FAMOUS PROBLEMS

OF

ELEMENTARY GEOMETRY

THE DUPLICATION OF THE CUBE
THE TRISECTION OF AN ANGLE
THE QUADRATURE OF THE CIRCLE

CONTENTS.

INTRODUCTION.

PART I.

The Possibility of the Construction of Algebraic Expressions.

CHAPTER IV. THE CONSTRUCTION OF THE REGULAR POLYGON OF 17 SIDES.

CHAPTER V. GENERAL CONSIDERATIONS ON ALGEBRAIC CONSTRUCTIONS.

PART II.

Transcendental Numbers and the Quadrature of the Circle.

CHAPTER I. CANTOR'S DEMONSTRATION OF THE EXISTENCE OF TRANSCENDENTAL NUMBERS.

CHAPTER II. HISTORICAL SURVEY OF THE ATTEMPTS AT THE COMPUTATION AND CONSTRUCTION OF π.

CHAPTER III. THE TRANSCENDENCE OF THE NUMBER e.

CHAPTER IV. THE TRANSCENDENCE OF THE NUMBER π.

CHAPTER V. THE INTEGRAPH AND THE GEOMETRIC CONSTRUCTION OF π.

INTRODUCTION.

THIS course of lectures is due to the desire on my part to bring the study of mathematics in the university into closer touch with the needs of the secondary schools. Still it is not intended for beginners, since the matters under discussion are treated from a higher standpoint than that of the schools. On the other hand, it presupposes but little preliminary work, only the elements of analysis being required, as, for example, in the development of the exponential function into a series.

We propose to treat of geometrical constructions, and our object will not be so much to find the solution suited to each case as to determine the *possibility* or *impossibility* of a solution.

Three problems, the object of much research in ancient times, will prove to be of special interest. They are

1. *The problem of the duplication of the cube* (also called the *Delian problem*).
2. *The trisection of an arbitrary angle.*
3. *The quadrature of the circle, i.e.*, the construction of π.

In all these problems the ancients sought in vain for a solution with straight edge and compasses, and the celebrity of these problems is due chiefly to the fact that their solution seemed to demand the use of appliances of a higher order. In fact, we propose to show that a solution by the use of straight edge and compasses is impossible.

The impossibility of the solution of the third problem was demonstrated only very recently. That of the first and second is implicitly involved in the Galois theory as presented to-day in treatises on higher algebra. On the other hand, we find no explicit demonstration in elementary form unless it be in Petersen's text-books, works which are also noteworthy in other respects.

At the outset we must insist upon the difference between *practical* and *theoretical* constructions. For example, if we need a divided circle as a measuring instrument, we construct it simply on trial. Theoretically, in earlier times, it was possible (*i.e.*, by the use of straight edge and compasses) only to divide the circle into a number of parts represented by 2^n, 3, and 5, and their products. Gauss added other cases by showing the possibility of the division into parts where p is a prime number of the form $p=2^{2^\mu}+1$, and the impossibility for all other numbers. No practical advantage is derived from these results; *the significance of Gauss's developments is purely theoretical.* The same is true of all the discussions of the present course.

Our fundamental problem may be stated: *What geometrical constructions are, and what are not, theoretically possible?* To define sharply the meaning of the word "construction," we must designate the instruments which we propose to use in each case. We shall consider

1. Straight edge and compasses,
2. Compasses alone,
3. Straight edge alone,
4. Other instruments used in connection with straight edge and compasses.

The singular thing is that elementary geometry furnishes no answer to the question. We must fall back upon algebra and the higher analysis. The question then arises: How shall we use the language of these sciences to express the employment of straight edge and compasses? This new method of attack is rendered necessary because elementary geometry possesses no general method, no *algorithm*, as do the last two sciences.

In analysis we have first *rational* operations: addition, subtraction, multiplication, and division. These operations can be directly effected geometrically upon two given segments by the aid of proportions, if, in the case of multiplication and division, we introduce an auxiliary unit-segment.

Further, there are *irrational* operations, subdivided into *algebraic* and *transcendental*. The simplest algebraic operations are the extraction of square and higher roots, and the solution of algebraic equations not solvable by radicals, such as those of the fifth and higher degrees. As we know how to construct $\sqrt{ab}$, rational operations in general, and irrational operations involving only square roots, can be constructed. On the other hand, every *individual* geometrical construction which can be reduced to the intersection of two straight lines, a straight line and a circle, or two circles, is equivalent to a rational operation or the extraction of a square root. In the higher irrational operations the construction is therefore impossible, *unless we can find a way of effecting it by the aid of square roots.* In all these constructions it is obvious that the number of operations must be limited.

We may therefore state the following fundamental theorem: *The necessary and sufficient condition that an analytic expression can be constructed with straight edge and compasses is that it can be derived from the known quantities by a finite number of rational operations and square roots.*

Accordingly, if we wish to show that a quantity cannot be constructed with straight edge and compasses, we must prove that the corresponding equation is not solvable by a finite number of square roots.

A fortiori the solution is impossible when the problem has *no* corresponding algebraic equation. An expression which satisfies no algebraic equation is called a transcendental number. This case occurs, as we shall show, with the number π.

PART I.

THE POSSIBILITY OF THE CONSTRUCTION OF ALGEBRAIC EXPRESSIONS.

CHAPTER I.

Algebraic Equations Solvable by Square Roots.

The following propositions taken from the theory of algebraic equations are probably known to the reader, yet to secure greater clearness of view we shall give brief demonstrations.

If x, *the quantity to be constructed, depends only upon rational expressions and square roots, it is a root of an irreducible equation* $\phi(x) = 0$, *whose degree is always a power of* 2.

1. To get a clear idea of the structure of the quantity x, suppose it, *e.g.*, of the form

$$x = \frac{\sqrt{a + \sqrt{c + ef}} + \sqrt{d + \sqrt{b}}}{\sqrt{a} + \sqrt{b}} + \frac{p + \sqrt{q}}{\sqrt{r}},$$

where a, b, c, d, e, f, p, q, r are rational expressions.

2. The number of radicals one over another occurring in any term of x is called the *order of the term;* the preceding expression contains terms of orders 0, 1, 2.

3. Let μ designate the *maximum order*, so that no term can have more than μ radicals one over another.

4. In the example $x = \sqrt{2} + \sqrt{3} + \sqrt{6}$, we have three expressions of the first order, but as it may be written

$$x = \sqrt{2} + \sqrt{3} + \sqrt{2} \cdot \sqrt{3},$$

it really depends on only two distinct expressions.

We shall suppose that this reduction has been made in all the terms of x, *so that among the* n *terms of order* μ *none can be expressed rationally as a function of any other terms of order* μ *or of lower order.*

We shall make the same supposition regarding terms of the order $\mu - 1$ or of lower order, whether these occur explicitly or implicitly. This hypothesis is obviously a very natural one and of great importance in later discussions.

5. Normal Form of x.

If the expression x is a sum of terms with different denominators we may reduce them to the same denominator and thus obtain x as the quotient of two integral functions.

Suppose $\sqrt{Q}$ one of the terms of x of order μ; it can occur in x only explicitly, since μ is the maximum order. Since, further, the powers of $\sqrt{Q}$ may be expressed as functions of $\sqrt{Q}$ and Q, which is a term of lower order, we may put

$$x = \frac{a + b\sqrt{Q}}{c + d\sqrt{Q}},$$

where a, b, c, d contain no more than $n - 1$ terms of order μ, besides terms of lower order.

Multiplying both terms of the fraction by $c - d\sqrt{Q}$, $\sqrt{Q}$ disappears from the denominator, and we may write

$$x = \frac{(ac - bdQ) + (bc - ad)\sqrt{Q}}{c^2 - d^2Q} = \alpha + \beta\sqrt{Q},$$

where α and β contain no more than $n - 1$ terms of order μ.

For a second term of order μ we have, in a similar manner, $x = \alpha_1 + \beta_1\sqrt{Q_1}$, etc.

The x *may, therefore, be transformed so as to contain a term of given order* μ *only in its numerator and there only linearly.*

We observe, however, that products of terms of order μ may occur, for α and β still depend upon $n-1$ terms of order μ. We may, then, put

$$\alpha = \alpha_{11} + \alpha_{12}\sqrt{Q_1}, \qquad \beta = \beta_{11} + \beta_{12}\sqrt{Q_1},$$

and hence

$$x = (\alpha_{11} + \alpha_{12}\sqrt{Q_1}) + (\beta_{11} + \beta_{12}\sqrt{Q_1})\sqrt{Q}.$$

6. We proceed in a similar way with the different terms of order $\mu - 1$, which occur explicitly and in Q, Q_1, etc., so that each of these quantities becomes an integral linear function of the term of order $\mu - 1$ under consideration. We then pass on to terms of lower order and finally obtain x, or rather its terms of different orders, under the form of rational integral linear functions of the individual radical expressions which occur explicitly. We then say that x is reduced to the *normal form.*

7. Let m be the total number of independent (4) square roots occurring in this normal form. Giving the double sign to these square roots and combining them in all possible ways, we obtain a system of 2^m values

$$x_1, x_2, \ldots x_{2^m},$$

which we shall call *conjugate* values.

We must now investigate the equation admitting these conjugate values as roots.

8. These values are not necessarily all distinct; thus, if we have $$x = \sqrt{a + \sqrt{b}} + \sqrt{a - \sqrt{b}},$$ this expression is not changed when we change the sign of $\sqrt{b}$.

9. If x is an arbitrary quantity and we form the polynomial

$$F(x) = (x - x_1)(x - x_2) \ldots (x - x_{2^m}),$$

$F(x) = 0$ is clearly an equation having as roots these conjugate values. It is of degree 2^m, but may have equal roots (8).

The coefficients of the polynomial $F(x)$ *arranged with respect to* x *are rational.*

For let us change the sign of one of the square roots; this will permute two roots, say x_λ and $x_{\lambda'}$, since the roots of $F(x) = 0$ are precisely all the conjugate values. As these roots enter $F(x)$ only under the form of the product

$$(x - x_\lambda)(x - x_{\lambda'}),$$

we merely change the order of the factors of $F(x)$. Hence the polynomial is not changed.

$F(x)$ remains, then, invariable when we change the sign of any one of the square roots; it therefore contains only their squares; and hence $F(x)$ has only rational coefficients.

10. *When any one of the conjugate values satisfies a given equation with rational coefficients,* $f(x) = 0$, *the same is true of all the others.*

$f(x)$ is not necessarily equal to $F(x)$, and may admit other roots besides the x_i's.

Let $x_1 = \alpha + \beta\sqrt{Q}$ be one of the conjugate values; $\sqrt{Q}$, a term of order μ; α and β now depend only upon other terms of order μ and terms of lower order. There must, then, be a conjugate value

$$x_1' = \alpha - \beta\sqrt{Q}.$$

Let us now form the equation $f(x_1) = 0$. $f(x_1)$ may be put into the normal form with respect to $\sqrt{Q}$,

$$f(x_1) = A + B\sqrt{Q};$$

this expression can equal zero only when A and B are simultaneously zero. Otherwise we should have

$$\sqrt{Q} = -\frac{A}{B};$$

i.e., $\sqrt{Q}$ could be expressed rationally as a function of terms of order μ and of terms of lower order contained in A and B, which is contrary to the hypothesis of the independence of all the square roots (4).

But we evidently have

$$f(x_1') = A - B\sqrt{Q};$$

hence if $f(x_1) = 0$, so also $f(x_1') = 0$. Whence the following proposition:

If x_1 *satisfies the equation* $f(x) = 0$, *the same is true of all the conjugate values derived from* x_1 *by changing the signs of the roots of order* μ.

The proof for the other conjugate values is obtained in an analogous manner. Suppose, for example, as may be done without affecting the generality of the reasoning, that the expression x_1 depends on only two terms of order μ, $\sqrt{Q}$ and $\sqrt{Q'}$. $f(x_1)$ may be reduced to the following normal form:

$$(a) \qquad f(x_1) = p + q\sqrt{Q} + r\sqrt{Q'} + s\sqrt{Q}\cdot\sqrt{Q'} = 0.$$

If x_1 depended on more than two terms of order μ, we should only have to add to the preceding expression a greater number of terms of analogous structure.

Equation (*a*) is possible only when we have separately

$$(b) \qquad p = 0, \quad q = 0, \quad r = 0, \quad s = 0.$$

Otherwise $\sqrt{Q}$ and $\sqrt{Q'}$ would be connected by a rational relation, contrary to our hypothesis.

Let now $\sqrt{R}$, $\sqrt{R'}$, . . . be the terms of order $\mu - 1$ on which x_1 depends; they occur in p, q, r, s; then can the quantities p, q, r, s, in which they occur, be reduced to the normal form with respect to $\sqrt{R}$ and $\sqrt{R'}$; and if, for the sake of simplicity, we take only two quantities, $\sqrt{R}$ and $\sqrt{R'}$, we have

$$(c) \qquad p = \kappa_1 + \lambda_1 \sqrt{R} + \mu_1 \sqrt{R'} + \nu_1 \sqrt{R} \cdot \sqrt{R'} = 0,$$

and three analogous equations for q, r, s.

The hypothesis, already used several times, of the independence of the roots, furnishes the equations

$$(d) \qquad \kappa = 0, \quad \lambda = 0, \quad \mu = 0, \quad \nu = 0.$$

Hence equations (*c*) and consequently $f(x) = 0$ are satisfied when for x_1 we substitute the conjugate values deduced by changing the signs of $\sqrt{R}$ and $\sqrt{R'}$.

Therefore *the equation* $f(x) = 0$ *is also satisfied by all the conjugate values deduced from* x_1 *by changing the signs of the roots of order* $\mu - 1$.

The same reasoning is applicable to the terms of order $\mu - 2$, $\mu - 3$, ... and our theorem is completely proved.

11. We have so far considered two equations

$$F(x) = 0 \quad \text{and} \quad f(x) = 0.$$

Both have rational coefficients and contain the x_1's as roots. $F(x)$ is of degree 2^m and may have multiple roots; $f(x)$ may have other roots besides the x_1's. We now introduce a third equation, $\phi(x) = 0$, defined as the equation of lowest degree, with rational coefficients, admitting the root x_1 and consequently all the x_1's (10).

12. PROPERTIES OF THE EQUATION $\phi(x) = 0$.

I. $\phi(x) = 0$ *is an irreducible equation, i.e.,* $\phi(x)$ cannot be resolved into two rational polynomial factors. This irreducibility is due to the hypothesis that $\phi(x) = 0$ is the rational equation of *lowest* degree satisfied by the x_1's.

For if we had

$$\phi(x) = \psi(x)\,\chi(x),$$

then $\phi(x_1) = 0$ would require either $\psi(x_1) = 0$, or $\chi(x_1) = 0$, or both. But since these equations are satisfied by all the conjugate values (10), $\phi(x) = 0$ would not then be the equation of lowest degree satisfied by the x_i's.

II. $\phi(x) = 0$ *has no multiple roots.* Otherwise $\phi(x)$ could be decomposed into rational factors by the well-known methods of Algebra, and $\phi(x) = 0$ would not be irreducible.

III. $\phi(x) = 0$ *has no other roots than the* x_i's. Otherwise $F(x)$ and $\phi(x)$ would admit a highest common divisor, which could be determined rationally. We could then decompose $\phi(x)$ into rational factors, and $\phi(x)$ would not be irreducible.

IV. Let M be the number of x_i's which have distinct values, and let

$$x_1, x_2, \ldots x_M$$

be these quantities. We shall then have

$$\phi(x) = C(x - x_1)(x - x_2) \ldots (x - x_M).$$

For $\phi(x) = 0$ is satisfied by the quantities x_i and it has no multiple roots. The polynomial $\phi(x)$ is then determined save for a constant factor whose value has no effect upon $\phi(x) = 0$

V. $\phi(x) = 0$ *is the only irreducible equation with rational coefficients satisfied by the* x_i's. For if $f(x) = 0$ were another rational irreducible equation satisfied by x_1 and consequently by the x_i's, $f(x)$ would be divisible by $\phi(x)$ and therefore would not be irreducible.

By reason of the five properties of $\phi(x) = 0$ thus established, we may designate this equation, in short, as *the* irreducible equation satisfied by the x_i's.

13. Let us now compare $F(x)$ and $\phi(x)$. These two polynomials have the x_i's as their only roots, and $\phi(x)$ has no multiple roots. $F(x)$ is, then, divisible by $\phi(x)$; that is,

$$F(x) = F_1(x)\,\phi(x).$$

$F_1(x)$ necessarily has rational coefficients, since it is the quotient obtained by dividing $F(x)$ by $\phi(x)$. If $F_1(x)$ is not a constant it admits roots belonging to $F(x)$; and admitting one it admits all the x_i's (10). Hence $F_1(x)$ is also divisible by $\phi(x)$, and

$$F_1(x) = F_2(x)\,\phi(x).$$

If $F_2(x)$ is not a constant the same reasoning still holds, the degree of the quotient being lowered by each operation. Hence at the end of a limited number of divisions we reach an equation of the form

$$F_{\nu-1}(x) = C_1 \cdot \phi(x),$$

and for $F(x)$,

$$F(x) = C_1 \cdot [\phi(x)]^\nu.$$

The polynomial $F(x)$ is then a power of the polynomial of minimum degree $\phi(x)$, except for a constant factor.

14. We can now determine the degree M of $\phi(x)$. $F(x)$ is of degree 2^m; further, it is the νth power of $\phi(x)$. Hence

$$2^m = \nu \cdot M.$$

Therefore M is also a power of 2 and we obtain the following theorem:

The degree of the irreducible equation satisfied by an expression composed of square roots only is always a power of 2.

15. Since, on the other hand, there is only one irreducible equation satisfied by all the x_i's (12, V.), we have the converse theorem:

If an irreducible equation is not of degree 2^h, it cannot be solved by square roots.