# FIRST COURSE IN THE THEORY OF EQUATIONS

# AUTHOR:

# LEONARD EUGENE DICKSON

*(PhD.)*

*(Professor of Mathematics in the University of Chicago)*

ILLUSTRATED
&
PUBLISHED BY
E-KİTAP PROJESİ & CHEAPEST BOOKS

**www.cheapestboooks.com**
Copyright, 2014 by e-Kitap Projesi
Istanbul

Printed in U. S. A.

# PREFACE

————

The theory of equations is not only a necessity in the subsequent mathematical courses and their applications, but furnishes an illuminating sequel to geometry, algebra and analytic geometry. Moreover, it develops anew and in greater detail various fundamental ideas of calculus for the simple, but important, case of polynomials. The theory of equations therefore affords a useful supplement to differential calculus whether taken subsequently or simultaneously.

It was to meet the numerous needs of the student in regard to his earlier and future mathematical courses that the present book was planned with great care and after wide consultation. It differs essentially from the author's *Elementary Theory of Equations*, both in regard to omissions and additions, and since it is addressed to younger students and may be used parallel with a course in differential calculus. Simpler and more detailed proofs are now employed. The exercises are simpler, more numerous, of greater variety, and involve more practical applications.

This book throws important light on various elementary topics. For example, an alert student of geometry who has learned how to bisect any angle is apt to ask if every angle can be trisected with ruler and compasses and if not, why not. After learning how to construct regular polygons of 3, 4, 5, 6, 8 and 10 sides, he will be inquisitive about the missing ones of 7 and 9 sides. The teacher will be in a comfortable position if he knows the facts and what is involved in the simplest discussion to date of these questions, as given in Chapter III. Other chapters throw needed light on various topics of algebra. In particular, the theory of graphs is presented in Chapter V in a more scientific and practical manner than was possible in algebra and analytic geometry.

There is developed a method of computing a real root of an equation with minimum labor and with certainty as to the accuracy of all the decimals obtained. We first find by Horner's method successive transformed equations whose number is half of the desired number of significant figures of the root. The final equation is reduced to a linear equation by applying to the constant term the correction computed from the omitted terms of the second and

higher degrees, and the work is completed by abridged division. The method combines speed with control of accuracy.

Newton's method, which is presented from both the graphical and the numerical standpoints, has the advantage of being applicable also to equations which are not algebraic; it is applied in detail to various such equations.

In order to locate or isolate the real roots of an equation we may employ a graph, provided it be constructed scientifically, or the theorems of Descartes, Sturm, and Budan, which are usually neither stated, nor proved, correctly.

The long chapter on determinants is independent of the earlier chapters. The theory of a general system of linear equations is here presented also from the standpoint of matrices.

For valuable suggestions made after reading the preliminary manuscript of this book, the author is greatly indebted to Professor Bussey of the University of Minnesota, Professor Roever of Washington University, Professor Kempner of the University of Illinois, and Professor Young of the University of Chicago. The revised manuscript was much improved after it was read critically by Professor Curtiss of Northwestern University. The author's thanks are due also to Professor Dresden of the University of Wisconsin for various useful suggestions on the proof-sheets.

CHICAGO, 1921.

# CONTENTS

Numbers refer to pages.

———

## CHAPTER I
### Complex Numbers

## CHAPTER II
### Theorems on Roots of Equations

## CHAPTER III
### Constructions with Ruler and Compasses

Laplace's Development by Columns, 137.    Laplace's Development by Rows, 138.
Product of Determinants, 139.

# CHAPTER IX
### Symmetric Functions

Sigma Functions, Elementary Symmetric Functions, 143.   Fundamental Theorem, 144.   Functions Symmetric in all but One Root, 147.   Sums of Like Powers of the Roots, 150.   Waring's Formula, 152.   Computation of Sigma Functions, 156. Computation of Symmetric Functions, 157.

# CHAPTER X
### Elimination, Resultants And Discriminants

Elimination, 159.    Resultant of Two Polynomials, 159.    Sylvester's Method of Elimination, 161.    Bézout's Method of Elimination, 164.    General Theorem on Elimination, 166.   Discriminants, 167.

# APPENDIX
### Fundamental Theorem of Algebra

# First Course in
# The Theory of Equations

—————

## CHAPTER I

**1. Square Roots.**   If $p$ is a positive real number, the symbol $\sqrt{p}$ is used to denote the positive square root of $p$. It is most easily computed by logarithms.

We shall express the square roots of negative numbers in terms of the symbol $i$ such that the relation $i^2 = -1$ holds. Consequently we denote the roots of $x^2 = -1$ by $i$ and $-i$. The roots of $x^2 = -4$ are written in the form $\pm 2i$ in preference to $\pm\sqrt{-4}$. In general, if $p$ is positive, the roots of $x^2 = -p$ are written in the form $\pm\sqrt{p}\,i$ in preference to $\pm\sqrt{-p}$.

The square of either root is thus $(\sqrt{p})^2 i^2 = -p$. Had we used the less desirable notation $\pm\sqrt{-p}$ for the roots of $x^2 = -p$, we might be tempted to find the square of either root by multiplying together the values under the radical sign and conclude erroneously that

$$\sqrt{-p}\,\sqrt{-p} = \sqrt{p^2} = +p.$$

To prevent such errors we use $\sqrt{p}\,i$ and not $\sqrt{-p}$.

**2. Complex Numbers.**   If $a$ and $b$ are any two real numbers and $i^2 = -1$, $a + bi$ is called a *complex number*[1] and $a - bi$ its *conjugate*. Either is said to be *zero* if $a = b = 0$. Two complex numbers $a + bi$ and $c + di$ are said to be *equal* if and only if $a = c$ and $b = d$. In particular, $a + bi = 0$ if and only if $a = b = 0$. If $b \neq 0$, $a + bi$ is said to be *imaginary*. In particular, $bi$ is called a *pure imaginary*.

---

[1]Complex numbers are essentially couples of real numbers. For a treatment from this standpoint and a treatment based upon vectors, see the author's *Elementary Theory of Equations*, p. 21, p. 18.

Addition of complex numbers is defined by

$$(a + bi) + (c + di) = (a + c) + (b + d)i.$$

The inverse operation to addition is called subtraction, and consists in finding a complex number $z$ such that

$$(c + di) + z = a + bi.$$

In notation and value, $z$ is

$$(a + bi) - (c + di) = (a - c) + (b - d)i.$$

Multiplication is defined by

$$(a + bi)(c + di) = ac - bd + (ad + bc)i,$$

and hence is performed as in formal algebra with a subsequent reduction by means of $i^2 = -1$. For example,

$$(a + bi)(a - bi) = a^2 - b^2 i^2 = a^2 + b^2.$$

Division is defined as the operation which is inverse to multiplication, and consists in finding a complex number $q$ such that $(a+bi)q = e+fi$. Multiplying each member by $a - bi$, we find that $q$ is, in notation and value,

$$\frac{e + fi}{a + bi} = \frac{(e + fi)(a - bi)}{a^2 + b^2} = \frac{ae + bf}{a^2 + b^2} + \frac{af - be}{a^2 + b^2}i.$$

Since $a^2 + b^2 = 0$ implies $a = b = 0$ when $a$ and $b$ are real, we conclude that division except by zero is possible and unique.

## EXERCISES

Express as complex numbers

**1.** $\sqrt{-9}$.                          **2.** $\sqrt{4}$.

**3.** $(\sqrt{25} + \sqrt{-25})\sqrt{-16}$.          **4.** $-\frac{2}{3}$.

**5.** $8 + 2\sqrt{3}$.      **6.** $\dfrac{3 + \sqrt{-5}}{2 + \sqrt{-1}}$.      **7.** $\dfrac{3 + 5i}{2 - 3i}$.      **8.** $\dfrac{a + bi}{a - bi}$.

**9.** Prove that the sum of two conjugate complex numbers is real and that their difference is a pure imaginary.

**10.** Prove that the conjugate of the sum of two complex numbers is equal to the sum of their conjugates. Does the result hold true if each word sum is replaced by the word difference?

**11.** Prove that the conjugate of the product (or quotient) of two complex numbers is equal to the product (or quotient) of their conjugates.

**12.** Prove that, if the product of two complex numbers is zero, at least one of them is zero.

**13.** Find two pairs of real numbers $x$, $y$ for which

$$(x + yi)^2 = -7 + 24i.$$

As in Ex. 13, express as complex numbers the square roots of

**14.** $-11 + 60i$.       **15.** $5 - 12i$.       **16.** $4cd + (2c^2 - 2d^2)i$.

**3. Cube Roots of Unity.** Any complex number $x$ whose cube is equal to unity is called a *cube root of unity*. Since

$$x^3 - 1 = (x - 1)(x^2 + x + 1),$$

the roots of $x^3 = 1$ are 1 and the two numbers $x$ for which

$$x^2 + x + 1 = 0, \qquad (x + \tfrac{1}{2})^2 = -\tfrac{3}{4}, \qquad x + \tfrac{1}{2} = \pm\tfrac{1}{2}\sqrt{3}i.$$

Hence there are three cube roots of unity, viz.,

$$1, \qquad \omega = -\tfrac{1}{2} + \tfrac{1}{2}\sqrt{3}i, \qquad \omega' = -\tfrac{1}{2} - \tfrac{1}{2}\sqrt{3}i.$$

In view of the origin of $\omega$, we have the important relations

$$\omega^2 + \omega + 1 = 0, \quad \omega^3 = 1.$$

Since $\omega\omega' = 1$ and $\omega^3 = 1$, it follows that $\omega' = \omega^2$, $\omega = \omega'^2$.

**4. Geometrical Representation of Complex Numbers.** Using rectangular axes of coördinates, $OX$ and $OY$, we represent the complex number $a + bi$ by the point $A$ having the coördinates $a$, $b$ (Fig. 1).

The positive number $r = \sqrt{a^2 + b^2}$ giving the length of $OA$ is called the *modulus* (or *absolute value*) of $a + bi$. The angle $\theta = XOA$, measured counter-clockwise from $OX$ to $OA$, is called the *amplitude* (or *argument*) of $a + bi$. Thus $\cos\theta = a/r$, $\sin\theta = b/r$, whence



Fig. 1

(1)                    $a + bi = r(\cos\theta + i\sin\theta).$
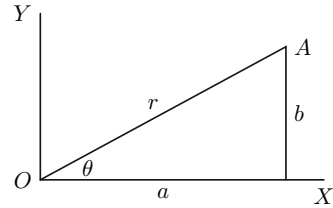
The second member is called the *trigonometric form* of $a + bi$.

For the amplitude we may select, instead of $\theta$, any of the angles $\theta \pm 360°$, $\theta \pm 720°$, etc.

Two complex numbers are equal if and only if their moduli are equal and an amplitude of the one is equal to an amplitude of the other.

For example, the cube roots of unity are 1 and
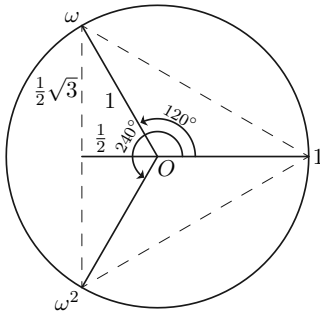


Fig. 2

$$\omega = -\tfrac{1}{2} + \tfrac{1}{2}\sqrt{3}i$$
$$= \cos 120° + i\sin 120°,$$
$$\omega^2 = -\tfrac{1}{2} - \tfrac{1}{2}\sqrt{3}i$$
$$= \cos 240° + i\sin 240°,$$

and are represented by the points marked 1, $\omega$, $\omega^2$ at the vertices of an equilateral triangle inscribed in a circle of radius unity and center at the origin $O$ (Fig. 2). The indicated amplitudes of $\omega$ and $\omega^2$ are 120° and 240° respectively, while the modulus of each is 1.

The modulus of $-3$ is 3 and its amplitude is 180° or 180° plus or minus the product of 360° by any positive whole number.

### 5. Product of Complex Numbers.   By actual multiplication,

$$\big[r(\cos\theta + i\sin\theta)\big]\big[r'(\cos\alpha + i\sin\alpha)\big]$$
$$= rr'\big[(\cos\theta\cos\alpha - \sin\theta\sin\alpha) + i(\sin\theta\cos\alpha + \cos\theta\sin\alpha)\big]$$
$$= rr'\big[\cos(\theta + \alpha) + i\sin(\theta + \alpha)\big], \quad \text{by trigonometry.}$$

Hence *the modulus of the product of two complex numbers is equal to the product of their moduli, while the amplitude of the product is equal to the sum of their amplitudes.*

For example, the square of $\omega = \cos 120° + i\sin 120°$ has the modulus 1 and the amplitude $120° + 120°$ and hence is $\omega^2 = \cos 240° + i\sin 240°$. Again, the

product of $\omega$ and $\omega^2$ has the modulus 1 and the amplitude $120° + 240°$ and hence is $\cos 360° + i \sin 360°$, which reduces to 1. This agrees with the known fact that $\omega^3 = 1$.

Taking $r = r' = 1$ in the above relation, we obtain the useful formula

(2) $$(\cos \theta + i \sin \theta)(\cos \alpha + i \sin \alpha) = \cos(\theta + \alpha) + i \sin(\theta + \alpha).$$

**6. Quotient of Complex Numbers.** Taking $\alpha = \beta - \theta$ in (2) and dividing the members of the resulting equation by $\cos \theta + i \sin \theta$, we get

$$\frac{\cos \beta + i \sin \beta}{\cos \theta + i \sin \theta} = \cos(\beta - \theta) + i \sin(\beta - \theta).$$

Hence *the amplitude of the quotient of* $R(\cos \beta + i \sin \beta)$ *by* $r(\cos \theta + i \sin \theta)$ *is equal to the difference* $\beta - \theta$ *of their amplitudes, while the modulus of the quotient is equal to the quotient* $R/r$ *of their moduli.*

The case $\beta = 0$ gives the useful formula

$$\frac{1}{\cos \theta + i \sin \theta} = \cos \theta - i \sin \theta.$$

**7. De Moivre's Theorem.** *If $n$ is any positive whole number,*

(3) $$(\cos \theta + i \sin \theta)^n = \cos n\theta + i \sin n\theta.$$

This relation is evidently true when $n = 1$, and when $n = 2$ it follows from formula (2) with $\alpha = \theta$. To proceed by mathematical induction, suppose that our relation has been established for the values $1, 2, \ldots, m$ of $n$. We can then prove that it holds also for the next value $m + 1$ of $n$. For, by hypothesis, we have

$$(\cos \theta + i \sin \theta)^m = \cos m\theta + i \sin m\theta.$$

Multiply each member by $\cos \theta + i \sin \theta$, and for the product on the right substitute its value from (2) with $\alpha = m\theta$. Thus

$$(\cos \theta + i \sin \theta)^{m+1} = (\cos \theta + i \sin \theta)(\cos m\theta + i \sin m\theta),$$
$$= \cos(\theta + m\theta) + i \sin(\theta + m\theta),$$

which proves (3) when $n = m + 1$. Hence the induction is complete.

Examples are furnished by the results at the end of §5:

$$(\cos 120° + i \sin 120°)^2 = \cos 240° + i \sin 240°,$$
$$(\cos 120° + i \sin 120°)^3 = \cos 360° + i \sin 360°.$$

**8. Cube Roots.**   To find the cube roots of a complex number, we first express the number in its trigonometric form. For example,

$$4\sqrt{2} + 4\sqrt{2}i = 8(\cos 45° + i \sin 45°).$$

If it has a cube root which is a complex number, the latter is expressible in the trigonometric form

(4)                                $r(\cos \theta + i \sin \theta).$

The cube of the latter, which is found by means of (3), must be equal to the proposed number, so that

$$r^3(\cos 3\theta + i \sin 3\theta) = 8(\cos 45° + i \sin 45°).$$

The moduli $r^3$ and 8 must be equal, so that the positive real number $r$ is equal to 2. Furthermore, $3\theta$ and $45°$ have equal cosines and equal sines, and hence differ by an integral multiple of $360°$. Hence $3\theta = 45° + k \cdot 360°$, or $\theta = 15° + k \cdot 120°$, where $k$ is an integer.[2] Substituting this value of $\theta$ and the value 2 of $r$ in (4), we get the desired cube roots. The values 0, 1, 2 of $k$ give the distinct results

$$R_1 = 2(\cos 15° \ + i \sin 15°),$$
$$R_2 = 2(\cos 135° + i \sin 135°),$$
$$R_3 = 2(\cos 255° + i \sin 255°).$$

Each new integral value of $k$ leads to a result which is equal to $R_1$, $R_2$ or $R_3$. In fact, from $k = 3$ we obtain $R_1$, from $k = 4$ we obtain $R_2$, from $k = 5$ we obtain $R_3$, from $k = 6$ we obtain $R_1$ again, and so on periodically.

## EXERCISES

**1.** Verify that $R_2 = \omega R_1$, $R_3 = \omega^2 R_1$. Verify that $R_1$ is a cube root of $8(\cos 45° + i \sin 45°)$ by cubing $R_1$ and applying De Moivre's theorem. Why are the new expressions for $R_2$ and $R_3$ evidently also cube roots?

**2.** Find the three cube roots of $-27$; those of $-i$; those of $\omega$.

**3.** Find the two square roots of $i$; those of $-i$; those of $\omega$.

**4.** Prove that the numbers $\cos \theta + i \sin \theta$ and no others are represented by points on the circle of radius unity whose center is the origin.

---

[2]Here, as elsewhere when the contrary is not specified, zero and negative as well as positive whole numbers are included under the term "integer."

**5.** If $a+bi$ and $c+di$ are represented by the points $A$ and $C$ in Fig. 3, prove that their sum is represented by the fourth vertex $S$ of the parallelogram two of whose sides are $OA$ and $OC$. Hence show that the modulus of the sum of two complex numbers is equal to or less than the sum of their moduli, and is equal to or greater than the difference of their moduli.
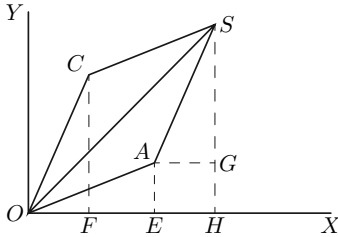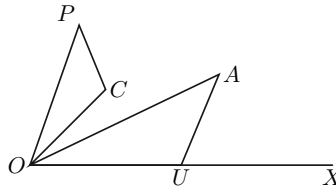


FIG. 3                                    FIG. 4

**6.** Let $r$ and $r'$ be the moduli and $\theta$ and $\alpha$ the amplitudes of two complex numbers represented by the points $A$ and $C$ in Fig. 4. Let $U$ be the point on the $x$-axis one unit to the right of the origin $O$. Construct triangle $OCP$ similar to triangle $OUA$ and similarly placed, so that corresponding sides are $OC$ and $OU, CP$ and $UA$, $OP$ and $OA$, while the vertices $O$, $C$, $P$ are in the same order (clockwise or counter-clockwise) as the corresponding vertices $O$, $U$, $A$. Prove that $P$ represents the product (§5) of the complex numbers represented by $A$ and $C$.

**7.** If $a + bi$ and $e + fi$ are represented by the points $A$ and $S$ in Fig. 3, prove that the complex number obtained by subtracting $a + bi$ from $e + fi$ is represented by the point $C$. Hence show that the absolute value of the difference of two complex numbers is equal to or less than the sum of their absolute values, and is equal to or greater than the difference of their absolute values.

**8.** By modifying Ex. 6, show how to construct geometrically the quotient of two complex numbers.

**9. $n$th Roots.**   As illustrated in §8, it is evident that the $n$th roots of any complex number $\rho(\cos A + i \sin A)$ are the products of the $n$th roots of $\cos A + i \sin A$ by the positive real $n$th root of the positive real number $\rho$ (which may be found by logarithms).

Let an $n$th root of $\cos A + i \sin A$ be of the form

(4)                                 $r(\cos \theta + i \sin \theta).$

Then, by De Moivre's theorem,

$$r^n(\cos n\theta + i \sin n\theta) = \cos A + i \sin A.$$

The moduli $r^n$ and 1 must be equal, so that the positive real number $r$ is equal to 1. Since $n\theta$ and $A$ have equal sines and equal cosines, they differ by an integral multiple of $360°$. Hence $n\theta = A + k \cdot 360°$, where $k$ is an integer. Substituting the resulting value of $\theta$ and the value 1 of $r$ in (4), we get

$$(5) \qquad \cos\left(\frac{A + k \cdot 360°}{n}\right) + i\sin\left(\frac{A + k \cdot 360°}{n}\right).$$

For each integral value of $k$, (5) is an answer since its $n$th power reduces to $\cos A + i\sin A$ by DeMoivre's theorem. Next, the value $n$ of $k$ gives the same answer as the value 0 of $k$; the value $n + 1$ of $k$ gives the same answer as the value 1 of $k$; and in general the value $n + m$ of $k$ gives the same answer as the value $m$ of $k$. Hence we may restrict attention to the values $0, 1, \ldots, n - 1$ of $k$. Finally, the answers (5) given by these values $0, 1, \ldots, n - 1$ of $k$ are all distinct, since they are represented by points whose distance from the origin is the modulus 1 and whose amplitudes are

$$\frac{A}{n}, \qquad \frac{A}{n} + \frac{360°}{n}, \qquad \frac{A}{n} + \frac{2 \cdot 360°}{n}, \ldots, \frac{A}{n} + \frac{(n-1)360°}{n},$$

so that these $n$ points are equally spaced points on a circle of radius unity. Special cases are noted at the end of §10. Hence *any complex number different from zero has exactly n distinct complex nth roots.*

**10. Roots of Unity.**    The trigonometric form of 1 is $\cos 0° + i\sin 0°$. Hence by §9 with $A = 0$, the $n$ distinct $n$th roots of unity are

$$(6) \qquad \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n} \quad (k = 0, 1, \ldots, n - 1),$$

where now the angles are measured in radians (an angle of 180 degrees being equal to $\pi$ radians, where $\pi = 3.1416$, approximately). For $k = 0$, (6) reduces to 1, which is an evident $n$th root of unity. For $k = 1$, (6) is

$$(7) \qquad R = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}.$$

By De Moivre's theorem, the general number (6) is equal to the $k$th power of $R$. Hence the $n$ distinct $n$th roots of unity are

$$(8) \qquad R, \ R^2, \ R^3, \ldots, \ R^{n-1}, \ R^n = 1.$$

As a special case of the final remark in §9, the $n$ complex numbers (6), and therefore the numbers (8), are represented geometrically by the vertices of a regular polygon of $n$ sides inscribed in the circle of radius unity and center at the origin with one vertex on the positive $x$-axis.
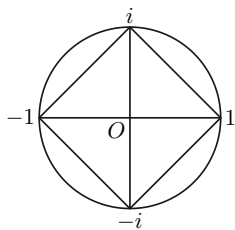
For $n = 3$, the numbers (8) are $\omega$, $\omega^2$, 1, which are represented in Fig. 2 by the vertices of an equilateral triangle.

For $n = 4$, $R = \cos \pi/2 + i \sin \pi/2 = i$. The four fourth roots of unity (8) are $i$, $i^2 = -1$, $i^3 = -i$, $i^4 = 1$, which are represented by the vertices of a square inscribed in a circle of radius unity and center at the origin $O$ (Fig. 5).

Fig. 5

## EXERCISES

**1.** Simplify the trigonometric forms (6) of the four fourth roots of unity. Check the result by factoring $x^4 - 1$.

**2.** For $n = 6$, show that $R = -\omega^2$. The sixth roots of unity are the three cube roots of unity and their negatives. Check by factoring $x^6 - 1$.

**3.** From the point representing $a + bi$, how do you obtain that representing $-(a + bi)$? Hence derive from Fig. 2 and Ex. 2 the points representing the six sixth roots of unity. Obtain this result another way.

**4.** Find the five fifth roots of $-1$.

**5.** Obtain the trigonometric forms of the nine ninth roots of unity. Which of them are cube roots of unity?

**6.** Which powers of a ninth root (7) of unity are cube roots of unity?

**11. Primitive $n$th Roots of Unity.** An $n$th root of unity is called *primitive* if $n$ is the smallest positive integral exponent of a power of it that is equal to unity. Thus $\rho$ is a primitive $n$th root of unity if and only if $\rho^n = 1$ and $\rho^l \neq 1$ for all positive integers $l < n$.

Since only the last one of the numbers (8) is equal to unity, the number $R$, defined by (7), is a primitive $n$th root of unity. We have shown that the powers (8) of $R$ give all of the $n$th roots of unity. Which of these powers of $R$ are primitive $n$th roots of unity?

For $n = 4$, the powers (8) of $R = i$ were seen to be

$$i^1 = i, \ i^2 = -1, \ i^3 = -i, \ i^4 = 1.$$

The first and third are primitive fourth roots of unity, and their exponents 1 and 3 are relatively prime to 4, i.e., each has no divisor $> 1$ in common with 4. But the second and fourth are not primitive fourth roots of unity (since the square of $-1$ and the first power of 1 are equal to unity), and their exponents 2 and 4 have the

divisor 2 in common with $n = 4$. These facts illustrate and prove the next theorem for the case $n = 4$.

THEOREM.    *The primitive nth roots of unity are those of the numbers* (8) *whose exponents are relatively prime to n.*

*Proof.*    If $k$ and $n$ have a common divisor $d$ $(d > 1)$, $R^k$ is not a primitive $n$th root of unity, since

$$(R^k)^{\frac{n}{d}} = (R^n)^{\frac{k}{d}} = 1,$$

and the exponent $n/d$ is a positive integer less than $n$.

But if $k$ and $n$ are relatively prime, i.e., have no common divisor $> 1$, $R^k$ is a primitive $n$th root of unity. To prove this, we must show that $(R^k)^l \neq 1$ if $l$ is a positive integer $< n$. By De Moivre's theorem,

$$R^{kl} = \cos \frac{2kl\pi}{n} + i \sin \frac{2kl\pi}{n}.$$

If this were equal to unity, $2kl\pi/n$ would be a multiple of $2\pi$, and hence $kl$ a multiple of $n$. Since $k$ is relatively prime to $n$, the second factor $l$ would be a multiple of $n$, whereas $0 < l < n$.

## EXERCISES

**1.** Show that the primitive cube roots of unity are $\omega$ and $\omega^2$.

**2.** For $R$ given by (7), prove that the primitive $n$th roots of unity are (i) for $n = 6$, $R$, $R^5$; (ii) for $n = 8$, $R$, $R^3$, $R^5$, $R^7$; (iii) for $n = 12$, $R$, $R^5$, $R^7$, $R^{11}$.

**3.** When $n$ is a prime, prove that any $n$th root of unity, other than 1, is primitive.

**4.** Let $R$ be a primitive $n$th root (7) of unity, where $n$ is a product of two different primes $p$ and $q$. Show that $R, \ldots, R^n$ are primitive with the exception of $R^p$, $R^{2p}, \ldots, R^{qp}$, whose $q$th powers are unity, and $R^q$, $R^{2q}, \ldots, R^{pq}$, whose $p$th powers are unity. These two sets of exceptions have only $R^{pq}$ in common. Hence there are exactly $pq - p - q + 1$ primitive $n$th roots of unity.

**5.** Find the number of primitive $n$th roots of unity if $n$ is a square of a prime $p$.

**6.** Extend Ex. 4 to the case in which $n$ is a product of three distinct primes.

**7.** If $R$ is a primitive 15th root (7) of unity, verify that $R^3$, $R^6$, $R^9$, $R^{12}$ are the primitive fifth roots of unity, and $R^5$ and $R^{10}$ are the primitive cube roots of unity. Show that their eight products by pairs give all the primitive 15th roots of unity.

**8.** If $\rho$ is any primitive $n$th root of unity, prove that $\rho$, $\rho^2, \ldots, \rho^n$ are distinct and give all the $n$th roots of unity. Of these show that $\rho^k$ is a primitive $n$th root of unity if and only if $k$ is relatively prime to $n$.

**9.** Show that the six primitive 18th roots of unity are the negatives of the primitive ninth roots of unity.