deg(f) + \deg(g)$;
(c) Show that if R is an integral domain, then $\deg(fg) = \deg(f) + \deg(g)$.

Problem 45. Let D be an integral domain. Show that $D[X]$ is an integral domain.

Problem 46. Let F be a field and let $f \in F[X]$. Show that f is invertible if and only if $f \in F \setminus \{0\}$.

10. Evaluation Map

Definition 24. Let R be a subring of a commutative ring S. Let $f \in R[X]$; then $f = \sum_{i=0}^{n} a_i X^i$. Let $s \in S$ and set $f(s) = \sum_{i=0}^{n} a_i s^i \in S$. We call $f(s)$ f *evaluated at* s. If $f(s) = 0_S$, we say that s is a *zero*, or *root*, of f.

Problem 47. (Universal Property of Polynomial Rings)
Let R be a subring of a commutative ring S. Let $s \in S$ and define a function

$$\psi_s : R[X] \to S \text{ by } \psi_s(f) = f(s).$$

Show that ψ_s is a homomorphism, called an *evaluation map*.

Problem 48. (Division Algorithm for Polynomials)
Let F be a field and let $f, d \in F[X]$.
Show that there exist unique polynomials $q, r \in F[X]$ with $\deg(r) < \deg(d)$ such that $f = dq + r$.
(Hint: consider the set $\{f - dq \mid q \in F[X]\} \subset F[X]$; this set contains a polynomial of minimal degree.)

Problem 49. (Remainder Theorem)
Let F be a field and let $f \in F[X]$. Let $a \in F$ and set $d(X) = (X - a)$.
Let $q, r \in F[X]$ with $\deg(r) < \deg(f)$ and $f = dq + r$. Show that $r \in F$ and $g(a) = r$.

Problem 50. (Factor Theorem)
Let F be a field. Let $f \in F[X]$ and let $a \in F$. Show that $f(a) = 0$ if and only if $(X - a) \mid f(X)$.

Problem 51. Let F be a field and let $f \in F[X]$ of degree n.
Show that f has at most n roots in R.

11. Principal Ideals

Definition 25. Let R be a ring and let $I \lhd R$.
We say that I is a *principal ideal* if $I = \text{gi}_R(\{a\})$ for some $a \in R$.

Problem 52. Let R be a commutative ring and let $a \in R$. Let $aR = \{ax \mid x \in R\}$.
Show that aR is the principal ideal generated by a.

Problem 53. Let R be a commutative ring and let $I \lhd R$ be a principal ideal.
Show that there exists $a \in R$ such that $I = aR$.

Problem 54. Let $\phi : R \to S$ be a surjective ring homomorphism, where R is commutative.

(a) Let $a \in R$. Show that $\phi(aR) = \phi(a)S$.
(b) Conclude that the surjective homomorphic image of a principal ideal is principal.

Definition 26. A *principal ring* is a commutative ring in which all ideals are principal.

Problem 55. Let R be a principal ring.

(a) Let $I \lhd R$. Show that R/I is a principal ring.
(b) Let $\phi : R \to S$ be a surjective ring homomorphism. Show that S is a principal ring.

Definition 27. A *principal ideal domain* (pid) is an integral domain in which all ideals are principal.

Notation 1. If R is a ring and $I \lhd R$, it is common to write

$$I = \langle a \rangle$$

to mean that I is the ideal generated by a. This is useful when dealing with pids.

Problem 56. Show that $\mathbb{Z}$ is a pid.

Problem 57. Let $I \lhd \mathbb{Z}$. Show that there exists a unique nonnegative integer $n \in \mathbb{Z}$ such that $I = \langle n \rangle$.

Problem 58. Let R be a ring. Show that there exists a unique ring homomorphism $\phi : \mathbb{Z} \to R$.

Definition 28. Let R be a ring. The *characteristic* of R is the nonnegative generator of the kernel of the unique homomorphism $\mathbb{Z} \to R$.

Example 16. Find the characteristic of the following rings:

$$\mathbb{Z}, \mathbb{Q}, \mathbb{Q}[X], \mathbb{Z}_5, \mathbb{Z}_5[X], \mathbb{Z}_6[X], \mathcal{P}(\{1,2,3\}), \mathcal{F}(\mathbb{N}, \mathbb{Z}_5).$$

Problem 59. Let F be a field. Show that $F[X]$ is a pid.

Definition 29. We say that a polynomial is *monic* if its leading coefficient is one.

Problem 60. Let F be a field and let $I \lhd F[X]$. Show that there exists a unique monic polynomial $f \in F[X]$ such that $I = \langle f \rangle$.

Definition 30. Let S be a commutative ring which contains a field F. Let $a \in S$ and let $\psi_a : F[X] \to S$ be the evaluation map given by $f \mapsto f(a)$.
The *minimum polynomial* of a in F is the a unique monic polynomial $f \in F[X]$ which generates the kernel of ψ_a.

Many common results from number theory carry over from the integers to polynomials based on the fact that both are pids.

Definition 31. Let E be a field which contains a field F. Let $a \in E$. We say that a is *algebraic* over F if there exists a polynomial $f \in F[X]$ such that $f(a) = 0$. Otherwise, we say that a is *transcendental* over F.

Problem 61. Let E be a field which contains a field F. Let $a \in E$ and let $F[a]$ denote the image of the evaluation map $\psi_a : F[X] \to E$. Explain why $F[a]$ is the smallest subring of E which contains F and a.

Problem 62. Let E be a field which contains a field F and let $a \in E$.

(a) Show that if a is algebraic over F, then $F[a]$ is a field.
(b) Show that if a is transcendental over F, then $F[a]$ is an integral domain isomorphic to $F[X]$.

(Hint: You may use Prob 77 if you wish; or, you may show this directly.)

12. Divisors and Associates

Definition 32. Let D be an integral domain 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 $a \nmid b$.
If $a|b$, we may say that a is a *divisor* of b, that a is a *factor* of b, or that b is a *multiple* of a.

Definition 33. 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 63. Let R be a commutative ring and let $a, b \in R^\bullet$.

(a) Show that $a \sim b$ if and only if there exists an invertible element $u \in R$ such that $b = ua$.
(b) Show that $\sim$ is an equivalence relation on $R^\bullet$.

Example 17. When are two integers associates? When are two polynomials associates?

Problem 64. 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 $abR \subset aR \cap bR$.

Definition 34. Let D be a domain and let $a, b \in R^\bullet$.
We say that $d \in R^\bullet$ is a *greatest common divisor* of a and b, and write $d \vDash \gcd(a, b)$, if

(GCD1) $d \mid a$ and $d \mid b$;
(GCD2) $e \mid a$ and $e \mid b \Rightarrow e \mid d$.

Problem 65. Let D be an integral domain and let $a, b, d, e, u \in D$, where u is invertible.

(a) Show that if $d \vDash \gcd(a, b)$, then $ud \vDash \gcd(a, b)$.
(b) Show that if $d \vDash \gcd(a, b)$ and $e \vDash \gcd(a, b)$, then $d \sim e$.

Problem 66. Let D be a pid and let $a, b \in D$. Show that there exists $d \in D$ such that $d \vDash \gcd(a, b)$.

Problem 67. Let D be a pid and let $a, b \in D$. Let $d \vDash \gcd(a, b)$.
Show that there exist $x, y \in D$ such that $d = ax + by$.

Definition 35. Let R be a commutative ring and let $a, b \in R^\bullet$.
We say that $l \in R^\bullet$ is a *least common multiple* of a and b, and write $l \vDash \operatorname{lcm}(a, b)$, if

(LCM1) $a \mid l$ and $b \mid l$;
(LCM2) $a \mid m$ and $b \mid m \Rightarrow l \mid m$.

Problem 68. Let D be an integral domain and let $a, b, l, m, u \in D$, where u is invertible.

(a) Show that if $l \vDash \operatorname{lcm}(a, b)$, then $ul \vDash \operatorname{lcm}(a, b)$.
(b) Show that if $l \vDash \operatorname{lcm}(a, b)$ and $m \vDash \operatorname{lcm}(a, b)$, then $l \sim m$.

Problem 69. Let D be a pid and let $a, b \in D$. Show that there exists $l \in D$ such that $l \vDash \operatorname{lcm}(a, b)$.

Problem 70. Let D be a pid and let $a, b \in D$. Let $d \vDash \gcd(a, b)$ and $l \vDash \operatorname{lcm}(a, b)$.
Show that $ab \sim dl$.

Problem 71. Let D be a pid, and let $a, b \in D$. Then

(a) $\langle a \rangle + \langle b \rangle = \langle \gcd(a, b) \rangle$.
(b) $\langle a \rangle \cap \langle b \rangle = \langle \operatorname{lcm}(a, b) \rangle$.

13. Maximal and Prime Ideals

Definition 36. Let R be a commutative ring and let $I \lhd R$.
We say that I is *prime* if $ab \in I \Rightarrow a \in I$ or $b \in I$ for all $a, b \in R$.

Problem 72. Let R be a commutative ring.
Show that $\{0\}$ is a prime ideal if and only if R is an integral domain.

Problem 73. Let R be a commutative ring and let $I \lhd R$.
Show that I is prime if and only if R/I is an integral domain.

Definition 37. Let R be a commutative ring and let $I \lhd R$.
We say that I is *maximal* if whenever $I \subset J \lhd R$, then either $J = I$ or $J = R$.

Problem 74. Let R be a commutative ring.
Show that $\{0\}$ is maximal if and only if R is a field.

Problem 75. Let R be a commutative ring and let $I \lhd R$.
Show that I is maximal if and only if R/I is a field.
(Hint: use the Correspondence Theorem.)

Problem 76. Let R be a commutative ring and let $I \lhd R$.
Show that if I is maximal, then I is prime.

Problem 77. Let R be a pid and let $I \lhd R$ be a nontrivial proper ideal.
Show that I is maximal if and only if I is prime.

Problem 78. Let R be a pid and let $I \lhd R$ be a nontrivial proper ideal.
Show that R/I is either a field or a nondomain.

Problem 79. Let $\phi : R \to S$ be a ring homomorphism, where R is a pid.
Show that $\phi(R)$ is either a field or a nondomain.

14. Irreducible and Prime Elements

Definition 38. Let R be a commutative ring and let $p \in R^\bullet \setminus R^*$.
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 80. Let R be a commutative ring and let $p, u \in R$, where u is invertible.

(a) Show that if p is irreducible, then so is up.

(b) Show that if p is prime, then so is up.

Problem 81. Let D be an integral domain and let $p \in D$.
Show that p is a prime element if and only if pD is a prime ideal.

Problem 82. Let D be a pid and let $p \in D$.
Show that pD is maximal if and only if p is irreducible.

Problem 83. Let D an integral domain and let $p \in D$.
Show that if p is prime, then p is irreducible.

Problem 84. Let D be a pid and let $p \in D$.
Show that p is prime if and only if p is irreducible.

Department of Mathematics, BASIS Scottsdale
Email address: paul.bailey@basised.com