EXERCISES

Section 1 Definition of a Ring

1.1. Prove that $7 + \sqrt[3]{2}$ and $\sqrt{3} + \sqrt{-5}$ are algebraic numbers.

1.2. Prove that, for $n \neq 0$, $\cos(2\pi/n)$ is an algebraic number.

1.3. Let $\mathbb{Q}[\alpha, \beta]$ denote the smallest subring of $\mathbb{C}$ containing the rational numbers $\mathbb{Q}$ and the elements $\alpha = \sqrt{2}$ and $\beta = \sqrt{3}$. Let $\gamma = \alpha + \beta$. Is $\mathbb{Q}[\alpha, \beta] = \mathbb{Q}[\gamma]$? Is $\mathbb{Z}[\alpha, \beta] = \mathbb{Z}[\gamma]$?

1.4. Let $\alpha = \frac{1}{2}i$. Prove that the elements of $\mathbb{Z}[\alpha]$ are dense in the complex plane.

1.5. Determine all subrings of $\mathbb{R}$ that are discrete sets.

1.6. Decide whether or not S is a subring of R, when

(a) S is the set of all rational numbers a/b, where b is not divisible by 3, and $R = \mathbb{Q}$,

(b) S is the set of functions which are linear combinations with integer coefficients of the functions $\{1, \cos nt, \sin nt\}$, $n \in \mathbb{Z}$, and R is the set of all real valued functions of t.

1.7. Decide whether the given structure forms a ring. If it is not a ring, determine which of the ring axioms hold and which fail:

(a) U is an arbitrary set, and R is the set of subsets of U. Addition and multiplication of elements of R are defined by the rules $A + B = (A \cup B) - (A \cap B)$ and $A \cdot B = A \cap B$.

(b) R is the set of continuous functions $\mathbb{R} \to \mathbb{R}$. Addition and multiplication are defined by the rules $[f + g](x) = f(x) + g(x)$ and $[f \circ g](x) = f(g(x))$.

1.8. Determine the units in: **(a)** $\mathbb{Z}/12\mathbb{Z}$, **(b)** $\mathbb{Z}/8\mathbb{Z}$, **(c)** $\mathbb{Z}/n\mathbb{Z}$.

1.9. Let R be a set with two laws of composition satisfying all ring axioms except the commutative law for addition. Use the distributive law to prove that the commutative law for addition holds, so that R is a ring.

Section 2 Polynomial Rings

2.1. For which positive integers n does $x^2 + x + 1$ divide $x^4 + 3x^3 + x^2 + 7x + 5$ in $[\mathbb{Z}/(n)][x]$?

2.2. Let F be a field. The set of all formal power series $p(t) = a_0 + a_1 t + a_2 t^2 + \cdots$, with a_i in F, forms a ring that is often denoted by $F[[t]]$. By *formal* power series we mean that the coefficients form an arbitrary sequence of elements of F. There is no requirement of convergence. Prove that $F[[t]]$ is a ring, and determine the units in this ring.

Section 3 Homomorphisms and Ideals

3.1. Prove that an ideal of a ring R is a subgroup of the additive group R^+.

3.2. Prove that every nonzero ideal in the ring of Gauss integers contains a nonzero integer.

3.3. Find generators for the kernels of the following maps:

(a) $\mathbb{R}[x, y] \to \mathbb{R}$ defined by $f(x, y) \rightsquigarrow f(0, 0)$,

(b) $\mathbb{R}[x] \to \mathbb{C}$ defined by $f(x) \rightsquigarrow f(2 + i)$,

(c) $\mathbb{Z}[x] \to \mathbb{R}$ defined by $f(x) \rightsquigarrow f(1 + \sqrt{2})$,

(d) $\mathbb{Z}[x] \to \mathbb{C}$ defined by $x \rightsquigarrow \sqrt{2} + \sqrt{3}$.
(e) $\mathbb{C}[x, y, z] \to \mathbb{C}[t]$ defined by $x \rightsquigarrow t,\ y \rightsquigarrow t^2,\ z \rightsquigarrow t^3$.

3.4. Let $\varphi: \mathbb{C}[x, y] \to \mathbb{C}[t]$ be the homomorphism that sends $x \rightsquigarrow t+1$ and $y \rightsquigarrow t^3 - 1$. Determine the kernel K of φ, and prove that every ideal I of $\mathbb{C}[x, y]$ that contains K can be generated by two elements.

3.5. The derivative of a polynomial f with coefficients in a field F is defined by the calculus formula $(a_n x^n + \cdots + a_1 x + a_0)' = n a_n x^{n-1} + \cdots + 1 a_1$. The integer coefficients are interpreted in F using the unique homomorphism $\mathbb{Z} \to F$.

(a) Prove the product rule $(fg)' = f'g + fg'$ and the chain rule $(f \circ g)' = (f' \circ g)g'$.
(b) Let α be an element of F. Prove that α is a multiple root of a polynomial f if and only if it is a common root of f and of its derivative f'.

3.6. An *automorphism* of a ring R is an isomorphism from R to itself. Let R be a ring, and let $f(y)$ be a polynomial in one variable with coefficients in R. Prove that the map $R[x, y] \to R[x, y]$ defined by $x \rightsquigarrow x + f(y),\ y \rightsquigarrow y$ is an automorphism of $R[x, y]$.

3.7. Determine the automorphisms of the polynomial ring $\mathbb{Z}[x]$ (see Exercise 3.6).

3.8. Let R be a ring of prime characteristic p. Prove that the map $R \to R$ defined by $x \rightsquigarrow x^p$ is a ring homomorphism. (It is called the *Frobenius map*.)

3.9. **(a)** An element x of a ring R is called *nilpotent* if some power is zero. Prove that if x is nilpotent, then $1 + x$ is a unit.

(b) Suppose that R has prime characteristic $p \neq 0$. Prove that if a is nilpotent then $1 + a$ is *unipotent*, that is, some power of $1 + a$ is equal to 1.

3.10. Determine all ideals of the ring $F[[t]]$ of formal power series with coefficients in a field F (see Exercise 2.2).

3.11. Let R be a ring, and let I be an ideal of the polynomial ring $R[x]$. Let n be the lowest degree among nonzero elements of I. Prove or disprove: I contains a monic polynomial of degree n if and only if it is a principal ideal.

3.12. Let I and J be ideals of a ring R. Prove that the set $I + J$ of elements of the form $x + y$, with x in I and y in J, is an ideal. This ideal is called the *sum* of the ideals I and J.

3.13. Let I and J be ideals of a ring R. Prove that the intersection $I \cap J$ is an ideal. Show by example that the set of products $\{xy \mid x \in I, y \in J\}$ need not be an ideal, but that the set of finite sums $\sum x_\nu y_\nu$ of products of elements of I and J is an ideal. This ideal is called the *product ideal*, and is denoted by IJ. Is there a relation between IJ and $I \cap J$?

Section 4 Quotient Rings

4.1. Consider the homomorphism $\mathbb{Z}[x] \to \mathbb{Z}$ that sends $x \rightsquigarrow 1$. Explain what the Correspondence Theorem, when applied to this map, says about ideals of $\mathbb{Z}[x]$.

4.2. What does the Correspondence Theorem tell us about ideals of $\mathbb{Z}[x]$ that contain $x^2 + 1$?

4.3. Identify the following rings: **(a)** $\mathbb{Z}[x]/(x^2 - 3, 2x + 4)$, **(b)** $\mathbb{Z}[i]/(2 + i)$, **(c)** $\mathbb{Z}[x]/(6, 2x - 1)$, **(d)** $\mathbb{Z}[x]/(2x^2 - 4, 4x - 5)$, **(e)** $\mathbb{Z}[x]/(x^2 + 3, 5)$.

4.4. Are the rings $\mathbb{Z}[x]/(x^2 + 7)$ and $\mathbb{Z}[x]/(2x^2 + 7)$ isomorphic?

Section 5 Adjoining Elements

5.1. Let $f = x^4 + x^3 + x^2 + x + 1$ and let α denote the residue of x in the ring $R = \mathbb{Z}[x]/(f)$. Express $(\alpha^3 + \alpha^2 + \alpha)(\alpha^5 + 1)$ in terms of the basis $(1, \alpha, \alpha^2, \alpha^3)$ of R.

5.2. Let a be an element of a ring R. If we adjoin an element α with the relation $\alpha = a$, we expect to get a ring isomorphic to R. Prove that this is true.

5.3. Describe the ring obtained from $\mathbb{Z}/12\mathbb{Z}$ by adjoining an inverse of 2.

5.4. Determine the structure of the ring R' obtained from $\mathbb{Z}$ by adjoining an element α satisfying each set of relations.

(a) $2\alpha = 6, 6\alpha = 15$, **(b)** $2\alpha - 6 = 0, \alpha - 10 = 0$, **(c)** $\alpha^3 + \alpha^2 + 1 = 0, \alpha^2 + \alpha = 0$.

5.5. Are there fields F such that the rings $F[x]/(x^2)$ and $F[x]/(x^2 - 1)$ are isomorphic?

5.6. Let a be an element of a ring R, and let R' be the ring $R[x]/(ax - 1)$ obtained by adjoining an inverse of a to R. Let α denote the residue of x (the inverse of a in R').

(a) Show that every element β of R' can be written in the form $\beta = \alpha^k b$, with b in R.

(b) Prove that the kernel of the map $R \to R'$ is the set of elements b of R such that $a^n b = 0$ for some $n > 0$.

(c) Prove that R' is the zero ring if and only if a is nilpotent (see Exercise 3.9).

5.7. Let F be a field and let $R = F[t]$ be the polynomial ring. Let R' be the ring extension $R[x]/(tx - 1)$ obtained by adjoining an inverse of t to R. Prove that this ring can be identified as the ring of *Laurent polynomials*, which are finite linear combinations of powers of t, negative exponents included.

Section 6 Product Rings

6.1. Let $\varphi : \mathbb{R}[x] \to \mathbb{C} \times \mathbb{C}$ be the homomorphism defined by $\varphi(x) = (1, i)$ and $\varphi(r) = (r, r)$ for r in $\mathbb{R}$. Determine the kernel and the image of φ.

6.2. Is $\mathbb{Z}/(6)$ isomorphic to the product ring $\mathbb{Z}/(2) \times \mathbb{Z}/(3)$? Is $\mathbb{Z}/(8)$ isomorphic to $\mathbb{Z}/(2) \times \mathbb{Z}/(4)$?

6.3. Classify rings of order 10.

6.4. In each case, describe the ring obtained from the field $\mathbb{F}_2$ by adjoining an element α satisfying the given relation:

(a) $\alpha^2 + \alpha + 1 = 0$, **(b)** $\alpha^2 + 1 = 0$, **(c)** $\alpha^2 + \alpha = 0$.

6.5. Suppose we adjoin an element α satisfying the relation $\alpha^2 = 1$ to the real numbers $\mathbb{R}$. Prove that the resulting ring is isomorphic to the product $\mathbb{R} \times \mathbb{R}$.

6.6. Describe the ring obtained from the product ring $\mathbb{R} \times \mathbb{R}$ by inverting the element $(2, 0)$.

6.7. Prove that in the ring $\mathbb{Z}[x]$, the intersection $(2) \cap (x)$ of the principal ideals (2) and (x) is the principal ideal $(2x)$, and that the quotient ring $R = \mathbb{Z}[x]/(2x)$ is isomorphic to the subring of the product ring $\mathbb{F}_2[x] \times \mathbb{Z}$ of pairs $(f(x), n)$ such that $f(0) \equiv n$ modulo 2.

6.8. Let I and J be ideals of a ring R such that $I + J = R$.

(a) Prove that $IJ = I \cap J$ (see Exercise 3.13).

(b) Prove the *Chinese Remainder Theorem*: For any pair a, b of elements of R, there is an element x such that $x \equiv a$ modulo I and $x \equiv b$ modulo J. (The notation $x \equiv a$ modulo I means $x - a \in I$.)

(c) Prove that if $IJ = 0$, then R is isomorphic to the product ring $(R/I)\times(R/J)$.
(d) Describe the idempotents corresponding to the product decomposition in (c).

Section 7 Fractions

7.1. Prove that a domain of finite order is a field.

7.2. Let R be a domain. Prove that the polynomial ring $R[x]$ is a domain, and identify the units in $R[x]$.

7.3. Is there a domain that contains exactly 15 elements?

7.4. Prove that the field of fractions of the formal power series ring $F[[x]]$ over a field F can be obtained by inverting the element x. Find a neat description of the elements of that field (see Exercise 11.2.1).

7.5. A subset S of a domain R that is closed under multiplication and that does not contain 0 is called a *multiplicative set*. Given a multiplicative set S, define S-fractions to be elements of the form a/b, where b is in S. Show that the equivalence classes of S-fractions form a ring.

Section 8 Maximal Ideals

8.1. Which principal ideals in $\mathbb{Z}[x]$ are maximal ideals?

8.2. Determine the maximal ideals of each of the following rings:
(a) $\mathbb{R}\times\mathbb{R}$, **(b)** $\mathbb{R}[x]/(x^2)$, **(c)** $\mathbb{R}[x]/(x^2-3x+2)$, **(d)** $\mathbb{R}[x]/(x^2+x+1)$.

8.3. Prove that the ring $\mathbb{F}_2[x]/(x^3+x+1)$ is a field, but that $\mathbb{F}_3[x]/(x^3+x+1)$ is not a field.

8.4. Establish a bijective correspondence between maximal ideals of $\mathbb{R}[x]$ and points in the upper half plane.

Section 9 Algebraic Geometry

9.1. Let I be the principal ideal of $\mathbb{C}[x, y]$ generated by the polynomial y^2+x^3-17. Which of the following sets generate maximal ideals in the quotient ring $R = \mathbb{C}[x, y]/I$? $(x-1, y-4)$, $(x+1, y+4)$, (x^3-17, y^2).

9.2. Let $f_1, \dots, f_r$ be complex polynomials in the variables $x_1, \dots, x_n$, let V be the variety of their common zeros, and let I be the ideal of the polynomial ring $R = \mathbb{C}[x_1, \dots, x_n]$ that they generate. Define a homomorphism from the quotient ring $\overline{R} = R/I$ to the ring $\mathcal{R}$ of continuous, complex-valued functions on V.

9.3. Let $U = \{f_i(x_1, \dots, x_m) = 0\}$, $V = \{g_j(y_1, \dots, y_n) = 0\}$ be varieties in $\mathbb{C}^m$ and $\mathbb{C}^n$, respectively. Show that the variety defined by the equations $\{f_i(x) = 0, g_j(y) = 0\}$ in x, y-space $\mathbb{C}^{m+n}$ is the product set $U\times V$.

9.4. Let U and V be varieties in $\mathbb{C}^n$. Prove that the union $U\cup V$ and the intersection $U\cap V$ are varieties. What does the statement $U\cap V = \emptyset$ mean algebraically? What about the statement $U\cup V = \mathbb{C}^n$?

9.5. Prove that the variety of zeros of a set $\{f_1, \dots, f_r\}$ of polynomials depends only on the ideal that they generate.

9.6. Prove that every variety in $\mathbb{C}^2$ is the union of finitely many points and algebraic curves.

9.7. Determine the points of intersection in $\mathbb{C}^2$ of the two loci in each of the following cases:
(a) $y^2-x^3+x^2=1,\ x+y=1$, **(b)** $x^2+xy+y^2=1,\ x^2+2y^2=1$,
(c) $y^2=x^3,\ xy=1$, **(d)** $x+y^2=0,\ y+x^2+2xy^2+y^4=0$.