of the continuous function $y-\alpha_i(x)$. Then V_i is also closed in the subset $\pi^{-1}(U)$ of $U \times \mathbb{C}$. It follows that V_1 is open in $\pi^{-1}(U)$, because it is the complement of the closed set $V_2 \cup \ldots \cup V_n$. Since U is open in $\mathbb{C}$, its inverse image $\pi^{-1}(U)$ is open in S. Thus V_1 is open in an open subset of S, which shows that V_1 is open in S too. Similarly, V_i is open for each i. □

We will look at these loci again in Chapter 13.

In helping geometry, modern algebra is helping itself above all.

Oscar Zariski

EXERCISES

1. Definition of a Ring

1. Prove the following identities in an arbitrary ring R.
   (a) $0a = 0$ **(b)** $-a = (-1)a$ **(c)** $(-a)b = -(ab)$
2. Describe explicitly the smallest subring of the complex numbers which contains the real cube root of 2.
3. Let $\alpha = \frac{1}{2}i$. Prove that the elements of $\mathbb{Z}[\alpha]$ form a dense subset of the complex plane.
4. Prove that $7 + \sqrt[3]{2}$ and $\sqrt{3} + \sqrt{-5}$ are algebraic numbers.
5. Prove that for all integers n, $\cos(2\pi/n)$ is an algebraic number.
6. Let $\mathbb{Q}[\alpha,\beta]$ denote the smallest subring of $\mathbb{C}$ containing $\mathbb{Q}$, $\alpha = \sqrt{2}$, and $\beta = \sqrt{3}$, and let $\gamma = \alpha + \beta$. Prove that $\mathbb{Q}[\alpha,\beta] = \mathbb{Q}[\gamma]$.
7. Let S be a subring of $\mathbb{R}$ which is a discrete set in the sense of Chapter 5 (4.3). Prove that $S = \mathbb{Z}$.
8. In each case, decide whether or not S is a subring of R.
   (a) S is the set of all rational numbers of the form a/b, where b is not divisible by 3, and $R = \mathbb{Q}$.
   (b) S is the set of functions which are linear combinations of the functions $\{1, \cos nt, \sin nt \mid n \in \mathbb{Z}\}$, and R is the set of all functions $\mathbb{R} \longrightarrow \mathbb{R}$.
   (c) (not commutative) S is the set of real matrices of the form $\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$, and R is the set of all real 2×2 matrices.
9. In each case, 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 $A + B = A \cup B$ and $A \cdot B = A \cap B$.
   (b) 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 $A \cdot B = A \cap B$.
   (c) R is the set of continuous functions $\mathbb{R} \longrightarrow \mathbb{R}$. Addition and multiplication are defined by the rules $[f + g](x) = f(x) + g(x)$ and $[f \circ g](x) = f(g(x))$.
10. Determine all rings which contain the zero ring as a subring.

11. Describe the group of units in each ring.
    (a) $\mathbb{Z}/12\mathbb{Z}$ (b) $\mathbb{Z}/7\mathbb{Z}$ (c) $\mathbb{Z}/8\mathbb{Z}$ (d) $\mathbb{Z}/n\mathbb{Z}$
12. Prove that the units in the ring of Gauss integers are $\{\pm 1, \pm i\}$.
13. An element x of a ring R is called *nilpotent* if some power of x is zero. Prove that if x is nilpotent, then $1 + x$ is a unit in R.
14. Prove that the product set $R \times R'$ of two rings is a ring with component-wise addition and multiplication:

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

This ring is called the *product ring*.

2. Formal Construction of Integers and Polynomials

1. Prove that every natural number n except 1 has the form m' for some natural number m.
2. Prove the following laws for the natural numbers.
   (a) the commutative law for addition
   (b) the associative law for multiplication
   (c) the distributive law
   (d) the cancellation law for addition: if $a + b = a + c$, then $b = c$
   (e) the cancellation law for multiplication: if $ab = ac$, then $b = c$
3. The relation $<$ on $\mathbb{N}$ can be defined by the rule $a < b$ if $b = a + n$ for some n. Assume that the elementary properties of addition have been proved.
   (a) Prove that if $a < b$, then $a + n < b + n$ for all n.
   (b) Prove that the relation $<$ is transitive.
   (c) Prove that if a, b are natural numbers, then precisely one of the following holds:

$$a < b,\ a = b,\ b < a.$$

   (d) Prove that if $n \neq 1$, then $a < an$.
4. Prove the principle of *complete induction:* Let S be a subset of $\mathbb{N}$ with the following property: If n is a natural number such that $m \in S$ for every $m < n$, then $n \in S$. Then $S = \mathbb{N}$.

*5. Define the set $\mathbb{Z}$ of all integers, using two copies of $\mathbb{N}$ and an element representing zero, define addition and multiplication, and derive the fact that $\mathbb{Z}$ is a ring from the properties of addition and multiplication of natural numbers.

6. Let R be a ring. The set of all formal power series $p(t) = a_0 + a_1 t + a_2 t^2 + \cdots$, with $a_i \in R$, forms a ring which is usually denoted by $R[[t]]$. (By *formal power series* we mean that there is no requirement of convergence.)
   (a) Prove that the formal power series form a ring.
   (b) Prove that a power series $p(t)$ is invertible if and only if a_0 is a unit of R.
7. Prove that the units of the polynomial ring $\mathbb{R}[x]$ are the nonzero constant polynomials.

3. Homomorphisms and Ideals

1. Show that the inverse of a ring isomorphism $\varphi: R \longrightarrow R'$ is an isomorphism.
2. Prove or disprove: If an ideal I contains a unit, then it is the unit ideal.
3. For which integers n does $x^2 + x + 1$ divide $x^4 + 3x^3 + x^2 + 6x + 10$ in $\mathbb{Z}/n\mathbb{Z}[x]$?

4. Prove that in the ring $\mathbb{Z}[x]$, $(2) \cap (x) = (2x)$.

5. Prove the equivalence of the two definitions (3.11) and (3.12) of an ideal.

6. Is the set of polynomials $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ such that 2^{k+1} divides a_k an ideal in $\mathbb{Z}[x]$?

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

8. Describe the kernel of the following maps.

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

(b) $\mathbb{R}[x] \longrightarrow \mathbb{C}$ defomed by $f(x) \rightsquigarrow f(2 + i)$

9. Describe the kernel of the map $\mathbb{Z}[x] \longrightarrow \mathbb{R}$ defined by $f(x) \rightsquigarrow f(1 + \sqrt{2})$.

* **10.** Describe the kernel of the homomorphism $\varphi: \mathbb{C}[x, y, z] \longrightarrow \mathbb{C}[t]$ defined by $\varphi(x) = t$, $\varphi(y) = t^2$, $\varphi(z) = t^3$.

* **11.** (a) Prove that the kernel of the homomorphism $\varphi: \mathbb{C}[x, y] \longrightarrow \mathbb{C}[t]$ defined by $x \rightsquigarrow t^2$, $y \rightsquigarrow t^3$ is the principal ideal generated by the polynomial $y^2 - x^3$.

(b) Determine the image of φ explicitly.

12. Prove the existence of the homomorphism (3.8).

13. State and prove an analogue of (3.8) when $\mathbb{R}$ is replaced by an arbitrary infinite field.

14. Prove that if two rings R, R′ are isomorphic, so are the polynomial rings $R[x]$ and $R'[x]$.

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

16. Prove that a polynomial $f(x) = \Sigma a_i x^i$ can be expanded in powers of $x - a$: $f(x) = \Sigma c_i (x - a)^i$, and that the coefficients c_i are polynomials in the coefficients a_i, with integer coefficients.

17. Let R, R' be rings, and let $R \times R'$ be their product. Which of the following maps are ring homomorphisms?

(a) $R \longrightarrow R \times R'$, $r \rightsquigarrow (r, 0)$

(b) $R \longrightarrow R \times R$, $r \rightsquigarrow (r, r)$

(c) $R \times R' \longrightarrow R$, $(r_1, r_2) \rightsquigarrow r_1$

(d) $R \times R \longrightarrow R$, $(r_1, r_2) \rightsquigarrow r_1 r_2$

(e) $R \times R \longrightarrow R$, $(r_1, r_2) \rightsquigarrow r_1 + r_2$

18. (a) Is $\mathbb{Z}/(10)$ isomorphic to $\mathbb{Z}/(2) \times \mathbb{Z}/(5)$?

(b) Is $\mathbb{Z}/(8)$ isomorphic to $\mathbb{Z}/(2) \times \mathbb{Z}/(4)$?

19. Let R be a ring of characteristic p. Prove that the map $R \longrightarrow R$ defined by $x \rightsquigarrow x^p$ is a ring homomorphism. This map is called the *Frobenius homomorphism*.

20. Determine all automorphisms of the ring $\mathbb{Z}[x]$.

21. Prove that the map $\mathbb{Z} \longrightarrow R$ (3.9) is compatible with multiplication of positive integers.

22. Prove that the characteristic of a field is either zero or a prime integer.

23. Let R be a ring of characteristic p. Prove that if a is nilpotent then $1 + a$ is *unipotent*, that is, some power of $1 + a$ is equal to 1.

24. (a) The *nilradical* N of a ring R is the set of its nilpotent elements. Prove that N is an ideal.

(b) Determine the nilradicals of the rings $\mathbb{Z}/(12)$, $\mathbb{Z}/(n)$, and $\mathbb{Z}$.

25. (a) Prove Corollary (3.20).

(b) Prove Corollary (3.22).

26. Determine all ideals of the ring $\mathbb{R}[[t]]$ of formal power series with real coefficients.

27. Find an ideal in the polynomial ring $F[x,y]$ in two variables which is not principal.

***28.** Let R be a ring, and let I be an ideal of the polynomial ring $R[x]$. Suppose that the lowest degree of a nonzero element of I is n and that I contains a monic polynomial of degree n. Prove that I is a principal ideal.

29. Let I, J be ideals of a ring R. Show by example that $I \cup J$ need not be an ideal, but show that $I + J = \{r \in R \mid r = x + y, \quad \text{with } x \in I, y \in J\}$ is an ideal. This ideal is called the *sum* of the ideals I, J.

30. **(a)** Let I, J be ideals of a ring R. Prove that $I \cap J$ is an ideal.
(b) 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 $\Sigma\, x_\nu y_\nu$ of products of elements of I and J is an ideal. This ideal is called the *product ideal*.
(c) Prove that $IJ \subset I \cap J$.
(d) Show by example that IJ and $I \cap J$ need not be equal.

31. Let I, J, J' be ideals in a ring R. Is it true that $I(J + J') = IJ + IJ'$?

***32.** If R is a noncommutative ring, the definition of an *ideal* is a set I which is closed under addition and such that if $r \in R$ and $x \in I$, then both rx and xr are in I. Show that the noncommutative ring of $n \times n$ real matrices has no proper ideal.

33. Prove or disprove: If $a^2 = a$ for all a in a ring R, then R has characteristic 2.

34. An element e of a ring S is called *idempotent* if $e^2 = e$. Note that in a product $R \times R'$ of rings, the element $e = (1,0)$ is idempotent. The object of this exercise is to prove a converse.
(a) Prove that if e is idempotent, then $e' = 1 - e$ is also idempotent.
(b) Let e be an idempotent element of a ring S. Prove that the principal ideal eS is a ring, with identity element e. It will probably not be a subring of S because it will not contain 1 unless $e = 1$.
(c) Let e be idempotent, and let $e' = 1 - e$. Prove that S is isomorphic to the product ring $(eS) \times (e'S)$.

4. *Quotient Rings and Relations in a Ring*

1. Prove that the image of the homomorphism φ of Proposition (4.9) is the subring described in the proposition.

2. Determine the structure of the ring $\mathbb{Z}[x]/(x^2 + 3, p)$, where (a) $p = 3$, (b) $p = 5$.

3. Describe each of the following rings.
(a) $\mathbb{Z}[x]/(x^2 - 3, 2x + 4)$ **(b)** $\mathbb{Z}[i]/(2 + i)$

4. Prove Proposition (4.2).

5. Let R' be obtained from a ring R by introducing the relation $\alpha = 0$, and let $\psi: R \longrightarrow R'$ be the canonical map. Prove the following *universal property* for this construction: Let $\varphi: R \longrightarrow \tilde{R}$ be a ring homomorphism, and assume that $\varphi(\alpha) = 0$ in $\tilde{R}$. There is a unique homomorphism $\varphi': R' \longrightarrow \tilde{R}$ such that $\varphi' \circ \psi = \varphi$.

6. Let I, J be ideals in a ring R. Prove that the residue of any element of $I \cap J$ in R/IJ is nilpotent.

7. Let I, J be ideals of a ring R such that $I + J = R$.
(a) Prove that $IJ = I \cap J$.

*(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 $x - a \in I$.]

8. Let I, J be ideals of a ring R such that $I + J = R$ and $IJ = 0$.
(a) Prove that R is isomorphic to the product $(R/I) \times (R/J)$.
(b) Describe the idempotents corresponding to this product decomposition (see exercise 34, Section 3).

5. Adjunction of Elements

1. Describe the ring obtained from $\mathbb{Z}$ by adjoining an element α satisfying the two relations $2\alpha - 6 = 0$ and $\alpha - 10 = 0$.

2. Suppose we adjoin an element α to $\mathbb{R}$ satisfying the relation $\alpha^2 = 1$. Prove that the resulting ring is isomorphic to the product ring $\mathbb{R} \times \mathbb{R}$, and find the element of $\mathbb{R} \times \mathbb{R}$ which corresponds to α.

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

4. Prove that the elements $1, t - \alpha, (t - \alpha)^2, \ldots, (t - \alpha)^{n-1}$ form a $\mathbb{C}$-basis for $\mathbb{C}[t]/((t - \alpha)^n)$.

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

6. In each case, describe the ring obtained from $\mathbb{F}_2$ by adjoining an element α satisfying the given relation.
(a) $\alpha^2 + \alpha + 1 = 0$ (b) $\alpha^2 + 1 = 0$

7. Analyze the ring obtained from $\mathbb{Z}$ by adjoining an element α which satisfies the pair of relations $\alpha^3 + \alpha^2 + 1 = 0$ and $\alpha^2 + \alpha = 0$.

8. Let $a \in R$. If we adjoin an element α with the relation $\alpha = a$, we expect to get back a ring isomorphic to R. Prove that this is so.

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

10. Determine the structure of the ring R' obtained from $\mathbb{Z}$ by adjoining element α satisfying each set of relations.
(a) $2\alpha = 6, 6\alpha = 15$ (b) $2\alpha = 6, 6\alpha = 18$ (c) $2\alpha = 6, 6\alpha = 8$

11. Let $R = \mathbb{Z}/(10)$. Determine the structure of the ring obtained by adjoining an element α satisfying each relation.
(a) $2\alpha - 6 = 0$ (b) $2\alpha - 5 = 0$

12. Let a be a unit in a ring R. Describe the ring $R' = R[x]/(ax - 1)$.

13. (a) Prove that the ring obtained by inverting x in the polynomial ring $R[x]$ is isomorphic to the ring of Laurent polynomials, as asserted in (5.9).
(b) Do the formal Laurent series $\sum_{-\infty}^{\infty} a_n x^n$ form a ring?

14. Let a be an element of a ring R, and let $R' = R[x]/(ax - 1)$ be the ring obtained by adjoining an inverse of a to R. Prove that the kernel of the map $R \longrightarrow R'$ is the set of elements $b \in R$ such that $a^n b = 0$ for some $n > 0$.

15. Let a be an element of a ring R, and let R' be the ring obtained from R by adjoining an inverse of a. Prove that R' is the zero ring if and only if a is nilpotent.

16. Let F be a field. Prove that the rings $F[x]/(x^2)$ and $F[x]/(x^2 - 1)$ are isomorphic if and only if F has characteristic 2.
17. Let $\overline{R} = \mathbb{Z}[x]/(2x)$. Prove that every element of $\overline{R}$ has a unique expression in the form $a_0 + a_1x + \cdots + a_nx^n$, where a_i are integers and $a_1, \ldots, a_n$ are either 0 or 1.

6. *Integral Domains and Fraction Fields*

1. Prove that a subring of an integral domain is an integral domain.
2. Prove that an integral domain with finitely many elements is a field.
3. Let R be an integral domain. Prove that the polynomial ring $R[x]$ is an integral domain.
4. Let R be an integral domain. Prove that the invertible elements of the polynomial ring $R[x]$ are the units in R.
5. Is there an integral domain containing exactly 10 elements?
6. Prove that the field of fractions of the formal power series ring $F[[x]]$ over a field F is obtained by inverting the single element x, and describe the elements of this field as certain power series with negative exponents.
7. Carry out the verification that the equivalence classes of fractions from an integral domain form a field.
8. A semigroup S is a set with an associative law of composition having an identity element. Let S be a commutative semigroup which satisfies the cancellation law: $ab = ac$ implies $b = c$. Use fractions to prove that S can be embedded into a group.

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

7. *Maximal Ideals*

1. Prove that the maximal ideals of the ring of integers are the principal ideals generated by prime integers.
2. Determine the maximal ideals of each of the following.
   (a) $\mathbb{R} \times \mathbb{R}$ **(b)** $\mathbb{R}[x]/(x^2)$ **(c)** $\mathbb{R}[x]/(x^2 - 3x + 2)$ **(d)** $\mathbb{R}[x]/(x^2 + x + 1)$
3. Prove that the ideal $(x + y^2, y + x^2 + 2xy^2 + y^4)$ in $\mathbb{C}[x, y]$ is a maximal ideal.
4. Let R be a ring, and let I be an ideal of R. Let M be an ideal of R containing I, and let $\overline{M} = M/I$ be the corresponding ideal of $\overline{R}$. Prove that M is maximal if and only if $\overline{M}$ is.
5. 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 $R = \mathbb{C}[x, y]/I$?
   (a) $(x - 1, y - 4)$ **(b)** $(x + 1, y + 4)$ **(c)** $(x^3 - 17, y^2)$
6. Prove that the ring $\mathbb{F}_5[x]/(x^2 + x + 1)$ is a field.
7. 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. Let $R = \mathbb{C}[x_1, \ldots, x_n]/I$ be a quotient of a polynomial ring over $\mathbb{C}$, and let M be a maximal ideal of R. Prove that $R/M \approx \mathbb{C}$.
9. Define a bijective correspondence between maximal ideals of $\mathbb{R}[x]$ and points in the upper half plane.

10. Let R be a ring, with M an ideal of R. Suppose that every element of R which is not in M is a unit of R. Prove that M is a maximal ideal and that moreover it is the only maximal ideal of R.

11. Let P be an ideal of a ring R. Prove that $\overline{R} = R/P$ is an integral domain if and only if $P \neq R$, and that if $a, b \in R$ and $ab \in P$, then $a \in P$ or $b \in P$. (An ideal P satisfying these conditions is called a *prime ideal*.)

12. Let $\varphi: R \longrightarrow R'$ be a ring homomorphism, and let P' be a prime ideal of R'.
   (a) Prove that $\varphi^{-1}(P')$ is a prime ideal of R.
   (b) Give an example in which P' is a maximal ideal, but $\varphi^{-1}(P')$ is not maximal.

*13. Let R be an integral domain with fraction field F, and let P be a prime ideal of R. Let R_P be the subset of F defined by

$$R_P = \{a/d \mid a, d \in R, d \notin P\}.$$

This subset is called the *localization of R at P*.
   (a) Prove that R_P is a subring of F.
   (b) Determine all maximal ideals of R_P.

14. Find an example of a "ring without unit element" and an ideal not contained in a maximal ideal.

8. Algebraic Geometry

1. Determine the points of intersection of the two complex plane curves in each of the following.
   (a) $y^2 - x^3 + x^2 = 1, \quad x + y = 1$
   (b) $x^2 + xy + y^2 = 1, \quad x^2 + 2y^2 = 1$
   (c) $y^2 = x^3, \quad xy = 1$
   (d) $x + y + y^2 = 0, \quad x - y + y^2 = 0$
   (e) $x + y^2 = 0, \quad y + x^2 + 2xy^2 + y^4 = 0$

2. Prove that two quadratic polynomials f, g in two variables have at most four common zeros, unless they have a nonconstant factor in common.

3. Derive the Hilbert Nullstellensatz from its classical form (8.7).

4. Let U, V be varieties in $\mathbb{C}^n$. Prove that $U \cup V$ and $U \cap V$ are varieties.

5. Let $f_1,\ldots,f_r;\ g_1,\ldots,g_s \in \mathbb{C}[x_1,\ldots,x_n]$, and let U, V be the zeros of $\{f_1,\ldots,f_r\}$, $\{g_1,\ldots,g_s\}$ respectively. Prove that if U and V do not meet, then $(f_1,\ldots,f_r; g_1,\ldots,g_s)$ is the unit ideal.

6. Let $f = f_1 \cdots f_m$ and $g = g_1 \cdots g_n$, where f_i, g_j are irreducible polynomials in $\mathbb{C}[x, y]$. Let $S_i = \{f_i = 0\}$ and $T_j = \{g_j = 0\}$ be the Riemann surfaces defined by these polynomials, and let V be the variety $f = g = 0$. Describe V in terms of S_i, T_j.

7. Prove that the variety defined by a set $\{f_1,\ldots,f_r\}$ of polynomials depends only on the ideal $(f_1,\ldots,f_r)$ they generate.

8. Let R be a ring containing $\mathbb{C}$ as subring.
   (a) Show how to make R into a vector space over $\mathbb{C}$.
   (b) Assume that R is a finite-dimensional vector space over $\mathbb{C}$ and that R contains exactly one maximal ideal M. Prove that M is the *nilradical* of R, that is, that M consists precisely of its nilpotent elements.

9. Prove that the complex conic $xy = 1$ is homeomorphic to the plane, with one point deleted.

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

11. The three polynomials $f_1 = x^2 + y^2 - 1$, $f_2 = x^2 - y + 1$, and $f_3 = xy - 1$ generate the unit ideal in $\mathbb{C}[x, y]$. Prove this in two ways: (i) by showing that they have no common zeros, and (ii) by writing 1 as a linear combination of f_1, f_2, f_3, with polynomial coefficients.

12. **(a)** Determine the points of intersection of the algebraic curve S: $y^2 = x^3 - x^2$ and the line L: $y = \lambda x$.
(b) Parametrize the points of S as a function of λ.
(c) Relate S to the complex λ-plane, using this parametrization.

***13.** The *radical* of an ideal I is the set of elements $r \in R$ such that some power of r is in I.
(a) Prove that the radical of I is an ideal.
(b) Prove that the varieties defined by two sets of polynomials $\{f_1,\dots, f_r\}, \{g_1,\dots, g_s\}$ are equal if and only if the two ideals $(f_1,\dots, f_r), (g_1,\dots, g_s)$ have the same radicals.

***14.** Let $R = \mathbb{C}[x_1,\dots, x_n]/(f_1,\dots, f_m)$. Let A be a ring containing $\mathbb{C}$ as subring. Find a bijective correspondence between the following sets:
(i) homomorphisms $\varphi: R \longrightarrow A$ which restrict to the identity on $\mathbb{C}$, and
(ii) n-tuples $a = (a_1,\dots, a_n)$ of elements of A which solve the system of equations $f_1 = \dots = f_m = 0$, that is, such that $f_i(a) = 0$ for $i = 1,\dots, m$.

Miscellaneous Exercises

1. Let F be a field, and let K denote the vector space F^2. Define multiplication by the rules $(a_1, a_2) \cdot (b_1, b_2) = (a_1 b_1 - a_2 b_2, a_1 b_2 + a_2 b_1)$.
(a) Prove that this law and vector addition make K into a ring.
(b) Prove that K is a field if and only if there is no element in F whose square is -1.
(c) Assume that -1 is a square in F and that F does not have characteristic 2. Prove that K is isomorphic to the product ring $F \times F$.

2. **(a)** We can define the derivative of an arbitrary polynomial $f(x)$ with coefficients in a ring R 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 R using the homomorphism (3.9). Prove the product formula $(fg)' = f'g + fg'$ and the chain rule $(f \circ g)' = (f' \circ g)g'$.
(b) Let $f(x)$ be a polynomial with coefficients in a field F, and let α be an element of F. Prove that α is a multiple root of f if and only if it is a common root of f and of its derivative f'.
(c) Let $F = \mathbb{F}_5$. Determine whether or not the following polynomials have multiple roots in F: $x^{15} - x$, $x^{15} - 2x^5 + 1$.

3. Let R be a set with two laws of composition satisfying all the ring axioms except the commutative law for addition. Prove that this law holds by expanding the product $(a + b)(c + d)$ in two ways using the distributive law.

4. Let R be a ring. Determine the units in the polynomial ring $R[x]$.

5. Let R denote the set of sequences $a = (a_1, a_2, a_3,\dots)$ of real numbers which are eventually constant: $a_n = a_{n+1} = \dots$ for sufficiently large n. Addition and multiplication are component-wise; that is, addition is vector addition and $ab = (a_1 b_1, a_2 b_2,\dots)$.
(a) Prove that R is a ring.
(b) Determine the maximal ideals of R.

6. **(a)** Classify rings R which contain $\mathbb{C}$ and have dimension 2 as vector space over $\mathbb{C}$.
***(b)** Do the same as (a) for dimension 3.

*7. Consider the map φ: $\mathbb{C}[x,y] \longrightarrow \mathbb{C}[x] \times \mathbb{C}[y] \times \mathbb{C}[t]$ defined by $f(x,y) \rightsquigarrow (f(x,0), f(0,y), f(t,t))$. Determine the image of φ explicitly.

8. Let S be a subring of a ring R. The *conductor* C of S in R is the set of elements $\alpha \in R$ such that $\alpha R \subset S$.
   (a) Prove that C is an ideal of R and also an ideal of S.
   (b) Prove that C is the largest ideal of S which is also an ideal of R.
   (c) Determine the conductor in each of the following three cases:
   (i) $R = \mathbb{C}[t]$, $S = \mathbb{C}[t^2, t^3]$;
   (ii) $R = \mathbb{Z}[\zeta]$, $\zeta = \frac{1}{2}(-1 + \sqrt{-3})$, $S = \mathbb{Z}[\sqrt{-3}]$;
   (iii) $R = \mathbb{C}[t, t^{-1}]$, $S = \mathbb{C}[t]$.

9. A *line* in $\mathbb{C}^2$ is the locus of a linear equation L: $\{ax + by + c = 0\}$. Prove that there is a unique line through two points $(x_0, y_0), (x_1, y_1)$, and also that there is a unique line through a point (x_0, y_0) with a given tangent direction (u_0, v_0).

10. An algebraic curve C in $\mathbb{C}^2$ is called *irreducible* if it is the locus of zeros of an irreducible polynomial $f(x,y)$—one which can not be factored as a product of nonconstant polynomials. A point $p \in C$ is called a *singular point* of the curve if $\partial f/\partial x = \partial f/\partial y = 0$ at p. Otherwise p is a *nonsingular* point. Prove that an irreducible curve has only finitely many singular points.

11. Let L: $ax + by + c = 0$ be a line and C: $\{f = 0\}$ a curve in $\mathbb{C}^2$. Assume that $b \neq 0$. Then we can use the equation of the line to eliminate y from the equation $f(x,y) = 0$ of C, obtaining a polynomial $g(x)$ in x. Show that its roots are the x-coordinates of the intersection points.

12. With the notation as in the preceding problem, the *multiplicity of intersection* of L and C at a point $p = (x_0, y_0)$ is the multiplicity of x_0 as a root of $g(x)$. The line is called a *tangent line* to C at p if the multiplicity of intersection is at least 2. Show that if p is a nonsingular point of C, then there is a unique tangent line at (x_0, y_0), and compute it.

13. Show that if p is a singular point of a curve C, then the multiplicity of intersection of every line through p is at least 2.

14. The *degree* of an irreducible curve C: $\{f = 0\}$ is defined to be the degree of the irreducible polynomial f.
   (a) Prove that a line L meets C in at most d points, unless $C = L$.
   *(b) Prove that there exist lines which meet C in precisely d points.

15. Determine the singular points of $x^3 + y^3 - 3xy = 0$.

*16. Prove that an irreducible cubic curve can have at most one singular point.

*17. A nonsingular point p of a curve C is called a *flex point* if the tangent line L to C at p has an intersection of multiplicity at least 3 with C at p.
   (a) Prove that the flex points are the nonsingular points of C at which the *Hessian*

$$\det \begin{bmatrix} \dfrac{\partial^2 f}{\partial x^2} & \dfrac{\partial^2 f}{\partial x \partial y} & \dfrac{\partial f}{\partial x} \\ \dfrac{\partial^2 f}{\partial x \partial y} & \dfrac{\partial^2 f}{\partial y^2} & \dfrac{\partial f}{\partial y} \\ \dfrac{\partial f}{\partial x} & \dfrac{\partial f}{\partial y} & f \end{bmatrix}$$

   vanishes.
   (b) Determine the flex points of the cubic curves $y^2 - x^3$ and $y^2 - x^3 + x^2$.

***18.** Let C be an irreducible cubic curve, and let L be a line joining two flex points of C. Prove that if L meets C in a third point, then that point is also a flex.

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

20. Prove that the locus $y = \sin x$ in $\mathbb{R}^2$ doesn't lie on any algebraic curve.

***21.** Let f, g be polynomials in $\mathbb{C}[x,y]$ with no common factor. Prove that the ring $R = \mathbb{C}[x,y]/(f,g)$ is a finite-dimensional vector space over $\mathbb{C}$.

22. **(a)** Let s, c denote the functions $\sin x$, $\cos x$ on the real line. Prove that the ring $\mathbb{R}[s,c]$ they generate is an integral domain.

(b) Let $K = \mathbb{R}(s,c)$ denote the field of fractions of $\mathbb{R}[s,c]$. Prove that the field K is isomorphic to the field of rational functions $\mathbb{R}(x)$.

***23.** Let $f(x)$, $g(x)$ be polynomials with coefficients in a ring R with $f \neq 0$. Prove that if the product $f(x)g(x)$ is zero, then there is a nonzero element $c \in R$ such that $cg(x) = 0$.

***24.** Let X denote the closed unit interval $[0,1]$, and let R be the ring of continuous functions $X \longrightarrow \mathbb{R}$.

(a) Prove that a function f which does not vanish at any point of X is invertible in R.

(b) Let $f_1,\dots,f_n$ be functions with no common zero on X. Prove that the ideal generated by these functions is the unit ideal. (Hint: Consider $f_1^2 + \cdots + f_n^2$.)

(c) Establish a bijective correspondence between maximal ideals of R and points on the interval.

(d) Prove that the maximal ideals containing a function f correspond to points of the interval at which $f = 0$.

(e) Generalize these results to functions on an arbitrary compact set X in $\mathbb{R}^k$.

(f) Describe the situation in the case $X = \mathbb{R}$.