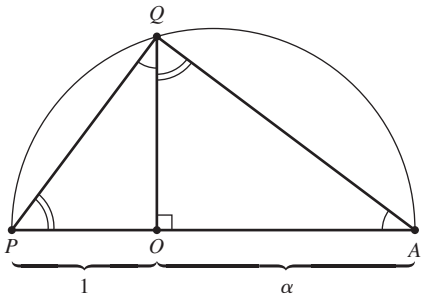
of field operations. However, if $\alpha > 0$ is constructible, then Fig. 41.7 shows that $\sqrt{\alpha}$ is constructible. Let $\overline{OA}$ have length α, and find P on $\overline{OA}$ extended so that $\overline{OP}$ has length 1. Find the midpoint of $\overline{PA}$ and draw a semicircle with $\overline{PA}$ as diameter. Erect a perpendicular to $\overline{PA}$ at O, intersecting the semicircle at Q. Then the triangles OPQ and OQA are similar, so

$$\frac{|\overline{OQ}|}{|\overline{OA}|} = \frac{|\overline{OP}|}{|\overline{OQ}|},$$

and $|\overline{OQ}|^2 = 1\alpha = \alpha$. Thus $\overline{OQ}$ is of length $\sqrt{\alpha}$. Therefore square roots of constructible numbers are constructible.

Theorem 41.1 showed that field operations are possible by construction. ◆



41.7 Figure

41.8 Corollary If γ is constructible and $\gamma \notin \mathbb{Q}$, then there is a finite sequence of real numbers $\alpha_1, \cdots, \alpha_n = \gamma$ such that $\mathbb{Q}(\alpha_1, \cdots, \alpha_i)$ is an extension of $\mathbb{Q}(\alpha_1, \cdots, \alpha_{i-1})$ of degree 2. In particular, $[\mathbb{Q}(\gamma) : \mathbb{Q}] = 2^r$ for some integer $r \geq 0$.

Proof The existence of the α_i is immediate from Theorem 41.6. Then

$$\begin{aligned} 2^n &= [\mathbb{Q}(\alpha_1, \cdots, \alpha_n) : \mathbb{Q}] \\ &= [\mathbb{Q}(\alpha_1, \cdots, \alpha_n) : \mathbb{Q}(\gamma)][\mathbb{Q}(\gamma) : \mathbb{Q}], \end{aligned}$$

by Theorem 40.4, which completes the proof. ◆

The Impossibility of Certain Constructions

We can now show the impossibility of certain geometric constructions.

41.9 Theorem *Doubling the cube is impossible,* that is, given a side of a cube, it is not always possible to construct with a straightedge and a compass the side of a cube that has double the volume of the original cube.

Proof Let the given cube have a side of length 1, and hence a volume of 1. The cube being sought would have to have a volume of 2, and hence a side of length $\sqrt[3]{2}$. But $\sqrt[3]{2}$ is a zero of irreducible $x^3 - 2$ over $\mathbb{Q}$, so

$$[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3.$$

Corollary 41.8 shows that to double this cube of volume 1, we would need to have $3 = 2^r$ for some integer r, but no such r exists. ◆

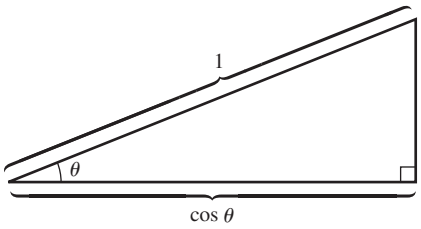
41.10 Theorem *Squaring the circle is impossible;* that is, given a circle, it is not always possible to construct with a straightedge and a compass a square having area equal to the area of the given circle.

Proof Let the given circle have a radius of 1, and hence an area of π. We would need to construct a square of side $\sqrt{\pi}$. But π is transcendental over $\mathbb{Q}$, so $\sqrt{\pi}$ is transcendental over $\mathbb{Q}$ also. ◆

41.11 Theorem *Trisecting the angle is impossible;* that is, there exists an angle that cannot be trisected with a straightedge and a compass.

Proof Figure 41.12 indicates that the angle θ can be constructed if and only if a segment of length $|\cos\theta|$ can be constructed. Now 60° is a constructible angle, and we shall show that it cannot be trisected. Note that

$$\begin{aligned}\cos 3\theta &= \cos(2\theta + \theta)\\ &= \cos 2\theta\cos\theta - \sin 2\theta\sin\theta\\ &= (2\cos^2\theta - 1)\cos\theta - 2\sin\theta\cos\theta\sin\theta\\ &= (2\cos^2\theta - 1)\cos\theta - 2\cos\theta(1 - \cos^2\theta)\\ &= 4\cos^3\theta - 3\cos\theta.\end{aligned}$$



41.12 Figure

[We realize that some students have not seen the trigonometric identities we just used. Exercise 1 repeats Exercise 42 of Section 3 and asks you to prove the identity $\cos 3\theta = 4\cos^3\theta - 3\cos\theta$ from Euler's formula.]

Let $\theta = 20°$, so that $\cos 3\theta = \frac{1}{2}$, and let $\alpha = \cos 20°$. From the identity $4\cos^3\theta - 3\cos\theta = \cos 3\theta$, we see that

$$4\alpha^3 - 3\alpha = \frac{1}{2}.$$

Thus α is a zero of $8x^3 - 6x - 1$. This polynomial is irreducible in $\mathbb{Q}[x]$, since, by Theorem 28.12, it is enough to show that it does not factor in $\mathbb{Z}[x]$. But a factorization in $\mathbb{Z}[x]$ would entail a linear factor of the form $(8x \pm 1), (4x \pm 1), (2x \pm 1)$, or $(x \pm 1)$. We can quickly check that none of the numbers $\pm\frac{1}{8}, \pm\frac{1}{4}, \pm\frac{1}{2}$, and ± 1 is a zero of $8x^3 - 6x - 1$. Thus

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3,$$

so by Corollary 41.8, α is not constructible. Hence 60° cannot be trisected. ◆

Note that the regular n-gon is constructible for $n \geq 3$ if and only if the angle $2\pi/n$ is constructible, which is the case if and only if a line segment of length $\cos(2\pi/n)$ is constructible.

HISTORICAL NOTE

Greek mathematicians as far back as the fourth century B.C. had tried without success to find geometric constructions using straightedge and compass to trisect the angle, double the cube, and square the circle. Although they were never able to prove that such constructions were impossible, they did manage to construct the solutions to these problems using other tools, including the conic sections.

It was Carl Gauss in the early nineteenth century who made a detailed study of constructibility in connection with his solution of cyclotomic equations, the equations of the form $x^p - 1 = 0$ with p prime whose roots form the vertices of a regular p-gon. He showed that although all such equations are solvable using radicals, if $p - 1$ is not a power of 2, then the solutions must involve roots higher than the second. In fact, Gauss asserted that anyone who attempted to find a geometric construction for a p-gon where $p - 1$ is not a power of 2 would "spend his time uselessly." Interestingly, Gauss did not prove the assertion that such constructions were impossible. That was accomplished in 1837 by Pierre Wantzel (1814–1848), who in fact proved Corollary 41.8 and also demonstrated Theorems 41.9 and 41.11. The proof of Theorem 41.10, on the other hand, requires a proof that π is transcendental, a result finally achieved in 1882 by Ferdinand Lindemann (1852–1939).

EXERCISES 41

Computations

1. Prove the trigonometric identity $\cos 3\theta = 4\cos^3\theta - 3\cos\theta$ from the Euler formula, $e^{i\theta} = \cos\theta + i\sin\theta$.

Concepts

2. Determine whether each of the following is true or false.

a. It is impossible to double any cube of constructible edge by compass and straightedge constructions.

b. It is impossible to double every cube of constructible edge by compass and straightedge constructions.

c. It is impossible to square any circle of constructible radius by straightedge and compass constructions.

d. No constructible angle can be trisected by straightedge and compass constructions.

e. Every constructible number is of degree 2^r over $\mathbb{Q}$ for some integer $r \geq 0$.

f. We have shown that every real number of degree 2^r over $\mathbb{Q}$ for some integer $r \geq 0$ is constructible.

g. The fact that factorization of a positive integer into a product of primes is unique (up to order) was used strongly at the conclusion of Theorems 41.9 and 41.11.

h. Counting arguments are exceedingly powerful mathematical tools.

i. We can find any constructible number in a finite number of steps by starting with a given segment of unit length and using a straightedge and a compass.

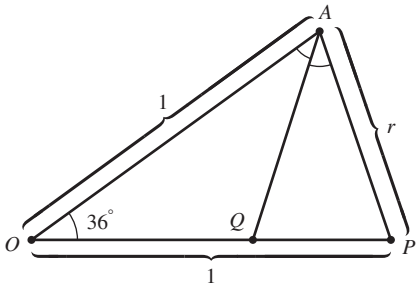
j. We can find the totality of all constructible numbers in a finite number of steps by starting with a given segment of unit length and using a straightedge and a compass.

Theory

3. Using the proof of Theorem 41.11, show that the regular 9-gon is not constructible.

4. Show *algebraically* that it is possible to construct an angle of 30°.

5. Referring to Fig. 41.13, where $\overline{AQ}$ bisects angle OAP, show that the regular 10-gon is constructible (and therefore that the regular pentagon is also). [*Hint:* Triangle OAP is similar to triangle APQ. Show algebraically that r is constructible.]



41.13 Figure

In Exercises 6 through 9 use the results of Exercise 5 where needed to show that the statement is true.

6. The regular 20-gon is constructible.

7. The regular 30-gon is constructible.

8. The angle 72° can be trisected.

9. The regular 15-gon can be constructed.

10. Suppose you wanted to explain roughly in just three or four sentences, for a high school plane geometry teacher who never had a course in abstract algebra, how it can be shown that it is impossible to trisect an angle of 60°. Write down what you would say.

11. Let $S = \{n \in \mathbb{Z} \mid \text{an } n \text{ degree angle is constructible with a compass and straightedge}\}$. We are assuming that if an angle of n degrees is constructed, then $n + k(360)$ is also constructed for any integer k. Prove that S is the principal ideal $\langle 3 \rangle \subseteq \mathbb{Z}$. It may be helpful to use Exercise 5.

12. The proof of Theorem 41.11 can be simplified by making a different choice of the angle θ. Find a constructible real number α so that the angle $\theta = \frac{\arccos(\alpha)}{3}$ can be used in the formula $\cos 3\theta = 4\cos^3\theta - 3\cos\theta$ to arrive at a polynomial that meets Eisenstein's criteria. Then finish the proof of Theorem 4.11.

13. Prove that for at least one constructible angle 5θ, θ is not constructible.

14. Continuing Exercise 13,

a. Use Euler's formula to show that for any integer $n \geq 2$, $\cos(n\theta) = 2\cos(\theta)\cos((n-1)\theta) - \cos((n-2)\theta)$.
b. Use part a to rewrite $\cos(7\theta)$ and use this formula to prove that there is a constructible angle 7θ such that θ is not constructible.
c. For each integer $1 \leq n \leq 10$, is there a constructible angle $n\theta$ such that θ is not constructible?

(The polynomials used in this exercise are called Chebyshev polynomials.)

SECTION 42 FINITE FIELDS

The purpose of this section is to determine the structure of all finite fields. We shall show that for every prime p and positive integer n, there is exactly one finite field (up to isomorphism) of order p^n. This field $\mathrm{GF}(p^n)$ is usually referred to as the **Galois field of order** p^n. We shall be using quite a bit of our material on cyclic groups. The proofs are simple and elegant.

The Structure of a Finite Field

We now show that all finite fields must have prime-power order.

42.1 Theorem Let E be a finite extension of degree n over a finite field F. If F has q elements, then E has q^n elements.

Proof Let $\{\alpha_1, \cdots, \alpha_n\}$ be a basis for E as a vector space over F. By Exercise 21 of Section 33, every $\beta \in E$ can be *uniquely* written in the form

$$\beta = b_1\alpha_1 + \cdots + b_n\alpha_n$$

for $b_i \in F$. Since each b_i may be any of the q elements of F, the total number of such distinct linear combinations of the α_i is q^n. ◆

42.2 Corollary If E is a finite field of characteristic p, then E contains exactly p^n elements for some positive integer n.

Proof Every finite field E is a finite extension of a prime field isomorphic to the field $\mathbb{Z}_p$, where p is the characteristic of E. The corollary follows at once from Theorem 42.1. ◆

We now turn to the study of the multiplicative structure of a finite field. The following theorem will show us how any finite field can be formed from the prime subfield.

42.3 Theorem Let E be a field of p^n elements contained in an algebraic closure $\overline{\mathbb{Z}}_p$ of $\mathbb{Z}_p$. The elements of E are precisely the zeros in $\overline{\mathbb{Z}}_p$ of the polynomial $x^{p^n} - x$ in $\mathbb{Z}_p[x]$.

Proof The set E^* of nonzero elements of E forms a multiplicative group of order $p^n - 1$ under the field multiplication. For $\alpha \in E^*$, the order of α in this group divides the order $p^n - 1$ of the group. Thus for $\alpha \in E^*$, we have $\alpha^{p^n-1} = 1$, so $\alpha^{p^n} = \alpha$. Therefore, every element in E is a zero of $x^{p^n} - x$. Since $x^{p^n} - x$ can have at most p^n zeros, we see that E contains precisely the zeros of $x^{p^n} - x$ in $\overline{\mathbb{Z}}_p$. ◆

42.4 Definition An element α of a field is an ***n*th root of unity** if $\alpha^n = 1$. It is a **primitive *n*th root of unity** if $\alpha^n = 1$ and $\alpha^m \neq 1$ for $0 < m < n$. ■

Thus the nonzero elements of a finite field of p^n elements are all $(p^n - 1)$th roots of unity.

Recall that in Corollary 28.7, we showed that the multiplicative group of nonzero elements of a finite field is cyclic. This is a very important fact about finite fields; it has actually been applied to coding theory and combinatorics. For the sake of completeness in this section, we now state it here as a theorem, give a corollary, and illustrate with an example.

42.5 Theorem The multiplicative group $\langle F^*, \cdot \rangle$ of nonzero elements of a finite field F is cyclic.

Proof See Corollary 28.7. ◆

42.6 Corollary A finite extension E of a finite field F is a simple extension of F.

Proof Let α be a generator for the cyclic group E^* of nonzero elements of E. Then $E = F(\alpha)$. ◆

42.7 Example Consider the finite field $\mathbb{Z}_{11}$. By Theorem 42.5 $\langle {\mathbb{Z}_{11}}^*, \cdot \rangle$ is cyclic. Let us try to find a generator of ${\mathbb{Z}_{11}}^*$ by brute force and ignorance. We start by trying 2. Since $|{\mathbb{Z}_{11}}^*| = 10$, 2 must be an element of ${\mathbb{Z}_{11}}^*$ of order dividing 10, that is, either 2, 5, or 10. Now

$$2^2 = 4, \quad 2^4 = 4^2 = 5, \quad \text{and} \quad 2^5 = (2)(5) = 10 = -1.$$

Thus neither 2^2 nor 2^5 is 1, but, of course, $2^{10} = 1$, so 2 is a generator of ${\mathbb{Z}_{11}}^*$, that is, 2 is a primitive 10th root of unity in $\mathbb{Z}_{11}$. We were lucky.

By the theory of cyclic groups, all the generators of ${Z_{11}}^*$, that is, all the primitive 10th roots of unity in $\mathbb{Z}_{11}$, are of the form 2^n, where n is relatively prime to 10. These elements are

$$2^1 = 2, \quad 2^3 = 8, \quad 2^7 = 7, \quad 2^9 = 6.$$