The proof of this fact is similar to the proof of Lemma (9.6). For our purposes, the factor $\frac{1}{2}$ could be replaced by any positive real number less than 1. This inequality shows us that, as z^n winds n times around the circle of radius r^n, $f(z)$ also winds n times around the origin. A good way to visualize this conclusion is with the dog-on-a-leash model. If someone walks a dog n times around the block, the dog also goes around n times, though following a different path. This will be true provided that the leash is shorter than the radius of the block. Here z^n represents the position of the person at the time θ, and $f(z)$ represents the position of the dog. The length of the leash is $\frac{1}{2}r^n$.

We now vary the radius r. Since f is a continuous function, the image $f(C_r)$ will vary continuously with r. When the radius r is very small, $f(C_r)$ makes a small loop around the constant term a_0 of f. This small loop won't wind around the origin at all. But as we just saw, $f(C_r)$ winds n times around the origin if r is large enough. The only explanation for this is that for some intermediate radius r', $f(C_{r'})$ passes through the origin. This means that for some point α on the circle $C_{r'}$, $f(\alpha) = 0$. This number α is a root of f.

Note that all n loops have to cross the origin, which agrees with the fact that a polynomial of degree n has n roots.

I don't consider this algebra,
but this doesn't mean that algebraists can't do it.

Garrett Birkhoff

EXERCISES

1. Examples of Fields

15.8

1. Let F be a field. Find all elements $a \in F$ such that $a = a^{-1}$.

2. Let K be a subfield of $\mathbb{C}$ which is not contained in $\mathbb{R}$. Prove that K is a dense subset of $\mathbb{C}$.

3. Let R be an integral domain containing a field F as subring and which is finite-dimensional when viewed as vector space over F. Prove that R is a field.

4. Let F be a field containing exactly eight elements. Prove or disprove: The characteristic of F is 2.

2. Algebraic and Transcendental Elements

22.8

1. Let α be the real cube root of 2. Compute the irreducible polynomial for $1 + \alpha^2$ over $\mathbb{Q}$.

2. Prove Lemma (2.7), that $(1, \alpha, \alpha^2, \ldots, \alpha^{n-1})$ is a basis of $F[\alpha]$.

3. Determine the irreducible polynomial for $\alpha = \sqrt{3} + \sqrt{5}$ over each of the following fields.
(a) $\mathbb{Q}$ **(b)** $\mathbb{Q}(\sqrt{5})$ **(c)** $\mathbb{Q}(\sqrt{10})$ **(d)** $\mathbb{Q}(\sqrt{15})$

4. Let α be a complex root of the irreducible polynomial $x^3 - 3x + 4$. Find the inverse of $\alpha^2 + \alpha + 1$ in $F(\alpha)$ explicitly, in the form $a + b\alpha + c\alpha^2$, $a, b, c \in \mathbb{Q}$.

22.8

5. Let $K = F(\alpha)$, where α is a root of the irreducible polynomial $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$. Determine the element α^{-1} explicitly in terms of α and of the coefficients a_i.

6. Let $\beta = \zeta\sqrt[3]{2}$, where $\zeta = e^{2\pi i/3}$, and let $K = \mathbb{Q}(\beta)$. Prove that -1 can not be written as a sum of squares in K.

3. The Degree of a Field Extension

1. Let F be a field, and let α be an element which generates a field extension of F of degree 5. Prove that α^2 generates the same extension.
2. Let $\zeta = e^{2\pi i/7}$, and let $\eta = e^{2\pi i/5}$. Prove that $\eta \notin \mathbb{Q}(\zeta)$.
3. Define $\zeta_n = e^{2\pi i/n}$. Find the irreducible polynomial over $\mathbb{Q}$ of **(a)** ζ_4, **(b)** ζ_6, **(c)** ζ_8, **(d)** ζ_9, **(e)** ζ_{10}, **(f)** ζ_{12}.
4. Let $\zeta_n = e^{2\pi i/n}$. Determine the irreducible polynomial over $\mathbb{Q}(\zeta_3)$ of **(a)** ζ_6, **(b)** ζ_9, **(c)** ζ_{12}.
5. Prove that an extension K of F of degree 1 is equal to F.
6. Let a be a positive rational number which is not a square in $\mathbb{Q}$. Prove that $\sqrt[4]{a}$ has degree 4 over $\mathbb{Q}$.
7. Decide whether or not i is in the field **(a)** $\mathbb{Q}(\sqrt{-2})$, **(b)** $\mathbb{Q}(\sqrt[4]{-2})$, **(c)** $\mathbb{Q}(\alpha)$, where $\alpha^3 + \alpha + 1 = 0$.
8. Let K be a field generated over F by two elements α, β of relatively prime degrees m, n respectively. Prove that $[K:F] = mn$.
9. Let α, β be complex numbers of degree 3 over $\mathbb{Q}$, and let $K = \mathbb{Q}(\alpha, \beta)$. Determine the possibilities for $[K:\mathbb{Q}]$.
10. Let α, β be complex numbers. Prove that if $\alpha + \beta$ and $\alpha\beta$ are algebraic numbers, then α and β are also algebraic.
11. Let α, β be complex roots of irreducible polynomials $f(x), g(x) \in \mathbb{Q}[x]$. Let $F = \mathbb{Q}[\alpha]$ and $K = \mathbb{Q}[\beta]$. Prove that $f(x)$ is irreducible in K if and only if $g(x)$ is irreducible in F.
12. **(a)** Let $F \subset F' \subset K$ be field extensions. Prove that if $[K:F] = [K:F']$, then $F = F'$. **(b)** Give an example showing that this need not be the case if F is not contained in F'.
13. Let $\alpha_1, \ldots, \alpha_k$ be elements of an extension field K of F, and assume that they are all algebraic over F. Prove that $F(\alpha_1, \ldots, \alpha_k) = F[\alpha_1, \ldots, \alpha_k]$.
14. Prove or disprove: Let α, β be elements which are algebraic over a field F, of degrees d, e respectively. The monomials $\alpha^i\beta^j$ with $i = 0, \ldots, d-1$, $j = 0, \ldots, e-1$ form a basis of $F(\alpha, \beta)$ over F.
15. Prove or disprove: Every algebraic extension is a finite extension.

4. Constructions with Ruler and Compass

22.8

1. Express $\cos 15°$ in terms of square roots.
2. Prove that the regular pentagon can be constructed by ruler and compass **(a)** by field theory, and **(b)** by finding an explicit construction.

3. Derive formula (4.12).
4. Determine whether or not the regular 9-gon is constructible by ruler and compass.
5. Is it possible to construct a square whose area is equal to that of a given triangle?
6. Let α be a real root of the polynomial $x^3 + 3x + 1$. Prove that α can not be constructed by ruler and compass.
7. Given that π is a transcendental number, prove the impossibility of squaring the circle by ruler and compass. (This means constructing a square whose area is the same as the area of a circle of unit radius.)
8. Prove the impossibility of "duplicating the cube," that is, of constructing the side length of a cube whose volume is 2.
9. **(a)** Referring to the proof of Proposition (4.8), prove that the discriminant D is negative if and only if the circles do not intersect.
   (b) Determine the line which appears at the end of the proof of Proposition (4.8) geometrically if $D \geq 0$ and also if $D < 0$.
10. Prove that if a prime integer p has the form $2^r + 1$, then it actually has the form $2^{2^k} + 1$.
11. Let C denote the field of constructible real numbers. Prove that C is the smallest subfield of $\mathbb{R}$ with the property that if $a \in C$ and $a > 0$, then $\sqrt{a} \in C$.
12. The points in the plane can be considered as complex numbers. Describe the set of constructible points explicitly as a subset of $\mathbb{C}$.
13. Characterize the constructible real numbers in the case that three points are given in the plane to start with.

*14. Let the rule for construction in three-dimensional space be as follows:
   (i) Three non-collinear points are given. They are considered to be constructed.
   (ii) One may construct a plane through three non-collinear constructed points.
   (iii) One may construct a sphere with center at a constructed point and passing through another constructed point.
   (iv) Points of intersection of constructed planes and spheres are considered to be constructed if they are isolated points, that is, if they are not part of an intersection curve.
   Prove that one can introduce coordinates, and characterize the coordinates of the constructible points.

5. Symbolic Adjunction of Roots

1. Let F be a field of characteristic zero, let f' denote the derivative of a polynomial $f \in F[x]$, and let g be an irreducible polynomial which is a common divisor of f and f'. Prove that g^2 divides f.
2. For which fields F and which primes p does $x^p - x$ have a multiple root?
3. Let F be a field of characteristic p.
   (a) Apply (5.7) to the polynomial $x^p + 1$.
   (b) Factor this polynomial into irreducible factors in $F[x]$.
4. Let $\alpha_1, \ldots, \alpha_n$ be the roots of a polynomial $f \in F[x]$ of degree n in an extension field K. Find the best upper bound that you can for $[F(\alpha_1, \ldots, \alpha_n) : F]$.

6. Finite Fields

1. Identify the group $\mathbb{F}_4^+$.
2. Write out the addition and multiplication tables for $\mathbb{F}_4$ and for $\mathbb{Z}/(4)$, and compare them.
3. Find a thirteenth root of 3 in the field $\mathbb{F}_{13}$.
4. Determine the irreducible polynomial over $\mathbb{F}_2$ for each of the elements (6.12) of $\mathbb{F}_8$.
5. Determine the number of irreducible polynomials of degree 3 over the field $\mathbb{F}_3$.
6. **(a)** Verify that (6.9, 6.10, 6.13) are irreducible factorizations over $\mathbb{F}_2$.
   (b) Verify that (6.11, 6.13) are irreducible factorizations over $\mathbb{Z}$.
7. Factor $x^9 - x$ and $x^{27} - x$ in $\mathbb{F}_3$. Prove that your factorizations are irreducible.
8. Factor the polynomial $x^{16} - x$ in the fields **(a)** $\mathbb{F}_4$ and **(b)** $\mathbb{F}_8$.
9. Determine all polynomials $f(x)$ in $\mathbb{F}_q[x]$ such that $f(\alpha) = 0$ for all $\alpha \in \mathbb{F}_q$.
10. Let K be a finite field. Prove that the product of the nonzero elements of K is -1.
11. Prove that every element of $\mathbb{F}_p$ has exactly one pth root.
12. Complete the proof of Proposition (6.19) by showing that the difference $\alpha - \beta$ of two roots of $x^q - x$ is a root of the same polynomial.
13. Let p be a prime. Describe the integers n such that there exist a finite field K of order n and an element $\alpha \in K^\times$ whose order in $K^\times$ is p.
14. Work this problem without appealing to Theorem (6.4).
    (a) Let $F = \mathbb{F}_p$. Determine the number of monic irreducible polynomials of degree 2 in $F[x]$.
    (b) Let $f(x)$ be one of the polynomials described in (a). Prove that $K = F[x]/(f)$ is a field containing p^2 elements and that the elements of K have the form $a + b\alpha$, where $a, b \in F$ and α is a root of f in K. Show that every such element $a + b\alpha$ with $b \neq 0$ is the root of an irreducible quadratic polynomial in $F[x]$.
    (c) Show that every polynomial of degree 2 in $F[x]$ has a root in K.
    (d) Show that all the fields K constructed as above for a given prime p are isomorphic.
15. The polynomials $f(x) = x^3 + x + 1$, $g(x) = x^3 + x^2 + 1$ are irreducible over $\mathbb{F}_2$. Let K be the field extension obtained by adjoining a root of f, and let L be the extension obtained by adjoining a root of g. Describe explicitly an isomorphism from K to L.
16. **(a)** Prove Lemma (6.21) for the case $F = \mathbb{C}$ by looking at the roots of the two polynomials.
    (b) Use the principle of permanence of identities to derive the conclusion when F is an arbitrary ring.

7. Function Fields

1. Determine a real polynomial in three variables whose locus of zeros is the projected Riemann surface (7.9).
2. Prove that the set $\mathcal{F}(U)$ of continuous functions on U' forms a ring.
3. Let $f(x)$ be a polynomial in $F[x]$, where F is a field. Prove that if there is a rational function $r(x)$ such that $r^2 = f$, then r is a polynomial.
4. Referring to the proof of Proposition (7.11), explain why the map $F \longrightarrow \mathcal{F}(S)$ defined by $g(x) \rightsquigarrow g(X)$ is a homomorphism.

5. Determine the branch points and the gluing data for the Riemann surfaces of the following polynomials.
   (a) $y^2 - x^2 + 1$ (b) $y^5 - x$ (c) $y^4 - x - 1$ (d) $y^3 - xy - x$
   (e) $y^3 - y^2 - x$ (f) $y^3 - x(x-1)$ (g) $y^3 - x(x-1)^2$ (h) $y^3 + xy^2 + x$
   (i) $x^2y^2 - xy - x$
6. (a) Determine the number of isomorphism classes of function fields K of degree 3 over $F = \mathbb{C}(x)$ which are ramified only at the points ± 1.
   (b) Describe the gluing data for the Riemann surface corresponding to each isomorphism class of fields as a pair of permutations.
   (c) For each isomorphism class, determine a polynomial $f(x, y)$ such that $K = F[x]/(f)$ represents the isomorphism class.

*7. Prove the Riemann Existence Theorem for quadratic extensions.

*8. Let S be a branched covering constructed with branch points $\alpha_1, \ldots, \alpha_r$, curves $C_1, \ldots, C_r$, and permutations $\sigma_1, \ldots, \sigma_r$. Prove that S is connected if and only if the subgroup Σ of the symmetric group S_n which is generated by the permutations σ_ν operates transitively on the indices $\mathbf{1}, \ldots, \mathbf{n}$.

*9. It can be shown that the Riemann surface S of a function field is homeomorphic to the complement of a finite set of points in a compact oriented two-dimensional manifold $\bar{S}$. The *genus* of such a surface is defined to be the number of holes in the corresponding manifold $\bar{S}$. So if $\bar{S}$ is a sphere, the genus of S is 0, while if $\bar{S}$ is a torus, the genus of S is 1. The genus of a function field is defined to be the genus of its Riemann surface. Determine the genus of the field defined by each polynomial.
   (a) $y^2 - (x^2 - 1)(x^2 - 4)$ (b) $y^2 - x(x^2 - 1)(x^2 - 4)$ (c) $y^3 + y + x$
   (d) $y^3 - x(x-1)$ (e) $y^3 - x(x-1)^2$

8. Transcendental Extensions

1. Let $K = F(\alpha)$ be a field extension generated by an element α, and let $\beta \in K$, $\beta \notin F$. Prove that α is algebraic over the field $F(\beta)$.
2. Prove that the isomorphism $\mathbb{Q}(\pi) \longrightarrow \mathbb{Q}(e)$ sending $\pi \rightsquigarrow e$ is discontinuous.
3. Let $F \subset K \subset L$ be fields. Prove that $\operatorname{tr\,deg}_F L = \operatorname{tr\,deg}_F K + \operatorname{tr\,deg}_K L$.
4. Let $(\alpha_1, \ldots, \alpha_n) \subset K$ be an algebraically independent set over F. Prove that an element $\beta \in K$ is transcendental over $F(\alpha_1, \ldots, \alpha_n)$ if and only if $(\alpha_1, \ldots, \alpha_n; \beta)$ is algebraically independent.
5. Prove Theorem (8.3).

9. Algebraically Closed Fields

1. Derive Corollary (9.5) from Theorem (9.4).
2. Prove that the field $\bar{F}$ constructed in this text as the union of finite fields is algebraically closed.

*3. With notation as at the end of the section, a comparison of the images $f(C_r)$ for varying radii shows another interesting geometric feature: For large r, the curve $f(C_r)$ has n loops. This can be expressed formally by saying that its total curvature is $2\pi n$. For small r, the linear term $a_1 z + a_0$ dominates $f(z)$. Then $f(C_r)$ makes a single loop around a_0. Its

total curvature is only 2π. Something happens to the loops and the curvature, as r varies. Explain.

*4. If you have access to a computer with a good graphics system, use it to illustrate the variation of $f(C_r)$ with r. Use log-polar coordinates $(\log r, \theta)$.

Miscellaneous Exercises

1. Let $f(x)$ be an irreducible polynomial of degree 6 over a field F, and let K be a quadratic extension of F. Prove or disprove: Either f is irreducible over K, or else f is a product of two irreducible cubic polynomials over K.
2. **(a)** Let p be an odd prime. Prove that exactly half of the elements of $\mathbb{F}_p^\times$ are squares and that if α, β are nonsquares, then $\alpha\beta$ is a square.
   (b) Prove the same as (a) for any finite field of odd order.
   (c) Prove that in a finite field of even order, every element is a square.
3. Write down the irreducible polynomial for $\alpha = \sqrt{2} + \sqrt{3}$ over $\mathbb{Q}$ and prove that it is reducible modulo p for every prime p.

*4. (a) Prove that any element of $GL_2(\mathbb{Z})$ of finite order has order $1, 2, 3, 4$, or 6.
   (b) Extend this theorem to $GL_3(\mathbb{Z})$, and show that it fails in $GL_4(\mathbb{Z})$.

5. Let c be a real number, not ± 2. The plane curve C: $x^2 + cxy + y^2 = 1$ can be parametrized rationally. To do this, we choose the point $(0, 1)$ on C and parametrize the lines through this point by their slope: $L_t: y = tx + 1$. The point at which the line L_t intersects C can be found algebraically.
   (a) Find the equation of this point explicitly.
   (b) Use this procedure to find all solutions of the equation $x^2 + cxy + y^2 = 1$ in the field $F = \mathbb{F}_p$, when c is in that field and $c \neq \pm 2$.
   (c) Show that the number of solutions is $p - 1$, p, or $p + 1$, and describe how this number depends on the roots of the polynomial $t^2 + ct + 1$.
6. The *degree* of a rational function $f(x) = p(x)/q(x) \in \mathbb{C}(x)$ is defined to be the maximum of the degrees of p and q, when p, q are chosen to be relatively prime. Every rational function f defines a map $P' \longrightarrow P'$, by $x \rightsquigarrow f(x)$. We will denote this map by f too.
   (a) Suppose that f has degree d. Show that for any point y_0 in the plane, the fibre $f^{-1}(y_0)$ contains at most d points.
   (b) Show that $f^{-1}(y_0)$ consists of precisely d points, except for a finite number of y_0. Identify the values y_0 where there are fewer than d points in terms of f and df/dx.

*7. **(a)** Prove that a rational function $f(x)$ generates the field of rational functions $\mathbb{C}(x)$ if and only if it is of the form $(ax + b)/(cx + d)$, with $ad - bc \neq 0$.
   (b) Identify the group of automorphisms of $\mathbb{C}(x)$ which are the identity on $\mathbb{C}$.

*8. Let K/F be an extension of degree 2 of rational function fields, say $K = \mathbb{C}(t)$ and $F = \mathbb{C}(x)$. Prove that there are generators x', t' for the two fields, such that $t = (\alpha t' + \beta)/(\gamma t' + \delta)$ and $x = (ax' + b)/(cx' + d)$, $\alpha, \beta, \gamma, \delta, a, b, c, d \in \mathbb{C}$, such that $t'^2 = x'$.

*9. Fill in the following outline to give an algebraic proof of the fact that $K = \mathbb{C}(x)[y]/(y^2 - x^3 + x)$ is not a pure transcendental extension of $\mathbb{C}$. Suppose that $K = \mathbb{C}(t)$ for some t. Then x and y are rational functions of t.

(a) Using the result of the previous problem and replacing t by t' as necessary, reduce to the case that $x = (at^2 + b)/(ct^2 + d)$.

(b) Say that $y = p(t)/q(t)$. Then the equation $y^2 = x(x + 1)(x - 1)$ reads

$$\frac{p(t)^2}{q(t)^2} = \frac{(at^2 + b)((a + c)t^2 + b + d)((a - c)t^2 + b - d)}{(ct^2 + d)^3}.$$

Either the numerators and denominators on the two sides agree, or else there is cancellation on the right side.

(c) Complete the proof by analyzing the two possibilities given in (b).

***10.** **(a)** Prove that the homomorphism $SL_2(\mathbb{Z}) \longrightarrow SL_2(\mathbb{F}_p)$ obtained by reducing the matrix entries modulo 2 is surjective.

(b) Prove the analogous assertion for SL_n.

***11.** Determine the conjugacy classes of elements order 2 in $GL_n(\mathbb{Z})$.