Rapid #: -15940550

CROSS REF ID: **1639297**

LENDER: **H2E :: Main Library**

BORROWER: **UUM :: Marriott Library**

TYPE:	Book Chapter
BOOK TITLE:	What is Mathematics
USER BOOK TITLE:	What is Mathematics
CHAPTER TITLE:	Chapter III, The Algebra of Number Fields (Introduction + Part I)
BOOK AUTHOR:	
EDITION:	Second
VOLUME:	
PUBLISHER:	
YEAR:	1996
PAGES:	117-140
ISBN:	9780195105193
LCCN:	
OCLC #:	

Processed by RapidX: 3/23/2020 1:41:47 AM

6

Rapid #: -15940550

Odyssey
utah.illiad.oclc.org/UUM

Status	Rapid Code	Branch Name	Start Date
New	UUM	Marriott Library	03/21/2020 09:51 AM
Pending	H2E	Main Library	03/21/2020 09:51 AM
Batch Not Printed	H2E	Main Library	03/23/2020 09:44 AM

CALL #: **QA37.2 .C69 1996** 4 K~

LOCATION: **H2E :: Main Library :: cci2**

REQUEST TYPE:	Book Chapter
USER BOOK TITLE:	What is Mathematics
H2E CATALOG TITLE:	What is mathematics
CHAPTER TITLE:	Chapter III, The Algebra of Number Fields (Introduction + Part I)
BOOK AUTHOR:	
EDITION:	Second
VOLUME:	
PUBLISHER:	
YEAR:	1996
PAGES:	117-140
ISBN:	9780195105193
LCCN:	
OCLC #:	
CROSS REFERENCE ID:	[TN:1639297][ODYSSEY:utah.illiad.oclc.org/UUM]
VERIFIED:	

BORROWER: **UUM :: Marriott Library**

RAPID ILL

the n digits 1, 2, 3, $\cdots$, n are written down in random order, the probability that at least one digit will occupy its proper place is

$$p_n = 1 - \frac{1}{2!} + \frac{1}{3!} - \frac{1}{4!} + \cdots \pm \frac{1}{n!}, \tag{5}$$

where the last term is taken with a plus or minus sign according as n is odd or even. In particular, for $n = 5$ the probability is

$$p_5 = 1 - \frac{1}{2!} + \frac{1}{3!} - \frac{1}{4!} + \frac{1}{5!} = \frac{19}{30} = 0.63333 \cdots .$$

We shall see in Chapter VIII that as n tends to infinity the expression

$$S_n = \frac{1}{2!} - \frac{1}{3!} + \frac{1}{4!} - \cdots \pm \frac{1}{n!}$$

tends to a limit, $1/e$, whose value to five places of decimals is .36788. Since from (5) $p_n = 1 - S_n$, this shows that as n tends to infinity

$$p_n \to 1 - 1/e = .63212.$$

CHAPTER III

GEOMETRICAL CONSTRUCTIONS. THE ALGEBRA OF NUMBER FIELDS

INTRODUCTION

Construction problems have always been a favorite subject in geometry. With ruler and compass alone a great variety of constructions may be performed, as the reader will remember from school: a line segment or an angle may be bisected, a line may be drawn from a point perpendicular to a given line, a regular hexagon may be inscribed in a circle, etc. In all these problems the ruler is used merely as a straightedge, an instrument for drawing a straight line but not for measuring or marking off distances. The traditional restriction to ruler and compass alone goes back to antiquity, although the Greeks themselves did not hesitate to use other instruments.

One of the most famous of the classical construction problems is the so-called contact problem of Apollonius (circa 200 B.C.) in which three arbitrary circles in the plane are given and a fourth circle tangent to all three is required. In particular, it is permitted that one or more of the given circles have degenerated into a point or a straight line (a "circle" with radius zero or "infinity," respectively). For example, it may be required to construct a circle tangent to two given straight lines and passing through a given point. While such special cases are rather easily dealt with, the general problem is considerably more difficult.

Of all construction problems, that of constructing with ruler and compass a regular polygon of n sides has perhaps the greatest interest. For certain values of n—e.g. $n = 3, 4, 5, 6$—the solution has been known since antiquity, and forms an important part of school geometry. But for the regular heptagon ($n = 7$) the construction has been proved impossible. There are three other classical Greek problems for which a solution has been sought in vain: to trisect an arbitrary given angle, to double a given cube (i.e. to find the edge of a cube whose volume shall be twice that of a cube with a given segment as its edge) and to square the circle (i.e. to construct a square having the same area as a given

circle). In all these problems, ruler and compass are the only instruments permitted.

Unsolved problems of this sort gave rise to one of the most remarkable and novel developments in mathematics, when, after centuries of futile search for solutions, the suspicion grew that these problems might be definitely unsolvable. Thus mathematicians were challenged to investigate the question: *How is it possible to prove that certain problems cannot be solved?*

In algebra, it was the problem of solving equations of degree 5 and higher which led to this new way of thinking. During the sixteenth century mathematicians had learned that algebraic equations of degree 3 or 4 could be solved by a process similar to the elementary method for solving quadratic equations. All these methods have the following characteristic in common: the solutions or "roots" of the equation can be written as algebraic expressions obtained from the coefficients of the equation by a sequence of operations, each of which is either a rational operation—addition, subtraction, multiplication, or division—or the extraction of a square root, cube root, or fourth root. One says that algebraic equations up to the fourth degree can be solved "by radicals" (radix is the Latin word for root). Nothing seemed more natural than to extend this procedure to equations of degree 5 and higher, by using roots of higher order. All such attempts failed. Even distinguished mathematicians of the eighteenth century deceived themselves into thinking that they had found the solution. It was not until early in the nineteenth century that the Italian Ruffini (1765–1822) and the Norwegian genius N. H. Abel (1802-1829) conceived the then revolutionary idea of proving the *impossibility of the solution of the general algebraic equation of degree* n *by means of radicals.* One must clearly understand that the question is not whether any algebraic equation of degree *n possesses* solutions. This fact was first proved by Gauss in his doctoral thesis in 1799. So there is no doubt about the *existence* of the roots of an equation, especially since these roots can be found by suitable procedures to any degree of accuracy. The art of the numerical solution of equations is, of course, very important and highly developed. But the problem of Abel and Ruffini was quite different: can the solution be effected *by means of rational operations and radicals alone*? It was the desire to attain full clarity about this question that inspired the magnificent development of modern algebra and group theory started by Ruffini, Abel, and Galois (1811–1832).

The question of proving the impossibility of certain geometrical constructions provides one of the simplest examples of this trend in algebra. By the use of algebraic concepts we shall be able in this chapter to prove the impossibility of trisecting the angle, constructing the regular heptagon, or doubling the cube, by ruler and compass alone. (The problem of squaring the circle is much more difficult to dispose of; see p. 140.) Our point of departure will be not so much the negative question of the impossibility of certain constructions, but rather the positive question: How can all constructible problems be completely characterized? After we have answered this question, it will be an easy matter to show that the problems mentioned above do not fall into this category.

At the age of seventeen Gauss investigated the constructibility of regular "p-gons" (polygons with p sides), where p is a prime number. The construction was then known only for $p = 3$ and $p = 5$. Gauss discovered that the regular p-gon is constructible if and only if p is a prime "Fermat number,"

$$p = 2^{2^n} + 1.$$

The first Fermat numbers are 3, 5, 17, 257, 65537 (see p. 26). So overwhelmed was young Gauss by his discovery that he at once gave up his intention of becoming a philologist and resolved to devote his life to mathematics and its applications. He always looked back on this first of his great feats with particular pride. After his death, a bronze statue of him was erected in Goettingen, and no more fitting honor could be devised than to shape the pedestal in the form of a regular 17-gon.

When dealing with a geometrical construction, one must never forget that the problem is not that of drawing figures in practice with a certain degree of accuracy, but of whether, by the use of straightedge and compass alone, the solution can be found theoretically, supposing our instruments to have perfect precision. What Gauss proved is that his constructions could be performed in principle. His theory does not concern the simplest way actually to perform them or the devices which could be used to simplify and to cut down the number of necessary steps. This is a question of much less theoretical importance. From a practical point of view, no such construction would give as satisfactory a result as could be obtained by the use of a good protractor. Failure properly to understand the theoretical character of the question of geometrical construction and stubbornness in refusing to take cognizance of well-established scientific facts are responsible for the persistence of

an unending line of angle-trisectors and circle-squarers. Those among them who are able to understand elementary mathematics might profit by studying this chapter.

Once more it should be emphasized that in some ways our concept of geometrical construction seems artificial. Ruler and compass are certainly the simplest instruments for drawing, but the restriction to these instruments is by no means inherent in geometry. As the Greek mathematicians recognized long ago, certain problems—for example that of doubling the cube—can be solved if, e.g., the use of a ruler in the form of a right angle is permitted; it is just as easy to invent instruments other than the compass by means of which one can draw ellipses, hyperbolas, and more complicated curves, and whose use enlarges considerably the domain of constructible figures. In the next sections, however, we shall adhere to the standard concept of geometrical constructions using only ruler and compass.

PART I

IMPOSSIBILITY PROOFS AND ALGEBRA

§1. FUNDAMENTAL GEOMETRICAL CONSTRUCTIONS

1. Construction of Fields and Square Root Extraction

To shape our general ideas we shall begin by examining a few of the classical constructions. The key to a more profound understanding lies in translating the geometrical problems into the language of algebra. Any geometrical construction problem is of the following type: a certain set of line segments, say $a, b, c, \cdots$, is given, and one or more other segments $x, y, \cdots$, are sought. It is always possible to formulate problems in this way, even when at first glance they have a quite different aspect. The required segments may appear as sides of a triangle to be constructed, as radii of circles, or as the rectangular coördinates of certain points (see e.g. p. 137). For simplicity we shall suppose that only one segment x is required. The geometrical construction then amounts to solving an algebraic problem: first we must find a relationship (equation) between the required quantity x and the given quantities $a, b, c, \cdots$; next we must find the unknown quantity x by solving this equation, and finally we must determine whether this solution can be obtained by algebraic processes that correspond to ruler and compass constructions. It is the principle of analytic geometry, the quantitative characterization of geometrical objects by real numbers, based on the introduction of the real number continuum, that provides the foundation for the whole theory.

First we observe that some of the simplest algebraic operations correspond to elementary geometrical constructions. If two segments are given with lengths a and b (as measured by a given "unit" segment), then it is very easy to construct $a + b$, $a - b$, ra (where r is any rational number), a/b, and ab.

To construct $a + b$ (Fig. 27) we draw a straight line and on it mark off with the compass the distances $OA = a$ and $AB = b$. Then $OB = a + b$. Similarly, for $a - b$ we mark off $OA = a$ and $AB = b$, but this time with AB in the opposite direction from OA. Then $OB = a - b$. To construct $3a$ we simply add $a + a + a$; similarly we can

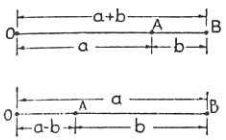

Fig. 27. Construction of $a + b$ and $a - b$.

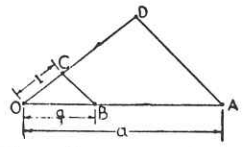

Fig. 28. Construction of $a/3$.

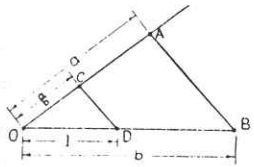

Fig. 29. Construction of a/b.

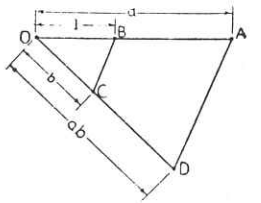

Fig. 30. Construction of ab.

construct pa, where p is any integer. We construct $a/3$ by the following device (Fig. 28): we mark off $OA = a$ on one line, and draw any second line through O. On this line we mark off an arbitrary segment $OC = c$, and construct $OD = 3c$. We connect A and D, and draw a line through C parallel to AD, intersecting OA at B. The triangles OBC and OAD are similar; hence $OB/a = OB/OA = OC/OD = 1/3$, and $OB = a/3$. In the same way we can construct a/q, where q is any integer. By performing this operation on the segment pa, we can thus construct ra, where $r = p/q$ is any rational number.

To construct a/b (Fig. 29) we mark off $OB = b$ and $OA = a$ on the sides of any angle O, and on OB we mark off $OD = 1$. Through D we draw a line parallel to AB meeting OA in C. Then OC will have the

length a/b. The construction of ab is shown in Figure 30, where AD is a line parallel to BC through A.

From these considerations it follows that *the "rational" algebraic processes,*—addition, subtraction, multiplication, and division of known quantities—*can be performed by geometrical constructions.* From any given segments, measured by real numbers $a, b, c, \cdots$, we can, by successive application of these simple constructions, construct any quantity that is expressible in terms of $a, b, c, \cdots$ in a rational way, i.e. by repeated application of addition, subtraction, multiplication and division. The totality of quantities that can be obtained in this way from $a, b, c, \cdots$ constitute what is called a *number field,* a set of numbers such that any rational operations applied to two or more members of the set again yield a number of the set. We recall that the rational numbers, the real numbers, and the complex numbers form such fields. In the present case, the field is said to be *generated* by the given numbers $a, b, c, \cdots$.

The decisive new construction which carries us beyond the field just obtained is the extraction of a square root: if a segment a is given, then $\sqrt{a}$ can also be constructed by using only ruler and compass. On a straight line we mark off $OA = a$ and $AB = 1$ (Fig. 31). We draw a circle with the segment OB as its diameter and construct the perpendicular to OB through A, which meets the circle in C. The triangle OBC has a right angle at C, by the theorem of elementary geometry which states that an angle inscribed in a semicircle is a right angle. Hence, $\angle OCA = \angle ABC$, the right triangles OAC and CAB are similar, and we have for $x = AC$,

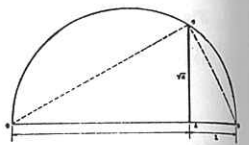

Fig. 31. Construction of $\sqrt{a}$.

$$\frac{a}{x} = \frac{x}{1}, \qquad x^2 = a, \qquad x = \sqrt{a}.$$

2. Regular Polygons

Let us now consider a few somewhat more elaborate construction problems. We begin with the *regular decagon.* Suppose that a regular decagon is inscribed in a circle with radius 1 (Fig. 32), and call its side x. Since x will subtend an angle of 36° at the center of the circle, the other two angles of the large triangle will each be 72°, and hence the dotted line which bisects angle A divides triangle OAB into two isosceles triangles, each with equal sides of length x. The radius of the circle is thus divided into two segments, x and $1 - x$. Since OAB is similar to the smaller isosceles triangle, we have $1/x = x/(1 - x)$. From this proportion we get the quadratic equation $x^2 + x - 1 = 0$, the solution of which is $x = (\sqrt{5} - 1)/2$. (The other solution of the equation is irrelevant, since it yields a negative x.) From this it is clear that x can be constructed geometrically. Having the length x, we may now construct the regular decagon by marking off this length ten times as a chord of the circle. The regular pentagon may now be constructed by joining alternate vertices of the regular decagon.

Instead of constructing $\sqrt{5}$ by the method of Figure 31 we can also obtain it as the hypotenuse of a right triangle whose other sides have lengths 1 and 2. We then obtain x by subtracting the unit length from $\sqrt{5}$ and bisecting the result.

The ratio $OB{:}AB$ of the preceding problem has been called the golden ratio, because the Greek mathematicians considered a rectangle whose two sides are in this ratio to be aesthetically the most pleasing. Its value, incidentally, is about 1.62.

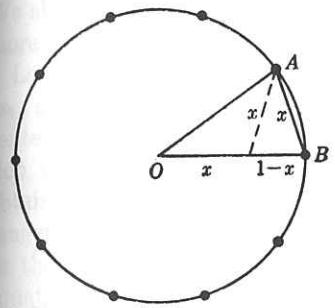

Fig. 32 Regular decagon.

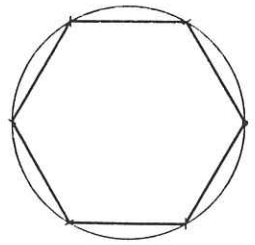

Fig. 33. Regular hexagon.

Of all the regular polygons the hexagon is simplest to construct. We start with a circle of radius r; the length of the side of a regular hexagon inscribed in this circle will then be equal to r. The hexagon itself can be constructed by successively marking off from any point of the circle chords of length r until all six vertices are obtained.

From the regular n-gon we can obtain the regular $2n$-gon by bisecting the arc subtended on the circumscribed circle by each edge of the n-gon, using the additional points thus found as well as the original vertices for the required $2n$-gon. Starting with the diameter of a circle (a "2-gon"), we can therefore construct the 4, 8, 16, $\cdots$, 2^n-gon. Similarly, we can obtain the 12-, 24-, 48-gon, etc. from the hexagon, and the 20-, 40-gon, etc. from the decagon.

If s_n denotes the length of the side of the regular n-gon inscribed in the unit circle (circle with radius 1), then the side of the $2n$-gon is of length

$$s_{2n} = \sqrt{2 - \sqrt{4 - s_n^2}}$$

This may be proved as follows: In Figure 34 s_n is equal to $DE = 2DC$, s_{2n} equal to DB, and AB equal to 2. The area of the right triangle ABD is given by $\frac{1}{2}BD \cdot AD$ and by $\frac{1}{2}AB \cdot CD$. Since $AD = \sqrt{AB^2 - DB^2}$, we find, by substituting $AB = 2$, $BD = s_{2n}$, $CD = \frac{1}{2}s_n$, and by equating the two expressions for the area,

$$s_n = s_{2n}\sqrt{4 - s_{2n}^2} \qquad \text{or} \qquad s_n^2 = s_{2n}^2 (4 - s_{2n}^2).$$

Solving this quadratic equation for $x = s_{2n}^2$ and observing that x must be less than 2, one easily finds the formula given above.

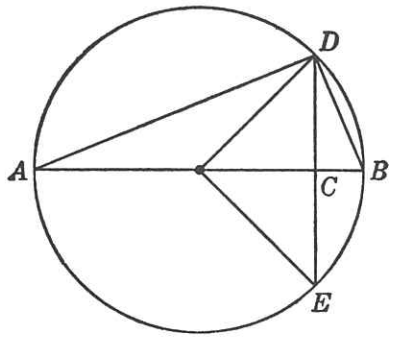

Fig. 34.

From this formula and the fact that s_4 (the side of the square) is equal to $\sqrt{2}$ it follows that

$$s_8 = \sqrt{2 - \sqrt{2}}, \qquad s_{16} = \sqrt{2 - \sqrt{2 + \sqrt{2}}},$$

$$s_{32} = \sqrt{2 - \sqrt{2 + \sqrt{2 + \sqrt{2}}}}, \text{ etc.}$$

As a general formula we obtain, for $n > 2$,

$$s_{2^n} = \sqrt{2 - \sqrt{2 + \sqrt{2 + \cdots + \sqrt{2}}}}$$

with $n - 1$ nested square roots. The circumference of the 2^n-gon in the circle is $2^n s_{2^n}$. As n tends to infinity, the 2^n-gon tends to the circle. Hence $2^n s_{2^n}$ approaches the length of the circumference of the unit circle, which is by definition 2π. Thus we obtain, by substituting m for $n - 1$ and cancelling a factor 2, the limiting formula for π:

$$2^m \underbrace{\sqrt{2 - \sqrt{2 + \sqrt{2 + \cdots + \sqrt{2}}}}}_{m \text{ square roots}} \to \pi \quad \text{as} \quad m \to \infty.$$

Exercise: Since $2^m \to \infty$, prove as a consequence that

$$\underbrace{\sqrt{2 + \sqrt{2 + \cdots + \sqrt{2}}}}_{n \text{ square roots.}} \to 2 \quad \text{as} \quad n \to \infty.$$

The results obtained thus far exhibit the following characteristic feature: *The sides of the 2^n-gon, the $5 \cdot 2^n$-gon, and the $3 \cdot 2^n$-gon, can all be found entirely by the processes of addition, subtraction, multiplication, division, and the extraction of square roots.*

*3. Apollonius' Problem

Another construction problem that becomes quite simple from the algebraic standpoint is the famous contact problem of Apollonius already mentioned. In the present context it is unnecessary for us to find a particularly elegant construction. What matters here is that in principle the problem can be solved by straightedge and compass alone. We shall give a brief indication of the proof, leaving the question of a more elegant method of construction to page 161.

Let the centers of the three given circles have coördinates (x_1, y_1), (x_2, y_2) and (x_3, y_3), respectively, with radii r_1, r_2, and r_3. Denote the center and radius of the required circle by (x, y) and r. Then the condition that the required circle be tangent to the three given circles is obtained by observing that the distance between the centers of two tangent circles is equal to the sum or difference of the radii, according as the circles are tangent externally or internally. This yields the equations

$$(1) \qquad (x - x_1)^2 + (y - y_1)^2 - (r \pm r_1)^2 = 0,$$

$$(2) \qquad (x - x_2)^2 + (y - y_2)^2 - (r \pm r_2)^2 = 0,$$

$$(3) \qquad (x - x_3)^2 + (y - y_3)^2 - (r \pm r_3)^2 = 0,$$

or

$$(1a) \qquad x^2 + y^2 - r^2 - 2xx_1 - 2yy_1 \pm 2rr_1 + x_1^2 + y_1^2 - r_1^2 = 0,$$

etc. The plus or minus sign is to be chosen in each of these equations according as the circles are to be externally or internally tangent. (See Fig. 35.) Equations (1), (2), (3) are three quadratic equations in three unknowns x, y, r with the property that the second degree terms are the same in each equation, as is seen from the expanded form (1a). Hence, by subtracting (2) from (1), we get a linear equation in x, y, r:

$$(4) \qquad ax + by + cr = d,$$

where $a = 2(x_2 - x_1)$, etc. Similarly, by subtracting (3) from (1), we get another linear equation,

$$(5) \qquad a'x + b'y + c'r = d'.$$

Solving (4) and (5) for x and y in terms of r and then substituting in (1) we get a quadratic equation in r, which can be solved by rational operations and the extraction of a square root (see p. 91). There will in general be two solutions of this equation, of which only one will be positive. After finding r from this equation we obtain x and y from the two linear equations (4) and (5). The circle with center (x, y) and radius r will be tangent to the three given circles. In the whole process we have used only rational operations and square root extractions. It follows that r, x, and y can be constructed by ruler and compass alone.

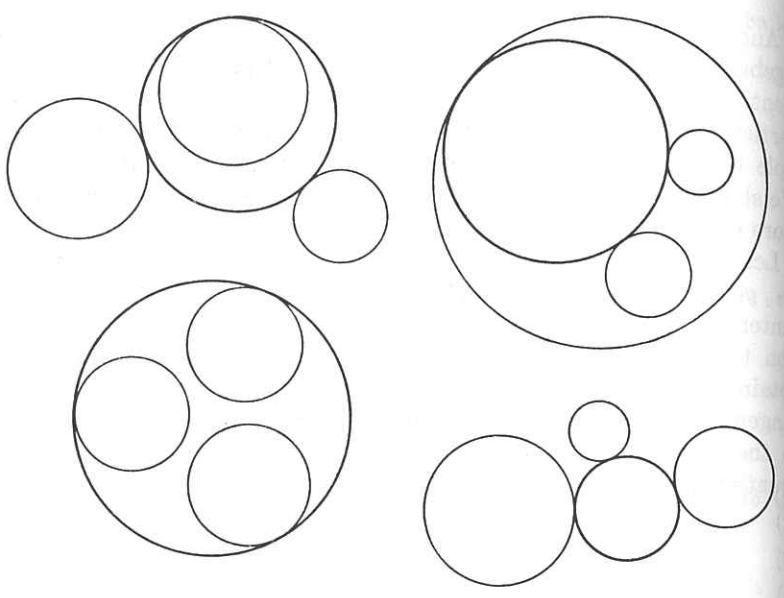

Fig. 35. Apollonius circles.

There will in general be eight solutions of the problem of Apollonius, corresponding to the $2 \cdot 2 \cdot 2 = 8$ possible combinations of $+$ and $-$ signs in equations (1), (2), and (3). These choices correspond to the conditions that the desired circles be externally or internally tangent to each of the three given circles. It may happen that our algebraic procedure does not actually yield real values for x, y, and r. This will be the case, for example, if the three given circles are concentric, so that no solution to the geometrical problem exists. Likewise, we must expect possible "degenerations" of the solution, as in the case when the three given circles degenerate into three points on a line. Then the Apollonius circle degenerates into this line. We shall not discuss these possibilities in detail; a reader with some algebraic experience will be able to complete the analysis.

*§2. CONSTRUCTIBLE NUMBERS AND NUMBER FIELDS

1. General Theory

Our previous discussion indicates the general algebraic background of geometrical constructions. Every ruler and compass construction consists of a sequence of steps, each of which is one of the following: 1) connecting two points by a straight line, 2) finding the point of intersection of two lines, 3) drawing a circle with a given radius about a point, 4) finding the points of intersection of a circle with another circle or with a line. An element (point, line, or circle) is considered to be known if it was given at the outset or if it has been constructed in some previous step. For a theoretical analysis we may refer the whole construction to a coördinate system x, y (see p. 73). The given elements will then be represented by points or segments in the x, y plane. If only one segment is given at the outset, we may take this as the unit length, which fixes the point $x = 1$, $y = 0$. Sometimes there appear "arbitrary" elements: arbitrary lines are drawn, arbitrary points or radii are chosen. (An example of such an arbitrary element appears in constructing the midpoint of a segment; we draw two circles of equal but arbitrary radius from each endpoint of the segment, and join their intersections.) In such cases we may choose the element to be rational; i.e. arbitrary points may be chosen with rational coordinates x, y, arbitrary lines $ax + by + c = 0$ with rational coefficients a, b, c, arbitrary circles with centers having rational coördinates and with rational radii. We shall make such a choice of rational arbitrary elements throughout; if the elements are indeed arbitrary this restriction cannot affect the result of a construction.

For the sake of simplicity, we shall assume in the following discussion that only one element, the unit length 1, is given at the outset. Then according to §1 we can construct by ruler and compass all numbers that can be obtained from unity by the rational processes of addition, subtraction, multiplication and division, i.e. all the rational numbers r/s, where r and s are integers. The system of rational numbers is "closed" with respect to the rational operations; that is, the sum, difference, product, or quotient of any two rational numbers—excluding division by 0, as always—is again a rational number. Any set of numbers possessing this property of closure with respect to the four rational operations is called a *number field.*

Exercise: Show that every field contains all the rational numbers at least. (Hint: If $a \neq 0$ is a number in the field F, then $a/a = 1$ belongs to F, and from 1 we can obtain any rational number by rational operations.)

Starting from the unit, we can thus construct the whole rational number field and hence all the rational points (i.e. points with both coördinates rational) in the x, y plane. We can reach new, irrational, numbers by using the compass to construct e.g. the number $\sqrt{2}$ which, as we know from Chapter II, §2, is not in the rational field. Having constructed $\sqrt{2}$ we may then, by the "rational" constructions of §1, find all numbers of the form

$$a + b\sqrt{2}, \tag{1}$$

where a, b are rational, and therefore are themselves constructible. We may likewise construct all numbers of the form

$$\frac{a + b\sqrt{2}}{c + d\sqrt{2}} \quad \text{or} \quad (a + b\sqrt{2})(c + d\sqrt{2}),$$

where a, b, c, d are rational. These numbers, however, may always be written in the form (1). For we have

$$\frac{a + b\sqrt{2}}{c + d\sqrt{2}} = \frac{a + b\sqrt{2}}{c + d\sqrt{2}} \cdot \frac{c - d\sqrt{2}}{c - d\sqrt{2}} = \frac{ac - 2bd}{c^2 - 2d^2} + \frac{bc - ad}{c^2 - 2d^2}\sqrt{2} = p + q\sqrt{2},$$

where p, q are rational. (The denominator $c^2 - 2d^2$ cannot be zero, for if $c^2 - 2d^2 = 0$, then $\sqrt{2} = c/d$, contrary to the fact that $\sqrt{2}$ is irrational.) Likewise

$$(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (bc + ad)\sqrt{2} = r + s\sqrt{2},$$

where r, s are rational. Hence all that we reach by the construction of $\sqrt{2}$ is the set of numbers of the form (1), with arbitrary rational a, b.

Exercises: From $p = 1 + \sqrt{2}$, $q = 2 - \sqrt{2}$, $r = -3 + \sqrt{2}$ obtain the numbers

$$\frac{p}{q},\ p + p^2,\ (p - p^2)\frac{q}{r},\ \frac{pqr}{1 + r^2},\ \frac{p + qr}{q + pr^2},$$

in the form (1).

These numbers (1) again form a field, as the preceding discussion shows. (That the sum and difference of two numbers of the form (1) are also of the form (1) is obvious.) This field is larger than the rational field, which is a part or *subfield* of it. But, of course, it is smaller than the field of *all* real numbers. Let us call the rational field F_0 and the new field of numbers of the form (1), F_1. The constructibility of

every number in the "extension field" F_1 has been established. We may now extend the scope of our constructions, e.g. by taking a number of F_1, say $k = 1 + \sqrt{2}$, and extracting the square root, thus obtaining the constructible number

$$\sqrt{1 + \sqrt{2}} = \sqrt{k},$$

and with it, according to §1, the field consisting of all the numbers

$$p + q\sqrt{k}, \tag{2}$$

where now p and q may be arbitrary numbers of F_1, i.e. of the form $a + b\sqrt{2}$, with a, b in F_0, i.e. rational.

Exercises: Represent

$$(\sqrt{k})^3,\ \frac{1 + (\sqrt{k})^2}{1 + \sqrt{k}},\ \frac{\sqrt{2}\sqrt{k} + \frac{1}{\sqrt{2}}}{(\sqrt{k})^3 - 3},\ \frac{(1 + \sqrt{k})(2 - \sqrt{k})\left(\sqrt{2} + \frac{1}{\sqrt{k}}\right)}{1 + \sqrt{2}\,k},$$

in the form (2).

All these numbers have been constructed on the assumption that only one segment was given at the outset. If two segments are given we may select one of them as the unit length. In terms of this unit suppose that the length of the other segment is α. Then we can construct the field G consisting of all numbers of the form

$$\frac{a_m\alpha^m + a_{m-1}\alpha^{m-1} + \cdots + a_1\alpha + a_0}{b_n\alpha^n + b_{n-1}\alpha^{n-1} + \cdots + b_1\alpha + b_0}$$

where the numbers $a_0, \cdots, a_m$ and $b_0, \cdots, b_n$ are rational, and m and n are arbitrary positive integers.

Exercise: If two segments of lengths 1 and α are given, give actual constructions for $1 + \alpha + \alpha^2$, $(1 + \alpha)/(1 - \alpha)$, α^3.

Now let us assume more generally that we are able to construct all the numbers of some number field F. We shall show that *the use of the ruler alone will never lead us out of the field* F. The equation of the straight line through two points whose coördinates a_1, b_1 and a_2, b_2 are in F is $(b_1 - b_2)x + (a_2 - a_1)y + (a_1b_2 - a_2b_1) = 0$ (see p. 491); its coefficients are rational expressions formed from numbers in F, and therefore, by definition of a field, are themselves in F. Moreover, if we have two lines, $\alpha x + \beta y - \gamma = 0$ and $\alpha' x + \beta' y - \gamma' = 0$, with coefficients in F, then the coördinates of their point of intersection, found by solving these two simultaneous equations, are $x = \dfrac{\gamma\beta' - \beta\gamma'}{\alpha\beta' - \beta\alpha'}$, $y = \dfrac{\alpha\gamma' - \gamma\alpha'}{\alpha\beta' - \beta\alpha'}$. Since these are likewise numbers of F, it is clear that the use of the ruler alone cannot take us beyond the confines of the field F.

Exercises: The lines $x + \sqrt{2}y - 1 = 0$, $2x - y + \sqrt{2} = 0$, have coefficients in the field (1). Calculate the coördinates of their point of intersection, and verify that these have the form (1).—Join the points $(1, \sqrt{2})$ and $(\sqrt{2}, 1 - \sqrt{2})$ by a line $ax + by + c = 0$, and verify that the coefficients are of the form (1).—Do the same with respect to the field (2) for the lines $\sqrt{1 + \sqrt{2}}x + \sqrt{2}y = 1$, $(1 + \sqrt{2})x - y = 1 - \sqrt{1 + \sqrt{2}}$, and the points $(\sqrt{2}, -1)$, $(1 + \sqrt{2}, \sqrt{1 + \sqrt{2}})$, respectively.

We can only break through the walls of F by using the compass. For this purpose we select an element k of F which is such that $\sqrt{k}$ is not in F. Then we can construct $\sqrt{k}$ and therefore all the numbers

$$a + b\sqrt{k}, \tag{3}$$

where a and b are rational, or even arbitrary elements of F. The sum and the difference of two numbers $a + b\sqrt{k}$ and $c + d\sqrt{k}$, their product, $(a + b\sqrt{k})(c + d\sqrt{k}) = (ac + kbd) + (ad + bc)\sqrt{k}$, and their quotient,

$$\frac{a + b\sqrt{k}}{c + d\sqrt{k}} = \frac{(a + b\sqrt{k})(c - d\sqrt{k})}{c^2 - kd^2} = \frac{ac - kbd}{c^2 - kd^2} + \frac{bc - ad}{c^2 - kd^2}\sqrt{k},$$

are again of the form $p + q\sqrt{k}$ with p and q in F. (The denominator $c^2 - kd^2$ cannot vanish unless c and d are both zero; for otherwise we would have $\sqrt{k} = c/d$, a number in F, contrary to the assumption that $\sqrt{k}$ is not in F.) Hence the set of numbers of the form $a + b\sqrt{k}$ forms a field F'. The field F' contains the original field F, for we may, in particular, choose $b = 0$. F' is called an *extension field* of F, and F a *subfield* of F'.

As an example, let F be the field $a + b\sqrt{2}$ with rational a, b, and take $k = \sqrt{2}$. Then the numbers of the extension field F' are represented by $p + q\sqrt[4]{2}$, where p and q are in F, $p = a + b\sqrt{2}$, $q = a' + b'\sqrt{2}$, with rational a, b, a', b'. Any number in F' can be reduced to that form; for example

$$\begin{aligned}\frac{1}{\sqrt{2} + \sqrt[4]{2}} &= \frac{\sqrt{2} - \sqrt[4]{2}}{(\sqrt{2} + \sqrt[4]{2})(\sqrt{2} - \sqrt[4]{2})} = \frac{\sqrt{2} - \sqrt[4]{2}}{2 - \sqrt{2}} \\ &= \frac{\sqrt{2}}{2 - \sqrt{2}} - \frac{\sqrt[4]{2}}{2 - \sqrt{2}} = \frac{\sqrt{2}(2 + \sqrt{2})}{4 - 2} - \frac{(2 + \sqrt{2})}{4 - 2}\sqrt[4]{2} \\ &= (1 + \sqrt{2}) - (1 + \tfrac{1}{2}\sqrt{2})\sqrt[4]{2}\end{aligned}$$

Exercise: Let F be the field $p + q\sqrt{2 + \sqrt{2}}$, where p and q are of the form $a + b\sqrt{2}$, a, b rational. Represent $\dfrac{1 + \sqrt{2 + \sqrt{2}}}{2 - 3\sqrt{2 + \sqrt{2}}}$ in this form.

We have seen that if we start with any field F of constructible numbers containing the number k, then by use of the ruler and a single application of the compass we can construct $\sqrt{k}$ and hence any number of the form $a + b\sqrt{k}$, where a, b, are in F.

We now show, conversely, that by a single application of the compass we can obtain *only* numbers of this form. For what the compass does in a construction is to define points (or their coördinates) as points of intersection of a circle with a straight line, or of two circles. A circle with center ξ, η and radius r has the equation $(x - \xi)^2 + (y - \eta)^2 = r^2$; hence, if ξ, η, r are in F, the equation of the circle can be written in the form

$$x^2 + y^2 + 2\alpha x + 2\beta y + \gamma = 0,$$

with the coefficients α, β, γ in F. A straight line,

$$ax + by + c = 0,$$

joining any two points whose coördinates are in F, has coefficients a, b, c in F, as we have seen on page 129. By eliminating y from these simultaneous equations, we obtain for the x-coördinate of a point of intersection of the circle and line a quadratic equation of the form

$$Ax^2 + Bx + C = 0,$$

with coefficients A, B, C in F (explicitly: $A = a^2 + b^2$, $B = 2(ac + b^2\alpha - ab\beta)$, $C = c^2 - 2bc\beta + b^2\gamma$). The solution is given by the formula

$$x = \frac{-B \pm \sqrt{B^2 - 4AC}}{2A},$$

which is of the form $p + q\sqrt{k}$, with p, q, k in F. A similar formula holds for the y-coördinate of a point of intersection.

Again, if we have two circles,

$$\begin{aligned}x^2 + y^2 + 2\alpha x + 2\beta y + \gamma &= 0, \\ x^2 + y^2 + 2\alpha' x + 2\beta' y + \gamma' &= 0,\end{aligned}$$

then by subtracting the second equation from the first we obtain the linear equation

$$2(\alpha - \alpha')x + 2(\beta - \beta')y + (\gamma - \gamma') = 0,$$

which may be solved with the equation of the first circle as before. In either case, the construction yields the x- and y-coördinates of either

one or two new points, and these new quantities are of the form $p + q\sqrt{k}$, with p, q, k in F. In particular, of course, $\sqrt{k}$ may itself belong to F, e.g., when $k = 4$. Then the construction does not yield anything essentially new, and we remain in F. But in general this will not be the case.

Exercises: Consider the circle with radius $2\sqrt{2}$ about the origin, and the line joining the points $(1/2, 0)$, $(4\sqrt{2}, \sqrt{2})$. Find the field F' determined by the coördinates of the points of intersection of the circle and the line. Do the same with respect to the intersection of the given circle with the circle with radius $\sqrt{2}/2$ and center $(0, 2\sqrt{2})$.

Summarizing again: If certain quantities are given at the outset, then we can construct with a straightedge alone all the quantities in the field F generated by rational processes from the given quantities. Using the compass we can then extend the field F of constructible quantities to a wider extension field by selecting any number k of F, extracting the square root of k, and constructing the field F' consisting of the numbers $a + b\sqrt{k}$, where a and b are in F. F is called a subfield of F'; all quantities in F are also contained in F', since in the expression $a + b\sqrt{k}$ we may choose $b = 0$. (It is assumed that $\sqrt{k}$ is a new number not lying in F, since otherwise the process of adjunction of $\sqrt{k}$ would not lead to anything new, and F' would be identical with F.) We have shown that any step in a geometrical construction (drawing a line through two known points, drawing a circle with known center and radius, or marking the intersection of two known lines or circles) will either produce new quantities lying in the field already known to consist of constructible numbers, or, by the construction of a square root, will open up a new extension field of constructible numbers.

The totality of all constructible numbers can now be described with precision. We start with a given field F_0, defined by whatever quantities are given at the outset, e.g. the field of rational numbers if only a single segment, chosen as the unit, is given. Next, by the adjunction of $\sqrt{k_0}$, where k_0 is in F_0, but $\sqrt{k_0}$ is not, we construct an extension field F_1 of constructible numbers, consisting of all numbers of the form $a_0 + b_0\sqrt{k_0}$, where a_0 and b_0 may be any numbers of F_0. Then F_2, a new extension field of F_1, is defined by the numbers $a_1 + b_1\sqrt{k_1}$, where a_1 and b_1 are any numbers of F_1, and k_1 is some number of F_1 whose square root does not lie in F_1. Repeating this procedure, we shall reach a field F_n after n adjunctions of square roots. *Constructible numbers are those and only those which can be reached by such a sequence of extension fields; that is, which lie in a field* F_n *of the type described.* The

size of the number n of necessary extensions does not matter; in a way it measures the degree of complexity of the problem.

The following example may illustrate the process. We want to reach the number

$$\sqrt{6} + \sqrt{\sqrt{\sqrt{1 + \sqrt{2} + \sqrt{3}} + 5}}.$$

Let F_0 denote the rational field. Putting $k_0 = 2$, we obtain the field F_1, which contains the number $1 + \sqrt{2}$. We now take $k_1 = 1 + \sqrt{2}$ and $k_2 = 3$. As a matter of fact, 3 is in the original field F_0, and *a fortiori* in the field F_2, so that it is perfectly permissible to take $k_2 = 3$. We then take $k_3 = \sqrt{1 + \sqrt{2} + \sqrt{3}}$, and finally $k_4 = \sqrt{\sqrt{1 + \sqrt{2} + \sqrt{3}} + 5}$. The field F_5 thus constructed contains the desired number, for $\sqrt{6}$ is also in F_5, since $\sqrt{2}$ and $\sqrt{3}$, and therefore their product, are in F_3 and therefore also in F_5.

Exercises: Verify that, starting with the rational field, the side of the regular 2^m-gon (see p. 124) is a constructible number, with $n = m - 1$. Determine the sequence of extension fields. Do the same for the numbers

$$\sqrt{1 + \sqrt{2} + \sqrt{3} + \sqrt{5}}, \qquad (\sqrt{5} + \sqrt{11})/(1 + \sqrt{7 - \sqrt{3}}),$$
$$(\sqrt{2 + \sqrt{3}})(\sqrt[3]{2} + \sqrt{1 + \sqrt{2 + \sqrt{5}} + \sqrt{3 - \sqrt{7}}}).$$

2. All Constructible Numbers are Algebraic

If the initial field F_0 is the rational field generated by a single segment, then all constructible numbers will be algebraic. (For the definition of algebraic numbers see p. 103). The numbers of the field F_1 are roots of quadratic equations, those of F_2 are roots of fourth degree equations, and, in general, the numbers of F_k are roots of equations of degree 2^k, with rational coefficients. To show this for a field F_2 we may first consider as an example $x = \sqrt{2} + \sqrt{3 + \sqrt{2}}$. We have $(x - \sqrt{2})^2 = 3 + \sqrt{2}$, $x^2 + 2 - 2\sqrt{2}x = 3 + \sqrt{2}$, or $x^2 - 1 = \sqrt{2}(2x + 1)$, a quadratic equation with coefficients in a field F_1. By squaring, we finally obtain

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

which is an equation of the fourth degree with rational coefficients.

In general, any number in a field F_2 has the form

$$x = p + q\sqrt{w}, \tag{4}$$

where p, q, w are in a field F_1, and hence have the form $p = a + b\sqrt{s}$, $q = c + d\sqrt{s}$, $w = e + f\sqrt{s}$, where a, b, c, d, e, f, s are rational. From (4) we have

$$x^2 - 2px + p^2 = q^2w,$$

where all the coefficients are in a field F_1, generated by $\sqrt{s}$. Hence this equation may be rewritten in the form

$$x^2 + ux + v = \sqrt{s}(rx + t),$$

where r, s, t, u, v are rational. By squaring both sides we obtain an equation of the fourth degree

$$(x^2 + ux + v)^2 = s(rx + t)^2 \tag{5}$$

with rational coefficients, as stated.

Exercises: 1) Find the equations with rational coefficients for a) $x = \sqrt{2 + \sqrt{3}}$; b) $x = \sqrt{2} + \sqrt{3}$; c) $x = 1/\sqrt{5 + \sqrt{3}}$.

2) Find by a similar method equations of the eighth degree for a) $x = \sqrt{2 + \sqrt{2 + \sqrt{2}}}$; b) $x = \sqrt{2} + \sqrt{1 + \sqrt{3}}$; c) $x = 1 + \sqrt{5 + \sqrt{3 + \sqrt{2}}}$.

To prove the theorem in general for x in a field F_k with arbitrary k, we show by the procedure used above that x satisfies a quadratic equation with coefficients in a field F_{k-1}. Repeating the procedure, we find that x satisfies an equation of degree $2^2 = 4$ with coefficients in a field F_{k-2}, etc.

Exercise: Complete the general proof by using mathematical induction to show that x satisfies an equation of degree 2^l with coefficients in a field F_{k-l}, $0 < l \leq k$. This statement for $l = k$ is the desired theorem.

*§3. THE UNSOLVABILITY OF THE THREE GREEK PROBLEMS

1. Doubling the Cube

Now we are well prepared to investigate the old problems of trisecting the angle, doubling the cube, and constructing the regular heptagon. We consider first the problem of doubling the cube. If the given cube has an edge of unit length, its volume will be the cubic unit; it is required that we find the edge x of a cube with twice this volume. The required edge x will therefore satisfy the simple cubic equation

$$x^3 - 2 = 0. \tag{1}$$

Our proof that this number x cannot be constructed by ruler and compass alone is indirect. We assume tentatively that a construction is possible. According to the preceding discussion this means that x lies in some field F_k obtained, as above, from the rational field by successive extensions through adjunction of square roots. As we shall show, this assumption leads to an absurd consequence.

We already know that x cannot lie in the rational field F_0, for $\sqrt[3]{2}$ is an irrational number (see Exercise 1, p. 60). Hence x can only lie in some extension field F_k, where k is a positive integer. We may as well assume that k is the *least* positive integer such that x lies in some F_k. It follows that x can be written in the form

$$x = p + q\sqrt{w},$$

where p, q, and w belong to some F_{k-1}, but $\sqrt{w}$ does not. Now, by a simple but important type of algebraic reasoning, we shall show that if $x = p + q\sqrt{w}$ is a solution of the cubic equation (1), then $y = p - q\sqrt{w}$ is also a solution. Since x is in the field F_k, x^3 and $x^3 - 2$ are also in F_k, and we have

$$x^3 - 2 = a + b\sqrt{w}, \tag{2}$$

where a and b are in F_{k-1}. By an easy calculation we can show that $a = p^3 + 3pq^2w - 2$, $b = 3p^2q + q^3w$. If we put

$$y = p - q\sqrt{w},$$

then a substitution of $-q$ for q in these expressions for a and b shows that

$$y^3 - 2 = a - b\sqrt{w}. \tag{2'}$$

Now x was supposed to be a root of $x^3 - 2 = 0$, hence

$$a + b\sqrt{w} = 0. \tag{3}$$

This implies—and here is the key to the argument—that a and b must both be zero. If b were not zero, we would infer from (3) that $\sqrt{w} = -a/b$. But then $\sqrt{w}$ would be a number of the field F_{k-1} in which a and b lie, contrary to our assumption. Hence $b = 0$, and it follows immediately from (3) that $a = 0$ also.

Now that we have shown that $a = b = 0$, we immediately infer from (2') that $y = p - q\sqrt{w}$ is also a solution of the cubic equation (1), since $y^3 - 2$ is equal to zero. Furthermore, $y \neq x$, i.e. $x - y \neq 0$; for, $x - y = 2q\sqrt{w}$ can only vanish if $q = 0$, and if this were so then $x = p$ would lie in F_{k-1}, contrary to our assumption.

We have therefore shown that, if $x = p + q\sqrt{w}$ is a root of the cubic equation (1), then $y = p - q\sqrt{w}$ is a different root of this equation. This leads immediately to a contradiction. For there is only one real number x which is a cube root of 2, the other cube roots of 2 being imaginary (see p. 98); $y = p - q\sqrt{w}$ is obviously real, since p, q, and $\sqrt{w}$ were real.

Thus our basic assumption has led to an absurdity, and hence is proved to be wrong; a solution of (1) cannot lie in a field F_k, so that doubling the cube by ruler and compass is impossible.

2. A Theorem on Cubic Equations

Our concluding algebraic argument was especially adapted to the particular problem at hand. If we want to dispose of the two other Greek

problems, it is desirable to proceed on a more general basis. All three problems depend algebraically on cubic equations. It is a fundamental fact concerning the cubic equation

$$z^3 + az^2 + bz + c = 0 \tag{4}$$

that, if x_1, x_2, x_3 are the three roots of this equation, then

$$x_1 + x_2 + x_3 = -a.\dagger \tag{5}$$

Let us consider any cubic equation (4) where the coefficients a, b, c are rational numbers. It may be that one of the roots of the equation is rational; for example, the equation $x^3 - 1 = 0$ has the rational root 1, while the two other roots, given by the quadratic equation $x^2 + x + 1 = 0$, are necessarily imaginary. But we can easily prove the general theorem: *If a cubic equation with rational coefficients has no rational root, then none of its roots is constructible starting from the rational field* F_0.

Again we give the proof by an indirect method. Suppose x were a constructible root of (4). Then x would lie in the last field F_k of some chain of extension fields, $F_0, F_1, \cdots, F_k$, as above. We may assume that k is the *smallest* integer such that a root of the cubic equation (4) lies in an extension field F_k. Certainly k must be greater than zero, since in the statement of the theorem it is assumed that no root x lies in the rational field F_0. Hence x can be written in the form

$$x = p + q\sqrt{w},$$

where p, q, w are in the preceding field, F_{k-1}, but $\sqrt{w}$ is not. It follows, exactly as for the special equation, $z^3 - 2 = 0$, of the preceding article, that another number of F_k,

$$y = p - q\sqrt{w},$$

will also be a root of the equation (4) As before, we see that $q \neq 0$ and hence $x \neq y$.

From (5) we know that the third root u of the equation (4) is given by $u = -a - x - y$. But since $x + y = 2p$, this means that

$$u = -a - 2p,$$

† The polynomial $z^3 + az^2 + bz + c$ may be factored into the product $(z - x_1)(z - x_2)(z - x_3)$, where x_1, x_2, x_3, are the three roots of the equation (4) (see p. 101). Hence

$$z^3 + az^2 + bz + c = z^3 - (x_1 + x_2 + x_3)z^2 + (x_1x_2 + x_1x_3 + x_2x_3)z - x_1x_2x_3,$$

so that, since the coefficient of each power of z must be the same on both sides,

$$-a = x_1 + x_2 + x_3, \quad b = x_1x_2 + x_1x_3 + x_2x_3, \quad -c = x_1x_2x_3.$$

where $\sqrt{w}$ has disappeared, so that u is a number in the field F_{k-1}. This contradicts the hypothesis that k is the *smallest* number such that some F_k contains a root of (4). Hence the hypothesis is absurd, and no root of (4) can lie in such a field F_k. The general theorem is proved. On the basis of this theorem, a construction by ruler and compass alone is proved to be impossible if the algebraic equivalent of the problem is the solution of a cubic equation with no rational roots. This equivalence was at once obvious for the problem of doubling the cube, and will now be established for the other two Greek problems.

3. Trisecting the Angle

We shall now prove that the trisection of the angle by ruler and compass alone is *in general* impossible. Of course, there are angles, such as 90° and 180°, for which the trisection can be performed. What we have to show is that the trisection cannot be effected by a procedure valid for *every* angle. For the proof, it is quite sufficient to exhibit only one angle that cannot be trisected, since a valid *general method* would have to cover every single example. Hence the non-existence of a general method will be proved if we can demonstrate, for example, that the angle 60° cannot be trisected by ruler and compass alone.

We can obtain an algebraic equivalent of this problem in different ways; the simplest is to consider an angle θ as given by its cosine: $\cos\theta = g$. Then the problem is equivalent to that of finding the quantity $x = \cos(\theta/3)$. By a simple trigonometrical formula (see p. 97), the cosine of $\theta/3$ is connected with that of θ by the equation

$$\cos\theta = g = 4\cos^3(\theta/3) - 3\cos(\theta/3).$$

In other words, the problem of trisecting the angle θ with $\cos\theta = g$ amounts to constructing a solution of the cubic equation

$$4z^3 - 3z - g = 0. \tag{6}$$

To show that this cannot in general be done, we take $\theta = 60°$, so that $g = \cos 60° = \frac{1}{2}$. Equation (6) then becomes

$$8z^3 - 6z = 1. \tag{7}$$

By virtue of the theorem proved in the preceding article, we need only show that this equation has no rational root. Let $v = 2z$. Then the equation becomes

$$v^3 - 3v = 1. \tag{8}$$

If there were a rational number $v = r/s$ satisfying this equation, where r and s are integers without a common factor > 1, we should have $r^3 - 3s^2r = s^3$. From this it follows that $s^3 = r(r^2 - 3s^2)$ is divisible by r, which means that r and s have a common factor unless $r = \pm 1$. Likewise, s^2 is a factor of $r^3 = s^2(s + 3r)$, which means that r and s have a common factor unless $s = \pm 1$. Since we assumed that r and s had no common factor, we have shown that the only rational numbers which could possibly satisfy equation (8) are $+1$ or -1. By substituting $+1$ and -1 for v in equation (8) we see that neither value satisfies it. Hence (8), and consequently (7), has no rational root, and the impossibility of trisecting the angle is proved.

The theorem that the general angle cannot be trisected with ruler and compass alone is true only when the ruler is regarded as an instrument for drawing a straight line through any two given points and *nothing else*. In our general characterization of constructible numbers the use of the ruler was always limited to this operation only. By permitting other uses of the ruler the totality of possible constructions may be greatly extended. The following method for trisecting the angle, found in the works of Archimedes, is a good example.

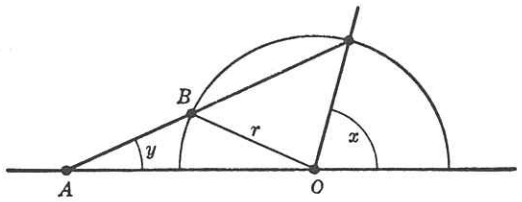

Fig. 36. Archimedes' trisection of an angle.

Let an arbitrary angle x be given, as in Fig. 36. Extend the base of the angle to the left, and swing a semicircle with O as center and arbitrary radius r. Mark two points A and B on the edge of the ruler such that $AB = r$. Keeping the point B on the semicircle, slide the ruler into the position where A lies on the extended base of the angle x, while the edge of the ruler passes through the intersection of the terminal side of the angle x with the semicircle about O. With the ruler in this position draw a straight line, making an angle y with the extended base of the original angle x.

Exercise: Show that this construction actually yields $y = x/3$.

4. The Regular Heptagon

We shall now consider the problem of finding the side x of a regular heptagon inscribed in the unit circle. The simplest way to dispose of this problem is by means of complex numbers (see Ch. II, §5). We know that the vertices of the heptagon are given by the roots of the equation

$$z^7 - 1 = 0, \tag{9}$$

the coördinates x, y of the vertices being considered as the real and imaginary parts of complex numbers $z = x + yi$. One root of this equation is $z = 1$, and the others are the roots of the equation

$$\frac{z^7 - 1}{z - 1} = z^6 + z^5 + z^4 + z^3 + z^2 + z + 1 = 0, \tag{10}$$

obtained from (9) by factoring out $z - 1$ (see p. 99). Dividing (10) by z^3, we obtain the equation

$$z^3 + 1/z^3 + z^2 + 1/z^2 + z + 1/z + 1 = 0. \tag{11}$$

By a simple algebraic transformation this may be written in the form

$$(z + 1/z)^3 - 3(z + 1/z) + (z + 1/z)^2 - 2 + (z + 1/z) + 1 = 0. \tag{12}$$

Denoting the quantity $z + 1/z$ by y, we find from (12) that

$$y^3 + y^2 - 2y - 1 = 0. \tag{13}$$

We know that z, the seventh root of unity, is given by

$$z = \cos\phi + i \sin\phi, \tag{14}$$

where $\phi = 360°/7$ is the angle subtended at the center of the circle by the edge of the regular heptagon; likewise we know from Exercise 2, page 97, that $1/z = \cos\phi - i \sin\phi$, so that $y = z + 1/z = 2\cos\phi$. If we can construct y, we can also construct $\cos\phi$, and conversely. Hence, if we can prove that y is not constructible, we shall at the same time show that z, and therefore the heptagon, is not constructible. Thus, considering the theorem of Article 2, it remains merely to show that the equation (13) has no rational roots. This, too, is proved indirectly. Assume that (13) has a rational root r/s, where r and s are integers having no common factor. Then we have

$$r^3 + r^2s - 2rs^2 - s^3 = 0; \tag{15}$$

whence it is seen as above that r^3 has the factor s, and s^3 the factor r. Since r and s have no common factor, each must be ± 1; therefore y can have only the possible values $+1$ and -1, if it is to be rational. On substituting these numbers in the equation, we see that neither of them satisfies it. Hence y, and therefore the edge of the regular heptagon, is not constructible.

5. Remarks on the Problem of Squaring the Circle

We have been able to dispose of the problems of doubling the cube, trisecting the angle, and constructing the regular heptagon, by comparatively elementary methods. The problem of squaring the circle is much more difficult and requires the technique of advanced mathematical analysis. Since a circle with radius r has the area πr^2, the problem of constructing a square with area equal to that of a given circle whose radius is the unit length 1 amounts to the construction of a segment of length $\sqrt{\pi}$ as the edge of the required square. This segment will be constructible if and only if the number π is constructible. In the light of our general characterization of constructible numbers, we could show the impossibility of squaring the circle by showing that the number π cannot be contained in any field F_k that can be reached by the successive adjunction of square roots to the rational field F_0. Since all the members of any such field are algebraic numbers, i.e. numbers that satisfy algebraic equations with integer coefficients, it will be sufficient if the number π can be shown to be not algebraic, i.e. to be transcendental (see p. 104).

The technique necessary for proving that π is a transcendental number was created by Charles Hermite (1822–1905), who proved the number e to be transcendental. By a slight extension of Hermite's method F. Lindemann succeeded (1882) in proving the transcendence of π, and thus definitely settled the age-old question of squaring the circle. The proof is within the reach of the student of advanced analysis, but is beyond the scope of this book.

PART II

VARIOUS METHODS FOR PERFORMING CONSTRUCTIONS

§4. GEOMETRICAL TRANSFORMATIONS. INVERSION

1. General Remarks

In the second part of this chapter we shall discuss in a systematic way some general principles that may be applied to construction problems. Many of these problems can be more clearly viewed from the general standpoint of "geometrical transformations"; instead of studying an individual construction, we shall consider simultaneously a whole class of problems connected by certain processes of transformation. The clarifying power of the concept of a class of geometrical transformations is by no means restricted to construction problems, but affects almost everything in geometry. In Chapters IV and V we shall deal with this general aspect of geometrical transformations. Here we shall study a particular type of transformation, the inversion of the plane in a circle, which is a generalization of ordinary reflection in a straight line.

By a *transformation*, or *mapping*, of the plane onto itself we mean a rule which assigns to every point P of the plane another point P', called the *image* of P under the transformation; the point P is called the *antecedent* of P'. A simple example of such a transformation is given by the *reflection* of the plane in a given straight line L as in a mirror: a point P on one side of L has as its image the point P', on the other side of L, and such that L is the perpendicular bisector of the segment PP'. A transformation may leave certain points of the plane fixed; in the case of a reflection this is true of the points on L.

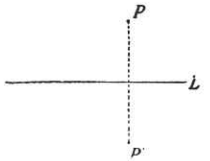

Fig. 37. Reflection of a point in a line.

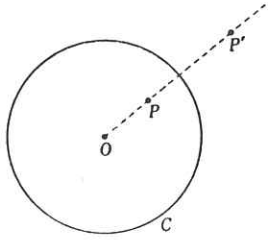

Fig. 38. Inversion of a point in a circle.

Other examples of transformations are the *rotations* of the plane about a fixed point O, the parallel *translations*, which move every point a distance d in a given direction (such a transformation has no fixed points), and, more generally, the *rigid motions* of the plane, which may be thought of as compounded of rotations and parallel translations.

The particular class of transformations of interest to us now are the *inversions* with respect to circles. (These are sometimes known as circular reflections, because to a certain approximation they represent the relation between original and image in reflection by a circular mirror.) In a fixed plane let C be a given circle with center O (called the center of inversion) and radius r. The image of a point P is defined to be the point P' lying on the line OP on the same side of O as P and such that

$$OP \cdot OP' = r^2. \tag{1}$$

The points P and P' are said to be *inverse points* with respect to C. From this definition it follows that, if P' is the inverse point of P,