CONGRUENCE OF SETS

AND OTHER MONOGRAPHS

ON THE CONGRUENCE OF SETS AND THEIR EQUIVALENCE BY FINITE DECOMPOSITION

BY W. SIERPIŃSKI

THE MATHEMATICAL THEORY OF THE TOP

BY F. KLEIN

GRAPHICAL METHODS

BY C. RUNGE

INTRODUCTION TO THE THEORY OF ALGEBRAIC EQUATIONS

BY L. E. DICKSON

CHELSEA PUBLISHING COMPANY
BRONX, NEW YORK

ON THE CONGRUENCE OF SETS AND THEIR EQUIVALENCE BY FINITE DECOMPOSITION (1954) WAS ORIGINALLY PUBLISHED BY THE LUCKNOW UNIVERSITY, LUCKNOW

THE MATHEMATICAL THEORY OF THE TOP (1897) WAS ORIGINALLY PUBLISHED BY CHARLES SCRIBNER'S SONS, NEW YORK

GRAPHICAL METHODS (1912) WAS ORIGINALLY PUBLISHED BY THE ERNEST KEMPTON ADAMS FUND FOR PHYSICAL RESEARCH, COLUMBIA UNIVERSITY PRESS, NEW YORK

INTRODUCTION TO THE THEORY OF ALGEBRAIC EQUATIONS (1903) WAS ORIGINALLY PUBLISHED BY JOHN WILEY AND SONS, NEW YORK

LIBRARY OF CONGRESS CATALOGUE CARD NO. 67-17000

PRINTED IN THE UNITED STATES OF AMERICA

ON THE CONGRUENCE OF SETS AND THEIR EQUIVALENCE BY FINITE DECOMPOSITION.

by

WACLAW SIERPINSKI

Professor of Mathematics at the University of Warsaw, Member of the Polish Academy of Science, Corresponding Member of the Institute of France.

PREFACE.

Five years ago I had the pleasure and the privilege to be invited by the University of Lucknow to deliver a course of lectures in January and February, 1949. The text of those lectures is being presented in this volume.

I take this opportunity to express my affectionate gratitude to Professor A. N. Singh, Head of the Department of Mathematics, for the kind invitation to me to deliver this course of lectures at Lucknow and for making their publication possible, and to Dr A. Sharma who has translated into English several additions which I have made in the original text and who has read the proofs and directed the printing.

Warsaw, W. SIERPIŃSKI.
December, 1953.

CONTENTS

ON THE CONGRUENCE OF SETS AND THEIR EQUIVALENCE BY FINITE DECOMPOSITION

1. *Congruence of sets.* The congruence of geometrical figures is a well known notion of elementary geometry. Two geometrical figures i.e., two sets of points lying on a straight line, on a plane or in a space of three dimensions are *congruent* if they can be obtained one from the other by translation, rotation or symmetrical reflexion. It has been proved that a necessary and sufficient condition that two sets A and B should be congruent ($A \cong B$) is that there exists an univocally reciprocal conformity conserving the distances, i.e., a relation such that if a_1 and a_2 are two arbitrary points of the set A, and b_1 and b_2 their corresponding points in the set B, then the distance between a_1 and a_2 is equal to the distance between b_1 and b_2.

Transformations of sets conserving distances are called *isometric*. Thus instead of saying "congruent sets" we can say *isometric sets* too. The notion of isometry may be applied not only to sets of Euclidean spaces of arbitrary finite number of dimensions, but even to more general spaces called *metric* in which the notion of the *distance* between two elements is defined.

There exist sets of points, even on the straight line, which are congruent with their proper part (which is different from the whole)—the half-straight line for example.

According to A. Lindenbaum, a set is *monomorphic* when it is not congruent with any of its proper parts.[1] We shall prove the following:

Theorem 1 :—*Each bounded set of points on a straight line is monomorphic.*

Proof—We begin by proving that by a rotation of the straight line by $180°$ around an arbitrary point, no linear set can pass into its own proper part. Suppose, however, that by such a rotation the linear set E passes into its own part H. Let us denote by x an arbitrary point of the set E. By rotation let it pass into the point x' of the set H. x' is therefore a point of the set E which by the rotation passes into a point of the set H. It is plain that by the mentioned rotation the point x' will pass into the point x; thus this belongs to H. We have proved in this way that each

---

[1] Fundamenta Mathematicae 8 (1926), p. 217,

point of the set E belongs to H. Hence the set E is comprised in H, i.e., $E \subset H$ and as the contrary is also true, i.e., $H \subset E$ (H has been supposed to be a part of E), we have $H=E$. Therefore, the set H is not a proper part of the set E.

Suppose now that E denotes an arbitrary linear set and $E(a)$, for a real number a, the translation of the set E along the straight line by length a. $E(a)$ is therefore a set of all real numbers $x+a$, where x is an element of the set E (i.e., $x \epsilon E$). It is obvious that if $H = E(a)$, then $H(-a) = E$ and $H(b) = E(a+b)$.

Suppose the linear set E is bounded. There exists then a positive (finite) number d, such that for each pair of points x and x' of the set E their distance is less than d, i.e., $|x - x'| < d$. If by a translation of length a the set E passes into its part, that is if $E(a) \subset E$, then we have $E(2a) \subset E(a) \subset E$ and generally $E(na) \subset E$ for $n = 1,2,\ldots$. If $x_0 \epsilon E$, then for a positive integer n, $x_0 + na \epsilon E(na) \subset E$, whence $|(x_0+na)-x_0| \leqslant d$, or $|na| \leqslant d$ for $n=1,2,\ldots$, which for $a \neq 0$ is impossible. Thus a linear bounded set cannot by any translation (different from zero) pass into its own proper part.

As we proved, neither by rotation nor by translation can a bounded set pass into its own proper part. Theorem **1** has been, therefore, proved.

Theorem **1** is not true for sets of points on a plane. Instead of it we have

Theorem 2—*There exists a plane bounded set congruent with its own proper part.*

Proof—Let α denote an angle incommensurable with π and ρ a positive number. The set E of the plane having as polar coordinates $(\rho, k\alpha)$, where $k = 0, 1, 2, \ldots$ is congruent, as may be easily seen, with its own proper part $E - \{(\rho, 0)\}$, obtained by the rotation through the angle α around the origin of the coordinates.

The set E is obtained by the successive settings of the arc $\alpha\rho$ (incommensurable with the length of the perimeter of the circle) repeated an infinite number of times on the perimeter of the circle $(x^2+y^2=\rho^2)$ in the positive direction (counter-clockwise sense) beginning from the point $p_0 = (x, y)$, where $x=\rho$, $y=0$. The set $E - \{(\rho, 0)\}$ is here obtained from the set E by removing the point p_0.

The set E is, of course, a countable one. If we wanted to obtain an uncountable bounded set, congruent with its own part, it would be enough to replace the points of the set E by radii, meeting in the centre of the circle excepting the centre itself.

It should be observed that an example of an uncountable set (of the power of the continuum), congruent with its own part could be found on the perimeter of a circle as well. Such an example, however, would be much more difficult. It may be proved with the aid of Zermelo's axiom that there exists a plane bounded set E, congruent with its own proper part H, and such that the set $E-H$ will not be of surface measure zero.

It will be observed that the necessary and sufficient condition, that a set comprised in the Euclidean space should be monomorphic, is that it is no proper part of any set of the space with which it is congruent.

Two sets each of which is congruent with a part of the other, are not necessarily congruent. For instance: the set A of all real non-negative numbers and the set B obtained from the set A by adjoining to it the number -1, are not congruent. In order to see that the set B is congruent with a part of the set A, we move it through the length 1. The sets A and B are not congruent, as there exists for each point of the set A a point at a distance less than 1/2, while the point −1, belonging to B, does not possess this property.

Some theorems, apparently easy, concerning the congruence of sets (even though linear), are difficult to prove and require the use of Zermelo's axiom, e.g., the following theorem of Kuratowski :

If a set E can be decomposed in two ways into sums of two disjoint congruent sets $E = A_1 + A_2 = B_1 + B_2$, where $A_1 \cong A_2$ and $B_1 \cong B_2$, then the sets A_1 and B_1 are each sums of four disjoint sets, respectively congruent (i.e., $A_1 = M_1 + M_2 + M_3 + M_4$, $B_1 = N_1 + N_2 + N_3 + N_4$, where $M_i \cong N_i$ for $i = 1, 2, 3, 4$)[1)]

*Here is a problem regarding the congruence of sets which seems to be very elementary, but whose solution I know only for the case of linear sets:

E being any set of points whatsoever, can we always take out one point from E in such a way that the residual set may not be congruent with E ?

I can prove that this is so for a linear set E, but I do not know if this is true for all infinite

[1)] Fund. Math., 6, p. 243.

*Added to § 1 in 1952 while in press.

plane sets (or for sets in three dimensional space).

For linear sets, the following theorem (an immediate result of this is the positive solution of our problem for linear sets) holds good:

Theorem 2 a. *E being a linear set, there exists at most one point P of E such that $E-\{p\}\cong E$,* ($A\cong B$ denotes that the sets A and B are superposable by translation or by rotation).

Proof: Let E be a linear set and let us suppose that it contains two distinct points p and q such that

$$E-\{p\}\cong E \text{ and } E-\{q\}\cong E.$$

I say that the set $E-\{p\}$ can not be superposable with E by rotation (of the straight line on which it is situated, through an angle π about any point of this straight line). Indeed, let ϕ be the rotation which transforms the set E into the set $E-\{p\}$; that is to say $\phi(E)= E-\{p\}$. Let $p'=\phi(p)$; we have then $p' \epsilon E-\{p\}$, therefore $p' \epsilon E$ and $\phi(p') \epsilon \phi(E) = E-\{p\}$, whence $\phi(p')\neq p$, which is impossible, since evidently $\phi(p')=\phi\phi(p)=p$.

The set $E-\{p\}$ is therefore superposable with E by translation, and so also is $E-\{q\}$. There exist, therefore, two real numbers a and b such that $E-\{p\}=E(a)$ and $E-\{q\}=E(b)$, where $E(c)$ denotes the translation by a length c of the set E (along the straight line) that is to say, the set of all numbers $x+c$, where $x \in E$. As $p \in E$, whence $E \neq E-\{p\}$, we have $a \neq 0$. As $q \neq p$, we have $q \in E-\{p\}$, so that $q \in E(a)$, whence $q-a \in E$.

As $a \neq 0$, $q-a \neq q$, therefore $q-a \in E-\{q\}$, that is to say $q-a \in E(b)$, whence $q-a-b \in E$ and $q-b \in E(a)$, and as $E(a) \subset E$, we find that $q-b \in E$, whence $q \in E(b)=E-\{q\}$, which is impossible.

The hypothesis that we have $p \in E$, $q \in E$ and $E-\{p\} \cong E \cong E-\{q\}$ implies a contradiction and the theorem is proved.

Corollary.—If E is a non-empty linear set, there exists a point p of E such that the sets E and $E-\{p\}$ *are not superposable.*

Proof. The corollary is evident for sets containing only one point O. If E contains two distinct points p and q, we conclude from theorem **2a** that at least one of the sets $E-\{p\}$ and $E-\{q\}$ is not superposable with E.

Now for plane sets we can prove the following:

There exists a plane set E containing two distinct points p and q such that $E-\{p\}\cong E$ and $E-\{q\}\cong E$ [1].

The set E and the points p and q can be defined in the following way:

Let $\alpha = e^i$ and let $\beta = \exp(\theta i)$ be a complex number of modulus 1 which is algebraically independent of the number α. Let c be a complex number which is not a rational function of α and β with rational coefficients.

Let ϕ be the rotation of the plane through the $\angle 1$ about the point 0, and let ψ be the rotation of the plane through the angle θ about the point c; we then have, for complex z:

$$\phi(z) = \alpha z \text{ and } \psi(z) = (z-c)\beta + c.$$

We put, for complex z: $\phi^{\circ}(z) = \psi^{\circ}(z) = z$ and denote by ϕ^{-1} and ψ^{-1} rotations inverse with respect to ϕ and ψ.

Let E be the smallest plane set such that

(1) $0 \in E$ and $1 \in E$,

(2) if $z \in E$, we have $\phi(z) \in E$ and $\psi(z) \in E$,

(3) if $z \in E$ and $z \neq 1$, we have $\phi^{-1}(z) \in E$,

[1]) See p.116.

(4) if $z \in E$ and $z \neq 0$, we have $\psi^{-1}(z) \in E$.
We can prove that [1])

(5) $\phi(E) = E - \{1\}$ and $\psi(E) = E - \{0\}$.

It follows from the above that the sets $E - \{1\}$ and $E - \{0\}$ are superposable with E.

The following problem is open:

Does there exist a non-empty plane set E (or situated in the space of three dimensions) such that $E - \{p\} \cong E$ whatever the point p of E may be?

Now, there exists in Hilbert space an enumerable set E such that, whatever the point p of E may be, the set $E - \{p\}$ is congruent (*i.e.*, isometric) with E. Such a set is, for example, the set E of all those points of Hilbert space of which all the coordinates are zero except only one (whatsoever) which $=1$.

2. *Translation of sets*—There exists of course no linear set containing more than one point and disjoined with each of its translations.

It is easy to give examples of linear infinite sets having with each of their translations one common point at most. Such a set is for instance

[1]) See W. Sierpiński, Fundamenta Mathematicæ 37 (1950) p. 2—4.

the set composed of all the numbers 10^n, where $n=1,2,\ldots$. There may also be defined a linear perfect set (not empty), having with each of its translations one common point at most. See my note published with late S. Ruziewicz in 1932.[1] It may be proved that such a perfect set, generally measurable, is necessarily of measure zero.

Zermelo's axiom of choice is used to prove the existence of a linear set (non-measurable), the complement of which is of interior measure zero and which has with each of its translations one common point at most.

It may be proved without any difficulty that there do not exist two linear sets M and N such that each is the complement of the other, each contains more than one point and each translation of M has with each translation of N one common point at most.[2] S. Banach proved in 1932 [3] the existence of two linear sets M and N of the power of the continuum such that they are complements each of the other and each translation of M has with each translation of N less than $2^{\aleph_0}$ (thus if $2^{\aleph_0} = \aleph_1$, at most $\aleph_0$) common points.

[1] Fund. Math., 19. p. 17.

[2] S. Ruziewicz and W. Sierpiński, Fund Math., 19, p. 20.

[3] Fund. Math., 19. p. 13.

If we admit the continuum hypothesis, we can prove the existence of a family F of $2^{2^{\aleph_0}}$ linear sets of the power $2^{\aleph_0}$ such that for two arbitrary sets of the family F, each translation of one of them has with each translation of the other an enumerable set of common points at most.[1]

It may also be proved that if $2^{\aleph_0} = \aleph_1$, there exists a linear set of power $2^{\aleph_0}$ and measure zero, which differs from each of its translations by an enumerable set of points at most.[2]

On the other hand we can prove the following proposition with the admission of the hypothesis of the continuum:

There exists a decomposition of the straight line into $2^{\aleph_0}$ disjoint sets each of the power $2^{\aleph_0}$, such that any translation along the straight line transforms each of these sets into itself, with the exception of an enumerable set of points at most.[3]

I shall prove here that *a family F (of the power of the continuum) of infinite sets of positive integers may be defined in such a way that for two arbitrary*

---

1) Fund. Math., 19, p.21.

2) Fund Math., 19, p. 22

3) W. Sierpiński: Comm. Math. Helvetici, 22(1949) p. 317

sets of the family F the translation of one of them has with each translation of the other a finite set of common points.

Indeed such is the family of all the sets E_x corresponding to real numbers $x > 0$, where E_x denotes the set of all integers

$$2^n (2Enx+1), \quad (n=1, 2, \ldots)$$

where Et denotes the greatest integer not surpassing t.

If x and y are two distinct real numbers > 0 and a and b two real numbers, let us suppose that

$$t \in E_x(a) \; E_y(b).$$

According to the definition of the sets E_x and E_y there exist positive integers m and n such that

$$(1) \qquad t = 2^m (2Emx+1)+a = 2^n(2Eny+1)+b,$$

hence

$$(2) \qquad 2^m (2Emx+1) - 2^n (2Eny+1) = b - a.$$

Therefore, $b - a$ is an integer.

If $a = b$, formula (2) gives

$$2^m (2Emx+1) = 2^n (2Eny+1),$$

hence $m = n$ and $Emx = Eny$, and it follows that and as $b \bar{\epsilon} E$, we have $E(b-a) \neq E$. So $E \epsilon \phi(E)$ and $E(c) \epsilon \phi(E)$ for real c, and it is seen that the family $\phi(E)$ contains more than one set.

Now the following problem arises: *May the family $\phi(E)$ be composed of a finite number $n > 1$ of sets?* We shall prove that the answer is in the negative.

Lemma. *Let n denote a positive integer > 1. If there exists for a linear set E a real number a such that the sets*

(1) $E(ka)$, *where* $k = 0, 1 \ldots, n-1$,

are all distinct, then there exists another real number b such that the sets

(2) $E(kb)$, *where* $k = 0, 1, 2 \ldots, n-1, n$,

are all distinct.

Proof:—We put $b = a/n$ and admit that there exist two sets among the sets (2) which are equal. Let

(3) $E(k_1 b) = E(k_2 b)$, where $0 \leqslant k_1 < k_2 \leqslant n$.

As $n \geqslant 2$, it cannot be that $k_1 = 0$ and $k_2 = n$, considering that $E = E(0) \neq E(a) = E(nb)$. Therefore we have $0 < k_2 - k_1 < n$. It is, however, plain that the equality $E(c_1) = E(c_2)$ gives $E = E(c_2 - c_1)$ and according to (3) we have

(4) $E = E((k_2 - k_1) b)$, where $0 \leqslant k_1 < k_2 \leqslant n$.

Now from the equality $E = E(c)$ it follows that $E = E(kc)$ for k integral, and (4) gives

$$E = E(k(k_2 - k_1)b)$$

for k integral, and in particular for $k = n$ (as $b = a/n$)

$$E = E((k_2 - k_1)a),$$

where $k_2 - k_1$ is one of the numbers 1, 2, ..., $n - 1$, which is contrary to the hypothesis that the sets (1) are all distinct. This proves the lemma.

Let E now be a linear set neither empty nor containing all the real numbers. As we have proved above, the family $\phi(E)$ contains more than one set and there exists a real number a such that $E \neq E(a)$. The hypothesis of our lemma is therefore valid for $n = 2$. It results, then, from our lemma, by induction, that it is valid for each positive integer n. So the family $\phi(E)$ cannot be finite. Thus we have proved the

Theorem 3—*If E is a linear set neither empty nor containing all the real numbers, then there exists an infinity of linear distinct sets superposable by translation on E.*

Now the problem arises : *Can the family* $\phi(E)$

be enumerable? The question is rather delicate. In the present state of the science it is impossible to give an effective example of a linear set E such that the family $\phi(E)$ should be enumerable, since, as we shall see, such a set should not be measurable in the Lebesgue sense. We can demonstrate the existence of such a set by the aid of Zermelo's axiom.

In reality G. Hamel has proved by the aid of Zermelo's axiom the existence of a *basis* B of all the real numbers, *i. e.*, the (uncountable) set of real numbers a, b, c, ... different from zero, such that each real number x may be represented in one way only in the form

$$x = \alpha a + \beta b + \gamma c + \ldots, \tag{5}$$

where α, β, γ, ... are rational numbers among which, in each particular case there is a finite number (or nul) of non nul values.

Let a be a given number of the basis B and E the set of all the real numbers of the form (5), where $\alpha=0$.

It results easily from the property of the basis B that if α and α_1 are distinct rational numbers, then $E(\alpha a)E(\alpha_1 a) = 0$. Indeed, if there exists a real number x such that $x \epsilon E(\alpha a)$ and

$x \in E(\alpha_1 a)$, then $x - \alpha a \in E$ and $x - \alpha_1 a \in E$, which gives immediately (according to the definition of E), $(\alpha_1 - \alpha)a \in E$, and that is impossible, since $\alpha \neq \alpha_1$.

On the other hand let (5) denote an arbitrary real number. It is obvious that $E(x) = E(\alpha a)$. The family $\phi(E)$ which is evidently coincident with the family of all the distinct sets $E(x)$, where x is an arbitrary real number, coincides also with the family of all the sets $E(\alpha a)$, where α is a rational number, and the family $\phi(E)$ is consequently enumerable (since the number a, a given number of B, is not equal to zero). Thus we have with the aid of Zermelo's axiom the

Theorem 4—*There exists a linear set E and an infinite sequence of linear sets, each two of which are disjoint, and such that each linear set superposable by translation with E is one of the elements of the sequence and vice versa.*

One can also prove with the aid of Zermelo's axiom the following theorem due to Prof. E. Čech:

There exists a linear set E neither empty nor containing all the real numbers, such that for any real number t the infinite sequence of sets

(6) $$E,\ E(t),\ E(2t),\ E(3t),\ \ldots$$

contains merely a finite number of distinct sets.

Let $B = \{a, b, c, \ldots\}$ denote the Hamel basis and E the set of all the numbers of the form

$$pa + qb + rc + \ldots,$$

where the coefficients are integers, of which only a finite number is not equal to zero. The set E does not contain every real number, since it results from the property of the basis B, for instance, that the number $a/2$ does not belong to E.

Now let t be any real number, $t = \alpha a + \beta b + \gamma c + \ldots$, where $\alpha, \beta, \gamma, \ldots$ are rational numbers of which a finite number is not nul. If m is the common denominator of the numbers $\alpha, \beta, \gamma, \ldots$ (not nul), it may be easily seen that $mt \in E$ and $E(mt) = E$. This implies immediately that each term of the infinite sequence (6) is equal to one of the sets

$$E, E(t), E(2t) \ldots, E((m-1)t).$$

Thus *Cech's* assertion has been established.

Suppose now that E is a linear set such that the family $\phi(E)$ is enumerable, and let $\phi(E)$ be $\{E_1, E_2, \ldots\}$. Now the set $E_1 + E_2 + E_3 + \ldots$ covers the whole straight line and as the sets $E_1, E_2, \ldots$, are superposable with F, the latter cannot be of zero measure (since the sum of an enumerable infinity of sets of measure zero is of measure zero and consequently cannot cover the straight line).

As $E(x) \in \phi(E)$ for real x – an uncountable infinity of numbers—and as $\phi(E) = \{E_1, E_2, \ldots\}$, it follows that there exists an index m such that the equality $E(x) = E_m$ is valid for an uncountable infinity of real numbers x. Let ϵ be any positive number. There exist then real numbers x and x' such that $0 < x - x' < \epsilon$ and $E(x) = E_m$, $E(x') = E_m$, giving immediately $E(x) = E(x')$ and $E(x - x') = E$. Therefore, there exist arbitrarily small real numbers $t > 0$ such that $E(t) = E$, which implies $E(kt) = E$ for k integral. It follows immediately that there exists an infinite sequence of real numbers $t_1, t_2, \ldots$ dense in the straight line and such that $E(t_i) = E$ for $i = 1, 2, \ldots$, and $E = \sum_{i=1}^{\infty} E(t_i)$ Now, as we know from the theory of Lebesgue measure, if a set E is not of measure zero, then the sum $\sum_{i=1}^{\infty} E(t_i)$ is a set the exterior measure of which is equal in each interval to the length of this interval. As this sum is equal to E, it may be seen that the exterior measure of the set E in any interval is equal to its length.

Let the complement of the set E be denoted by H and for $i = 1, 2, \ldots$ the complement of E_i

by H_i. Of course, the equality $E(x)=E$ gives $H(x)=H$ and it may be easily deduced from it that $\phi(H)=(H_1, H_2, \ldots)$. It may be proved as for the case of the set E, that the exterior measure of the set H in any interval is equal to the length of the interval. Hence the sets E and H which are complements of each other are both of the interior measure nul. So they are not measurable in the Lebesgue sense. Thus we have proved the

Theorem 5. *Each linear set E satisfying the theorem* **4** *is not measurable in the Lebesgue sense.*

From theorems **3** and **5** there results the

Theorem 6. *If $2^{\aleph_0}=\aleph_1$, then each linear measurable (in the Lebesgue sense) set E, neither empty nor containing all the real numbers, admits an infinity of linear distinct sets of the power of the continuum superposable by translation on E.*

I do not know any proof of the theorem **6** which would not be based on the hypothesis of the continuum. It is easily seen that if E is a linear set composed of only one point, or a bounded interval, or the whole straight line devoid of one point only, then the family $\phi(E)$ is of the power of the continuum. Now the following question may be raised : if m is a given arbitrary cardinal number, not finite, and not superior to the power of the continuum, does there always exist a linear set such that the family $\phi(E)$ is of the power m ? In the light of theorem **4** this problem does not present any interest unless it is proved without the use of the hypothesis of the continuum.

If we modify the above proof of the case $m = \aleph_0$, (theorem **4**) we can prove with the aid of Zermelo's theorem on well ordering (and without using the hypothesis of the continuum) that the answer to the question is positive. The notion of the Hamel's basis should be generalized at this stage by the substitution of the field of rational numbers which constitute the coefficients of the development (5) by a field of real numbers of the power m.[1]

Now the following problems arise :

Does there exist a linear set E such that the family of all the linear distinct sets similar to E in the sense of elementary geometry should be enumerable ?

Does there exist a plane set E such that the family of all the plane distinct sets congruent

---

[1] Fund, Math,, 35, (1948), *p.* 161.

with E (i.e. superposable by translation or by rotation) should be enumerable?

T. Kapuano has proved in 1951 that the reply to each of these two problems is in the negative.[1]

3. *Equivalence of sets by finite decomposition.* Let A and B be two sets situated in an Euclidean space (or more generally in an arbitrary metric space). We write $A \overset{=}{_n} B$ and say that the sets A and B are equivalent by decomposition into n parts if there exist sets $A_1, A_2, \ldots, A_n$ and $B_1, B_2, \ldots, B_n$ such that

1° $A = A_1 + A_2 + \ldots + A_n$, $B = B_1 + B_2 + \ldots + B_n$,

2° $A_k A_l = B_k B_l = 0$ for $1 \leqslant k < l \leqslant n$,

3° $A_k \cong B_k$ for $k = 1, 2, \ldots, n$.

If there exists for two sets A and B a positive integer n such that $A \overset{=}{_n} B$, we shall say that the sets A and B *are equivalent by finite decomposition.* That means that the sets A and B may be decomposed into the same finite number of disjoint parts, respectively congruent. We shall write then $A \overset{f}{=} B$.

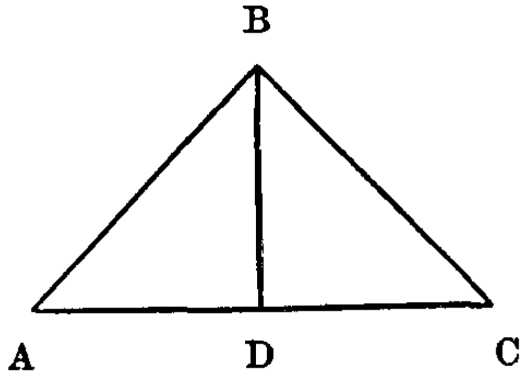
---

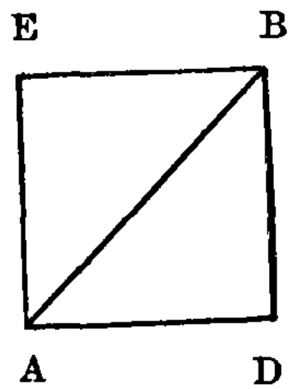
[1] Comptes Rendus, Paris, 232 p. 1621-1622.

We shall mainly treat here the equivalence of sets by decomposition into two parts, which represents an immediate generalisation of the congruence of sets; they differ, however, from it very sensibly.

The notion of the equivalence of geometrical figures by decomposition into two parts is very well known from elementary geometry. We should, however, stress the essential difference between the definition of this equivalence in elementary geometry and that adopted here.

For instance it is well known from elementary geometry that a right angled isosceles triangle ABC may be decomposed by its height BD into two triangles from which a square may be formed (i.e., by the rotation of the triangle BDC around the point B by 270°). This, however, does not enable us to state that our triangle and square are equivalent by decomposition into two parts (in our meaning), since the triangles ABD and BDC into which the triangle ABC has been decomposed, are not disjoint, as they possess the common side BD.





Two polygons (or polyhedrons) are said in elementary geometry to be equivalent by decomposition if they can be decomposed into a finite and equal number of polygons (or polyhedrons) respectively congruent, which do not possess common interior points.

In our sense two sets are *equivalent by finite decomposition* if they can be decomposed into a finite and equal number of arbitrary sets of points, respectively congruent and possessing no common points.

If E is a non-empty set situated in an Euclidean space, there exist, as may be easily proved, $2^{\aleph_0}$ distinct sets of this space at most, congruent with E. There exist $2^{2^{\aleph_0}}$ linear distinct sets equivalent by decomposition into two parts to the straight line. In order to show this, I shall first prove

Theorem 7. *The straight line is equivalent by decomposition into two parts to the set obtained from the straight line by the retraction of an arbitrary bounded set.*

Proof. Let P be the set of all the points of the straight line and B an arbitrary bounded subset of P. Thus the set B is contained in the interior of a finite segment of length l. Let us put

$$(1) \quad P_1 = B + B(l) + B(2l) + \ldots,$$

where $B(l)$ denotes the translation of the set B along the straight line by the length l.

Any two terms of the sum (1) are certainly disjoint and congruent, so we have $P_1(l) \cong P_1$. Let us put $P_2 = P - P_1$. We shall have evidently $P = P_1 + P_2$, $P_1 P_2 = 0$, $P - B = P_1(l) + P_2$, $P_1(l) \cdot P_2 = 0$; taking into consideration that $P_1(l) \cong P_1$, we deduce $P \underset{2}{=} P - B$, which was to be proved.

As the family of all the bounded subsets of the straight line is of the power $2^{\aleph_0}$, it results immediately from theorem 7 that there exist $2^{2^{\aleph_0}}$ linear distinct sets equivalent to the straight line by decomposition into two parts.

If $A = \{1,2,3, \ldots\}$, $B = \{2,3,4, \ldots\}$, $C = \{3,4,5, \ldots\}$ we have

$A \supset B$, $A \supset C$, $B \cong C$, but $(A - B)$ is not $\underset{f}{=}$ $(A - C)$, since $\overline{\overline{A - B}} = 1$, $\overline{\overline{A - C}} = 2$.

Therefore if B and C are two congruent subsets of the linear set A, the sets $A - B$ and $A - C$ can be not equivalent by finite decomposition.

Evidently the relation $\underset{n}{=}$ is symmetrical, yet it is not transitive for $n \geqslant 2$.

Indeed let $A = \{1,2,3,4\}$, $B = \{1,2,5,6\}$ and $C = \{1,5,9,13\}$. As $A = \{1,2\} + \{3,4\}$, $B = \{1,2\} + \{5,6\}$, $\{3,4\} \cong \{5,6\}$, we have $A \overset{=}{_2} B$, and taking into consideration that $B = \{1,5\} + \{2,6\}$, $C = \{1,5\} + \{9,13\}$, $\{2,6\} \cong \{9,13\}$, we have $B \overset{=}{_2} C$. So we have $A \overset{=}{_2} B$ and $B \overset{=}{_2} C$, but we do not have $A \overset{=}{_2} C$, nor even $A \overset{=}{_3} C$. Now if we had $A \overset{=}{_3} C$, there would exist decompositions into disjoint sets $A = A_1 + A_2 + A_3$ and $C = C_1 + C_2 + C_3$, where $A_1 \cong C_1, A_2 \cong C_2, A_3 \cong C_3$. As the set A contains 4 elements one at least of the sets A_1, A_2, A_3, say A_1, contains more than one element. Hence there would exist elements a and b of A_1 such that $a \neq b$; a and b belong, however, to A_1 and all the more to A, hence $|a - b| \leqslant 3$. As $A_1 \cong C_1$ there would exist in C two elements at a distance $\leqslant 3$, which is inconsistent with the definition of the set C. So $A \overset{=}{_3} C$ is not true.

Now it may be easily shown that whatever be the sets of points A, B, C the formulae $A \overset{=}{_2} B$ and $B \overset{=}{_2} C$ imply the formula $A \overset{=}{_4} C$. Indeed, if $A \overset{=}{_2} B$, there exist decompositions $A = A_1 + A_2$, $B = B_1 + B_2$, where $A_1 A_2 = B_1 B_2 = 0$, $A_1 \cong B_1$, $A_2 \cong B_2$, and if $B \overset{=}{_2} C$, there exist decompositions $B = B_1' + B_2'$, $C = C_1 + C_2$, where $B_1' B_2' = C_1 C_2 = 0$, $B_1' \cong C_1$, $B_2' \cong C_2$. These decompositions give immediately decompositions into two disjoint sets:

$$B_1 = B_1 B_1' + B_1 B_2', \; B_2 = B_2 B_1' + B_2 B_2',$$
$$B_1' = B_1 B_1' + B_2 B_1', \; B_2' = B_1 B_2' + B_2 B_2'.$$

As $A_1 \cong B_1$, there exists a decomposition of A_1 into two disjoint sets:

$$A_1 = A_1' + A_1'', \text{ where } A_1' \cong B_1 B_1'$$
$$A_1'' \cong B_1 B_2', \text{ and } A_1' A_1'' = 0.$$

Similarly as $A_2 \cong B_2$, it may be seen that

$$A_2 = A_2' + A_2'', \text{ where } A_2' \cong B_2 B_1'$$
$$A_2'' \cong B_2 B_2' \text{ and } A_2' A_2'' = 0.$$

and as $B_1' \cong C_1$, $B_2' \cong C_2$, it follows that

$$C_1 = C_1' + C_1'', \text{ where } C_1' C_1'' = 0,$$
$$C_1' \cong B_1 B_1' \text{ and } C_1'' \cong B_2 B_1',$$
$$C_2 = C_2' + C_2'', \text{ where } C_2' C_2'' = 0,$$
$$C_2' \cong B_1 B_2', \text{ and } C_2'' \cong B_2 B_2'.$$

Thus decompositions into 4 sets have been obtained:

$$A = A_1' + A_1'' + A_2' + A_2'', \quad C = C_1' + C_2' + C_1'' + C_2'',$$

where $A_1' \cong C_1'$, $A_1'' \cong C_2'$, $A_2' \cong C_1''$, $A_2'' \cong C_2''$.

It results at once that $A \underset{4}{=} C$.[1] Later we shall prove more generally that the formulae $A \underset{m}{=} B$ and $B \underset{n}{=} C$ imply the formula $A \underset{mn}{=} C$. It follows that the relation $\underline{f}$ is transitive.[1]

It may be proved that for a bounded segment $I\,[0 \leqslant x \leqslant 1]$ we have $I \underset{3}{=} I - \{0\}$, but not $I \underset{2}{=} I - \{0\}$.

---

[1] A and C being two sets (e. g., linear), such that $A \underset{3}{=} C$, I do not know if there always exists a set B, such that $A \underset{2}{=} B$ and $B \underset{2}{=} C$.

*For the equivalence by finite decomposition in the sense of elementary geometry, it may be remarked that F. Bolyai has proved that two polygons having equal surfaces are equivalent by finite decomposition to a finite number of triangles.

H. Steinhaus has proposed the problem whether we can divide the square into a finite number of squares of which no two are congruent. It has been proved that the square whose side is 175 can be divided into 24 squares, not congruent two by two, whose sides are expressible by natural numbers. We do not know if we can divide the square into less than 24 parts not congruent two by two.[1)]

Theorem 7a. *Let E be a linear infinite set. There exists an infinite sub-set H of E, such that the sets E and H are not equivalent by finite decomposition,* i.e., there exists no natural number m such that

---

* Added to §3 while in Press in 1952.

[1)] See The Dissection of Rectangles into Squares, Duke Math. Jour. 7 (1940) pp. 312-340 ; R. Sprague, Math. Zeit. 46 (1940) p. 460 - 471; M. Goldberg, Amer. Math. Monthly 47 (1940) p. 570 - 571 and Scripta Mathematical 18 (1952) p. 17-24; E. Bodewig, Indagationes Mathematicae 9 (1947) p. 34; C. J. Bouwkamp, ibid p. 58, and B.A. Kordemskij and N. Rusaleff, The strange square (in Russian) Moscou-Leningrad 1952 (159 pages).

$$E = E_1 + E_2 + \dots + E_m,$$
(1) and
$$H = H_1 + H_2 + \dots + H_m,$$

where $E_k E_l = H_k H_l = 0$ for $1 \leqslant k < l \leqslant m$, and where the set E_k is superposable (by translation or rotation) with H_k for $k = 1, 2, \dots, m$) (i.e., $E_k \cong H_k$ for $k = 1, 2, \dots, m$).

Proof. There are two cases.

(i) The set E is unbounded. The linear set E being infinite, there exists, for each natural number n, an interval d_n of length $\bar{d}_n$ containing at least n distinct points of E. I define by induction an infinite set $p_1, p_2, \dots$ of points of E as follows:–

Let n be a natural number > 1, and suppose that we have already defined the points $p_1, p_2, \dots$ $\dots, p_{n-1}$.

Since the set E is not bounded, there exist points in E whose distance from each of the points $p_1, p_2, \dots, p_{n-1}$ is greater than $\bar{d}_1, \bar{d}_2, \dots, \bar{d}_{n^2}$: let p_n be one of these points.

Put $H = \{p_1, p_2, \dots\}$. We see easily that, if $k \geqslant m > 1$ and if n is a natural number $\neq k$, the distance of p_k from p_n is $> \bar{d}_{m^2}$. It follows immediately that there does not exist in H any system of m (> 1) points, the distance between any two of which is $\leqslant \bar{d}_{m^2}$ (because one at least of these points will have an index $k \geqslant m$).

Let us suppose that formulae (1) hold, where m is a natural number which we can suppose > 1. As the interval d_{m^2} contains at least m^2 distinct points of E, one at least of the sets $E_1, E_2, \ldots, E_m$, say E_k, contains at least m points of d_{m^2}. If we had $E_k \cong H_k$, the set H_k and *a fortiori*, the set H would contain at least m distinct points having two of the distances $\leqslant \bar{d}_{m^2}$, which is, as we have proved, impossible. The sets E and $H \subset E$ are therefore not equivalent by finite decomposition.

(ii) The set E is bounded. The set E being infinite (and bounded), there exists, by the theorem of Bolzano-Weierstrass, a point of accumulation a of E (i.e., $a \epsilon E'$). We shall define an infinite set $p_1, p_2, \ldots$ of points of E by induction as follows. Let p_1 be any point whatsoever of E other than a. Let n be a natural number > 1 and suppose that we have already defined the points $p_1, p_2, \ldots, p_{n-1}$ and that they are all different from a. Let ϵ_n be a positive number such that $2\epsilon_n$ is smaller than the distance between any two of the points $a, p_1, p_2, \ldots, p_{n-1}$. As $a \epsilon E'$, there exists a point p_n of E whose distance $\rho(p_n, a)$ from a is less than each of the numbers $\epsilon_1, \epsilon_2, \ldots, \epsilon_n$. Put

$$H = \{p_{2^2+1}, p_{3^2+1}, \ldots, p_{n^2+1}, \ldots\}.$$

If H contains m (> 1) distinct points, at least two of them, say p_{k^2+1} and p_{l^2+1}, will have indices. $\geqslant m^2+1$, and from the definition of the points p_n, we will have

$$\rho(p_{k^2+1}, a) < \epsilon_{m^2+1}$$

and $$\rho(p_{l^2+1}, a) < \epsilon_{m^2+1},$$

whence $$\rho(p_{k^2+1}, p_{l^2+1}) < 2\,\epsilon_{m^2+1}.$$

Therefore there does not then exist in H for a natural number $m > 1$, m distinct points having their mutual distances $\geqslant 2\epsilon_{m^2+1}$.

Let us suppose that formulae (1) hold true where m is a natural number > 1. The distance between two distinct points of the set $p_1, p_2, \ldots, p_{m^2}$ being $> 2\epsilon_{m^2+1}$, one at least of the sets $E_1, E_2, \ldots, E_m$, say E_k, contains at least m points of E having their mutual distances $> 2\epsilon_{m^2+1}$. This is then true for the set $H_k \cong E_k$ and, *a fortiori*, for the set H, which is, as we have shown, impossible.

In the cases (i) and (ii) the sets E and H are not equivalent by finite decomposition and our theorem is proved. It can be generalised easily to infinite sets situated in an euclidean space of a finite number of dimensions, but not to any infinite metric spaces.

Theorem 7b. *If* $E_1, E_2, \ldots$ *is an infinite aggregate of infinite linear sets such that for every natural number* n, E_{n+1} *is equivalent by finite decomposition to a subset of* E_n, *then there exists an infinite set* E *such that for every natural number* n, E *is equivalent by finite decomposition to a subset of* E_n, *but not to* E_n.

Proof. By hypothesis, there exists a set $H_2 \subset E_1$, such that $E_2 \stackrel{f}{=} H_2$ (*i.e.*, E_2 is equivalent by finite decomposition to H_2). Similarly, there exists a set $H \subset E_2$ such that $E_3 \stackrel{f}{=} H$. The formulae $E_3 \stackrel{f}{=} H$, $H \subset E_2$ and $E_2 \stackrel{f}{=} H_2$ prove (See corollary of Theorem **23**) that there exists a set $H_3 \subset H_2$, such that $E_3 \stackrel{f}{=} H_3$. We thus obtain by induction an infinite aggregate of sets $E_1 = H_1 \supset H_2 \supset H_3 \supset \ldots$ such that $E_n \stackrel{f}{=} H_n$ for $n = 1, 2, \ldots$.

We now define by induction two infinite sets of points $p_1, p_2, \ldots$ and $q_1, q_2, \ldots$ as follows. Let p_1 and q_1 be two distinct points of H_1. Let n be a natural number > 1 and suppose that we have already defined the points $p_1, p_2, \ldots, p_{n-1}$ and $q_1, q_2, \ldots, q_{n-1}$. The set H_n being infinite (and also equivalent by finite decomposition to the infinite set E_n), there exist distinct points p_n and q_n

of H_n, distinct from each of the points $p_1, p_2, \ldots, p_{n-1}, q_1, q_2, \ldots, q_{n-1}$. Put $H_0 = \{p_1, p_2, \ldots\}$. Seeing that $H_1 \supset H_2 \supset \ldots$, we evidently have, for every natural number n:

$$\{p_n, p_{n+1}, p_{n+2}, \ldots\} \subset H_n$$

and
$$\{q_n, q_{n+1}, q_{n+2}, \ldots\} \subset H_n - H_0.$$

From theorem **1**, there exists an infinite sub-set E of H_0 which is not equivalent by finite decomposition to H_0.

By means of the properties of the sets $p_1, p_2, \ldots$ and $q_1, q_2, \ldots$, we find easily the following decompositions into two disjoint sets

$$H_0 = \{p_1, p_2, \ldots, p_{n-1}\} + \{p_n, p_{n+1}, \ldots\}$$

and

$$T_n = \{q_n, q_{n+1}, \ldots, q_{2n-2}\} + \{p_n, p_{n+1}, \ldots\},$$

where evidently

$$\{p_1, p_2, \ldots, p_{n-1}\} \underset{n-1}{=} \{q_n, q_{n+1}, \ldots, q_{2n-2}\}.$$

We deduce from this at once that the set H_0 is equivalent by decomposition into n parts to the subset T_n of H_n. As $E \subset H_0$ and $H_n \overset{f}{=} E_n$, we conclude from this that the set E is equivalent by finite decomposition to a sub-set of E_n (for $n = 1, 2, \ldots$).

Now let us suppose that for a natural number n we have $E \underline{\not\,} E_n$. Since $E \subset H_0$ and $H_0 \underline{\not\,} T_n \subset H_n$, there exists a set G such that $E \underline{\not\,} G \subset T_n \subset H_n$ and, as $E \underline{\not\,} E_n$ and $E_n \underline{\not\,} H_n$, this gives, as we know,[1] $T_n \underline{\not\,} H_n$; therefore, seeing that $H_0 \underline{\not\,} T_n$ and $H_n \underline{\not\,} E_n$, we find that $H_0 \underline{\not\,} E_n$ and since $E \underline{\not\,} E_n$, we get $H \underline{\not\,} E$, contrary to the definition of the set E.

The theorem **2** is thus proved.

4. *Some theorems on the equivalence of sets by decomposition into two parts.*

Theorem 8. *The straight line is equivalent by decomposition into two parts to the set obtained by the retraction of an arbitrary enumerable set from the straight line.*

Proof. Let P be the set of all the points of the straight line and D a given enumerable subset of P. It is known that the set of all the numbers $\frac{x-y}{k}$, where $x \in D$, $y \in D$ and $k = \pm 1, \pm 2, \ldots$, is enumerable. As the set of all positive numbers is uncountable, there exists a positive number a such that

$$a \neq \frac{x-y}{k}, \quad \text{for } x \in D, y \in D, k = \pm 1, \pm 2, \ldots$$

Let p and q be two distinct integers. If we suppose that $D(pa).D(qa) \neq 0$ then there would

[1] See Corollary of Theorem 23.

exist elements x and y of D such that $x+pa = y+qa$, and putting $k = q-p \neq 0$ we should have $a = \frac{x-y}{k}$, which is in contradiction with the definition of the number a. Thus we have $D(pa).D(qa) = 0$ if p and q are both distinct integers. We put

$$P_1 = D + D(a) + D(2a) + \dots .$$

The terms of this sum are sets any two of which are disjoint and congruent. Considerations similar to those of theorem **7** will complete the demonstration. Thus one gets $P \underset{2}{=} P - D$ and the proof is completed.

The word 'enumerable' in the theorem **8** could be substituted by 'of the power inferior to that of the continuum', the demonstration, however, would then require, in the general case, the use of Zermelo's axiom to enable the deduction of $\aleph_0 m^2 < 2^{\aleph_0}$ from $m < 2^{\aleph_0}$.

Corollary. The set of all the real numbers is equivalent by decomposition into two parts to the set of all the irrational numbers as well as to the set of all the transcendental numbers.

The proof of the corollary results immediately from the fact that the sets of all the rational numbers as well as all the algebraical numbers are enumerable sets. Now we have

Theorem 9. *The set of all the irrational numbers is equivalent by decomposition into two parts to the set of all the transcendental numbers.*

Proof. Theorem **9** cannot be immediately derived from the corollary, since the relation $\overset{=}{\scriptstyle 2}$ is not transitive. Let P denote the set of all the real numbers, R the set of all the rational numbers and A the set of all the algebraical numbers, and a a transcendental number.

We put $A_1 = A - R$. It is easily seen that the terms of the sum

$$P_1 = A_1 + A_1(a) + A_1(2a) + \dots$$

are two by two superposable and disjoint (since the equality $x + ka = y + la$, where $x \in A$, $y \in A$, and where k and l are distinct integers, would lead to $a = \frac{x-y}{l-k}$, which is impossible, considering that a is a transcendental number). We put

$$P_2 = (P - R) + P_1$$

and it gives

$$P - R = P_1 + P_2,\ P_1 P_2 = 0,\ P - A = (P_1 - A) + P_2,$$

$$(P_1 - A_1)\, P_2 = 0,\ P_1 - A \cong P_1.$$

It is readily verified that $P - R \underset{2}{=} P - A$ and the theorem is proved.

Theorem 10. *The set of all the rational numbers and the set of all the algebraical numbers are not equivalent by finite decomposition.*

Proof. Let $A = A_1 + A_2 + A_3 + A_4 + \dots + A_n$ be a finite decomposition of the set A of all the algebraical numbers. One term at least of this sum, say A_1, contains an infinity of numbers of the form $k\sqrt{2}$ where $k = 1, 2, \dots$. As the difference between two distinct numbers of this form is always irrational, the set A_1 cannot be congruent with any part whatsoever of the set R of all the rational numbers. So the relation $A \underset{n}{=} R$ does not hold. This demonstration of the theorem **10** is due to *Prof. S. Mazur.*

Theorem 11. *The set R of all the rational numbers and the set D of all finite decimal fractions are not equivalent by finite decomposition.*

Proof (given by S. Mazur). Let $R = R_1 + R_2 + \dots + R_n$ be a finite decomposition of the set R. One at least of the terms of this decomposition, say R_1, contains an infinity of numbers of the form $1/p$, where p is a prime number. So there exist two prime numbers $p > 5$ and $q > p$ such that the numbers $1/p$ and $1/q$ belong to R_1. As the difference $(1/p) - (1/q)$ is not a finite decimal number, the set R_1 is not congruent with any subset of D. Thus the relation $R \underset{n}{=} D$ does not hold.

Theorem 12. *The set D of all the finite decimal fractions and the set E of all the finite dyadic fractions are not equivalent by finite decomposition.*

Proof. Let $D = D_1 + D_2 + \ldots + D_n$. One at least of the terms of the decomposition, say D_1, contains an infinity of numbers of the form $1/5^k$, where $k = 1, 2, \ldots$ (since evidently all these positive numbers belong to the set D). Hence there exist two positive integers k and $l > k$, such that $1/5^k \in D$ and $1/5^l \in D$. Now it is easily seen that $(1/5^k) - (1/5^l)$ does not belong to E and this implies that D_1 cannot be congruent with a part of E. Thus the relation $D \underset{n}{=} E$ does not hold. It may be proved that each infinite set situated in the Euclidean space contains an infinite subset to which it is not equivalent by finite decomposition. This is not generally true for infinite metric spaces. For instance, an enumerable metric space in which the distance between two distinct arbitrary points is equal to 1, is congruent (isometric) with each of its infinite subsets.

Theorem 13. *If a and b are two arbitrary real numbers, A is the set of all the rational numbers $< a$ and B the set of all the rational numbers $< b$, then $A \underset{2}{=} B$.*

Proof. Let us suppose, as we may, $a \neq b$, *e.g.*, $a < b$. Let m be a positive integer such that $m > b-a$. We denote by Q the set of all the rational numbers x satisfying $a \leq x < b$ and we put

$$B_1 = Q + Q(-m) + Q(-2m) + Q(-3m)....$$

It is really seen that the terms of this sum are sets two by two disjoint and superposable. We put $B_2 = B - B_1$, which gives

$$B = B_1 + B_2,\ B_1 B_2 = 0,\ A = B - Q = (B_1 - Q) + B_2,$$
$$(B_1 - Q)B_2 = 0,\ B_1 - Q = B_1(-m) \cong B_1.$$

It follows from it immediately that $A \underset{2}{=} B$, which was to be proved.

It is plain that we have $A \cong B$ only in the case when $b-a$ is a rational number. For $a = \sqrt{2}$ and $b = \sqrt{3}$ the sets A and B are not congruent. The same is true for $a = -\sqrt{2}$ and $b = \sqrt{2}$. The set of all the rational numbers $< \sqrt{2}$ and the set of all the rational numbers $> \sqrt{2}$ (the latter is not superposable by rotation around the point zero with the set of the rational numbers $< \sqrt{2}$) are not congruent. They are, however, equivalent by decomposition into two parts.

It should be observed that in theorem **13** the words 'rational' could be replaced by 'algebraical', 'irrational' or 'transcendental'.

Let us point out that it results immediately from a theorem of *Banach*[1] that if for two sets X and Y the formulae $X \cong Y_1 \subset Y$ and $Y \cong X_1 \subset X$ are valid then $X \underset{2}{\mp} Y$.

Theorem 14. *If S denotes a spherical surface (in the space of 3 dimensions), D a finite or enumerable subset of S, then $S - D \underset{2}{\mp} S$.*

Proof. Suppose, as we evidently may, that S is the sphere $x^2 + y^2 + z^2 = 1$. As the set D is finite or enumerable there exist straight lines crossing the centre of the sphere and containing no point of D. Now it may be admitted that the axis OZ is one of these straight lines. If p is a given point of D, let $\alpha(p)$ be the angle $\geqslant 0$ and $< 2\pi$ formed by the plane passing through p and the axis OZ and the plane XOZ. Let β be a given angle, and $D(\beta)$ the set into which D is transformed by the rotation of the sphere S around the axis OZ through the angle β. I say that the angle β may be chosen in such a way that the sets

$$(2) \quad D,\ D(\beta),\ D(2\beta),\ D(3\beta),\ \ldots$$

should be two by two disjoint.

Indeed, if for integers k and $l \geqslant 0$, where $k < l$, there is $q \in D(k\beta)D(l\beta)$, then evidently there exist points p_1 and p_2 of D, such that

[1] Fund. Math., 6, p. 239, Th. 2.

$\alpha(q)=\alpha(p_1)+k\beta-2k_1\pi$ and $\alpha(q)=\alpha(p_2)+l\beta-2l_1\pi$, where k_1 and l_1 are integers. Thus we obtain

$$(3)\qquad \beta=\frac{\alpha(p_1)-\alpha(p_2)+2(l_1-k_1)\,\pi}{l-k}$$

As the set of all the numbers

$$(4)\qquad \frac{\alpha(p_1)-\alpha(p_2)+2s\pi}{n}$$

(where $p_1\in D$, $p_2\in D$, s is an integer and n a positive integer) is enumerable, there evidently exists among the numbers (4) a distinct number β (where $0<\beta<2\pi$). This number β does not satisfy the equality (3) and the sets (2) are disjoint two by two. Let us put

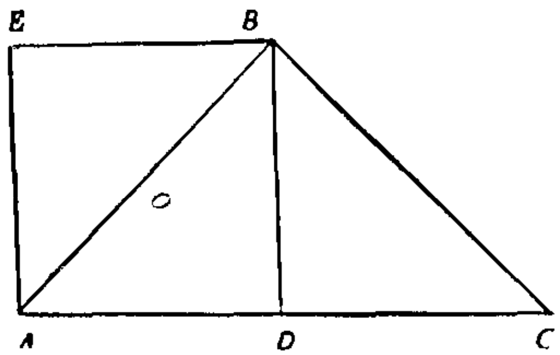
$$I=D+D(\beta)+D(2\beta)+$$

and $R=S-I$.

We have $I(\beta)=I-D$, hence $I-D\cong I$, and since $S=I+R$, $IR=0$, $S-D=(I-D)+R$, $(I-D)R=0$, it may be deduced that $S-D \underset{2}{=} S$. This proves theorem **14**.

5. Theorem 15. *A rectangular isosceles triangle is equivalent to a square by finite decomposition.*

Proof. We divide the square $K=AEBD$, the the sides of which are equal to 1, into 3 disjoint parts: (1) the triangle ABD, its side included, (2) the interior of the triangle AEB with its side EA and without its end-points (i.e., without the points E and A) and (3) the side EB with the end point E and without B. In order to form from these three sets of points the triangle ABC, we need,



of course, a segment of a straight line of the length $BC - EB = \sqrt{2}-1$, containing only one of its endpoints. Thus, if we want to prove that a rectangular isosceles triangle is equivalent to a square by finite decomposition, it will be sufficient to show that the square K is equivalent by finite decomposition to the same square devoid of a segment of the straight line $\sqrt{2}-1$ long, containing only one of its end points. O being the centre of the square, we take for this purpose the segment $S = OP$ of the length $\sqrt{2}-1$ with P and without O. Let a denote an angle incommensurable with 2π, for instance $a=1$. $S(a)$ is the segment obtained by the rotation of the segment S around the point O through the angle a. One evidently has the decomposition into the disjoint sets

$$E = S + S(a) + S(2a) + S(3a) + \dots$$

and it is easily found that $E \subset K$ and $E(a) = E - S$.

It may be deduced from it at once that $K \underset{2}{=} K - S$ and this proves theorem **15.**

Naturally the problem may be put: what is the smallest positive integer n for which the triangle is $\underset{n}{=} K$? S. Banach and A. Tarski have proved[1]) that the necessary and sufficient condition that two polygons (situated in a plane) should be equivalent by finite decomposition, is that they should have the same area (it may be observed that the necessity of this condition is much more difficult to prove than its sufficiency). As to the polyhedron the situation is quite different. According to a theorem of Banach and Tarski (proved with the aid of Zermelo's axiom) two bounded polyhedra are always equivalent by finite decomposition (even if their volumes are distinct)[2]). In particular the solid sphere is equivalent to a cube by finite decomposition. Now we do not know if a circle is equivalent by finite decomposition to a square of the same area.

Theorem 16. *Each segment of the straight line is equivalent by finite decomposition to one of its proper subsets (resp. supersets).*

---

1) Fund. Math., 6, p. 260 (cor. 20). cf. A. Tarski 'On the equivalence of polygons' (Polish), Przeglad Mat. Fiz., 2, 1924, p. 12 and p. 14.

2) l.c. p. 263, Th. 27.

Proof. Suppose I is the segment $0 \leqslant x \leqslant 1$ and a an irrational number, $0 < a < 1$. We put $p_k = ka - Eka$, for $k=0, 1, 2, \dots$, where Et denotes the greatest integer $\leqslant t$, and X denotes the set of all such numbers p_k $(k=0, 1, 2, \dots)$ and Y the set of all numbers p_k of X such that $0 \leqslant p_k < 1-a$. One puts $Z = X-Y$, $T = I - X$; Z' denotes the set of all the numbers p_k of X satisfying $0 < p_k < a$.

We have $I = T + Y + Z$ and therefore a decomposition of the set I into three disjoint sets. Now $Z = X-Y$ is evidently the set of all the numbers p_k $(k=0, 1, 2, \dots)$ satisfying $1-a \leqslant p_k < 1$, or what comes to the same, satisfying $1-a < p_k < 1$, since $p_k = 1-a$ would have had as a consequence $ka - Eka = 1-a$, whence $(k+1)a = Eka + 1$, which is impossible (for $k=0, 1, 2, \dots$) as a is an irrational number. I say that the set Z is a translation of the set Z' by the length $1-a$.

Indeed, if $p_k \in Z$, then $1-a < p_k < 1$, hence $0 < p_k + a - 1 < a < 1$ and $E(p_k + a - 1) = 0$, therefore as $p_k + a - 1 = ka - Eka + a - 1 = (k+1)a - Eka - 1$, $0 = E(p_k + a - 1) = E(k+1)a - Eka - 1$, then $p_k + a - 1 = (k+1)a - E(k+1)a = p_{k+1}$, ie., $0 < p_{k+1} < 1$, and hence $p_{k+1} \in Z'$. On the other hand if $p_k \in Z'$, then $0 < p_k < a$ whence $k > 0$ and $1-a < p_k + 1 - a < 1$; therefore as $0 < 1-a$, then $E(p_k + 1 - a) = 0$, hence as $p_k + 1 - a = ka - Eka + 1 - a = (k-1)a - Eka + 1$, $E(k-1)a - Eka + 1 = 0$, and $p_k + 1 - a = (k-1)a - E(k-1)a = p_{k-1}$, $1-a < p_{k-1} < 1$, hence $p_{k-1} \epsilon Z$. Thus $Z \cong Z'$.

Now, suppose $Y' = X - [Z' + \{0\}]$. So Y' is the set of all numbers p_k $(k = 0, 1, 2, \ldots)$ such that $a \leqslant p_k < 1$. If $p_k \epsilon Y$, then $0 \leqslant p_k < 1-a$, hence $a \leqslant p_k + a < 1$, therefore $E(p_k + a) = 0$, and as $p_k + a = (k+1)a - Eka$, $E(k+1)a = E(ka)$, then $p_k + a = (k+1)a - E(k+1)a = p_{k+1}$, $a \leqslant p_{k+1} < 1$, thus $p_{k+1} \epsilon Y'$. If, however, $p_k \epsilon Y'$, then $a \leqslant p_k < 1$, thus $k > 0$ and $0 \leqslant p_k - a < 1 - a$, hence considering that $1 - a < 1$, one obtains $E(p_k - a) = 0$, so that on account of $p_k - a = (k-1)a - Eka$, we have $E(k-1)a = Eka$, and $p_k - a = (k-1)a - E(k-1)a = p_{k-1}$, $0 \leqslant p_{k-1} < 1 - a$, therefore $p_{k-1} \epsilon Y$. It may be seen that the set Y' is a translation of the set Y by the length a, so that $Y \cong Y'$.

We put $I' = T + Y' + Z'$. As the sets T, Y' and Z' are disjoint, there is $I \underset{3}{=} I'$. Now, we evidently have $I' = I - \{0\}$. On the other hand, suppose $I'' = I + \{2\}$. It gives $I = I' + \{0\} = T + Y' + Z' + \{0\}$, $I'' = I + \{2\} = T + Y + Z + \{2\}$, which leads immediately to $I \underset{4}{=} I''$. The proof of theorem **16** is completed.

It results easily from the demonstrations of the theorems **15** and **16** that a (closed) square is $\underset{2}{=}$ to any of its proper subsets and that a (closed) segment of a straight line is $\underset{3}{\equiv}$ to any of its proper subsets. Now, it may be proved that a (closed) segment is not $\underset{2}{\equiv}$ to any of its proper subsets. On the other hand, it may be proved with the aid of Zermelo's axiom that a (closed) segment of a straight line is $\underset{3}{\equiv}$ to a non-measurable (in the Lebesgue sense) set containing the segment[1].

The set of all the rational numbers is $\underset{2}{\equiv}$ to one of its proper subsets (e.g., to the set of all the rational numbers < 0 or $\geqslant 1$). Now we have

Theorem 17. *A bounded set of rational numbers is not equivalent by finite decomposition to any of its proper subsets.*

Proof: Suppose A is a bounded set of rational numbers equivalent by finite decomposition to a set B, where $B \subset A$ and $B \neq A$. So there exists a positive integer n and the decompositions

$$A = A_1 + A_2 + A_3 + \dots + A_n$$

and

$$B = B_1 + B_2 + B_3 + \dots + B_n$$

into non-empty disjoint sets, where $A_k \cong B_k$ for $k = 1, 2, \dots, n$.

Thus there exists for $k = 1, 2, \dots, n$ a transformation f_k of A_k into B_k which is either a translation or a rotation. This implies immediately the

[1] Sierpiński, Prace Math, Fizyczne 43, 1935 p. 1.

into (non-empty) disjoint sets where $A_k \cong B_k$ for $k=1,2, ..., n$.

Thus there exists for $k=1,2,..., n$ a transformation f_k of A_k into B_k which is either a translation or a rotation. This implies immediately the existence for $(k=1,2,\ldots,n)$ of a real number a_k such that $f_k(x) = a_k + x$ or $f_k(x) = a_k - x$ for $x \in A_k$. Considering that the sets A_k and B_k are formed of rational numbers, we see that a_k is also rational. We put $f(x) = f_k(x)$ for $x \in A_k$ $(k = 1, 2,... ,n)$. So the function $f(x)$ will be defined for $x \in A$ and it is easily seen that it transforms in a reciprocally univocal way the set A into B. It may also be verified at once that for $x \in A$,

$$f(x) = l_1(x).a_1 + l_2(x).a_2 + ... + l_n(x).a_n \pm x,$$

where $l_1(x), l_2(x), ..., l_n(x)$ are integers depending upon x (we have namely, for $x \in A_k$: $l_k(x) = 1$ and $l_i(x)=0$ if $i \neq k$), and the sign $\pm$ depends upon x.

Denoting by $f^{(m)}(x)$ the m^{th} iteration of $f(x)$ (*i.e.*, the function $\underbrace{fff....f}_{m\ times}(x)$) we obtain for $m=1, 2,\ldots,$ and $x \in A$:

$$f^{(m)}(x) = k_1(x).a_1 + k_2(x).a_2 + ... + k_n(x).a_n \pm x,$$

where $k_i(x)$ $(i=1,2, ...,n)$ are integers depending on x (and on m), and the sign $\pm$ depends on x (and on m).

Let q be the common denominator of rational numbers $a_1, a_2, \ldots, a_n$. We have

$$f^{(m)}(x) = \frac{c(x)}{q} \pm x, \quad \text{for} \quad x \in A,$$

where $c(x)$ is an integer (depending on x and m).

As the set A is bounded, the function $c(x)$ is also bounded, and it assumes only integral values of which a finite number are distinct. It follows from it that when x is a given number of A, the infinite sequence

$$x, f(x), ff(x), fff(x), \ldots$$

cannot be formed of numbers different from one another.

Considering that $B \subset A$ and $B \neq A$, there exists a number $x_0 \in A - B$. Therefore there exist positive integers k and p such that

$$f^{(k-1)}(x_0) = f^{(k-1+p)}(x_0).$$

Now as the function f assumes distinct values in A we have

$$x_0 = f^{(p)}(x_0),$$

which is impossible since $x_0 \epsilon B, f^{(p)}(x) \epsilon B$, for $x \epsilon A$ and p is a positive integer. The hypothesis that $A \underset{=}{f} B$ implies a contradiction, whereby theorem **17** is proved.

It is to be observed that *there exists a linear enumerable bounded set which is equivalent by finite decomposition to any of its proper parts.* Such is the set $E=\{p_1, p_2, \ldots\}$ where $p_k = ka - Eka$ for $k=0$, 1, 2,... , where a is an irrational number of the interval $(0,1)$, *e.g.*, $a=\sqrt{2}-1$. Indeed we have $E \underset{2}{=} E-\{p_0\}$. In reality, let E_1 denote the set of all the numbers $p_k < 1-a$ of E, and let us put $E_2 = E - E_1$. It may be easily verified that

$$E = E_1 + E_2, \qquad E-\{p_0\} = E_1(a) + E_2(a-1),$$

$$E_1 E_2 = 0, \qquad E_1(a) E_2(a-1) = 0.$$

Theorem 18.—*There exists a family of infinite sets of positive integers of the power of the continuum no two of which are equivalent by finite decomposition.*

Such is the family of all the sets $\{Ex, E2x, E3x, \ldots\}$ *where* x *assumes all real values* $\geqslant 1$ (where Et denotes the greatest integer $\leqslant t$).

Proof. Let A and B be two infinite sets of positive integers equivalent by finite decompositions into disjoint sets so that,

$$A = A_1 + A_2 + \ldots + A_m, \quad B = B_1 + B_2 + \ldots + B_m,$$
where $A_i \cong B_i$ for $i = 1, 2, \ldots, m$.

We suppose that for $i = 1, 2, \ldots, p$ the sets A_i and B_i are superposable by translation, (let $B_i = A_i(a_i)$ for $i = 1, 2, \ldots, p$) and that for $i = p+1, p+2, \ldots, m$ they are superposable by rotation. It is plain that the numbers a_i $(i = 1, 2, \ldots, p)$ are integers and that A_i $(i = p+1, p+2, \ldots, m)$ are finite (two infinite sets of positive integers could not be superposable by rotation).

If n is a given positive integer, we denote by $P^{(n)}$ the number of all the numbers of the set of positive integers P which are $\leqslant n$. It is easily seen that for each integer a, $|P^{(n)}(a) - P^{(n)}| \leqslant |a|$. It results from it immediately that $|B_i^{(n)} - A_i^{(n)}| \leqslant |a_i|$ for $i = 1, 2, \ldots, p$ and it implies that $|A^{(n)} - B^{(n)}| \leqslant q$ where
$$q = |a_1| + |a_2| + \ldots + |a_p| + \overline{\overline{A}}_{p+1} + \overline{\overline{A}}_{p+2} + \ldots + \overline{\overline{A}}_m,$$
is an integer independent of n.

Let x and y be two real distinct numbers $\geqslant 1$, for instance $x < y$, and let us put

$$A = \{Ex, E2x, \ldots\} \text{ and } B = \{Ey, E2y, \ldots\}.$$

It is readily verified that

$$E\,\frac{n+1}{x} - 1 \leqslant A^{(n)} \leqslant E\,\frac{n+1}{x}$$

and $$E\frac{n+1}{y}-1 \leqslant B^{(n)} \leqslant E\frac{n+1}{y}$$

whence, $A^{(n)} > \frac{n+1}{x} - 2$, $B^{(n)} \leqslant \frac{n+1}{y}$;

hence $A^{(n)} - B^{(n)} > (n+1)\frac{y-x}{xy} - 2$

so that we have

$$\lim_{n=\infty} (A^{(n)} - B^{(n)}) = +\infty$$

which is contradictory to the inequality $|A^{(n)} - B^{(n)}| \leqslant q$ for $n = 1, 2, \ldots$ shown above under the assumption that $A \overset{f}{=} B$. Thus the sets A and B cannot be equivalent by finite decomposition and this proves the theorem **18**.

It is to be observed, that *one can name a family F of power $2^{\aleph_0}$ of linear enumerable sets such that none of them is equivalent by finite decomposition to a subset of another one*[1]. This theorem is an immediate corollary of the

Theorem 18.* *There exists a family F (of the power of the continuum) of distinct infinite sets of positive integers, such that if $E \in F$, $H \in F$, $E \neq H$ and if E_1 and H_1 are infinite sets such that $E_1 \subset E$ and $H_1 \subset H$, then $E_1 \overset{f}{=} H_1$ is not true.*

Proof. Let $N(x)$ denote the set of all the numbers

1) W. Sierpiński, Annals of Math. 48 (1947) p. 642.

$2^{2^n}(2Enx+1)$ for x real and $\geqslant 1$, where $n=1,2,\ldots$.

Let x and y be two distinct real numbers and E_1 and H_1 two infinite sets such that $E_1 \subset N(x)$ and $H_1 \subset N(y)$, and let us suppose that $E_1 \underset{=}{f} H_1$.

There exists a positive integer m such that $E_1 \underset{m}{=} H_1$. Therefore there exist sets $A_1, A_2, \ldots, A_m$ and $B_1, B_2, \ldots, B_m$ such that

$$E_1 = A_1 + A_2 + \ldots + A_m, \quad H_1 = B_1 + B_2 + \ldots + B_m,$$

$$A_k A_l = B_k B_l = 0 \text{ for } 1 \leqslant k < l \leqslant m, \text{ and}$$

$$A_k \cong B_k \text{ for } k = 1, 2, \ldots.$$

As the set E_1 is infinite, one at least of the sets $A_1, A_2, \ldots, A_m$, for instance the set A_1, is infinite. Therefore there exist two points

$$p_1 = 2^{2^{n_1}}(2En_1x+1) \text{ and } p_2 = 2^{2^{n_2}}(2En_2x+1) \text{ of } A_1$$

such that

$$(1) \qquad n_1 > n_2 > \frac{1}{|x-y|}$$

As $A_1 \cong B_1$, there correspond to points p_1 and p_2 of A_1 two points of B_1,

$$q_1 = 2^{2^{n_3}}(2En_3y+1) \text{ and } q_2 = 2^{2^{n_4}}(2En_4y+1)$$

such that

$$p_1 - p_2 = q_1 - q_2$$

(because two congruent infinite sets of positive integers are superposable by translation).
Then

$$2^{2^{n_2}(2En_2x+1)}\left(2^{2^{n_1}(2En_1x+1)-2^{n_2}(2En_2x+1)}-1\right)$$

$$=2^{2^{n_4}(2En_4y+1)}\left(2^{2^{n_3}(2En_3y+1)-2^{n_4}(2En_4y+1)}-1\right)$$

which gives at once

$$2^{2^{n_2}(2En_2x+1)}=2^{2^{n_4}(2En_4y+1)},$$

thus $n_2=n_4$ and $2En_2x+1=2En_4y+1$, then $En_2x=En_4y$ and $|n_2x-n_2y|<1$;

thus $$n_2<\frac{1}{|x-y|},$$

which is contradictory to (1).

Therefore the formula $E \underset{=}{f} H$ cannot be true. Now it is easily seen that the family F of all the sets $N(x)$, where $x \geqslant 1$, possesses the required property. The proof of the theorem **18*** is therefore completed.

7. We say that a set of points E admits a *paradoxical decomposition* if it is the sum of two disjoint sets, each of which is equivalent to E by finite decomposition.

Theorem 19:—*No linear set (not empty) admits a paradoxical decomposition*[1] .

Lemma. *Suppose r and s are two positive integers. If $u_1, u_2, \ldots, u_r$ are r given real numbers then the number of all the distinct sums formed of s terms (equal or unequal), each of which is one of the numbers $u_1, u_2, \ldots, u_r$ is $\leqslant (s+1)^r$.*

Indeed, each of the above mentioned sums is defined, when for each $i = 1, 2, \ldots, r$, the number n_i of terms equal to u_i that it contains, is known. Now each of the numbers $n_1, n_2, \ldots, n_r$ is evidently $\geqslant 0$ and $\leqslant s$. The number of all the distinct systems of numbers $n_1, n_2, \ldots, n_r$ is therefore $\leqslant (s+1)^r$. So we can consider our lemma as proved.

Suppose next that the linear nonempty set E admits of a paradoxical decomposition $E = A + B$. Then $AB = 0$ and there exist two positive integers p and q such that $E \underset{p}{=} A$ and $E \underset{q}{=} B$. Thus there exists a decomposition of the sets E, A and B into sums of disjoint sets:

$$E = E_1 + E_2 + \ldots + E_p, \quad A = A_1 + A_2 + \ldots + A_p$$

$$E = E'_1 + E'_2 + \ldots + E'_q, \quad B = B_1 + B_2 + \ldots + B_q,$$

where $E_i \cong A_i$ for $i = 1, 2, \ldots, p$ and $E_i' \cong B_i$ for $i = 1, 2, \ldots, q$.

1) W. Sierpiński, Actas Acad. Nac. Ciencias, Lima, Vol. 11, (1946).

Let ϕ_i (for $i=1, 2, ..., p$) be the transformation of E_i into A_i realizing the congruence $E_i \cong A_i$ and let ψ_i (for $i=1, 2, ..., q$) denote the transformation of E_i' into B_i realizing the congruence $E_i' \cong B_i$. We put

(1) $\phi(x)=\phi_i(x)$ for $x \in E_i$, $(i=1, 2, ..., p)$

and

(2) $\psi(x)=\psi_i(x)$ for $x \in E_i'$, $(i=1, 2, ..., q)$.

As the sets $A_1, A_2, ..., A_p$ are disjoint, the function $\phi(x)$ transforms the set E into A in a reciprocal univocal way and similarly the function $\psi(x)$ transforms in a reciprocal univocal way the set E into B. As the set E is not empty, there exists an element $x_0 \in E$ and it is easily seen that we may suppose without detriment to the generality of our demonstration that $x_0=0$. Thus we have $0 \in E$, hence $\phi(0) \in A$ and $\psi(0) \in B$; therefore $\phi(0) \neq \psi(0)$ since $AB=0$. Considering that the function ϕ (or ψ) possesses distinct values in E we have $\phi\phi(0) \neq \phi\psi(0)$ and $\psi\phi(0) \neq \psi\psi(0)$. Now we have for $x \in E$, $y \in E$: $\phi(x) \in A$, $\psi(y) \in B$; thus (since $AB=0$) $\phi(x) \neq \psi(y)$ and in particular

$$\phi\phi(0) \neq \psi\phi(0), \quad \phi\phi(0) \neq \psi\psi(0),$$

$$\phi\psi(0) \neq \psi\phi(0) \text{ and } \phi\psi(0) \neq \psi\psi(0).$$

Thus the numbers $\phi\phi(0)$, $\phi\psi(0)$, $\psi\phi(0)$ and $\psi\psi(0)$ are all distinct. An easy induction shows that if s is a given positive integer, the 2^s numbers

(3) $$\theta_1\theta_2 \dots \theta_s(0)$$

are all distinct where θ_i for $i=1, 2, \dots, s$ is one of the functions ϕ or ψ.

Suppose i is a number of the sequence 1, 2, ..., p. If the function ϕ_i realizes the congruence $E_i \cong A_i$ there exists a real number a_i such that

$$\phi_i(x) = \pm x + a_i \qquad \text{for } x \in E_i.$$

According to (1) there exists for each number x of E a number $i(x)$ of the sequence 1, 2, ..., p such that $\phi(x) = \pm x + a_{i(x)}$. Similarly there exist q real numbers $b_1, b_2, \dots, b_q$ and for each number x of E a number $j(x)$ of the sequence 1, 2, ..., q such that $\psi(x) = \pm x + b_{j(x)}$. It results from it at once that each number of (3) is of the form

(4) $$c_1 + c_2 + \dots + c_s,$$

where every c_i ($i=1, 2, \dots, s$) is one of the r ($=2p+2q$) numbers $\pm a_1, \pm a_2, \dots, \pm a_p, \pm b_1, \pm b_2, \dots, \pm b_q$. As the numbers (3) are different it may be deduced, according to the lemma (considering that (3) is of the form (4)) that $2^s \leqslant (s+1)^r$. Now it is known that this inequality is false for s sufficiently great (since $\lim_{s=\infty} (s+1)^r 2^{-s} = 0$ for r is a positive integer).

So the hypothesis that the set E admits of a paradoxical decomposition implies a contradiction. The theorem **19** is therefore proved.

It should be observed that the theorem **19** does not apply to plane sets. For plane sets we have the following

Theorem 20.—*There exists a plane set which is the sum of two disjoint sets, each of which is congruent with it.*

An example of such a set has been given by the late *S. Mazurkiewicz* and myself in 1914[1]. Suppose ϕ is the translation of the plane through the length 1 along the axis of abscissas and ψ the rotation of the plane around the point O through the angle equal to 1 radian (*i.e.*, $=(180/\pi)^\circ$). Let E be the set formed of the point O and of each point obtained from O by the use of the transformations ϕ and ψ a finite number of times in an arbitrary successiveness. Let $A=\phi(E)$, $B=\psi(E)$. Since evidently $A \cong E$, $B \cong E$, and $A \subset E$, $B \subset E$, it remains to prove that $AB=0$. It should be remarked by the way that the transformations ϕ and ψ are expressed in the plane of complex numbers by the formulae

$$\phi(z) = z+1 \text{ and } \psi(z)=e^i z$$

It results from it that each point p of E is a

[1]) C. R. Paris, t. 158, p. 618 (Séance du 2 mars 1914).

polynomial in e^i having integral coefficients. Moreover its constant term is positive, if p belongs to A and nul, if p belongs to B. If therefore A and B had a common point, we should have an algebraical equation in e^i having as coefficients nonidentical integers, and that is impossible taking into consideration that e^i is a transcendental number.

It may be proved that a plane set, which is the sum of two disjoint sets, each of which is congruent with it, cannot be bounded[1]. We shall see later on that there exist bounded sets in space of 3 dimensions which possess this property.

It should still be observed that it may be proved that *for each* $m \leqslant 2^{\aleph_0}$ *there exists a plane set which can be decomposed into* m *disjoint parts superposable with it*[2].

8 **Theorem 21**. *The set* $I_1 = [0 \leqslant x < 1]$ *is a sum of an enumerable infinity of disjoint sets each two of which are* $\underset{2}{=}$ [3].

Proof. Let us divide all the numbers of I_1 into classes putting two numbers of I_1 in the same class if and only if their difference is a rational

[1]) A. Lindenbaum, Fund. Math. 8, p. 218

[2]) W. Sierpinski, Fund. Math. 34, p. 9.

[3]) F. Hausdorff, Grundzüge der Mengenlehre, Leipzig 1914, p. 401.

number. Thus one gets a decomposition of I_1 into $2^{\aleph_0}$ enumerable disjoint classes. Let N denote a set containing one and only one number of each class. (Such a set N exists according to the Zermelo's axiom). Now, let r be a rational number $0 \leqslant r < 1$ and let us denote by $N[r]$ the set of all the numbers $x+r-E(x+r)$ where $x \epsilon N$. We evidently have $N[r] \epsilon I_1$. Let $y \epsilon I_1$. There exists, in view of the definition of N, an $x \epsilon N$ and a rational number r with $0 \leqslant r < 1$ such that $y - x = \pm r$. If $y - x = r$, we obtain $y = x + r$, and considering that $y \epsilon I_1$, $Ey = 0$, i.e., $E(x + r) = 0$, and $y = x + r - E(x + r)$, we have $y \epsilon N[r]$. If $y - x = -r$, where $r > 0$, we have $y = x - r$ and taking into consideration that $y \epsilon I_1$, $E(x-r) = 0$ and $y = x + 1 - r - E(x + 1 - r)$ we get $y \epsilon N[1-r]$, where $0 < 1-r < 1$. Consequently we have $I_1 = \sum_r N[r]$, where the summing is extended to all the rational numbers r, where $0 \leqslant r < 1$.

Now if r_1 and r_2 denote two rational numbers, $0 \leqslant r_1 < 1$, $0 \leqslant r_2 < 1$, $r_1 \neq r_2$, and if we suppose that $N[r_1]\, N[r_2] \neq 0$, then there exists a number y such that $y \epsilon N[r_1]$ and $y \epsilon N[r_2]$. According to the definition of the sets $N[r]$, there exist two real number x_1 and x_2 such that $x_1 \epsilon N$, $x_2 \epsilon N$, $y = x_1 + r_1 - E(x_1 + r_1)$, $y = (x_2 + r_2) - E(x_2 + r_2)$; whence $x_1 - x_2 = r_2 - r_1 + E(x_1 + r_1) - E(x_2 + r_2)$.

So the number $x_1 - x_2$ is rational and implies, as $x_1 \epsilon N$ and $x_2 \epsilon N$ (according to the definition of N), that $x_1 = x_2$; hence $r_1 - r_2 = E(x_1 + r_1) - E(x_2 + r_2)$. Therefore the number $r_1 - r_2$ is an integer, which is impossible, since $0 \leqslant r_1 < 1$, $0 \leqslant r_2 < 1$ and $r_1 \neq r_2$. Thus the terms of the sum $I_1 = \sum_r N[r]$ are disjoint sets.

Now suppose that r is a rational number, $0 \leqslant r < 1$. Let $N_1[r]$ denote the set of all the numbers x of N satisfying $x < 1 - r$ and let us put $N_2[r] = N - N_1[r]$. So the set N is the sum of two disjoint sets: $N = N_1[r] + N_2[r]$. We denote by $N_3[r]$ or by $N_4[r]$ the set of all the numbers $x + r - E(x + r)$ of $N[r]$ according as $x \epsilon N_1[r]$ or $x \epsilon N_2[r]$. We shall certainly have $N[r] = N_3[r] + N_4[r]$. Since for $x \epsilon N_1[r]$, we have $x < 1 - r$ (according to the definition of $N_1[r]$), therefore $0 \leqslant x + r < 1$ and $E(x + r) = 0$. $N_3[r]$ is the set of all the numbers $x + r$ where $x \epsilon N_1[r]$ *i.e.*, $N_3[r]$ is a translation of $N_1[r]$ through the length r. Now since for $x \epsilon N_2[r]$ we have $x \geqslant 1 - r$, then $1 \leqslant x + r < 2$ (since $x < 1$ and $r < 1$), whence $E(x + r) = 1$; $N_4(r)$ is the set of all the numbers $x + r - 1$, where $x \epsilon N_2[r]$ *i.e.*, $N_4[r]$ is a translation of $N_2[r]$ through the length $r - 1$. It gives $N_3[r] \cong N_1[r]$ and $N_4[r] \cong N_2[r]$.

If $N_3[r].N_4[r] \neq 0$ there would exist (according to the definition of $N_3[r]$ and $N_4[r]$)

two numbers $x_1 \in N_1[r]$ and $x_2 \in N_2[r]$ such that $x_1 + r - E(x_1 + r) = x_2 + r - E(x_2 + r)$ and the number $x_1 - x_2$ would be rational, hence (as $N_1[r] + N_2[r] \overset{=}{_2} N$) $x_1 = x_2$. This is impossible, since $N_1[r]\,N_2[r] = 0$. So the sets $N_3[r]$ and $N_4[r]$ are disjoint. Therefore we have for r rational, $0 \leqslant r < 1$:

$$\begin{aligned} N &= N_1[r] + N_2[r], & N_1[r]\,N_2[r] &= 0, \\ N[r] &= N_3[r] + N_4[r], & N_3[r]\,N_4[r] &= 0, \\ N_3[r] &\cong N_1[r], & N_4[r] &\cong N_2[r], \end{aligned}$$

and finally $N[r] \overset{=}{_2} N$. So I_1 is the sum of $\aleph_0$ disjoint sets, each of which is $\overset{=}{_2} N$. Thus the proof of theorem **21** is completed.

It should be observed that Prof. J. von *Neumann* has proved[1] that I_1 *is the sum of* $\aleph_0$ *disjoint sets two by two congruent* and the same applies to the closed interval $I = (0 \leqslant x \leqslant 1)$ and the open interval $(0 < x < 1)$. The demonstration, however, making use of the Zermelo's axiom, is rather long.

The set I_1 is evidently the sum of two sets disjoint and congruent ($[\,0 \leqslant x < \frac{1}{2}\,]$ and $[\,\frac{1}{2} \leqslant x < 1\,]$). Now it may be proved that a closed interval I is not a sum of two disjoint and congruent sets.

In 1924 the late S. Ruziewicz has proved (making use of the Zermelo's axiom but not admitting

1) Fund. Math. 11, p. 230.

the continuum hypothesis) that for each cardinal number $m \leqslant 2^{\aleph_0}$ the straight line is the sum of m disjoint sets two by two congruent [1]).

The sets into which S. Ruziewicz decomposes the straight line are not measurable in the Lebesgue meaning. A decomposition of the straight line into m (where $\aleph_0 \leqslant m < 2^{\aleph_0}$) disjoint and congruent (measurable or not) sets may be obtained in an easier way as follows.

Let E denote an arbitrary set of real positive numbers of the power m and let H be the set of all the numbers, which are sums of a finite number of numbers the absolute value of which belongs to E. It may be easily proved that $\overline{\overline{H}} = m$. Now we divide all the real numbers into classes, putting two real numbers into the same class if and only if their difference belongs to H. Let N be the set containing one and only one number of each of these classes. If a is a real number, we denote by $N(a)$ the translation of N by the length a. It is easily verified that the straight line is a sum of m disjoint congruent sets $N(a)$ where $a \in H$. *Admitting the continuum hypothesis it may be proved that there exists a plane set E such that the plane is a sum of $2^{\aleph_0}$ disjoint sets, each congruent with E*[2]),

1) Fund. Math., 5, p. 92.

2) Fund. Math. 21, p. 39.

and that at the same time the plane is the sum of an enumerable infinity of sets, each congruent with E[1]).

Now, if m is a given cardinal number and if the straight line is the sum of m disjoint sets congruent by translation with any set E, the straight line is not the sum of less than m sets congruent by translation or rotation with E[2]).

Let us point out that the following proposition may be proved with the admission of the hypothesis of the continuum:

The straight line is the sum of $2^{\aleph_0}$ *disjoint sets, each of which is equivalent to the straight line by enumerable decomposition* [3]).

Two sets of points A and B are said to be *equivalent by enumerable decomposition* and are denoted by $A \overset{d}{=} B$ if there exist two infinite sequences of sets $A_1, A_2, \ldots$ and $B_1, B_2, \ldots$ fulfilling the three following conditions: 1° $A = A_1 + A_2 + \ldots$ and $B = B_1 + B_2 + \ldots$, 2°. $A_k A_l = 0$ and $B_k B_l = 0$ for $k \neq l$, 3° $A_k \cong B_k$ for $k = 1, 2, \ldots$.

---

1) Fund, Math. 21, p. 39, and W. Sierpiński, Hypothèse du continu (Warszawa 1934, Monografje Matematyczne Vol. 4), p. 100 Proposition C_{48},

2) Fund, Math. 24, p. 247.

3) W. Sierpiński, Mathematica 23 (1947-48), p. 52.

9. Theorem 22. *If $A \supset E \supset B$ and $A \underset{n}{=} B$, then $A \underset{n+1}{=} E$.* [1]

Proof. According to $A \underset{n}{=} B$ there exist sets A_1, $A_2, \dots, A_n$ and $B_1, B_2, \dots, B_n$ such that

1° $A = A_1 + A_2 + \dots + A_n$, $B = B_1 + B_2 + \dots + B_n$,

2° $A_k A_l = B_k B_l = 0$ for $1 \leqslant k < l \leqslant n$,

and 3° $A_k \cong B_k$ for $k = 1, 2, \dots, n$.

It results from 3° that there exists for $k = 1, 2, \dots, n$, an isometric transformation (*i.e.*, conserving distances between two points) ϕ_k of the set A_k into B_k, *i.e.*,

$$(1) \quad B_k = \phi_k(A_k).$$

We put

$$(2) \quad \phi(x) = \phi_k(x) \text{ for } x \in A_k \ (k = 1, 2, \dots, n)$$

The function ϕ evidently transforms the set A into the set B in a reciprocal univocal way, and we shall say that it *realizes* the equivalence $A \underset{n}{=} B$. Thus we have $\phi(A) = B \subset A$ and generally $\phi^k(A) \subset A$ for $k = 1, 2, \dots$, so that $\phi^k(A - E) \subset A$ all the more for $k = 1, 2, \dots$. We put

$$(3) \quad A' = (A - E) + \phi(A - E) + \phi^2(A - E) + \phi^3(A - E) + \dots.$$

---

[1] S. Banach and A. Tarski, Fund, Math. 6, p. 252, Cerol. 9 ; A. Lindenbaum and A. Tarski, Comptes Rendus des séances de la Soc. des Sc. et L. de Varsovie, XIX, cl. III (1926), p. 328, Th, 9. W. Sierpiński, Fund. Math. 33 (1945), p. 230 (Lemma 1).

The set A' might have been defined without the use of an infinite series of sets, simply as the common part of all the subsets X of A verifying $A-E \subset X$ and $\phi(X) \subset X$.

We have $A' \subset A$. We put

(4) $A''=A-A'$

(5) $E'=\phi(A')$

According to (4) and $A' \subset A$, we have

(6) $A=A'+A''$ and $A'A''=0$.

It follows from (5), $A' \subset A$ and $\phi(A)=B \subset E$, that $E'=\phi(A') \subset \phi(A)=B \subset E$ and consequently

(7) $E' \subset E$.

The formula (3) gives

$\phi(A')=\phi(A-E)+\phi^2(A-E)+\phi^3(A-E)+\ldots$

and according to (3), (5) and (7):

(8) $A'=(A-E)+\phi(A')$

$=(A-E)+E'=A-(E-E')$

which, on considering $E \subset A$ and (4), gives $E-E'=A-A'=A''$. Hence

(9) $E=E'+A''$ and $E'A''=0$.

According to (6) we have $A=A'A+A''$ and it follows from 1° and 2° that the decomposition of A into $n+1$ disjoint sets is

(10) $A = A'A_1 + A'A_2 + \dots + A'A_n + A''$

As the function ϕ has distinct values in A we have from (6), (5) and (1),

(11) $\phi(A'A_k) = \phi(A') . \phi(A_k) = E'B_k$
for $k = 1, 2, \dots, n$.

Now, according to (2) we have $\phi(A'A_k) = \phi_k(A'A_k)$; as the function ϕ_k is an isometric transformation (of A_k into B_k) we also have $\phi(A'A_k) \cong A'A_k$, hence, according to (11):

(12) $A'A_k \cong E'B_k$ for $k = 1, 2, \dots, n$.

From 2° the sets $E'B_k (k = 1, 2, \dots, n)$ are disjoint.

The formula (7) and $E \subset B$ give $E' \subset B$, hence $E' = E'B$ and according to 1° and (9):

$$E - E'(B_1 + B_2 + \dots + B_n) = E - E'B = E - E' = A''.$$

Thus

(13) $E = E'B_1 + E'B_2 + \dots + E'B_n + A''$,

and from 2° and (9) the terms of this decomposition are disjoint sets.

We obtain $A \underset{n+1}{=} E$ from (10), (12) and (13).

Therefore the theorem **22** is proved. From this at once follows the

Corollary. *If $A \supset E \supset B$ and $A \underset{f}{=} B$, then $A \underset{f}{=} E$.*

In particular, the theorem **22** gives (for $n=1$):

(14) *If $A \supset E \supset B$ and $A \cong B$ then $A \underset{2}{=} E$.*

It should be observed that the equivalence $A \underset{2}{=} E$ cannot be here substituted by the congruence $A \cong B$. Indeed, if $A = \underset{x}{E}[x \geqslant 0]$,[1] $B = \underset{x}{E}[x \geqslant 1]$, $E = B + \{0\}$ then $A \cong B$, $A \supset E \supset B$ and A is not$\cong E$.

Theorem 23. *If $A \underset{n}{=} B$ and $B \underset{m}{=} C$ then $A \underset{mn}{=} C$*[2]

Proof. It results from $A \underset{n}{=} B$ that there exist decompositions 1° fulfilling the conditions 2° and 3°. From $B \underset{m}{=} C$ it results that there exist decompositions

$$(15) \quad \begin{aligned} &B = B_1' + B_2' + \ldots + B'_m \text{ and} \\ &C = C_1 + C_2 + \ldots + C_m. \end{aligned}$$

such that

(16) $B_k' B_l' = C_k C_l = 0$ for $1 \leqslant k < l \leqslant m$

and

(17) $B_l' \cong C_l$ for $l = 1, 2, \ldots, m$.

We put

---

[1]) $\underset{x}{E}[P(x)]$ denotes the set of all the real numbers fulfilling the condition $P(x)$.

[2]) S. Banach and A. Tarski, Fund. Math, 6 p. 246-248 (Th. 3).

(18) $B_{k,l} = B_k B_l'$ for $1 \leqslant k \leqslant n$ and $1 \leqslant l \leqslant m$

According to 1°, (15) and (18) we have

(19) $B_k = B_{k,1} + B_{k,2} + \dots + B_{k,m}$ for $1 \leqslant k \leqslant n$ an

(20) $B_l' = B_{1,l} + B_{2,l} + \dots + B_{n,l}$ for $1 \leqslant l \leqslant m$.

Now it follows from (18), 2° and (16), that for $k, k_1 = 1, 2, \dots, n$; $l, l_1 = 1, 2, \dots, m$,

(21) $B_{k,l}\ B_{k_1,l_1} = 0$ when $k \neq k_1$ or $l \neq l_1$

According to 3°, (19), 2° and (21) there exist for $k = 1, 2, \dots, n$, decompositions

(22) $A_k = A_{k,1} + A_{k,2} + \dots + A_{k,m}$

such that for $1 \leqslant k \leqslant n$, $1 \leqslant k_1 \leqslant n$, $1 \leqslant l \leqslant m$, $1 \leqslant l_1 \leqslant m$

we have

(23) $A_{k,l}\ A_{k_1,l_1} = 0$ when $k \neq k_1$ or $l \neq l_1$

and

(24) $A_{k,l} \cong B_{k,l}$ for $1 \leqslant k \leqslant n$, $1 \leqslant l \leqslant m$.

Similarly it results from (17), (20), (16) and (21) that there exist for $l = 1, 2, \dots, m$ decompositions

(25) $C_l = C_{1,l} + C_{2,l} + \dots + C_{n,l}$

such that

(26) $C_{k,l}\ C_{k_1,l_1} = 0$ when $k \neq k_1$ or $l \neq l_1$,

and

(27) $B_{k,l} \cong C_{k,l}$ for $1 \leqslant k \leqslant n$, $1 \leqslant l \leqslant m$.

The formulae 1°, (15), (22) and (25) give

$$(28)\quad A = \sum_{k=1}^{n} \sum_{l=1}^{m} A_{k,l}\,,\; C = \sum_{l=1}^{m} \sum_{k=1}^{n} C_{k,l}$$

and since from (24) and (27), we have

$$A_{k,l} \cong C_{k,l} \text{ for } k=1,2,\ldots,n,\; l=1,2,\ldots,m,$$

the formula (28), (23) and (26) prove that $A \underset{mn}{\equiv} C$, which was to be demonstrated.

It should be mentioned that it is not possible to replace in theorem **23** the product mn by a smaller number. If indeed $A=\{1, 2, \ldots, mn\}$, B is the set of all the numbers $kmn+l$, where $k=1, 2, \ldots, n$; $l=1, 2, \ldots, m$, and if $C=\{mn, 2mn, \ldots, (mn)^2\}$ then it may be easily seen that $A \underset{n}{=} B$, $B \underset{m}{=} C$ and $A \underset{k}{=} C$ does not hold for any positive integer $k < mn$.

The theorem **23** implies the following

Corollary. *If $A \overset{f}{=} B$ and $B \overset{f}{=} C$ then $A \overset{f}{=} C$.*

Thus *the relation $\overset{f}{=}$ is transitive.*

Theorem 24. *If $A \overset{f}{=} B_1 \subset B$ and $B \overset{f}{=} A_1 \subset A$ then $A \overset{f}{=} B$.*

Proof. Let ϕ (and ψ) be the function realizing the equivalence $A \overset{f}{=} B_1$, (and $B \overset{f}{=} A_1$); thus $\phi(A) = B_1$ and $\psi(B) = A_1$.

We put $\psi[\phi(A)]=A_2$. As $\phi(A)=B_1 \subset B$ the function ψ realizes the equivalence $B_1 \overset{f}{=} A_2$, and since $A \overset{f}{=} B_1$ it results from the corollary that $A \overset{f}{=} A_2$. Now as $A_2=\psi(B_1) \subset \psi(B)=A_1 \subset A$, the equivalence $A \overset{f}{=} A_2$ gives according to the corollary of the theorem **22** that $A \overset{f}{=} A_1$ and from $B \overset{f}{=} A_1$ and the corollary of the theorem **23**, we see that $A \overset{f}{=} B$, which was to be proved.

It is to be observed that a slight modification of the proof of the theorem would lead to the theorem that

If $A \underset{n}{=} B_1 \subset B$ and $B \underset{m}{=} A_1 \subset A$, then $A \underset{m+n}{=} B$.[1]

Theorem 25. *A segment of the straight line is not equivalent by finite decomposition to any smaller segment.*

Proof. Let us admit that a segment of the straight line of length d is $\overset{f}{=}$ to a segment of a smaller length ad where $0<a<1$. It obviously results from it that if l is an arbitrary positive number then each segment of the length l is $\overset{f}{=}$ to a segment of the length al and therefore, according to the corollary of theorem **23**, also to a segment of the length $a^k l$, where $k=1, 2, \ldots$. As

[1]) This theorem has been announced by A. Lindenbaum and A. Tarski in 1926 without proof (l.c., p. 328, theorem 8).

$0<a<1$ there exists a positive integer k such that $0<a^k<\frac{1}{2}$. Thus each segment is $\overset{f}{=}$ to a segment contained in its half. It follows from it, according to the corollary of theorem **22** that each segment is $\overset{f}{=}$ to its half, the centre of the segment being counted or not. Now, this is inconsistent with theorem **19.** So the proof of theorem **25** is completed.

It should be observed that the word "segment" in the theorem **25** could be replaced by "square", the demonstration, however, would be much more complicated.

There exist theorems concerning the equivalence by finite decomposition, the wording of which is simple and the demonstration difficult. To this class belongs the following theorem of D. König and S.Valko'[1]):

If for a positive integer m there exist two decompositions of a linear set into m disjoint sets $A_1+A_2+\ldots+A_m=B_1+B_2+\ldots+B_m$, where $A_i \cong A_k$ and $B_i \cong B_k$ for $1 \leqslant i \leqslant m$ and $1 \leqslant k \leqslant m$, then $A_1 \underset{m^2}{=} B_1$. The proof is difficult even for $m=3$.

Generalizing the notion of equivalence by finite decomposition, the equivalence of sets by decom-

[1]) Fund. Math. **8**, p. 131. For $m=2$ see C. Kuratowski, Fund. Math. **6** p.236, and for $m=2^n$ see S. Banach and A, Tarski, Fund. Math. **6** p. 254.

position into m sets could be considered, where m denotes a cardinal number satisfying $\aleph_0 \leqslant m \leqslant 2^{\aleph_0}$.[1] We shall cite without demonstration the following theorem :

One can name a family ϕ of the power $2^{2^{\aleph_0}}$ of linear sets, such that for $m < 2^{\aleph_0}$ two distinct sets of the family ϕ are never equivalent by decomposition into m sets[2].

10. *The Hausdorff's paradox.*

Theorem 26.[3] *The surface S of the sphere is the sum of four disjoint sets A, B, C, D where D is an enumerable set and $A \cong B \cong C \cong B + C$.*

Proof. Let Ψ and Φ denote two axes passing through the centre O of the sphere S and $\frac{1}{2}\nu$ the angle between these axes ; this angle will be fixed later. ϕ denotes the rotation around the axis Φ by the angle $\pi (= 180°)$ and ψ the rotation around the axis Ψ by the angle $\frac{2}{3}\pi$ $(=120°)$. Evidently $\phi^2 = \psi^3 = 1$, where 1 indicates the identical transformation of the three-dimensional space R_3 into itself.

Let G be the set of all the transformations of R_3 into itself, obtained by the application of

---

1) See P. Erdös, Annals of Math. 44 (1943), p. 644

2) See W. Sierpinski, Annals of Math. 48 (1947), p. 641.

3) F. Hausdorff, Grundzüge der Mengenlehre, Leipzig 1914, pp. 469-472.

the transformations ϕ and ψ a finite number of times in arbitrary successiveness. (It is easily seen that G forms a group of transformations). Since $\phi^2 = \psi^3 = 1$, on writing the transformations which form G as products of a finite number of transformations ϕ and ψ, we shall be able to substitute each factor ϕ^m by the factor ϕ^r, where r is the remainder in the division of the number m by 2, and each factor ψ^m by $\psi^{r'}$, where r' is the remainder in the division of m by 3 (*e.g.*, $\phi^5 = \phi$, $\psi^5 = \psi^2$, $\phi^6 = \psi^6 = 1$). Consequently G will be formed from the identical transformation 1 and from transformations which are products of a finite number of factors ϕ, ψ and ψ^2 – let us call them fundamental factors – the factor ϕ being never followed by itself, while the factors ψ or ψ^2 are never preceded by the factors ψ nor by the factor ψ^2.

It should be pointed out that the transformations ϕ and ψ are not commutable: that is $\phi\psi \neq \psi\phi$ *i.e.*, there exist points p of R_3 such that $\phi(\psi(p)) \neq \psi(\phi(p))$. For instance it may be easily seen that it is true for each point p of the axis Φ different from O. So the group G does not form an abelian group.

In order to write systematically all the transformations forming G we divide them into classes, putting in the class G_n all those which are products of n fundamental factors and the identical transformation 1 constituting the class G_0. Thus the class G_1 will be formed by three transformations ϕ, ψ, ψ^2. It is readily verified that in order to obtain the class G_{n+1} from the class G_n it is sufficient to multiply (from the left) the transformations of G the first factor of which is ϕ, by ψ and by ψ^2, while those transformations the first factor of which is ψ or ψ^2, by ϕ.

Thus from $G_1=\{\phi, \psi, \psi^2\}$ we obtain that $G_2=\{\psi\phi, \psi^2\phi, \phi\psi, \phi\psi^2\}$.

Now from G_2, $G_3=\{\psi\phi\psi, \psi^2\phi\psi, \psi\phi\psi^2, \psi^2\phi\psi^2, \phi\psi\phi, \phi\psi^2\phi\}$, and from G_3 we have $G_4=\{\psi\phi\psi\phi, \psi^2\phi\psi\phi, \psi\phi\psi^2\phi, \psi^2\phi\psi^2\phi, \phi\psi\phi\psi, \phi\psi^2\phi\psi, \phi\psi\phi\psi^2, \phi\psi^2\phi\psi^2\}$.

(It may be calculated that for $n=1, 2, \ldots$ G_n contains $2^{E\frac{n}{2}}+2^{E\frac{n+1}{2}}$ transformations, namely $2^{E\frac{n}{2}}$ transformations the first factor of which is ϕ and $2^{E\frac{n+1}{2}}$ the first factor of which is ψ or ψ^2).

Now we arrange all the transformations of G in an infinite sequence, writing successively the transformations of the classes G_1, G_2, G_3,... :

(G) 1 ; ϕ, ψ, ψ^2 ; $\psi\phi$, $\psi^2\phi$, $\psi\phi$, $\phi\psi^2$;....

We shall prove that the angle between the axes Φ and Ψ can be chosen in such a way that all the transformations of this sequence should be distinct. Above all we notice that, except for the first, each transformation of G has one of the four forms

(1) $\alpha = \psi^{m_1}\phi\,\psi^{m_2}\phi\ldots\psi^{m_n}\phi$

(2) $\beta = \phi\psi^{m_1}\phi\psi^{m_2}\ldots\phi\psi^{m_n}$

(3) $\gamma = \phi\psi^{m_1}\phi\psi^{m_2}\ldots\phi\psi^{m_n}\phi$

(4) $\delta = \psi^{m_1}\phi\psi^{m_2}\phi\ldots\phi\psi^{m_n},$

where n is a positive integer (excepting the case $\gamma=\phi$) and the power exponents $m_1, m_2, \ldots, m_n$ are equal to 1 or 2.

We denote by $\frac{1}{2}\nu$ the angle between the axes Φ and Ψ. We take the axis Ψ as the axis OZ (in a rectangular system of co-ordinates) and the plane containing the axis Φ as the plane XZ. Let $N=(x, y, z)$ be a given point of the space R_3 and $\psi(N)=(x', y', z')$.

On applying the well known formulae of transformation of co-ordinates we at once get

$$(\psi)\quad \begin{cases} x' = x\lambda - y\mu \\ y' = x\mu - y\lambda \\ z' = z \end{cases}$$

where we have put for abbreviation $\lambda = \cos\frac{2}{3}\pi = -\frac{1}{2}$, $\mu = \sin\frac{2}{3}\pi = \frac{\sqrt{3}}{2}$.

Considering that $\psi^2 = \psi^{-1}$ is the rotation around the axis Ψ through the angle $-\frac{2}{3}\pi$, and putting $\psi^2(N) = (x', y', z')$ where $N = (x, y, z)$, we obtain the formulae

$$(\psi^{-1}) \quad \begin{cases} x' = x\lambda + y\mu \\ y' = -x\mu - y\lambda \\ z' = z. \end{cases}$$

The formulae (ψ) and (ψ^{-1}) may be written together as follows

$$(\psi^{\pm 1}) \quad \begin{cases} x' = x\lambda \mp y\mu \\ y' = \pm x\mu - y\lambda \\ z' = z. \end{cases}$$

Now putting $\phi(N) = (x', y', z')$ for $N = (x, y, z)$, we obtain

$$(\phi) \quad \begin{cases} x' = -x \cos \nu + z \sin \nu \\ y' = -y \\ z' = x \sin \nu + z \cos \nu. \end{cases}$$

We put $\psi^{\pm 1}\phi(N) = (x', y', z')$ for $N = (x, y, z)$; the formulae (ϕ) and $(\psi^{\pm 1})$ give immediately

$$(\psi^{\pm 1}\phi) \quad \begin{cases} x' = -x\lambda \cos \nu \pm y\mu + z\lambda \sin \nu \\ y' = \mp x\mu \cos \nu + y\lambda \pm z\mu \sin \nu \\ z' = x \sin \nu + z \cos \nu. \end{cases}$$

Now, let α be a transformation of G given by the form (1). We put $\alpha(N) = (\xi, \eta, \zeta)$ for $N = (0, 0, 1)$. I say that we shall obtain the formulae

$$(a)\quad \begin{cases} \xi = \sin\nu\,[\,a\cos^{n-1}\nu + \dots\,] \\ \eta = \sin\nu\,[\,b\cos^{n-1}\nu + \dots\,] \\ \xi = c\cos^{n}\nu + \dots, \end{cases}$$

where $a\cos^{n-1}\nu + \dots$, $b\cos^{n-1}\nu, \dots$, and $c\cos^{n}\nu + \dots$, are polynomials in $\cos\nu$ of degree $n-1$ and n respectively, the coefficients of which as polynomials in λ and μ with integral coefficients belong to the field $K(\surd 3)$.

Our assertion is evidently true for $n = 1$, since $\psi^2 = \psi^{-1}$, and the formulae $(\psi^{\pm1}\phi)$ give for $\psi^{\pm1}\phi(N) = (\xi, \eta, \zeta,)$, where $N = (0,0,1)$, the following ones

$$(5)\quad \xi = \lambda\sin\nu,\ \eta = \pm\mu\sin\nu,\ \zeta = \cos\nu.$$

Let us suppose our assertion to be true for a positive integer n *i.e.*, that when a is a transformation of the form (1) for a given n, we have for $a(N) = (\xi, \eta, \zeta)$ the formulæ (a). Let $a' = \psi^{\pm1}\phi a$. The formulæ $(\psi^{\pm1}\phi)$ and (a) give for $a'(N) = (x', y', z')$ the formulæ

$$\begin{aligned} x' = & -\sin\nu\,[a\cos^{n-1}\nu + \dots\,]\,\lambda\cos\nu \\ & \pm \sin\nu\,[b\cos^{n-1}\nu + \dots\,]\,\mu \\ & + [c\cos^{n}\nu + \dots]\lambda\sin\nu \\ = & \sin\nu\,[(c-a)\,\lambda\cos^{n}\nu + \dots\,] \end{aligned}$$

$$\begin{aligned} y' = & \mp\sin\nu\,[a\cos^{n-1}\nu + \dots]\,\mu\cos\nu \\ & - \sin\nu\,[b\cos^{n-1}\nu + \dots\,] \\ & \pm [c\cos^{n}\nu + \dots\,]\,\mu\sin\nu \\ = & \sin\nu[\pm(c-a)\,\mu\cos^{n}\nu + \dots\,] \end{aligned}$$

$$z' = \sin^2 \nu \, [a \cos^{n-1} \nu + \dots] + [c \cos^n \nu + \dots] \cos \nu$$

$$= (c - a) \cos^{n+1} \nu + \dots,$$

that is to say

$$x' = \sin \nu \, [a' \cos^n \nu + \dots]$$
$$y' = \sin \nu \, [b' \cos^n \nu + \dots]$$
$$z' = c' \cos^{n+1} \nu + \dots,$$

where

(6) $a' = (c - a)\lambda, \; b' = \pm (c - a)\mu, \;\; c' = c - a,$

which proves that our assertion is still true for $n + 1$. So it is proved by induction for $n = 1, 2, \dots$. Now the formulæ (6) give (as $\lambda = -\frac{1}{2}$)

$$c' - a' = (c - a)(1 - \lambda) = \tfrac{3}{2}(c - a)$$

where by easy induction

$$c - a = (\tfrac{3}{2})^n$$

(since for $n=1$, *i.e.*, for $a = \psi^{\pm 1}\phi$, evidently $a = \lambda$, $c = 1$ according to (5), thus $c - a = 1 - \lambda = \frac{3}{2}$). So $c' = c - a = (\frac{3}{2})^n$ therefore $c = (\frac{3}{2})^{n-1}$ (since c corresponds to an index less by one than that corresponding to c').

Thus we have proved that for $N = (0, 0, 1)$, $\alpha(N) = (\xi, \eta, \zeta)$, (when α is of the form (1))

$$\zeta = (\tfrac{3}{2})^{n-1} \cos^n \nu + \dots,$$

where on the right there is a polynomial of degree n in $\cos \nu$ with algebraic coefficients (belonging to the field $K(\sqrt{3})$). It results from it that if $\cos \nu$ is not a root of any polynomial with algebraic coefficients (*i.e.*, if $\cos \nu$ is a transcendental number), then the point $N=(0,0,1)$ will not be transformed into itself by any transformation of the type (1), and consequently no transformation of the type (1) will be identical (*i.e.*, $=1$). On the ground of the transcendence of the number e^i it may be proved that this condition will be satisfied for $\nu=2$, and that is the case in which the angle ν between the axes Φ and Ψ is $=1$.

Thus we have proved that the angle between the axes Φ and Ψ may be chosen in such a way that no transformation (1) will be $=1$. Now, we shall prove that it results from it that no transformation (2), (3) and (4) is $=1$. Suppose indeed that a transformation β of the type (2) is $=1$. According to $\beta=1$, evidently $\phi\beta\phi=\phi\phi=1$. Now, according to (2), $\phi\beta\phi$ is evidently of the form (1), which is impossible, since we have just proved that no transformation (1) is $=1$. Therefore no transformation (2) is $=1$.

Suppose now that a transformation δ of the type (4) is $=1$[1]). We denote $\psi^{m_1}\phi\psi^{m_2}\dots\phi\psi^{m_n}$

[1]) Hausdorff's proof (l. c. p. 470) is to be slightly modified as the transformation $\psi^{-m_1}\delta\psi^{m_1}$ is not always

by δ_n. If $\delta_n=1$, then $\psi^{3-m_1}\delta_n\psi^{m_1}=1$, therefore $\sigma=\phi\psi^{m_2}\phi\psi^{m_3}\cdots\phi\psi^{m_{n-1}}\phi\psi^{m_n+m_1}=1$. The sum m_n+m_1 may of course assume one of the values 2, 3 or 4. If $m_n+m_1=4$ or $m_n+m_1=2$, the transformation σ is of the type (2), which is inconsistent with the relation $\sigma=1$, as we have just proved. If $m_n+m_1=3$ then $\phi\sigma\phi=\psi^{m_2}\phi\psi^{m_3}\ldots\phi\psi^{m_{n-1}}$ and the transformation $\phi\psi\phi$ is of the type (4) (being $=1$ as $\sigma=1$ and $\phi^2=1$). It contains however less factors than δ' and it may be designated by δ_{n-2} in conformity with our notation. The process adopted above for δ_n may be repeated for δ'_{n-2} and we conclude (from $\delta'_{n-2}=1$) that there exists a transformation $\delta''_{n-4}=1$. Repeating this process a finite number of times we conclude that either $\delta_1^*=1$ or $\delta_2^*=1$. Yet both are impossible, since $\delta_1^*=\psi^p$ where $p=1$ or $p=2$, while on the other hand $\delta_2^*=\psi^p\phi\psi^q=1$ would imply $\phi=\psi^{-p-q}$ which is inconsistent with the fact that ϕ is distinct from 1, ψ and ψ^2. So we have proved that no transformation of the type (4) is $=1$.

Let us finally suppose that a transformation γ of the type (3) $=1$. $\gamma=1$ gives $\phi\gamma\phi=1$. Now $\phi\gamma\phi=\psi^{m_1}\phi\psi^{m_2}\ldots\phi\psi^{m_n}$ or (if $\gamma=\phi$) $\phi\gamma\phi=\phi$. The last case is impossible as $\phi\neq1$ and in the first

---

of the form (1), *e. g.*, for $m_1=1$, $\delta=\psi\phi\psi\phi\psi^2$, we have $\psi^{-m_1}\delta\psi^{-m_1}=\psi^{-1}\delta\psi=\phi\psi\phi$ and consequently $\psi^{m_1}\delta\psi^{m_1}$ is of the form (3) and not of the form (1).

case $\phi\gamma\phi$ is of the type (4), hence $\neq 1$, as we have previously proved, and this is inconsistent with $\phi\gamma\phi = 1$. Therefore no transformation of the type (3) $= 1$.

Thus we have proved that (for our choice of the angle ν) no transformation, (1), (2), (3) and (4) $= 1$, *i.e.*, no transformations of the sequence (G) excepting the first $= 1$. It results from it that all the transformations of the sequence (G) are distinct (for the angle ν chosen by us). Indeed, suppose that two terms σ and τ occupying two distinct places in the sequence (G) are equal, *i.e.*, $\sigma = \tau$. It gives $\sigma\tau^{-1} = 1$. Here τ cannot be equal to 1, because this would imply that $\sigma = 1$, which occupies a place in the sequence (G) other than τ. Thus $\tau \neq 1$, thereby $\sigma = \tau \neq 1$ and σ and τ are of the forms (1) to (4); hence

$$(7) \begin{cases} \sigma = \phi^k \psi^{m_1} \phi\psi^{m_2} \ldots \phi\psi^{m_n}\phi^l, \\ \tau = \phi^r \psi^{q_1} \phi\psi^{q_2} \ldots \phi\psi^{q_p}\phi^s, \end{cases}$$

where $m_1, m_2 \ldots, m_n, q_1, q_2, \ldots, q_p$ are the numbers 1 or 2 and k, l, r, s are either 0 or 1. It follows that $\phi^k \psi^{m_1} \phi\psi^{m_2} \ldots \phi\psi^{m_n}\phi^l\phi^{-s}\psi^{-q_p}\phi\psi^{-q_{p-1}} \ldots \phi\psi^{-q_1}\phi^{-r}$ $= \sigma\tau^{-1} = 1$.

According to the property proved concerning the transformations (1)—(4), the left side of this formula cannot represent any of these transformations. It is easily seen that this implies the equalities:

$$l=s,\ m_n=q_p,\ m_{n-1}=q_{n-1},\dots,\ m_1=q_1,\ k=r$$

which by means of (7) prove that the transformations σ and τ occupy the same place in the sequence (G) and this is inconsistent with the hypothesis. So the transformations of the sequence (G) are all distinct.

It should be observed that when ϕ denotes the rotation of the plane through the angle π around the point $z_0=x_0+iy_0\neq 0$ and ψ denotes the rotation of the plane, around another point of the plane, *e.g.*, $z_1=0$, through the angle $\frac{2\pi}{3}$ then the transformations of the sequence (G) are not all distinct. It is readily verified that we have then $\phi(z)=2z_0-z$, $\psi(z)=\epsilon z$, where $\epsilon=\frac{1}{2}(-1+i\sqrt{3})$ and it follows that $(\phi\psi)^6=1$.

Now we divide by induction each class G_n into three sub-classes G_n', G_n'', G_n''' in the following way. Let $G_0'=\{1\}$, $G_0''=G_0'''=0$ and let us suppose that we have already defined the disjoint subclasses G_n', G_n'', G_n''' for an integer n. If $\sigma\in G_{n+1}$, there exists only one $\rho\in G_n$ such that one of the three cases is to ensue:

1) $\sigma=\phi\rho$, where the first factor of ρ is ψ or ψ^2, 2) $\sigma=\psi\rho$, 3) $\sigma=\psi^2\rho$; while in the last two cases the first factor of ρ is ϕ.

We put in the first case

$\sigma \in G''_{n+1}$ if $\rho \in G'_n$ and $\sigma \in G'_{n+1}$ if $\rho \in G_n'' + G_n'''$.

In the second case we put

$\sigma \in G''_{n+1}$ if $\rho \in G'_n$, $\sigma \in G'''_{n+1}$ if $\rho \in G''_n$, $\sigma \in G'_{n+1}$ if $\rho \in G_n'''$.

In the third case we put

$\sigma \in G'''_{n+1}$ if $\rho \in G'_n$, $\sigma \in G'_{n+1}$ if $\rho \in G''_n$, $\sigma \in G''_{n+1}$ if $\rho \in G_n'''$.

The classes G'_{n+1}, G''_{n+1}, G'''_{n+1} will be evidently disjoint.

We put

$$G^{(i)} = G^{(i)}_0 + G^{(i)}_1 + G^{(i)}_2 + \dots \text{ for } i = 1, 2, 3:$$

so we shall have a decomposition of G into three disjoint parts

(G')	1		$\phi\psi,\ \phi\psi^2,\ \psi^2\phi$	$\phi\psi\phi$	...
(G'')		$\phi,\ \psi$		$\phi\psi^2\phi,\ \psi\phi\psi,\ \psi\phi\psi^2$	....
(G''')		ψ^2	$\psi\phi$	$\psi^2\phi\psi,\ \psi^2\phi\psi^2$	....

If K denotes a set of tranformations, we indicate by σK the set of all the transformations $\sigma\rho$ where $\rho \in K$. Let ρ belong to G'; there exists then an integer $n \geqslant 0$ such that $\rho \in G'_n$. If $n=0$ then $\rho=1$, hence $\phi\rho=\phi \in G_1''$, $\psi\rho=\psi \in G_1''$, $\psi^2\rho=\psi^2 \in G_1'''$. If $n \neq 0$, then $n \geqslant 2$ (since $G_1'=0$). There exists then $\rho_1 \in G_{n-1}$ such that three cases are possible:

1) $\rho=\phi\rho_1$ and ψ or ψ^2 is the first factor of ρ_1,

2) $\rho=\psi\rho_1$, (3) $\rho=\psi^2\rho_1$. In the last two cases ϕ is the first factor of ρ_1.

(1) If $\rho=\phi\rho_1$, then considering that $\rho \in G_n'$ and taking into account the definition of G_n', we find $\rho_1 \in G''_{n-1}+G'''_{n-1}$, hence $\phi\rho=\rho_1 \in G''_{n-1}+G'''_{n-1}$ and after the definition of G_n'' and G_n''', we have $\psi\rho \in G_n''$, $\psi^2\rho \in G_n'''$.

(2) If $\rho=\psi\rho_1$ the definition of G''_{n+1} gives $\phi\rho \in G''_{n+1}$ and as $\rho \in G_n'$, it is found from the definition of G'_n that $\rho_1 \in G''_{n-1}$, hence $\psi\rho=\psi^2\rho_1 \in G_n''$ and $\psi^2\rho=\rho_1 \in G'''_{n-1}$.

(3) If $\rho=\psi^2\rho_1$, then considering that $\rho \in G_n'$, we obtain $\rho_1 \in G''_{n-1}$, hence $\phi\rho \in G''_{n+1}$, $\phi\rho=\rho_1 \in G''_{n-1}$ $=\psi^2\rho=\psi\rho_1 \in G_n'''$.

Thus we have always $\phi\rho \in G''+G'''$, $\psi\rho \in G''$, $\psi^2\rho \in G'''$.

Hence, as ρ is an arbitrary element of G'

(8) $\phi G' \subset G''+G'''$, $\psi G' \subset G''$, $\psi^2 G' \subset G'''$.

Let now ρ belong to G''. There exists an integer n such that $\rho \epsilon G_n''$ and there exists a $\rho_1 \epsilon G_{n-1}$ such that three cases are possible: 1) $\rho = \phi\rho_1$, (2) $\rho = \psi\rho_1$, 3) $\rho = \psi^2\rho_1$ the first factors of ρ_1 being defined as above. 1) If $\rho = \phi\rho_1$, then on considering that $\rho \epsilon G_n''$ we have $\rho_1 \epsilon G'_{n-1}$, hence $\psi\rho = \rho_1 \epsilon G'_{n+1}$ and $\psi^2\rho \epsilon G'_{n+1}$ (by the definition of G'_{n+1}).

2) If $\rho = \psi\rho_1$, then $\rho_1 \epsilon G'_{n-1}$, hence $\phi\rho \epsilon G'_{n+1}$, $\psi^2\rho = \rho_1 \epsilon G'_{n+1}$.

3) If $\rho = \psi^2 \rho_1$, then $\rho_1 \epsilon G'''_{n-1}$, hence $\phi\rho \epsilon G'_{n-1}$, $\psi^2 \rho = \psi\rho_1 \epsilon G'_n$. Thus there is always $\phi\rho \epsilon G'$, hence

$$(9) \qquad \phi G'' \subset G', \ \psi^2 G'' \subset G',$$

whence $G'' = \psi^3 G'' \subset \psi G'$.

If finally $\rho \epsilon G'''$, then there exists a positive integer n such that $\rho \epsilon G_n'''$ and a $\rho_1 \epsilon G_{n-1}$ such that the following three cases are possible: 1) $\rho = \phi\rho_1$, 2) $\rho = \psi\rho_1$, 3) $\rho = \psi^2\rho_1$, the first factors of ρ_1 being defined as above.

1) If $\rho = \phi\rho_1$, then according to the definition of G'_n and G''_n there is a $\rho \epsilon G'_n + G''_n$ and this is inconsistent with $\rho \epsilon G_n'''$. Therefore this case is not possible.

2) If $\rho \epsilon \psi\rho_1$, then from $\rho \epsilon G_n'''$ we have $\rho_1 \epsilon G''_{n-1}$, hence $\phi\rho \epsilon G'_{n+1}$ and $\psi\rho = \psi^2\rho_1 \epsilon G_n'$.

3) If $\rho=\psi^2\rho_1$, then $\rho_1 \epsilon G'_{n-1}$, hence $\phi\rho \epsilon G'_{n+1}$ and $\psi\rho=\rho_1 \epsilon G'_{n-1}$. Thus we always have $\phi\rho \epsilon G'$, $\psi\rho \epsilon G'$ hence

$$(10) \quad \phi G''' \subset G', \quad \psi G''' \subset G',$$

whence $G'''=\psi^3 G''' \subset \psi^2 G'$.

The formulae (8), (9) and (10) give immediately

$$(11) \quad \phi G'=G''+G''', \quad \psi G'=G'', \quad \psi^2 G'=G'''$$

It is known from the geometry of movement that when a body is displaced in such a way that one of its points remains fixed, then such a movement is equivalent to a rotation (by a certain angle) around an axis passing through the fixed point. [1])

To each transformation of G different from 1 there corresponds an axis of an equivalent rotation. Such an axis intersects the given sphere in two points (poles). As the set of the transforma-

---

[1]) That axis could be found in the following way: Let T, U and T', U' denote two points of the given body before and after the considered movement. Through the centres of the segments $T\,T'$ and $U\,U'$ we draw planes perpendicular to those segments. If the planes are not identical, then the straight line of their intersection will be the required axis and if on the contrary they are identical then the required axis will be the straight line of intersection of the planes $T\,U\,O$ and $T'\,U'\,O$ where O is the fixed point of the movement.

tions of G is enumerable, the set D of all the poles is enumerable as well. It is plain that for each rotation around an axis passing through the centre of the sphere (the rotation which is an identical transformation, *i.e.*, the angle of which is a multiple of 2π, being excluded) two points and only two points of the surface of the sphere remain at their places, viz., the two poles of the considered rotation. We conclude that no point of the surface S of the sphere, the points of the set D excepted, remains at its place for any transformation of the sequence (G) save for the identical transformation 1. G being a group of transformations, we have

$$(12) \qquad \sigma(p) \neq \sigma'(p) \text{ for } p \in S-D, \quad \sigma \in G, \sigma' \in G, \sigma \neq \sigma'$$

Indeed, if we had for a certain $p \in S-D$ and for σ and σ' belonging to G, $\sigma(p)=\sigma'(p)$, then we would have $\sigma'\sigma^{-1}(p)=p$, which gives $\sigma'\sigma^{-1}=1$ (since $p \in S-D$, we have $p \,\bar{\in}\, D$) hence $\sigma=\sigma'$ and that is inconsistent with the hypothesis.

Let $G(p)$ denote the set of all the points obtained from the point p of $S-D$ by the application of any transformation of the sequence G. We have

$$G(p)=\{p\}+\{\phi(p)\}+\{\psi(p)\}+\{\psi^2(p)\}+\{\psi\phi(p)\}+\dots,$$

in short, $G(p) = \sum_{\sigma \in G} \{\sigma(p)\}$. All the terms of the series $G(p)$ are formed of distinct points of S.

Now, let p and p' be two distinct points of $S - D$. Then there is

(13) either $G(p) = G(p')$, or $G(p\, G(p') = 0$.

Indeed, if $G(p)G(p') \neq 0$, there exist two transformations σ_0 and σ'_0 of G such that $\sigma_0(p) = \sigma_0'(p')$. It results from it for $\sigma \in G$ that

$$\sigma(p) = \sigma\sigma_0^{-1}\sigma_0(p) = \sigma\ \sigma_0^{-1}\ \sigma_0'\ (p'),$$

and putting $\sigma' = \sigma\sigma_0^{-1}\sigma'_0$ we find $\sigma' \in G$ and $\sigma(p) = \sigma'(p')$ which proves that $\sigma(p) \in G(p')$ for $\sigma \in G$ and therefore $G(p) \subset G(p')$. Similarly we find that $G(p') \subset G(p)$, thus $G(p) = G(p')$, and the formula (13) is proved.

Now we divide all the points of the set $S - D$ into classes, two points p and p' of $S - D$ being ranged in the same class only if $G(p) = G(p')$. So the set $S - D$ is decomposed into disjoint (enumerable) classes. According to Zermelo's axiom there exists a set M containing one and only one element of each of those classes. Evidently we can write

$$S - D = \sum_{\sigma \in G} \sigma(M) = M + \phi(M) + \psi(M) + \psi^2(M) + \psi\phi(M) + \dots .$$

It is easy to see that the terms of this series are disjoint sets. Indeed, let us suppose that for $\sigma \in G$, $\sigma' \in G$, $\sigma \neq \sigma'$, we have $\sigma(M)\sigma'(M) \neq 0$; then there exist a $p \in M$ and $p' \in M$ such that $\sigma(p) = \sigma'(p')$ which gives, as we know $G(p) = G(p')$. Thus considering that $p \in M$, $p' \in M$ and from the definition of the set M, we have $p = p'$, which gives $\sigma(p) = \sigma'(p)$ contrary to (12), since $M \subset S - D$.

We put

$$(14) \quad A = \sum_{\sigma \in G'} \sigma(M),\ B = \sum_{\sigma \in G''} \sigma(M),\ C = \sum_{\sigma \in G'''} \sigma(M)$$

As $G = G' + G'' + G'''$ is a decomposition of G into three disjoint parts, we shall have a decomposition of $S - D$ into three disjoint sets :

$$(15) \qquad S - D = A + B + C.$$

It is easily found from (14) and (11) that

$$(16) \quad \phi(A) = B + C,\ \psi(A) = B,\ \psi^2(A) = C.$$

(It should be pointed out that $\phi(D) = D$ and $\psi(D) = D$). According to (16) we have

$$(17) \qquad A \cong B \cong C \cong B + C$$

and the formulae (15) and (17) show that the sets A, B, C and D satisfy the conditions of the theorem **26**. Thus the proof is completed.

It follows from (17) that $B+C$ is an uncountable bounded set (in the space of three dimensions) and that it is the sum of two disjoint sets each of which is congruent with it. According to what has been said above (§7) there exists no bounded plane set possessing this property.

11. *The paradox of Banach and Tarski.*

Suppose $S=A+B+C+D$ is the decomposition of the surface S of the sphere fulfilling the conditions of theorem **26.** Thus there exist the decompositions $A=A_1+A_2$, $B=B_1+B_2$, $C=C_1+C_2$ where the sets A_1, A_2, B_1, B_2, C_1, C_2 are two by two congruent and disjoint, and $A_1 \cong A$. We have

$$S=A_1+A_2+B_1+B_2+C_1+C_2+D$$

where the sets on the right are two by two disjoint. We put

$$S_1=A_1+B_1+C_1+D, \qquad S_2=A_2+B_2+C_2,$$

and it is easily seen that $S_1 \underset{4}{\mp} S$ and $S_2 \underset{3}{\mp} S-D$. Now, according to theorem **14,** we have $S-D \underset{2}{\mp} S$ and it is readily verified that the formulae $P \underset{3}{\mp} Q$ and $Q \underset{2}{\mp} R$ give $P \underset{6}{\mp} R$ (see theorem **23**). Thus $S_2 \underset{6}{\mp} S$.

So it has been proved that

(1) $S=S_1+S_2$, $S_1S_2=0$, $S_1 \underset{4}{\mp} S$ and $S_2 \underset{6}{\mp} S$.

In other words, the surface S of the sphere may be decomposed into 10 disjoint parts, the 4 and 6 of which give respectively after suitable rotations and translations, two surfaces of spheres of the same radius.

It should be mentioned that Mr. R. Robinson has recently proved in a different (though not so elementary) way that $S = S_1 + S_2$, where $S_1 S_2 = 0$, $S_1 \underset{2}{=} S$ and $S_2 \underset{2}{=} S$[1].

If instead of the points of the surface of the sphere, we take the corresponding radii with the exclusion of the centre and if we consider that the solid sphere deprived of one of its points is equivalent by decomposition into two parts to a whole sphere (which may be easily deduced from the theorem **14** by placing into the sphere the surface contained in it and passing through the point to be eliminated) we immediately conclude from (1) that *a (solid) sphere is equivalent by finite decomposition to two disjoint spheres of the same radius.* This last assertion has been deduced in 1924 in a much more complicated way by S.Banach and A. Tarski from Hausdorff's theorem.[2].

---

[1]) Fund. Math. 34, p. 254.

[2]) Fund. Math. 6, p. 62 (Lemme 22); c.f. W. Sierpiński Fund. Math. 33, p. 229.

The passage from the paradox of Hausdorff to the paradox of *Banach* and *Tarski* (*i.e.*, the correction of "the lack of the beauty" of the Hausdorff's theorem which had to take advantage of the enumerable set D) may be obtained by a simple application of the theorem **14**, the proof of which is quite elementary [1].

It may be proved that each solid sphere S is the sum of a family (of the power of the continuum) of disjoint sets, each of which is $\overset{f}{=} S$. The demonstration of this theorem is very troublesome [2].

Lemma [3]. *If a bounded set E situated in a three dimensional space contains a solid sphere K, then $E \overset{f}{=} K$.*

Proof. Let r be the radius of the sphere K. As the set E is bounded, it is contained in a finite number, say s, of cubes $Q_1, Q_2, \dots, Q_s$ each of which has a diagonal$=2r$. $K_1, K_2, \dots, K_s$ denote disjoint spheres, each of which is $\cong K$. According to the theorem of Banach and Tarski that we have just proved, we have $K \overset{f}{=} K_1+K_2$ and $K_2 \overset{f}{=} K_2+K_3$ hence $K \overset{f}{=} K_1+K_2+K_3$ and by easy induction it is found that

[1]) See W. Sierpiński, Rendiconti Accad. dei Lincei, Ser VIII, Vol. IV, p. 270-272, and Fund. Math. 35, p. 158.

[2]) See W. Sierpiński, Fund. Math. 33, p. 244.

[3]) Banach-Tarski, Fund. Math. 6, p. 263, lemma 23.

$$(2) \qquad K \stackrel{f}{=} K_1 + K_2 + \ldots + K_s.$$

Now, as $E \subset Q_1 + Q_2 + \ldots + Q_s$, the set E may be decomposed into s disjoint sets $E = E_1 + E_2 + \ldots + E_s$ where $E_i \subset Q_i$ for $i = 1, 2, \ldots, s$.

If i denotes a number of the sequence $1, 2, \ldots, s$ the cube Q_i whose diagonal $= 2r$ is congruent with a part of the sphere K_i (the radius of which is $= r$). Thus the set $E_i \subset Q_i$ is also congruent with a subset of K_i. It results from it at once that E is $\stackrel{f}{=}$ to a subset of $K_1 + K_2 + \ldots + K_s$, hence by (2) and the corollary of the theorem **23**, E is $\stackrel{f}{=}$ also to a subset H of K. Now, as $H \subset K \subset E$ and $E \stackrel{f}{=} H$, it follows by the corollary of the theorem **22** that $E \stackrel{f}{=} K$ and thus the proof of our lemma is completed.

Theorem 27 [1]. *If E_1 and E_2 are two bounded sets situated in the three dimensional space and if each of them contains a solid sphere, then $E_1 \stackrel{f}{=} E_2$.*

Proof. K_1 and K_2 denote solid spheres contained respectively in E_1 and E_2. Let us suppose, as we evidently may, that $K_1 \cong K_2$. We have from the above lemma $E_1 \stackrel{f}{=} K_1$ and $E_2 \stackrel{f}{=} K_2$; thus according to the corollary of theorem **23**, $E_1 \stackrel{f}{=} E_2$, which was to be proved.

---

[1]) Banach-Tarski, Fund Math, **6**, p. 244 and p. 263. Th. 24.

In particular it results from theorem **27** that *two solid spheres of different radii are equivalent by finite decomposition.* A sphere is also $\overset{f}{=}$ to a cube. With regard to circles *Banach* and *Tarski* have proved [1] that two circles are equivalent by finite decomposition only when their radii are equal. The question whether a circle is $\overset{f}{=}$ to a square (of the same area) has not been solved.

12. We shall deduce from theorem **27** an important consequence about the *Banach's* measure of sets of points.

In an m – dimensional Euclidean space R_m, by Banach's measure we mean each function f establishing a correspondence between an arbitrary bounded set E of R_m and a real finite number $f(E) \geqslant 0$ such that

(1) $f(E_1)=f(E_2)$ if $E_1 \cong E_2$ (where E_1 and E_2 are bounded sets of R_m),

(2) $f(E_1+E_2)=f(E_1)+f(E_2)$, if $E_1 E_2=0$,

(3) $f(T) = 1$, if T is a cube in R_m with sides equal to 1.

It results from (1), (2) and the definition of the relation $\overset{f}{=}$ that

$$f(E_1) = f(E_2) \text{ if } E_1 \overset{f}{=} E_2.$$

[1] l.c., p. 257.

Suppose there exists a *Banach's* measure in R_3 and let Q_1 and Q_2 denote disjoint cubes with sides $=1$. We have by theorem **27**: $Q_1 \stackrel{f}{=} Q_1 + Q_2$, hence by (**2**): $f(Q_1) = f(Q_1 + Q_2) = f(Q_1) + f(Q_2)$, thus $f(Q_2) = 0$ and this is in contradiction with (3). Therefore we have the

Theorem 28. *There exists no measure of Banach in* R_3.

A moment's consideration shows that there exists no measure of Banach in R_m where $m = 3, 4, 5, \ldots$. If there existed, for example, a measure of Banach in R_4, say μ, then there would exist such a measure f in R_3 simply by putting for the bounded sets E of R_3, $f(E) = \mu(H)$ where H is the set of all the points (x_1, x_2, x_3, x_4) of R_4 for which $(x_1, x_2, x_3) \in E$ and $0 \leqslant x_4 \leqslant 1$.

S. Banach proved, however, in 1923 the existence of Banach's measure in R_1 and in R_2 but the demonstration is still very troublesome[1]. In his book *Theory of linear operations*[2] he gave another proof. Moreover, a strictly algebraical demonstration of the existence of the Banach's measure is due to A. Tarski[3].

[1]) Fund. Math. 4, p. 7.

[2]) Monografje Matematyczne t. I (Warszawa-Lwow 1932), p. 32.

[3]) Fund. Math. 31, p. 56; c. f. C. R. Soc. Sc. Varsovie 21 (1929), p. 114.

It should be observed that a Banach's measure is not in an enumerable manner additive. Indeed, according to the theorem **21** the linear set $I_1=[0 \leqslant x < 1]$ is the sum of an enumerable infinity of disjoint sets two by two $\underset{2}{=}$, say $I_1 = E_1 + E_2 + \dots$ As $E_1 \underset{2}{=} E_k$, we have $\mu(E_k) = \mu(E_1)$ for $k = 1, 2, \dots$, where $\mu(E)$ denotes the Banach's measure of the linear set E. If $\mu(E_1)=0$, then $\mu(E_1)+\mu(E_2)+ \dots = 0$, and if $\mu(E_1) > 0$, then $\mu(E_1)+\mu(E_2)+ \dots = \infty$; thus there is always

$$\mu(I_1) \neq \mu(E_1) + \mu(E_2) + \dots$$

as it results from the demonstration of the theorem **16** that $I_1 \overset{f}{=} I$, where I is the interval $0 \leqslant x \leqslant 1$ and from (3), $\mu(I) = 1$, hence $\mu(I_1) = 1$.

Now it is known that Henri Lebesgue has defined for $m = 1, 2, \dots$ a family L_m of bounded sets of R_m and for each set $E \in L_m$ a real number $f(E) = f_m(E) \geqslant 0$ in such a way that for each finite or infinite sequence of disjoint sets of L_m, $E_1, E_2, \dots$ the formulae (1) and (3) hold as well as

$$(4) \quad f(E_1 + E_2 + \dots) = f(E_1) + f(E_2) + \dots.$$

The sets forming L_m are said to be measurable L in R_m and the function $f_m(E)$ is said to be the Lebesgue m-dimensional measure of E. The family L_m is very large: no set effectively defined is known at present, the non-measurability L of which could be proved (though there may be effectively defined linear sets for which there exists no method of discerning whether they are measurable L or not) [1]. The known demonstrations of the existence of non-measurable L sets make use of the Zermelo's axiom. It is plain that the sets E_1, $E_2, \ldots$ satisfying the conditions of the theorem **21** are not measurable L.

The following problem is said to be the *generalized problem of measure*:

Does there exist for a given set I a function establishing a correspondence between each subset E of I and a real non-negative finite number $f(E)$ in such a way that

(α) $f(I)=1$,

(β) $f(E_1+E_2+\ldots)=f(E_1)+f(E_2)+\ldots$, if $E_k \subset I$ $k=1, 2, \ldots$ and $E_k E_l=0$ for $k \neq l$,

(γ) $f(E)=0$ if E is composed of only one element of I?

It has been proved by the aid of the conti-

[1]) C. Kuratowski, C. R. du Congrès Intern. des Math. à Zürich, 1932.

nuum hypothesis[2] that when I is an interval (or more generally an arbitrary set of real numbers), the answer to the generalized problem of measure is in the *negative*. On the other hand it may be proved without making use of the hypothesis of the continuum that the answer to the generalized problem of measure is negative for any set I whatever of power $\leqslant \aleph_1$

I shall quote here, without proof, three theorems the demonstrations of which will appear in the vol. 37 (pp. 203-212) of the periodical *Fundamenta Mathematicae*:

If E is a bounded set situated in R_m and of the m-dimensional (Lebesgue) exterior measure $m_e(E)>0$ and if μ is an arbitrary real number $>m_e(E)$, then there exists in R_m a set H such that $H \overset{f}{=} E$ and $m_e(H)=\mu$.

When E is a set measurable L situated on the straight line or on the plane, there exists no set $H \overset{f}{=} E$ and such that $m_e(H) < m(E)$.

If E is a bounded set situated in R_m, where $m \geqslant 3$, and such that $m_e(E) > 0$, there exists for each real number μ, such that $0<\mu<m_e(E)$, a set H of R_m which is $\overset{f}{=} E$ and such that $m_e(H)=\mu$.

[2]) See my book *Hypothese du continu* (Monografje Matematyczne, IV, Warszawa—Lwów 1934), p.107; cf. S. Banach and C. Kuratowski, Fund. Math. 14. p. 129 and E. Szpilrajn, Fund. Math. 22 pp. 304-308.

13. *The absolute measure.* Let X be a linear bounded set. The upper bound of the lengths of all the (closed) intervals which are $\stackrel{f}{=}$ to a subset of X is called by Mr. Tarski the *absolute interior measure* of X and is denoted by $a_i(X)$. The lower bound of the lengths of all the intervals containing a subset equivalent to X by finite decomposition is called *absolute exterior measure* of X and is denoted by $a_e(X)$.

It results immediately from theorem **25** and the corollary of theorem **22** that a segment of a straight line is not $\stackrel{f}{=}$ to a subset of a smaller segment. This implies, after the definition of $a_i(X)$ and $a_e(X)$ that for each linear bounded set X

$$0 \leqslant a_i(X) \leqslant a_e(X) < +\infty .$$

If $a_i(X) = a_e(X)$ then the set X is said to be *absolutely* measurable and the number $a(X) = a_i(X) = a_e(X)$ is called *absolute measure* of X. It is easily seen that each finite segment is absolutely measurable and that its absolute measure coincides with its length.

It may be proved[1]) that if f is an arbitrary Banach's measure in R_1, then for each linear

---

[1]) A. Tarski, Fund. Math. **30**, p. 229, Th. 3 14.

bounded set X

$$a_i(X) \leqslant f(X) \leqslant a_e(X).$$

It results from it that if X is absolutely measurable, then $a(X) = f(X)$.

It may be proved that a necessary and sufficient condition that a linear bounded set X should be absolutely measurable is that $f(X) = g(X)$ where f and g denote two arbitrary Banach's measures in R_1.[1)]

There exist absolutely measurable linear sets which are not measurable in the Lebesgue sense *e.g.*, the sets obtained by the decomposition of a segment into an enumerable infinity of disjoint sets and $\underline{f}$ as in theorem **21**[2)]. Conversely there exist sets measurable in the Lebesgue sense which are not absolutely measurable (*e.g.*, the bounded sets of the first category of a positive Lebesgue measure).[3)]

14. *The paradox of J. von. Neumann.*

As we know (by theorem **19**) the segment (as well as the square) do not admit of paradoxical decompositions. There exists, however, another

1) l.c., p. 230, Cor. 3. 19.
2) l.c., p. 232, th. 4. 11.
3) l.c., p. 232, th. 4. 10.

paradox concerning the segment of the straight line and the square, shown by Mr. J. von Neumann in 1929.

Suppose A and B are two sets of points. The set B is said to be *metrically smaller* than A, if there exists a reciprocally univocal transformation f of A into B which diminishes the distances between the points. More precisely, if $\rho(p, q)$ denotes the distance from p to q one must always have $\rho(f(p), f(q)) < \rho(p,q)$ for any $p \in A$, $q \in B$.

We shall say that a set B is smaller *by finite decomposition* than A if there exists a decomposition of the set A and B into the same finite number n of disjoint sets $A = A_1 + A_2 + \ldots + A_n$, $B = B_1 + B_2 + \ldots + B_n$ such that for $k = 1, 2, \ldots, n$ the set B_k is metrically smaller than the set A_k.

Mr. J. von Neumann has proved with the aid of Zermelo's axiom that a segment of the straight line is smaller by finite decomposition than a segment of smaller length[1]. His demonstration is very tedious. Now, I have deduced in an elementary way from the paradox of Banach and Tarski that each circle ($0 \leqslant x^2 + y^2 \leqslant r^2$) is smaller by finite decomposition than any circle (the circle itself being comprised)[2].

[1]) Fund. Math. **13**, p. 115.

[2]) Fund. Math. 35, p. 204; cf. W. Sierpiński, Commentarii Math. Halvetici **19** (1946-1947), p. 22 3.

Appendix

During the weeks that I have lectured at the University of Lucknow, several problems have been put and some even resolved by my audience, specially by Mr. A. Sharma. This supplementary note contains their exposition.

Mr. A. Sharma has put the problem whether we can combine the theorems **7** and **8**. This is the answer.

Theorem 29. *If P is the aggregate of all the points of the line, N the aggregate of all the irrational numbers of the interval* (0, 1), *D the aggregate of all the rational numbers, then we do not have*

$$P-(N+D) \overset{=}{\underset{2}{}} P.$$

Proof: Let us suppose that $P-(N+D) \overset{=}{\underset{2}{}} P$ holds true. There exists then decompositions

$$P=P_1+P_2,\ P-(N+D)=Q_1+Q_2$$

where $P_1P_2=Q_1Q_2=0$, $P_1 \cong Q_1$, $P_2 \cong Q_2$. As $P_1 \cong Q_1$, there exists an isometric transformation f of the line P into itself which transforms P_1 into Q_1. We have then $f(P_1)=Q_1$. Put $Q=f(P_2)$. As $f(P)=P$, we have

$$P=f(P)=f(P_1+P_2)=f(P_1)+f(P_2)=Q_1+Q.$$

and seeing that $P_1P_2=0$ (and that f is a one to one transformation of the line),

$$0=f(P_1P_2)=f(P_1)\,f(P_2)=Q_1Q.$$

We have thus $P=Q_1+Q$ and $Q_1Q=0$ and $Q=f(P_2) \cong P_2$, so that from $P_2 \cong Q_2$, we have $Q \cong Q_2$. There exists then an isometric transformation ϕ of Q into Q_2. Now, as $Q_1Q_2=0$ and $Q_2 \subset P=Q_1+Q$, we find that $Q_2 \subset Q$ and $Q_2 \neq Q$, since $Q_1+Q_2=P-(N+D) \neq P=Q_1+Q$.

Now, as we know, a linear aggregate cannot be transformed into its aliquot part by a rotation: the transformation ϕ is then a translation (along the length of a line), say of length a, *i.e.*, we have $Q_2=Q(a)$. As $Q_1 \subset Q_1+Q_2=P-(N+D)$, we have $Q_1(N+D)=0$; hence seeing that $(N+D) \subset P=Q+Q_1$ we find that $N+D \subset Q$. The aggregate Q contains then all the rational numbers. If a is a rational number, it will be evidently the same for the aggregate $Q(a)=Q_2$, which is impossible, seeing that $Q_2 \subset Q_1+Q_2=P-(N+D)$, whence $Q_2D=0$. The number a is then irrational.

Put $\xi=Ea+1-a$; it will be evidently an irrational number of the interval $(0, 1)$ so that $\xi \in N \subset Q$, whence $\xi + a \epsilon Q(a) = Q_2$. Now, we evidently have

$$\xi + a = Ea + 1 \epsilon D.$$

We will then have $Q_2 D \neq 0$, which is impossible.

The hypothesis that $P \underset{2}{\equiv} P - (N + D)$ implies then a contradiction and our theorem is proved.

We now prove the following theorem :

Theorem 30. *If B is a bounded set of real numbers and D an enumerable set of real numbers, we have on denoting by P the set of all the points on the straight line :*

$$P - (B + D) \underset{5}{\equiv} P.$$

Proof. The set B being bounded, it is situated in an interval $a \leqslant x < b$. Let Q_1 be the set of all the real numbers $< a$ and Q_2 the set of all the real numbers $\geqslant b$. We evidently have

$$Q_1(b - a) + Q_2 = P$$

and we see easily that the translations of the set $Q_1 - D$ and the set $Q_2 - D$ give a sum which is equal to $P - D_1$, where D_1 is at most an enumerable set. This sum is then from our theorem **8**, $\underset{2}{\equiv} P$. On the other hand, this sum is evidently $\underset{2}{\equiv} (Q_1 - D) \dotplus (Q_2 - D)$. From theorem **23**, we have then

$$(Q_1 - D) + (Q_2 - D) \underset{4}{\equiv} P.$$

Also we evidently have

$$(Q_1 - D) + (Q_2 - D) \subset P - (B + D) \subset P.$$

From theorem **22**, we then find

$$P - (B + D) \underset{5}{\equiv} P.$$

The problem remains open whether in the general case, the number 5 could be replaced by a smaller number.

Theorem 31. *If E denotes the set of all the squares of natural numbers, we do not have* $E \overset{f}{\equiv} E - \{1\}$.

Proof. Suppose that we have

$$E \underset{m}{\equiv} E - \{1\},$$

where m is a given natural number. We have then the decompositions of E and $E - \{1\}$ into m disjoint sets :

$$E = E_1 + E_2 + \ldots + E_m$$

and

$$E - \{1\} = H_1 + H_2 + \ \ldots + H_m,$$

where $E_i \cong H_i$ for $i = 1, 2, \ldots, m$.

Let E_k be a term of the series for E which is an infinite aggregate. As $E_k \cong H_k$ and as E_k, in so far as it is an infinite aggregate of natural numbers, can not be congruent by rotation with the aggregate of natural numbers H_k, we conclude that E_k is congruent with H_k by translation, say $H_k = E_k(a)$. If the number $a \neq 0$, then, on denoting by p^2 any element whatsoever of E_k we have $p^2 + a \in H_k$ hence (observing that $H_k \subset E - \{1\}$) $p^2 + a = q^2$, whence $(q+p)(q-p) = a$ and $q + p < |a|$, so that $p < |a|$, contrary to the fact that the aggregate E is infinite. We have then $a = 0$ and $H_k = E_k$ for each infinite term of the series $E_1 + E_2 + ... + E_m$. If the terms $E_1, E_2, \cdots, E_s$ of E are finite and the terms $E_{s+1}, E_{s+2}, ..., E_m$ infinite we have $E_i = H_i$ for $i = s + 1, s + 2, \cdots, m$, and if we put

$$P = E_{s+1} + E_{s+2} + ... + E_m$$

then $E = E_1 + E_2 + \cdots + E_s + P$, and $E - \{1\} = H_1 + H_2 + \cdots + H_s + P$. Now as $E_i \cong H_i$ for $i = 1, 2, ..., m$, and as the aggregates $E_1, E_2, ..., E_s$ and $H_1, H_2, \cdots, H_s$ are respectively finite and disjoint, the aggregates $E_1 + E_2 + \cdots + E_s$ and $H_1 + H_2 + ... + H_s$ have the same number of elements, hence also the aggregates $E - P = E_1 + E_2 + ... + E_s$ (since $P(E_1 + E_2 + ... + E_s) = 0$) and $E - \{1\} - P$ have the same finite number of elements.

Now, this is impossible since $E - \{1\} \subset E$, $\{1\} \bar{\in} P \subset E - \{1\}$ and $\{1\} \in E - P$, and $E - \{1\} - P$

is an aliquot part of $E - P$.
We then cannot have

$$E \overset{f}{=} E - \{1\}.$$

As for the problem whether for two aggregates A and C such that $A \underset{3}{=} C$, there always exists a set B such that $A \underset{2}{=} B \underset{2}{=} C$, the problem remains still open even for finite aggregates of natural numbers. Now, Mr. A. Sharma has shown that the answer to this problem is positive for all the aggregates A containing at most 7 elements.

Mr. A.Sharma has also shown that there exist aggregates A and C, such that $A \underset{4}{=} C$, for which there does not exist any aggregate B such that $A \underset{2}{=} B \underset{2}{=} C$. Such are for example the aggregates

$$A = \{1, 2, 3, 4\} \text{ and } C = \{1, 10, 10^2, 10^3\}.$$

The problem remains open whether for two aggregates A and C such that $A \underset{4}{=} C$ there always exists an aggregate B such that $A \underset{3}{=} B \underset{3}{=} C$.

I do not know also whether n being a natural number >2 and A and C being two non-bounded aggregates such that $A \underset{n}{=} C$, whether there always exist $n-1$ aggregates $B_1, B_2, \ldots B_{n-1}$ such that

$$A \underset{2}{=} B_1 \underset{2}{=} B_2 \underset{2}{=} \ldots \underset{2}{=} B_{n-1} \underset{2}{=} C.$$

Theorem 32 *Let n be a natural number. When the sets A and B are congruent and AB contains less than $\frac{1}{2}n(n+1)$ points, then $A-B \underset{n}{=} B-A$*[1].

Proof. Our theorem is evidently true for $n = 1$, since then the sets A and B are disjoint.

Let now n be a natural number and suppose that our theorem is true for the number n. Let A and B be two sets (situated in any metric space whatsoever) such that $A \cong B$ and the set $P = AB$ contains less than $\frac{1}{2}(n+1)(n+2)$ points.

As $A \cong B$, there exists an isometric transformation f of the set A into B since $P = AB \subset A$, we have $P \cong f(P)$. Let f^{-1} be the inverse transformation of f (that is, an isometric transformation of B into A). As $P = AB \subset B$, we have

$$f^{-1}(P) \subset f^{-1}(B) = A$$

and

$$(1)\quad A-B = A-P = [A-(P+f^{-1}(P))]+[f^{-1}(P)-P]$$

and

$$(2)\quad B-A = B-P = [B-(P+f(P))]+[f(P)-P].$$

Now

$$f(A-[P+f^{-1}(P)]) = f(A)-f(P+f^{-1}(P))$$
$$= B-[f(P)+P]$$

so that

[1] This theorem has been enunciated by A. Lindenbaum without proof in Fund. Math 8 (1926), p. 218.

$$(3 \qquad A - [P + f^{-1}(P)] \cong B - [f(P) + P].$$

Let us now distinguish two cases:

1) When the set $Pf(P)$ has less than $\frac{1}{2}n(n+1)$ points.

Our theorem being, by hypothesis, true for the number n, it follows from $P \cong f(P)$ that $P - f(P) \underset{n}{=} f(P) - P$. Now, as $f^{-1}(P) - P = f^{-1}(P - f(P)) \cong P - f(P)$, it follows that $f^{-1}(P) - P \underset{n}{=} f(P) - P$ and from (1), (2) and (3) we find at once that $A - B \underset{1+n}{=} B - A$.

2) When the set $Pf(P)$ has at least $\frac{1}{2}n(n+1)$ points. Now, as the set P, hence also the set $f(P)$, has less than $\frac{1}{2}(n+1)(n+2)$ points, the set $f(P) - P = f(P) - Pf(P)$ has less than $\frac{1}{2}(n+1)(n+2) - \frac{1}{2}n(n+1) = n+1$ points, hence at most n points. The sets P and $f(P)$ being finite and having the same number of points, the sets $P - f(P) = P - Pf(P)$ and $f(P) - P = f(P) - Pf(P)$ have the same number of points. As $f^{-1}(P) - P = f^{-1}(P - f(P))$, we conclude from it that the sets $f^{-1}(P) - P$ and $f(P) - P$ have the same number $\leqslant n$ of points and therefore we have $f^{-1}(P) \underset{n}{=} f(P) - P$. From (1), (2) and (3) we conclude that $A - B \underset{n+1}{=} B - A$.

We have thus proved that if our theorem is true for the natural number n, it is also true for the number $n+1$. Now, as it is true for $n=1$, it follows from it, by induction, that it is true for every natural number.

Theorem 33. *In the theorem of Lindenbaum, the number* $\frac{1}{2}n(n+1)$ *cannot be replaced by any larger natural number.*

Proof. It will be sufficient to prove that there exists for every natural number n, two finite sets of points of the straight line, A_n and B_n, such that $A_n \cong B_n$, that the set $A_n B_n$ has $\frac{1}{2}n(n+1)$ points and that $A_n - B_n \underset{n}{\cong} B_n - A_n$ does not hold.

To this end, we put $f(x) = x + 1$ for real x and let, for a natural number $n > 1$, A_{n-1} be the set of all the natural numbers $kn + l$, where $k = 1, 2, ..., n$ and $l = 0, 1, 2, ..., k-1$ that is,

$$A_{n-1} = \{n,$$

$$(4) \qquad \begin{array}{l} 2n, 2n+1 \\ 3n, 3n+1, 3n+2, \\ \ldots \quad \ldots \quad \ldots \quad \ldots \\ n^2, n^2+1, n^2+2, \ldots, n^2+(n-1)\} \end{array}$$

Now, put

$$(5) \qquad B_{n-1} = f(A_{n-1}).$$

As $kn + k < (k+1)n$ for $k = 1, 2, ..., n-1$, we easily see that

(6) $A_{n-1} - B_{n-1} = \{n, 2n, 3n, \ldots, n^2\}$

(7) $B_{n-1} - A_{n-1} = \{n+1, 2n+2, 3n+3, \ldots, n^2+n\}$.

From (4) the set A_{n-1} has $1+2+\ldots+n = \frac{1}{2}n(n+1)$ elements and since

$$A_{n-1}B_{n-1} = A_{n-1} - (A_{n-1} - B_{n-1})$$

and since from (6), the set $A_{n-1} - B_{n-1}$ has n elements, we conclude that the set $A_{n-1}\, B_{n-1}$ has $\frac{1}{2}n(n+1) - n = \frac{1}{2}n(n-1)$ elements.

Suppose that

$$A_{n-1} - B_{n-1} \underset{n-1}{\equiv} B_{n-1} - A_{n-1}.$$

It follows from it at once that the set $A_{n-1} - B_{n-1}$, although containing n points, contains at least a pair of points, say pn and qn, where $1 \leqslant p < q \leqslant n$, which is congruent with a pair of points of the set $B_{n-1} - A_{n-1}$, say $\{(n+1)r, (n+1)s\}$. We have then

$$qn - pn = |(n+1)r - (n+1)s| = (n+1)|r-s|$$

The number $(n+1)|r-s| = n|r-s| + |r-s|$ is then divisible by n, which is impossible, since r and s are two distinct numbers of the set $1, 2, \ldots, n$ and we have $0 < |r-s| < n$.

The formula $A_{n-1} - B_{n-1} \underset{n-1}{\equiv} B_{n-1} - A_{n-1}$ cannot then hold good. n being any natural number > 1, our assertion about the existence of the sets A_n and B_n for $n = 1, 2, \ldots$ is found proved. This completes the proof of our theorem.

Theorem 34. *If the sets A_1, A_2, A_3, and also the set C_1, C_2, C_3 are disjoint and if $A_i \cong C_i$ for $i = 1, 2, 3$, and if each of the sets A_2 and A_3 contain at most two elements, then there exists a set B such that*

$$A_1 + A_2 + A_3 \underset{2}{=} B \underset{2}{=} C_1 + C_2 + C_3.$$

Proof. As $A_1 \cong C_1$, there exists an isometric transformation of the space such that $f(A_1 = C_1$. Put

$$B = [\, A_1 + (A_2 + A_3) f^{-1}(C_2 + C_3) \,]$$
$$+ [A_2 - f^{-1}(C_2 + C_3)] + [f^{-1}(C_3) - (A_2 + A_3)\,].$$

We have

$$B = [\, A_1 + A_2 + A_3 f^{-1}(C_2 + C_3)]$$
$$+ [f^{-1}(C_3) - (A_2 + A_3)]$$

the two terms on the right being disjoint sets (because $C_1 C_3 = 0$, $f^{-1}(C_1) f^{-1}(C_3) = 0$ hence $A_1 f^{-1}(C_3) = 0$). The set A_3, hence also the set $C_3 \cong A_3$, have at most two points and the same is true of the sets $f^{-1}(C_3)$ and A_3. Now, as $\overline{\overline{A_2 + A_3}} = \overline{\overline{C_2 + C_3}} = \overline{\overline{f^{-1}(C_2 + C_3)}}$, we easily see from $f^{-1}(C_3) \cong C_3 \cong A_3$ that

$$f^{-1}(C_3) - (A_2 + A_3) \cong A_3 - f^{-1}(C_2 + C_3)$$

(since, if in each of the two congruent sets containing at most two points, we suppress one point or two points in each of them, we evidently obtain congruent sets).

We have thus:

$$B \underset{2}{\overline{\overline{\sim}}} [A_1 + A_2 + A_3 f^{-1}(C_2 + C_3)] + [A_3 - f^{-1}(C_2 + C_3)]$$

$$= A_1 + A_2 + A_3.$$

On the other hand we have

$$B \cong f(B) = f(A_1) + [f(A_2) + f(A_3)](C_2 + C_3)$$

$$+ [f(A_2) - (C_2 + C_3)]$$

$$+ \{C_3 - [f(A_2) + f(A_3)]\}$$

$$= C_1 + f(A_2) + C_2 f(A_3) + [C_3 - f(A_2)]$$

$$= [C_1 + C_2 f(A_3) + C_3] + [f(A_2) - C_3]$$

and the two terms on the right are disjoint (since $C_1 f(A_2) = f(A_1) f(A_2) = f(A_1 A_2) = 0$, because $A_1 A_2 = 0$).

Now as $C_3 \cong A_3 \cong f(A_3)$ and $\overline{\overline{C_3}} = \overline{\overline{f(A_3)}}$, we find as above (because $f(A_2) \cong A_2 \cong C_2$) that

$$f(A_2) - C_3 \cong C_2 - f(A_3).$$

Hence

$$[C_1 + C_2 f(A_3) + C_3] + [f(A_2) - C_3]$$

$$\underset{2}{\overline{\overline{\sim}}} [C_1 + C_2 f(A_3) + C_3] + [C_2 - f(A_3)] = C_1 + C_2 + C_3.$$

We have thus $B \underset{2}{\overline{\overline{\sim}}} C_1 + C_2 + C_3$.

ERRATA.

Page 9. The proof is inaccurate because of the assumption $\phi^{\circ}(z)=\psi^{\circ}(z)=z$ in line 16 which implies $c=0$. Therefore for page 9 and the first five lines of page 10, read the following :

"Now the following problem is open :

Does there exist a plane set E containing two distinct points p and q such that $E-\{p\}\cong E$ and $E-\{q\}\cong E$?

Mr. J. Mycielski has proved that the answer to the analogous problem for sets in three dimensional space is positive. His proof will appear in the Fundamenta Mathematicae Vol. 41 or 42. Mr. Mycielski also informs me that he has recently proved that there exists on the surface of the sphere (in three dimensional space) an enumerable set E such that $E-\{p\}\cong E$ for every point p of E, and a set H of the power of the continuum, such that we have $H-F\cong H$ for every set F which is at most enumerable."

THE

MATHEMATICAL THEORY OF THE TOP

LECTURES DELIVERED ON THE OCCASION OF THE SESQUICENTENNIAL CELEBRATION OF PRINCETON UNIVERSITY

BY

FELIX KLEIN

Professor of Mathematics in the University of Göttingen

WITH ILLUSTRATIONS

NOTE

THESE lectures on the analytical formulæ relating to the motion of the top were delivered on Monday, Tuesday, Wednesday, and Thursday, October 12–15, 1896. They were reported and prepared in manuscript form by Professor H. B. Fine of Princeton University, and the manuscript was revised by Professor Klein.

LECTURE I

In the following lectures it is proposed to consider certain interesting and important questions of dynamics from the standpoint of the theory of functions of the complex variable. I am to develop a new method, which, as I think, renders the discussion of these questions simpler and more attractive. My object in presenting it, however, is more general than that of throwing light on a particular class of problems in dynamics. I wish by an illustration which may fairly be regarded as representative to make evident the advantage which is to be gained by dynamics and astronomical and physical science in general from a more intimate association with the modern pure mathematics, the theory of functions especially.

I venture to hope, therefore, that my lectures may interest engineers, physicists, and astronomers as well as mathematicians. If one may accuse mathematicians as a class of ignoring the mathematical problems of the modern physics and astronomy, one may, with no less justice perhaps, accuse physicists and astronomers of ignoring departments of the pure mathematics which have reached a high degree of development and are fitted to render valuable service to physics and astronomy. It is the great need of the present in mathematical science that the pure science and those departments of physical science in which it finds its most important applications should again be brought into the intimate association which proved so fruitful in the work of Lagrange and Gauss.

I shall confine my discussion mainly to the problem presented in the motion of a top — meaning for the present by "top" a rigid body rotating about an axis, when a single point in this axis, not the centre of gravity, is fixed in position.

In the present lecture I shall present some preliminary considerations of a purely geometrical character. But it is necessary first of all to obtain an analytical representation of the rotation of a rigid body about a fixed point, and I shall begin with a statement of the methods ordinarily used.

We introduce two systems of rectangular axes both having their origin at the fixed point: the one system, x, y, z, fixed in space; the other, X, Y, Z, fixed in the rotating body. Then the ordinary equations of transformation from the one system to the other, which may be exhibited in the scheme:

$$(1)\qquad \begin{array}{c|ccc} & X & Y & Z \\ \hline x & a & b & c \\ y & a' & b' & c' \\ z & a'' & b'' & c'' \end{array}$$

give at once, when the nine direction cosines, a, b, c, a', $\cdots$ are known functions of the time t, the representation of the motion of the movable system X, Y, Z, with respect to the fixed system x, y, z.

As is well known, these cosines are not independent; they are rather functions of but three independent quantities or parameters. It is customary to employ one or other of the following sets of parameters, both of which were introduced by Euler.

The first set of parameters, which is non-symmetrical, consists of the angle ϑ which the Z-axis makes with the z-axis, and the angles ϕ and ψ, which the line of intersection of the xy- and XY-planes makes with the X-axis and the x-axis respectively. Because of the frequent use made of these parameters in astronomy, I shall call them the "astronomical parameters." When the cosines a, b, c, $\cdots$ have been expressed in terms of them, the orthogonal substitution (1) becomes:

$$
(2)\quad \begin{array}{c|ccc}
 & X & Y & Z \\
\hline
x & \cos\phi\cos\psi - \cos\vartheta\sin\phi\sin\psi, & -\sin\phi\cos\psi - \cos\vartheta\cos\phi\sin\psi, & \sin\vartheta\sin\psi \\
y & \cos\phi\sin\psi + \cos\vartheta\sin\phi\cos\psi, & -\sin\phi\sin\psi + \cos\vartheta\cos\phi\cos\psi, & -\sin\vartheta\cos\psi \\
z & \sin\vartheta\sin\phi\quad , & \sin\vartheta\cos\phi\quad , & \cos\vartheta
\end{array}
$$

The second set of parameters may be defined as follows. Every displacement of our body is equivalent to a simple rotation about a fixed axis. Let ω be the angle of rotation, and a, b, c the angles which the axis makes with OX, OY, OZ; and set

$$A = \cos a \sin\frac{\omega}{2},\ B = \cos b \sin\frac{\omega}{2},\ C = \cos c \sin\frac{\omega}{2},\ D = \cos\frac{\omega}{2}.$$

The quantities A, B, C, D (of which but three are independent, since, as will be seen at once, $A^2+B^2+C^2+D^2=1$) are the parameters under consideration. In terms of them our orthogonal substitution (1) is

$$
(3)\quad \begin{array}{c|ccc}
 & X & Y & Z \\
\hline
x & D^2+A^2-B^2-C^2, & 2(AB-CD), & 2(AC+BD) \\
y & 2(AB+CD), & D^2+B^2-C^2-A^2, & 2(BC-AD) \\
z & 2(AC-BD), & 2(BC+AD) & D^2+C^2-A^2-B^2
\end{array}
$$

or, if use be not made of the relation

$$A^2+B^2+C^2+D^2=1,$$

a substitution with these coefficients each divided by $A^2+B^2+C^2+D^2$. I shall call these the "quaternion parameters," inasmuch as the quaternionists make frequent use of them. The quaternion corresponding to our rotation is

$$q = D + iA + jB + kC.$$

These parameters are very symmetrical, and for that reason very attractive. Nevertheless, they do not prove to be the most advantageous system for our present purpose. Our problem is not a symmetrical problem. In it one of the axes, Oz, in the direction of gravity, plays an exceptional rôle; the motion of the top is not isotropic.

Instead of either of these commonly used systems of parameters, I propose to introduce another, which so far as I know has not yet been employed in dynamics.

Let x, y, z be the coordinates of a point on a sphere fixed in space which has the radius r and the centre O, and X, Y, Z the coordinates of a point on a sphere congruent with the first but fixed in the rotating body. As the body rotates, the second sphere slides about on the first, but remains always in congruence with it.

It is characteristic of every point on the first sphere that the relation

$$\frac{x + iy}{r - z} = \frac{r + z}{x - iy}$$

holds good between its coordinates.

If we represent the values of these equal ratios by ζ, obviously ζ is a parameter for the points of the sphere, which completely determines one of these points for every value that it may take. Thus the upper extremity of the z-axis is characterized by the value ∞ of ζ, the lower extremity by the value 0; to real values of ζ correspond the points on the great circle of the sphere in the plane $y = 0$, and to pure imaginary values the points of the great circle in the plane $x = 0$.

For the points of the second sphere, in like manner, there is a parameter Z connected with the coordinates X, Y, Z by the equations,

$$\frac{X + iY}{r - Z} = \frac{r + Z}{X - iY} = \mathrm{Z},$$

which defines these points as ζ defined the points of the fixed sphere.

If now ζ and Z be parameters of corresponding points on the two spheres, what is the relation between these parameters when the second sphere is subjected to a rotation? *It is a simple linear relation of the form*

$$\zeta = \frac{\alpha \mathrm{Z} + \beta}{\gamma \mathrm{Z} + \delta},$$

in which $\alpha, \beta, \gamma, \delta$ *are themselves in general complex quantities, but so related that* α *is the conjugate im-*

aginary to δ*, and* β *to* $-\gamma$ *; or, adopting the ordinary notation,* $\alpha = \bar{\delta}$ *and* $\beta = -\bar{\gamma}$.

It is obvious, *a priori,* that the relation must be linear, and a very simple reckoning such as I have given in my treatise on the Icosahedron (p. 32) establishes the special relations among the coefficients. There are but four real quantities involved in α, β, γ, δ, only the ratios of which need be considered independent, since these ratios alone appear in the expression for ζ; unless, as is generally more convenient, we introduce the further relation $\alpha\delta - \beta\gamma = 1$.

It is these quantities α, β, γ, δ connected by the relation $\alpha\delta - \beta\gamma = 1$, which together with ζ we propose to use as our parameters in the discussion of the problem now under consideration. They were introduced into mathematics by Riemann forty years ago, and have proved to be peculiarly useful in different geometrical problems intimately connected with the theory of functions, especially in the theory of minimal surfaces and the theory of the regular solids. *We hope to show that they may be employed to quite as great advantage in the study of all problems connected with the motion of a rigid body about a fixed point.*

Corresponding to the orthogonal substitution (1), we have in terms of our new parameters the substitution

$$(4)\qquad \begin{array}{r|ccc} & X+iY & -Z & -X+iY \\ \hline x+iy & \alpha^2 & 2\,\alpha\beta & \beta^2 \\ -z & \alpha\gamma & \alpha\delta+\beta\gamma & \beta\delta \\ -x+iy & \gamma^2 & 2\,\gamma\delta & \delta^2 \end{array}$$

as may be demonstrated without serious reckoning as follows. And I may remark incidentally that it seems to me better wherever possible to effect a mathematical demonstration by general considerations which bring to light its inner meaning rather than by a detailed reckoning, every step in which the mind may be forced to accept as incontrovertible, and yet have no understanding of its real significance.

Consider the sphere of radius 0,

$$x^2+y^2+z^2=0.$$

It is an imaginary cone whose generating lines join the origin to the so-called "imaginary circle at infinity," the circle in which all spheres intersect at infinity. For this sphere,

$$\zeta=\frac{x+iy}{-z}=\frac{z}{x-iy},$$

or $$x+iy:-z:x-iy=\zeta^2:\zeta:-1.$$

Here to each value of the parameter ζ there corresponds a single (imaginary) generating line of the cone, and *vice versa.* In other words, there is a relation of one-to-one correspondence between the (imaginary) generating lines of the cone and the values of ζ, or the cone is unicursal.

There is, of course, the same relation between the generating lines of the congruent cone

$$X^2 + Y^2 + Z^2 = 0,$$

which is fixed in the moving body, and the parameter

$$\mathrm{Z} = \frac{X + iY}{-Z} = \frac{Z}{X - iY}.$$

When the body rotates, this cone is simply carried over into itself, so that the generating lines in their new position are in one-to-one correspondence with the same generating lines in their original position. Between the parameters Z and ζ, which correspond to the generating lines in these two positions, there is, therefore, also a relation of one-to-one correspondence, or the two are connected linearly, *i.e.* by a relation of the form:

$$\zeta = \frac{\alpha \mathrm{Z} + \beta}{\gamma \mathrm{Z} + \delta},$$

where, as above, we suppose

$$\alpha\delta - \beta\gamma = 1.$$

If now we avail ourselves of the advantages to be had from the use of homogeneous equations and substitutions by replacing

$$\zeta \text{ by } \frac{\zeta_1}{\zeta_2}, \text{ and } \mathrm{Z} \text{ by } \frac{\mathrm{Z}_1}{\mathrm{Z}_2},$$

this single equation may be replaced by the two homogeneous equations:

$$\zeta_1 = \alpha Z_1 + \beta Z_2,$$
$$\zeta_2 = \gamma Z_1 + \delta Z_2,$$

and the equations connecting x, y, z, and ζ, and X, Y, Z, and Z become,

$$x + iy : -z : -x + iy = \zeta_1^2 : \zeta_1\zeta_2 : \zeta_2^2,$$
$$X + iY : -Z : -X + iY = Z_1^2 : Z_1 Z_2 : Z_2^2.$$

From these equations it follows that

$$x + iy = \alpha^2(X + iY) + 2\,\alpha\beta(-Z) + \beta^2(-X + iY)$$
$$-z = \alpha\gamma(X + iY) + (\alpha\delta + \beta\gamma)(-Z) + \beta\delta(-X + iY)$$
$$-x + iy = \gamma^2(X + iY) + 2\,\gamma\delta(-Z) + \delta^2(-X + iY).$$

For it is immediately obvious that $x + iy$ is proportional to ζ_1^2, therefore to

$$\alpha^2 Z_1^2 + 2\,\alpha\beta Z_1 Z_2 + \beta^2 Z_2^2,$$

and therefore finally to

$$\alpha^2(X + iY) + 2\,\alpha\beta\,(-Z) + \beta^2(-X + iY);$$

and in like manner, that $-z$ and $-x + iy$ are proportional to

$$\alpha\gamma\,(X + iY) + (\alpha\delta + \beta\gamma)(-Z) + \beta\delta(-X + iY),$$

and

$$\gamma^2(X + iY) + 2\,\gamma\delta\,(-Z) + \delta^2(-X + iY)$$

respectively. And that $x + iy$, $-z$, $-x + iy$ are severally *equal* to these expressions and not merely proportional to them, follows from the fact that the determinant of the orthogonal substitution connecting x, y, z with X, Y, Z must equal 1.

The demonstration, to be sure, applies directly to the points of the imaginary cone only. But it is known in advance that the transformation which we are considering is a linear one for *all* points of space. Its coefficients are the same for all points, and we have merely availed ourselves of the fact that the imaginary cone remains unchanged by the transformation to determine them. The same result might have been reached, though less simply, by using the general formula $\zeta = \dfrac{x + iy}{r - z}$. The equations (4), therefore, are those which connect the coordinates of the initial and final positions of any point rigidly attached to the rotating body.

The relations between our new parameters, α, β, γ, δ, and the astronomical parameters, ϑ, ϕ, ψ, on the one hand, and the quaternion parameters A, B, C, D, on the other, are of immediate interest and of importance in the subsequent discussion. They are to be had very simply by a comparison of the coefficients in the three schemes (2), (3), (4), and, after reduction, prove to be:

$$
(5) \quad \begin{cases} \alpha = \cos\frac{\vartheta}{2} \cdot e^{\frac{i(\phi+\psi)}{2}}, & \beta = i \sin\frac{\vartheta}{2} \cdot e^{\frac{i(-\phi+\psi)}{2}}, \\ \gamma = i \sin\frac{\vartheta}{2} \cdot e^{\frac{i(\phi-\psi)}{2}}, & \delta = \cos\frac{\vartheta}{2} \cdot e^{\frac{-i(\phi+\psi)}{2}}, \end{cases}
$$

and
$$
\begin{cases} \alpha = D + iC, & \beta = - B + iA, \\ \gamma = B + iA, & \delta = \quad D - iC. \end{cases}
$$

Our new parameters are thus imaginary combinations of the real parameters in ordinary use. Mathematical physics affords many examples of the advantage to be gained by employing such imaginary combinations of real quantities. It is only necessary to cite the use made of them in optics by Cauchy.

I may remark that Darboux in his *Leçons sur la théorie générale des surfaces*, Livre I., treats the subject of rotation in a manner which is very similar to that which we have followed. But with him the ζ itself is considered directly as a function of the time and not the separate coefficients α, β, γ, δ. His method thus lacks the simplicity which is possible when these are made the primary functions.

We now turn to a brief consideration of the meaning of the substitution

$$
\zeta = \frac{\alpha Z + \beta}{\gamma Z + \delta},
$$

when α, β, γ, δ are still regarded as functions of the time, but are general complex quantities, not connected by the special relations $\alpha = \bar{\delta}$, $\beta = -\bar{\gamma}$.

We shall consider t also as capable of complex values, not for the sake of studying the behavior of a fictitious, imaginary time, but because it is only by taking this step that it becomes possible to bring about the intimate association of kinetics and the theory of functions of a complex variable at which we are aiming.

What is the meaning of the above formula? It is still a real transformation of the sphere on which we have defined ζ into itself, a linear transformation in which the coefficients are all real.

If the radius of the sphere be 1, as we shall assume throughout the discussion of this general transformation, or its equation when written homogeneously, be:

$$x^2 + y^2 + z^2 - t^2 = 0,$$

the equations connecting x, y, z, t and X, Y, Z, T are those indicated in the following scheme:

(6)		$X + iY$	$X - iY$	$T + Z$	$T - Z$
	$x + iy$	$\alpha\bar{\delta}$	$\beta\bar{\gamma}$	$\alpha\bar{\gamma}$	$\beta\bar{\delta}$
	$x - iy$	$\gamma\bar{\beta}$	$\delta\alpha$	$\gamma\bar{\alpha}$	$\delta\bar{\beta}$
	$t + z$	$\alpha\bar{\beta}$	$\beta\bar{\alpha}$	$\alpha\ddot{\alpha}$	$\beta\bar{\beta}$
	$t - z$	$\gamma\bar{\delta}$	$\delta\bar{\gamma}$	$\gamma\bar{\gamma}$	$\delta\bar{\delta}$

and when these equations are solved for x, y, z, t, in terms of X, Y, Z, T, it will be found that the coefficients are real, as has been already stated.

This scheme may be derived in a manner analogous to that followed in deriving the scheme (4).

The equation of the sphere

$$x^2 + y^2 + z^2 - t^2 = 0,$$

or $$(x + iy)(x - iy) + (z + t)(z - t) = 0,$$

may, as is readily verified, be written in the form,

$$x + iy : x - iy : t + z : t - z = \zeta_1\zeta_2' : \zeta_2\zeta_1' : \zeta_1\zeta_1' : \zeta_2\zeta_2',$$

where $\dfrac{\zeta_1}{\zeta_2} = \zeta$, and ζ_1', ζ_2' are, for real values of x, y, z, t, the conjugate imaginaries to ζ_1, ζ_2 respectively.

As above, $$\zeta = \frac{x + iy}{t - z} = \frac{t + z}{x - iy}.$$

If then Z_1, Z_2, Z_1', Z_2' be quantities similarly defined with respect to the movable sphere

$$X^2 + Y^2 + Z^2 - T^2 = 0,$$

we have corresponding to the transformation

$$\zeta = \frac{\alpha Z + \beta}{\gamma Z + \delta},$$

the two pairs of equations:

$$\zeta_1 = \alpha Z_1 + \beta Z_2, \qquad \zeta_1' = \bar{\alpha} Z_1' + \bar{\beta} Z_2',$$
$$\zeta_2 = \gamma Z_1 + \delta Z_2, \qquad \zeta_2' = \bar{\gamma} Z_1' + \bar{\delta} Z_2',$$

if the transformation is to be real.

And from this series of equations it follows by the reasoning used on page 10 that $x + iy$ is equal to

$$\alpha\bar{\delta}(X+iY) + \beta\bar{\gamma}(X+iY) + \alpha\bar{\gamma}(T+Z) + \beta\bar{\delta}(T-Z),$$

and $x - iy$, $t + z$, $t - z$ to the corresponding expressions indicated in scheme (6).

The scheme (6) at once reduces to the scheme (4) when the special supposition is made that $\alpha = \bar{\delta}$ and $\beta = -\bar{\gamma}$. And since this is the sufficient and necessary condition that (6) reduce to (4), we have here an independent demonstration that these relations hold good among the parameters α, β, γ, δ when the motion is a rotation about a fixed point.

The general transformation (6) represents the totality of those projective transformations or collineations of space for which each system of generating lines of the sphere, $x^2 + y^2 + z^2 - t^2 = 0$, is transformed into itself, and among which all rotations of the sphere are obviously included as special cases. This is the geometrical meaning of the equation

$$\zeta = \frac{\alpha Z + \beta}{\gamma Z + \delta}$$

for unrestricted values of α, β, γ, δ.

But the transformation admits also of a very interesting kinematical interpretation which I shall consider at length in my third lecture. With respect to it our sphere of radius 1 plays the rôle of the fundamental surface or "absolute" in the Cayleyan or hyperbolic non-Euclidian geometry. For any free motion in such a space the absolute remains fixed in position as in ordinary space the imaginary circle at infinity $x^2 + y^2 + z^2 = 0$, $t = 0$, does, which is its absolute.

The transformation therefore represents a real free motion in non-Euclidean space, and the six independent real parameters involved in the ratios $\alpha : \beta : \gamma : \delta$ correspond to the ∞^6 such possible motions. Interpreted in Euclidean space, the transformation represents a motion of the body combined with a strain.

I close the present lecture with two remarks.

First, *there is nothing essentially new in the considerations with which we have been occupied thus far.* I have merely attempted to throw a method already well known into the most convenient form for application to mechanics.

Second, *the non-Euclidean geometry has no metaphysical significance here or in the subsequent discussion.* It is used solely because it is a convenient method of grouping in geometric form relations which must otherwise remain hidden in formulas.

LECTURE II

I NOW proceed at once to the discussion of the Lagrange equations of motion for our top, only pausing to remark once more that this problem of the top is for us typical of all dynamical questions which are related to a sphere. To this category belong also the problem of the spherical pendulum (which in fact is a special case of the problem of the top), the problem of the catenary on the sphere, and all problems of the motion of a rigid body about a fixed point. The simplest problem of the type is that of the motion of a rigid body about its centre of gravity, the Poinsot motion, as we shall name it after Poinsot who treated it very elegantly.

We shall first state the equations in terms of the astronomical parameters; and to give the expressions as simple a form as possible, I shall suppose the principal moments of inertia of the top about the fixed point of support each equal to 1. One may call such a top a spherical top, as its momental ellipsoid is a sphere. I wish it understood, however, that this restriction is not essential to the application of our method, but is rather made solely for the sake of rendering its presentation more easy.

On this assumption, we have for the kinetic energy, T, of the motion the expression

$$T = \frac{1}{2}(\phi'^2 + \psi'^2 + 2\,\phi'\psi'\cos\vartheta + \vartheta'^2),$$

where ϑ', ϕ', ψ' are the derivatives of ϑ, ϕ, ψ with respect to t; and for the potential energy, V, the expression

$$V = P\cos\vartheta,$$

where P represents the static moment of the top with respect to O.

The Lagrange equations are:

$$\frac{d\dfrac{\delta T}{\delta\phi'}}{dt} = 0, \quad \frac{d\dfrac{\delta T}{\delta\psi'}}{dt} = 0, \quad \frac{d\dfrac{\delta T}{\delta\vartheta'}}{dt} = \frac{\delta(T - V)}{\delta\vartheta}.$$

The first two equations are especially simple in having their right members equal to zero, and we are therefore able to derive immediately the two algebraic first integrals

$$\phi' + \psi'\cos\vartheta = n,$$
$$\psi' + \phi'\cos\vartheta = l.$$

The quantities n and l are constants of integration, to be determined from the initial conditions of the motion. In the following discussion we shall suppose them positive.

In addition to these integrals, we have the equation of energy

$$T + V = h,$$

where h also is a constant determined, like l and n, by the special conditions of the problem.

Solving the first two equations for ϕ' and ψ', and substituting the results in the third, and setting $\cos\vartheta = u$, and

$$U = 2\,Pu^3 - 2\,hu^2 + 2\,(ln - P)\,u + 2\,h - l^2 - n^2,$$

we obtain finally for t, ϕ, and ψ, expressed as functions of u, the formulas

$$t = \int\frac{du}{\sqrt{U}},\quad \phi = \int\frac{n - lu}{1 - u^2}\,\frac{du}{\sqrt{U}},\quad \psi = \int\frac{l - nu}{1 - u^2}\,\frac{du}{\sqrt{U}}.$$

The problem of the motion of the top is thus reduced to three simple integrations or quadratures, as indeed was demonstrated by Lagrange himself. These integrals are elliptic integrals, U being a polynomial of the third degree in u, the first an elliptic integral of the "first kind" (which is characterized by being finite for all values of the independent variable), the remaining two elliptic integrals of a more complex character.

It is often said that dynamics reached its ultimate form in the hands of Lagrange, and the cry "return to Lagrange" is frequently raised by those who set little store by the value for physical science of recent developments in the pure mathematics. But this is by no means just. Lagrange reduced our problem to quadratures, but Jacobi made a great stride beyond him, as we mathematicians think, by introducing the elliptic functions, which enabled him to assign to t the rôle of independent variable and to discuss the remaining variables u, ϕ, ψ directly as functions of the time. *An advantage was thus gained not only for the understanding of the essential relations of the variables to one another, but for simplicity of computation also.* The coefficients a, b, c, a', $\cdots$, are *uniform* (or one valued) functions of t, and one of the most useful properties a function can possess, if its values must be computed, is that it be uniform. This work of Jacobi is not as well known as it should be, having first appeared posthumously, in the second volume of his collected works, published by the Berlin Academy in 1882. I may add that his pupils, Lottner and Somoff, developed the same method in papers published in 1855 independently. It is shown in these papers that the nine cosines a, b, c, $\cdots$, may be expressed in terms of theta functions.*

* As is well known, Jacobi gave analogous formulas for the nine cosines of the Poinsot motion in 1849. Closely related to this representation of the cosines is the interesting theorem to which we shall return later on, that the motion of our top may be reproduced by compounding two Poinsot motions.

But while the a, b, c, $\cdots$, considered as functions of t, are much simpler than the integrals of Lagrange, they are at the same time much more complicated than our parameters α, β, γ, δ. These parameters prove to be the simplest possible elliptic functions of t; so that by introducing them we carry to its completion the work begun by Jacobi, of reducing our problem to its simplest elements.

For the proper understanding of this treatment of the motion of the top, some knowledge of the nature of elliptic functions is obviously necessary; and I know of no readier means of gaining this than *Riemann's method of conformal representation*, — of which, moreover, we shall have other important applications to make later on.

In accordance with this method, we construct the "Riemann surface" of the function $\sqrt{U}$ on the plane of the complex variable u, in the following manner: The polynomial U vanishes for three values of u, all of which may readily be shown to be real, and becomes infinite when $u = \infty$. Two of these roots, e_1, e_2, lie between -1 and $+1$; and the third, e_3, between $+1$ and ∞. Therefore, $\sqrt{U}$ is a two-valued function of u everywhere in the u-plane, except at the four points of the real axis, e_1, e_2, e_3, e_∞. To obtain a surface, therefore, between whose points and the values of $\sqrt{U}$ there shall be a one-to-one correspondence, we lay over the u-plane two sheets, which are everywhere distinct except at the points e_1, e_2, e_3, e_∞, in which they coalesce, and associate with the points in the two sheets which lie immediately over any point u in the u-plane, the two corresponding values of $\sqrt{U}$, one with each.

It will be found that if the point u describe any simple circuit in the u-plane, which encloses one and but one of the points e_1, e_2, e_3, e_∞, returning finally to its initial position, $\sqrt{U}$ will pass from the one to the other of the two values which correspond to the initial value of u; the point corresponding to u in the Riemann surface of $\sqrt{U}$, must, therefore, move from a position in the one sheet to a position immediately under (or over) this in the other. But this is possible only if we suppose the two sheets to cross along some line running out from each of the points, e_1, e_2, e_3, e_∞, — not to intersect, but to cross, as non-intersecting lines in space may be said to cross. Inasmuch as this is the simplest hypothesis possible, we shall take as these lines of crossing, in the present case, the segments, e_1e_2, e_3e_∞, of the real axis; and have, as a rough representation of the Riemann surface of $\sqrt{U}$, the following figure:

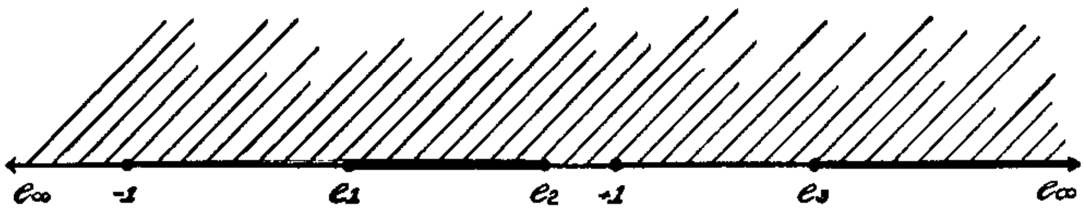


Fig. 1.

where we have shaded the positive half-sheets of the surface and have marked the segments, e_1e_2, e_3e_∞ by heavy lines.

The points, e_1, e_2, e_3, e_∞, are called the "branch points" and the segments, e_1e_2, e_3e_∞, the "branch lines" of the surface.

To construct in the t-plane the figure which is the conformal representation of this Riemann surface, we conceive of this surface as cut into four half-sheets, by an incision made all along the real axis, and seek first the conformal representation of the upper half-sheet. To obtain this, we cause the point u to move, in the positive sense, along the real axis, from e_1 through $e_2e_3e_\infty$, back (from the left) to e_1 and study the corresponding changes of value of t by means of the integral, $t=\int\frac{du}{\sqrt{U}}$, by which it is defined.

We thus find that as the point u traces out the real axis in its plane, the corresponding t traces out a rectangle in its plane, which we may represent by the figure:

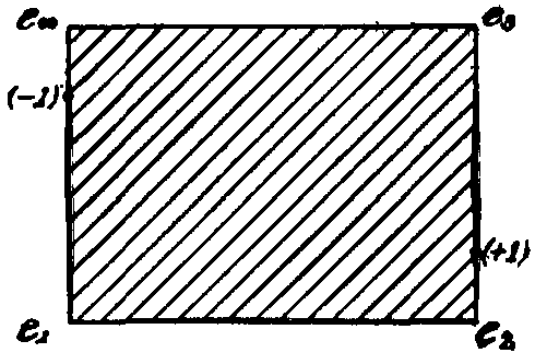


FIG. 2.

to the angular points of which we have attached the values of u to which they correspond, and which we have shaded, since the sense in which its perimeter was traced shows that it is its interior which corresponds to the shaded half-plane of the preceding figure.*

As long as the integral which defines t is left an indefinite integral, this rectangle remains free to occupy any position in the t-plane, — only the directions of its sides, parallel respectively to the real and imaginary axes, and their lengths, — call them ω_1 and ω_2, — are completely determined. But when the integral is made definite, by making e_∞ the lower limit of integration, the angular point, e_∞, coincides with the origin in the t-plane, and the rectangle takes a definite position in the plane.

From the image which we have thus obtained of the one half-sheet, the images of the three remaining half-sheets are to be had at once by the process of "symmetrical reproduction"; which yields for the Riemann surface, when cut in the manner indicated, the complete image:

* The figure is a rectangle since $\sqrt{U}$ is real from $u = e_1$ to $u = e_2$, and from $u = e_3$ to $u = e_\infty$, and a pure imaginary from $u = e_\infty$ to $u = e_1$, and from $u = e_2$ to $u = e_3$. At e_i, $t -$ const. vanishes as $(u - e_i)^{\frac{1}{2}}$.

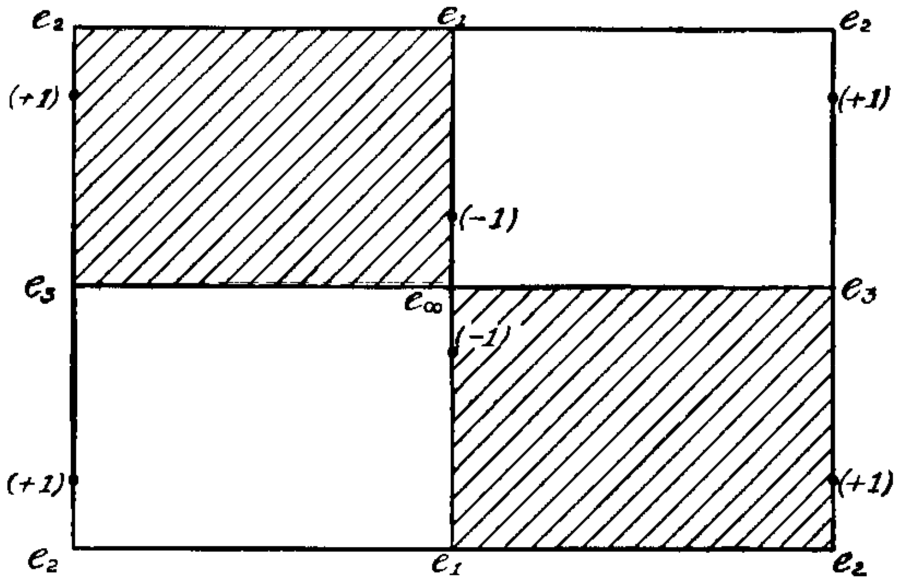


FIG. 3.

The symmetry of the figure with respect to the sides, $e_\infty e_1$, and $e_\infty e_3$, of the original rectangle, will be at once noticed. Each of the four smaller rectangles is the image of one half-sheet; the shaded, of the positive half-sheets; the non-shaded, of the negative.

But we have not yet obtained the complete geometrical representation of u, regarded as a function of t. The Riemann surface of two sheets, which we have thus far been considering, possesses a distinct point for every value of $\sqrt{U}$ regarded as a function of u, but not for t when so regarded. The integral t is affected by an additive constant if u be made to trace in the Riemann surface a closed path which surrounds e_1e_2, or one which surrounds e_2e_3, so that the Riemann surface of t is one possessing the same branch points as the Riemann surface of $\sqrt{U}$, but having an infinite number of sheets, into any one of which it is possible to move the tracing point, u, if no such cut be made in the surface as that made above along the real axis.

It is a great advantage of the Riemann method that the complete image in the t-plane of this uncut Riemann surface of an infinite number of sheets may be had from the image already obtained for the cut surface, by simply affixing a rectangle, congruent with this image, to each of its sides, repeating the process for the new rectangles, and so on indefinitely, until the entire t-plane is covered by congruent rectangles, any one of which may be brought into coincidence with any other by two translations, one in the direction of the real, the other in the direction of the imaginary, axis.

From the result of this construction, there at once follows a conclusion of the very first importance. The image of the complete Riemann surface of t entirely covers the t-plane, *but without the overlapping of any of its parts.* It follows immediately, therefore, that to each point in the t-plane there corresponds but a single point in the Riemann surface, or that u, and $\sqrt{U}$ as well, is a *uniform* function of t.

The equation connecting t and u is:

$$t = \int_{\infty}^{u} \frac{du}{\sqrt{U}}.$$

And the conclusion which we have reached is, that the functional relation of u with respect to t, defined by this equation, is vastly more simple than that of t with respect to u; to each value of u there corresponded an infinite number of values of t, while to each value of t there corresponds but one value of u. As thus defined, u is called an *elliptic function* of t.

Let ω_1 be the length of the side $e_\infty e_3$ of the small rectangle, which was the image of a half-sheet of the Riemann surface, and ω_2 the length of the side $e_\infty e_1$; then, obviously, if we set $u = \phi(t)$, and t_0 be any point of the complete rectangle (Fig. 3), since $t_0 + m_1 2\,\omega_1 + m_2 2\,i\omega_2$ is for any integral values of m_1, m_2, the corresponding point of another of the rectangles, $\phi(t_0 + 2\,m_1\omega_1 + 2\,m_2 i\omega_2) = \phi(t_0)$; or the elliptic function, u, is *doubly periodic*, with the periods $2\,\omega_1$, $2i\omega_2$.

Let us next consider the nature of ϕ and ψ when regarded as functions of t. The integrals by which they are expressed in terms of u are elliptic integrals of greater complexity than is the integral for t. There are on the Riemann surface of $\sqrt{U}$ four points, at which each of these integrals becomes logarithmically infinite; namely, the points -1, $+1$, in the upper sheet, and the same points in the lower sheet. Elliptic integrals possessing such points of logarithmic discontinuity are called "elliptic integrals of the third kind," and it is possible to express any such integral in terms of integrals of the first kind and "normal" integrals of the third kind, such, namely, as possess but two points of logarithmic discontinuity with the residues $+1$ and -1 respectively.

But if instead of making this reduction of the integrals directly, we introduce those combinations of ϕ and ψ which constitute our parameters α, β, γ, δ, *a remarkable simplification at once ensues such as renders any further reduction unnecessary.* Surely a preestablished harmony exists between the problem before us, and our parameters α, β, γ, δ.

Since $$\alpha = \cos\frac{\vartheta}{2}\cdot e^{\frac{i(\phi+\psi)}{2}},$$

and $$\cos\frac{\vartheta}{2} = \sqrt{\frac{u+1}{2}},$$

we have immediately

$$\log\alpha = \tfrac{1}{2}\log\frac{1+u}{2} + \frac{i(\phi+\psi)}{2}$$

$$= \int\frac{\sqrt{U}+i(l+n)}{2(u+1)}\cdot\frac{du}{\sqrt{U}} - \tfrac{1}{2}\log 2,$$

when for ϕ and ψ their values are substituted.

And in like manner,

$$\log \beta = \int \frac{\sqrt{U} - i(l-n)}{2(u-1)} \cdot \frac{du}{\sqrt{U}} - \tfrac{1}{2}\log 2,$$

$$\log \gamma = \int \frac{\sqrt{U} + i(l-n)}{2(u-1)} \cdot \frac{du}{\sqrt{U}} - \tfrac{1}{2}\log 2,$$

$$\log \delta = \int \frac{\sqrt{U} - i(l+n)}{2(u+1)} \cdot \frac{du}{\sqrt{U}} - \tfrac{1}{2}\log 2,$$

and *these are all normal integrals of the third kind, each with but two points of logarithmic discontinuity* which are distributed in the rectangle of the periods as indicated in the accompanying figure, if we sup-

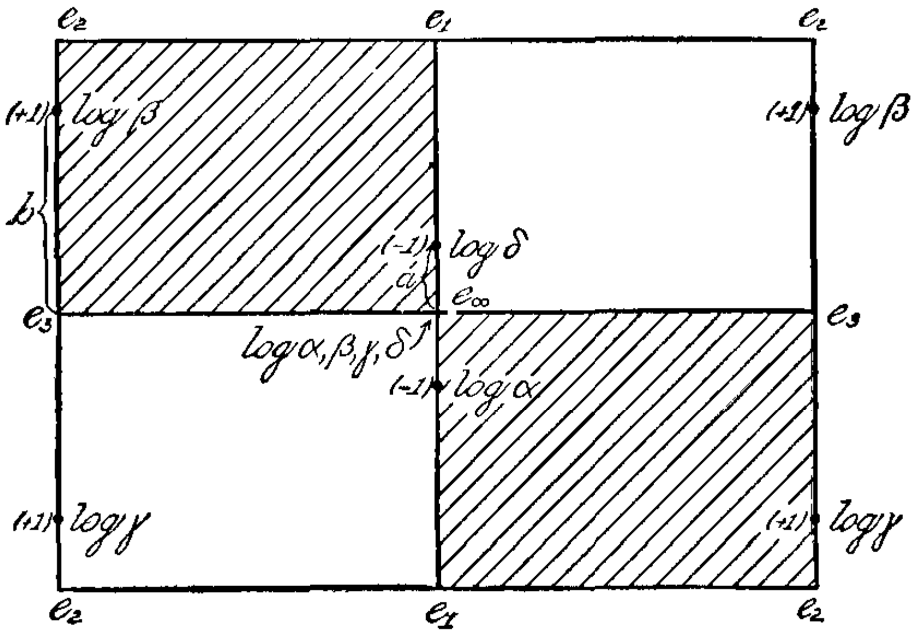


Fig. 4.

pose as we shall find it convenient to do later on that l is less than n.

For $U = -(l+n)^2$ when $u = -1$, and $U = -(l-n)^2$ when $u = +1$. If, therefore, of the two values of $\sqrt{U}$, which correspond to $u = -1$, we take $i(l+n)$, the factor $\sqrt{U} + i(l+n)$ in the numerator of the expression for $\log \alpha$ will be canceled by the factor $2\sqrt{U}$ in the denominator, while if we take $-i(l+n)$, the numerator vanishes; so that the point -1 in *one* of the sheets of the Riemann surface of $\sqrt{U}$ is the only finite point of discontinuity of the integral $\log \alpha$. It is, moreover, a logarithmic discontinuity with the residue 1, since $\log \alpha$ there becomes ∞ as $\log(u+1)$. On the other hand, for $u = \infty$, *i.e.* at e_∞, $\log \alpha$ becomes infinite as $\frac{1}{2} \log u$. This again is a logarithmic discontinuity, with the residue -1, since e_∞ is at infinity and a branch point. And like considerations apply to the remaining integrals.

By the introduction of the parameters α, β, γ, δ, therefore, the four logarithmic discontinuities of the integrals ϕ, ψ, are assigned one to each of the four normal integrals $\log \alpha$, $\log \beta$, $\log \gamma$, $\log \delta$ — normal integrals whose remaining points of discontinuity, corresponding to e_∞, coincide at the origin.

While $\log \alpha$, $\log \beta$, $\log \gamma$, $\log \delta$, as now defined are much simpler functions of u, and therefore of t, than are ϕ and ψ, their exponentials α, β, γ, δ are simpler still. These are uniform functions of t having each one null-point and one ∞-point in every parallelogram of periods. Such functions may always be expressed, apart from an exponential factor, by the quotient of two ϑ- or two σ-functions of the simplest kind — functions which possess one null-point in each parallelogram of periods, but no ∞-point.

Of the ϑ-functions we shall only pause to remark that Jacobi introduced them into analysis as being the simplest elements out of which the elliptic functions could be constructed. He obtained for them expressions in the form of infinite products and infinite series. They are affected by an exponential factor when the argument is increased by a period, but remain otherwise unchanged. The ϑ-functions of the simplest class, with which alone we are concerned, vanish when the argument takes the value zero or a congruent value.

The σ-function of Weierstrass is a more elegant function of the same character.

Inasmuch, therefore, as α, β, γ, δ, are functions of t, which vanish for $t = -ia$, $\omega_1 + ib$, $\omega_1 - ib$, $+ia$ respectively (the values of t corresponding to the points $u = \pm 1$ in the above figure) and which all become infinite for $t = 0$, we have for them the following expressions:

$$\alpha = k_1 e^{\lambda_1 t} \frac{\sigma(t + ia)}{\sigma(t)}, \qquad \beta = k_2 e^{\lambda_2 t} \frac{\sigma(t - \omega_1 - ib)}{\sigma(t)},$$

$$\gamma = k_3 e^{\lambda_3 t} \frac{\sigma(t - \omega_1 + ib)}{\sigma(t)}, \qquad \delta = k_4 e^{\lambda_4 t} \frac{\sigma(t - ia)}{\sigma(t)},$$

where k_i, λ_i are constants to be determined from the initial conditions of the motion. Their values depend on those of the "transcendental" constants ω_1, ω_2, a, b, as the values of these in turn depend on those of the "algebraic" constants, P, h, l, n.

We shall call functions such as α, β, γ, δ, which miss being doubly periodic by an exponential factor only, "multiplicative elliptic functions." All elliptic functions are expressible as quotients of ϑ- or σ-functions, and evidently of such quotients the simplest possible are those which have a single ϑ or σ of the simplest kind in both numerator and denominator. We may therefore state the result of our discussion in these terms: *We have shown that our parameters* α, β, γ, δ *are multiplicative elliptic functions of the simplest kind, so that by introducing them we have resolved the problem of the top into its simplest elements.*

From these expressions for α, β, γ, δ one may obtain expressions for the nine direction cosines $a, b, c \cdots$ in the form of quotients of σ- or ϑ-functions — such as Jacobi got for them — with the least possible reckoning.*

* Hess has remarked, in his paper on the gyroscope (*Math. Ann.* xxix., 1887) that the *quaternion* expressions for the nine direction cosines are very simple, and our parameters are but linear combinations of the quaternion parameters. Hess, however, makes no direct use of our parameters and probably was not aware of the formula, $\zeta = \dfrac{\alpha Z + \beta}{\gamma Z + \delta}$, which lies at the basis of our discussion.

LECTURE III

In the lecture of yesterday we reached the conclusion that our parameters α, β, γ, δ may be expressed as quotients of simple σ-functions of the time t, and we now turn to the geometrical interpretation of these formulas.

As I have already asked you to notice, α, β, γ, δ are not ordinary elliptic functions of t, but functions which are affected by an exponential factor when t is increased by a period; in consequence of which I called them "multiplicative elliptic functions." When t is increased by the period $2\omega_1$, they are affected by an imaginary factor of the form $e^{i\psi}$, and when t is increased by the period $2i\omega_2$, by a real factor of the form κ.

Let us first of all consider *the curve described by the apex of the top on the fixed sphere.* This is the point $Z=\infty$ of the movable sphere, so that, reverting to the formula:

$$\zeta=\frac{\alpha Z+\beta}{\gamma Z+\delta},$$

it is obvious that the equation of the curve is

$$\zeta=\frac{\alpha}{\gamma}=ke^{\lambda t}\,\frac{\sigma(t+ia)}{\sigma(t-\omega_1+ib)}.$$

Like α, β, γ, δ, this ζ is defined in terms of t by a multiplicative elliptic function of the first degree, involving besides the exponential factor only the quotient of two simple σ-functions.

This is an essential simplification of the representations of this motion given hitherto. Thus, were one to apply the methods used by Hermite in his *Applications des fonctions elliptiques*, published twenty years ago, and start not from the equation of ζ in terms of Z, but from those of $x+iy$, $-z$, $-x+iy$ in terms of $X+iY$, $-Z$, $-X+iY$ (see page 8), one would obtain for the motion of the apex of the top (whose coordinates are 0, 0, 1), the equation

$$x+iy=-2\,\alpha\beta,$$

which represents the motion by means of a multiplicative elliptic function of the second order. The curve thus defined is not the curve traced by the apex on the fixed sphere, but the orthogonal projection of this curve on the xy-plane.

I shall, for convenience, call curves like those which we have just been considering "multiplicative elliptic curves," distinguishing when necessary between those on the sphere and those on the plane, and assigning to them a degree corresponding to the number of simple σ-quotients in the expressions which define them. Thus the curve traced by the apex of the top on the fixed sphere is a multiplicative elliptic curve of the first degree, its orthogonal projection one of the second degree. The earliest example of such a curve of the first degree is the herpolhode of a Poinsot motion, the motion of a body about its centre of gravity. That this herpolhode is such a curve was first shown by Jacobi.*

It is easy to get a notion of the geometrical character of the curve traced by the apex of the top. For the particular case when $l - ne_2 = 0$, the stereographic projection of the curve has the shape indicated in the following figure:

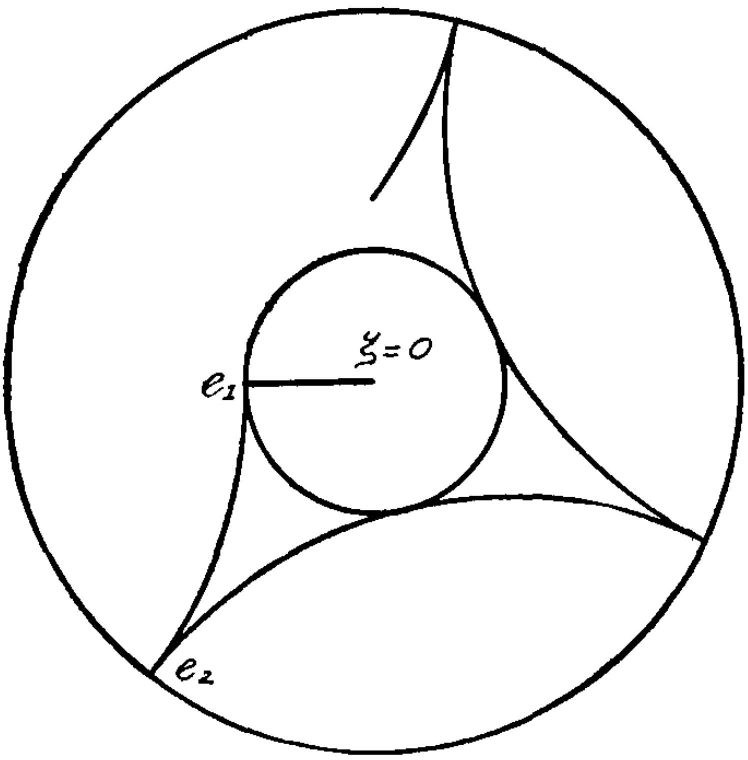


FIG. 5.

* Concerning the multiplicative elliptic curves, see Miss Winston's dissertation: *Ueber den Hermiteschen Fall der Laméschen Differentialgleichung*, Göttingen, 1897.

As we wish to restrict t to real values, we here make e_1 the lower limit of integration of the integral $t = \int \frac{du}{\sqrt{U}}$, or what comes to the same thing, suppose the t of the preceding formulas replaced by $t' = t + i\omega_2$.

The radius of the circle marked $u = e_1$ is the modulus of those points ζ for which t is 0, $2\,\omega_1, \cdots$; for all these points $u = e_1$. On the other hand, the radius of the circle marked $u = e_2$ is the modulus of those points ζ for which $t = \omega_1$, $3\,\omega_1, \cdots$.

The curve of the figure is that traced by the stereographic projection of ζ as t varies through real values, and consists of an infinite number of congruent arcs which touch the inner circle and form cusps at the outer one. If the top be given an initial thrust sideways (when $l - ne_2$ is no longer 0), these cusps will be replaced by loops or wave-crests.

Evidently any one of these arcs may be brought into coincidence with the consecutive one by one and the same rotation about the origin. The transformation which effects this rotation is $\zeta' = e^{i\psi_0}\zeta$, so that the meaning of the imaginary factor $e^{i\psi_0}$, by which ζ is affected when t is increased by the real period $2\,\omega_1$ is perfectly obvious. We shall find that since ζ is affected by the real factor κ when t is increased by the imaginary period $2\,i\omega_2$, the effect on the curve of this increase in t is to transform it into a curve similar to itself, and symmetrically placed with respect to the origin.

But before attempting a more minute examination of the curve traced by the apex of the top, let us consider *the polhode and herpolhode of the motion.*

On each instantaneous axis of rotation let a segment be measured from the fixed point, equal in sense and magnitude to the amount of rotation about this axis. The aggregate of these segments constitute a portion of one cone if they be caused to remain fixed in the moving body, of another if they be caused to remain fixed in space. The first cone, or the curve in which its elements terminate, is called the "polhode," the second the "herpolhode," and it is evident that the motion of the body may be had by rolling the first cone or curve on the second cone or curve.

To obtain the equation of the polhode, consider the infinitesimal rotation in time dt about the axis for which the components of rotation with respect to X, Y, Z, are p, q, r, respectively. The axis is for the instant fixed in space, and we have for the effect of the rotation on any point of the moving sphere the equations:

$$X = + X' \quad - rdtY' + qdtZ',$$
$$Y = + rdtX' + Y' \quad - pdtZ',$$
$$Z = - qdtX' + pdtY' + Z',$$

For this motion therefore the quaternion parameters (see page 4) are:

$$A' = \frac{p}{2}dt, \quad B' = \frac{q}{2}dt, \quad C' = \frac{r}{2}dt, \quad D' = 1,$$

and therefore the corresponding parameters $\alpha, \beta, \gamma, \delta$ are:

$$\alpha' = 1 + \frac{ir}{2}dt, \qquad \beta' = \frac{-q + ip}{2}dt,$$
$$\gamma' = \frac{q + ip}{2}dt, \qquad \delta' = 1 - \frac{ir}{2}dt.$$

If therefore α, β, γ, δ (unprimed) be the parameters of the transformation from the axes X, Y, Z fixed in the body to the axes x, y, z fixed in space, we may obtain the parameters $\alpha + d\alpha$, $\beta + d\beta$, $\gamma + d\gamma$, $\delta + d\delta$ of the transformation which defines the position of the body after the infinitesimal rotation, by combining the two substitutions:

$$\zeta_1 = \alpha\zeta_1' + \beta\zeta_2', \qquad \zeta_1' = \alpha' Z_1 + \beta' Z_2,$$
$$\zeta_2 = \gamma\zeta_1' + \delta\zeta_2', \qquad \zeta_2' = \gamma' Z_1 + \delta' Z_2,$$

the result of which is:

$$\zeta_1 = (\alpha\alpha' + \beta\gamma')Z_1 + (\alpha\beta' + \beta\delta')Z_2,$$
$$\zeta_2 = (\gamma\alpha' + \delta\gamma')Z_1 + (\gamma\beta' + \delta\delta')Z_2.$$

It follows, therefore, that

$$\alpha + d\alpha = \alpha\alpha' + \beta\gamma', \qquad \beta + d\beta = \alpha\beta' + \beta\delta',$$
$$\gamma + d\gamma = \gamma\alpha' + \delta\gamma', \qquad \delta + d\delta = \gamma\beta' + \delta\delta',$$

whence
$$d\alpha = \left(\frac{ir}{2}\alpha + \frac{q + ip}{2}\beta\right)dt,$$
$$d\beta = \left(\frac{-q + ip}{2}\alpha - \frac{ir}{2}\beta\right)dt,$$
$$d\gamma = \left(\frac{ir}{2}\gamma + \frac{q + ip}{2}\delta\right)dt,$$
$$d\delta = \left(\frac{-q + ip}{2}\gamma - \frac{ir}{2}\delta\right)dt.$$

Whence finally:
$$p + iq = 2i\left(\beta\frac{d\delta}{dt} - \delta\frac{d\beta}{dt}\right),$$
$$-p + iq = 2i\left(\alpha\frac{d\delta}{dt} - \delta\frac{d\alpha}{dt}\right),$$
$$r = 2i\left(\alpha\frac{d\delta}{dt} - \gamma\frac{d\beta}{dt}\right).$$

We will not stop to derive the corresponding equations for the components π, κ, ρ of the herpolhode. They differ from those just obtained for p, q, r only in having α and δ interchanged and the signs of β and γ changed.

But I wish to make two remarks which are suggested by the above reckoning, with regard to the usefulness of our parameters α, β, γ, δ. The one is that two linear substitutions in terms of them combine binarily instead of quaternarily as do the corresponding quaternion substitutions; the other, that the four linear differential equations which define them in terms of t, p, q, r break up into two pairs, in one of which only α and β are involved, in the other only γ and δ. To appreciate how important this advantage is, one need only compare with our discussion the discussion of the same question in Darboux's *Leçons sur la théorie générale des surfaces.*

Returning to our spherical top, and substituting in the general equations which we have just obtained the values of $\alpha, \beta, \gamma, \delta$ which characterize its motion, we have for its polhode and herpolhode not equations of the second degree, as was to have been expected from the expressions for $p + iq$, etc. in terms of $\alpha, \beta, \gamma, \delta$, but much simpler expressions. I cannot give the reckoning which leads to them since I have not given the values of the constants $k_1, \lambda_1, \cdots$ which appear in the formulas on page 31. But the expressions themselves are of the form

$$p + iq = k' e^{\lambda' t} \frac{\sigma(t + \omega_1 - ia - ib)}{\sigma(t)}, \quad r = n;$$

$$\pi + i\kappa = k'' e^{\lambda'' t} \frac{\sigma(t + \omega_1 - ia + ib)}{\sigma(t)}, \quad \rho = l.$$

Both the polhode and the herpolhode of the spherical top are elliptic plane curves of the first degree. Darboux has given this result in his edition of Despeyrous' Mechanics, obtaining it by the use of elliptic integrals instead of elliptic functions. He does not call the curves elliptic curves of the first degree, but curves of the same character as the herpolhode of a Poinsot motion. It should be added that the curves are of the first degree in the case of the *spherical* top only.

Our theorem is closely connected with the celebrated theorem of Jacobi already mentioned: that the motion of the top may be represented by the relative motion of two Poinsot motions (or rotations about the centre of gravity); for both the polhode and herpolhode of the top's motion are themselves herpolhodes of Poinsot motions, being elliptic curves of the first degree. One may demonstrate Jacobi's theorem most simply by expressing the α, β, γ, δ of each of the Poinsot motions in terms of t, and then combining the two motions.

I may finish this part of my discussion with the remark that the attention of students of the geometry of Salmon and Clebsch is apt to be confined too exclusively to algebraic curves. We have before us an illustration of the value of transcendental curves. It is only in the very exceptional case when the multiplicative factor $\kappa = 1$, and ψ_0 is commensurable with π, that the curves we have been studying become algebraic.

To sum up the conclusions which we have thus far established; we have proved that *the motion of* *the spherical top on a fixed point of support may be completely defined geometrically in terms of elliptic curves of the first degree.* We have also shown that the variation of the parameters α, β, γ, δ with the time t may be pictured by curves of the same character.

Let us now resume the study of the *curve traced by the apex of the top.*

The parameters α, β, γ, δ, and ζ are all elliptic functions of the argument t, and the full meaning of elliptic functions comes to light only when the argument is supposed capable of taking complex values. Thus only, in particular, will the double periodicity of the functions come into evidence. There exists, then, an analytical necessity, so to speak, that we complete our geometrical study of the top's motion by extending it to complex values of t. When that has been accomplished, I shall show that to the entire aggregate of possible motions of the top in complex time there corresponds the free motion of a certain rigid body in non-Euclidean space, and thus bring to a definite outcome the considerations which I presented at the close of my first lecture.

Our problem being to determine the path traced by the point ζ when the point t is made to describe *any* path in the t-plane, it is clearly of prime importance that we determine first of all the image on the ζ-sphere of a parallelogram of periods in the

t-plane. To that, indeed, we shall confine our attention. Instead, however, of finding this image directly we shall find it easier to obtain the images of the four half-sheets of the Riemann surface of $\sqrt{U}$, of which, it will be remembered, the four smaller rectangles into which the entire parallelogram of periods was subdivided were severally the images.

Let us first reproduce (in Fig. 6) the figure of the parallelogram of periods (see page 29) and that of the Riemann surface of $\sqrt{U}$.

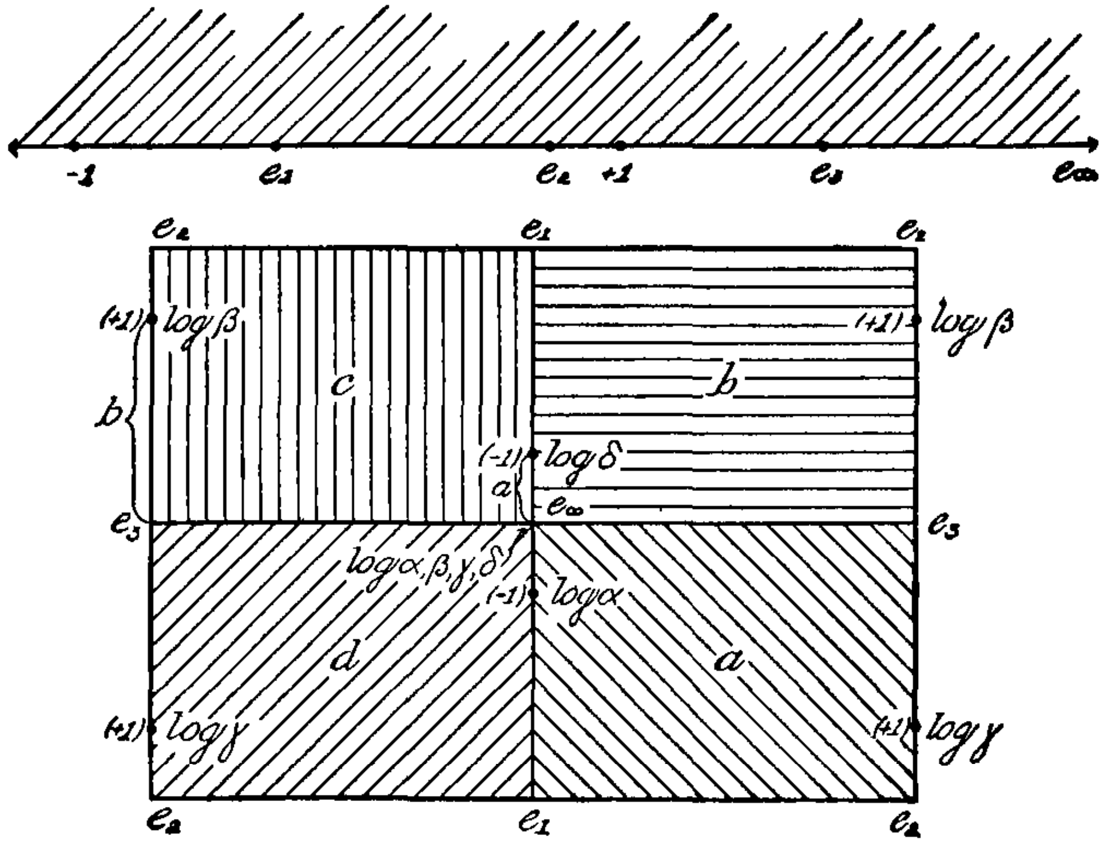


FIG. 6.

I have given different markings to all four rectangles in order to be able to distinguish readily between their several images in the figure which we are to construct. It will be remembered (see page 28) that $\log \alpha$ and $\log \gamma$ became infinite at the points $u = -1$ and $u = +1$, respectively, of one sheet of the $\sqrt{U}$-surface, and that $\log \beta$ and $\log \delta$ became infinite at the corresponding points of the other sheet — the other functions in each case remaining finite. In the figure, a and d are the images of the positive and negative halves of the first of these sheets, and c and b the images of the positive and negative halves of the second.

Our ζ is expressed in terms of u by the elliptic integral of the third kind:

$$\log \zeta = \log \left(\frac{\alpha}{\gamma}\right) = \int \frac{-\sqrt{U} + i(nu - l)}{u^2 - 1} \cdot \frac{du}{\sqrt{U}}.$$

We may now draw the following conclusions immediately:

$\frac{d}{du} \log \left(\frac{\alpha}{\gamma}\right)$ is complex along the segments $e_1 e_2$, $e_3 e_\infty$ of the real axis of the u-plane, but real along the segments $e_2 e_3$, $e_\infty e_1$. Therefore $\frac{\alpha}{\gamma}$ or ζ moves along a meridian of the ζ-sphere when u moves along the real axis from e_2 to e_3 or from e_∞ to e_1; but, on the other hand, describes one of the arcs which appeared in the figure of the real motion of the top's apex, when u moves on the real axis from e_1 to e_2, and an arc different from this, when u moves from e_3 to e_∞.

Again, $\frac{d}{du}\log\left(\frac{\alpha}{\gamma}\right)$ vanishes when $u=e_\infty$, in the first approximation as $\frac{1}{u^2}$, and takes the finite value $\frac{1}{1-e_2{}^2}$ when $u=e_2$ (this because of the hypothesis which we retain here, that $l-ne_2=0$); when $u=e_1$ or e_3, on the other hand, it becomes infinite, as $(u-e_1)^{-\frac{1}{2}}$ or $(u-e_3)^{-\frac{1}{2}}$. Therefore the curve traced by the point ζ as the point u moves along the real axis from e_∞ through e_1, e_2, e_3, to e_∞ will present angles whose measure is π at the points corresponding to e_∞ and e_2, and angles whose measure is $\frac{\pi}{2}$ at the points corresponding to e_1 and e_3.

I will not give the image of the $\sqrt{U}$-surface on the sphere, but the stereographic projection of this image on the xy-plane from the point $\zeta=\infty$. If to the explanations already given it be added that ζ, whose value in terms of t is $ke^{\lambda t}\frac{\sigma(t+ia)}{\sigma(t-\omega_1+ib)}$, becomes 0 and ∞ respectively at the points -1 and $+1$ of the contour of the half-sheet or rectangle a, and remains finite and different from 0 for all points on the contour of b, it will readily be seen that the images of the half-sheets or rectangles a, b, are roughly of the form indicated in the following figure: the two contours which we have marked $e_\infty\ e_1\ e_2\ e_3\ e_\infty$ being the stereographic projections of images of the real u-axis first when this axis is regarded as the contour of the positive half-sheet a, second when it is regarded as the contour of the negative half-sheet b.

The two arcs e_1e_2 are similar and symmetrically placed with respect to the point $\zeta = 0$. The one which lies to the left appeared in the figure of the real motion of the top's apex (Fig. 5).

If now we complete this figure by a second half symmetrical with this first half with respect to the horizontal axis e_1e_∞, we obtain the image of the entire

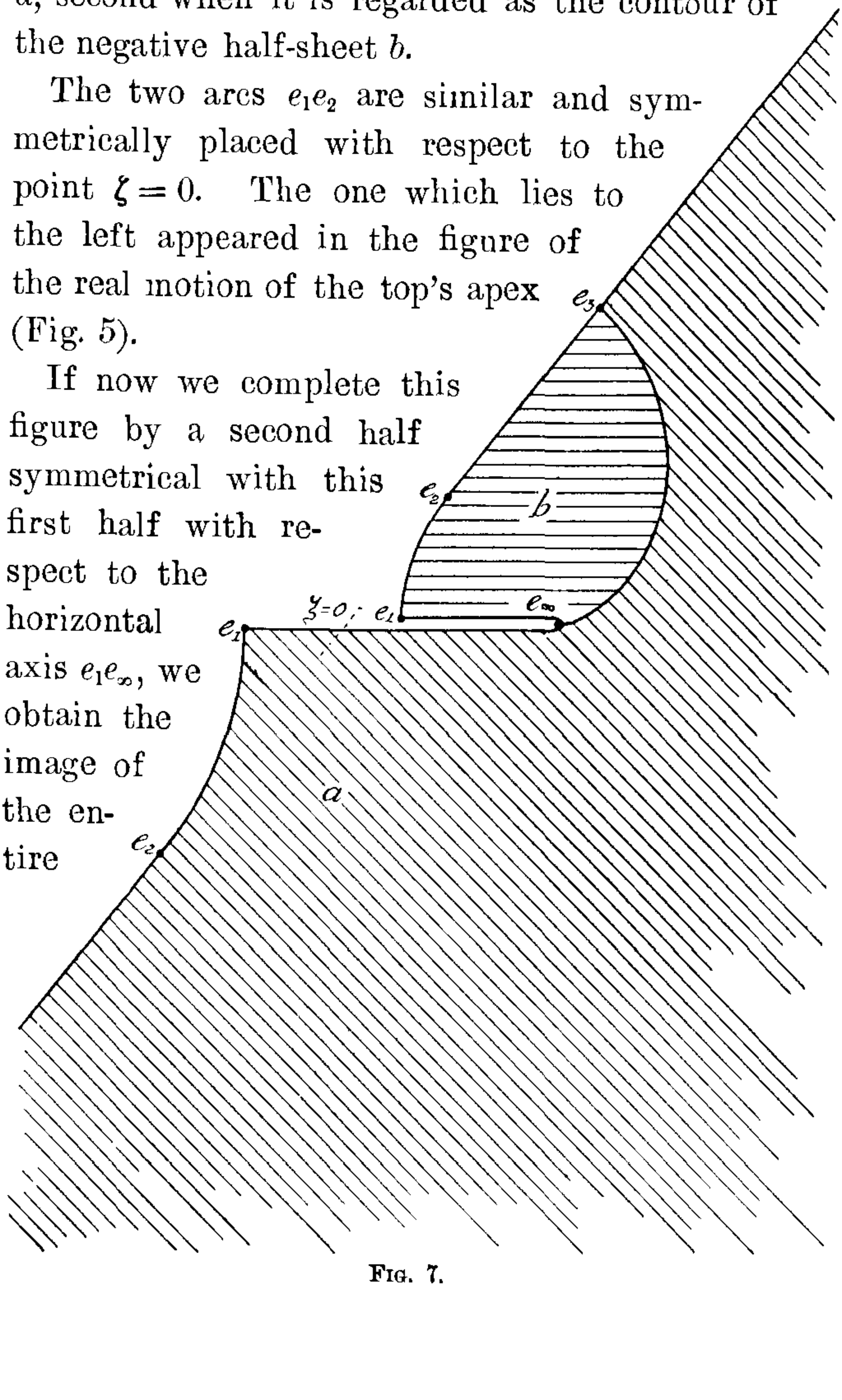


FIG. 7.

$\sqrt{U}$-surface or of the entire parallelogram of periods in the t-plane (Fig. 8). We suppose an incision made in the $\sqrt{U}$-surface along the segment $e_1e_2e_3$ of the real axis.

It will be noticed that the image covers doubly the portion of the plane which lies within the two arcs e_1, e_2, e_3, $\zeta = \infty$, which lie to the right, the two sheets being joined along a branch line which runs from e_∞ to $\zeta = \infty$. From the figure we infer that e_∞ is a branch point of t, but not so the point $\zeta = \infty$; for a circuit cannot be made of the point $\zeta = \infty$ without passing into the portion of the plane bounded by the half-arcs e_1, e_2, $\zeta = 0$, lying to the left, which does not belong to the image. And these conclusions may readily be verified by reckoning.

We may describe our figure as a quadrilateral, one of whose pairs of opposite sides are the rectilineal segments running from the points e_2, through $\zeta = \infty$, and which, were they produced, would intersect at $\zeta = 0$, and the other pair, the two curvilinear arcs $e_2e_1e_2$.

The sides of each pair go over into each other by the substitution of ζ which corresponds to a change of t by one of the periods $2\omega_1$, $2i\omega_2$: the straight sides by the rotation about $\zeta = 0$ defined by the "elliptic substitution" $\zeta' = e^{i\psi_0}\zeta$, which we have already considered and which we have indicated in the figure by the double-headed curved arrows; the curved sides by the transformation

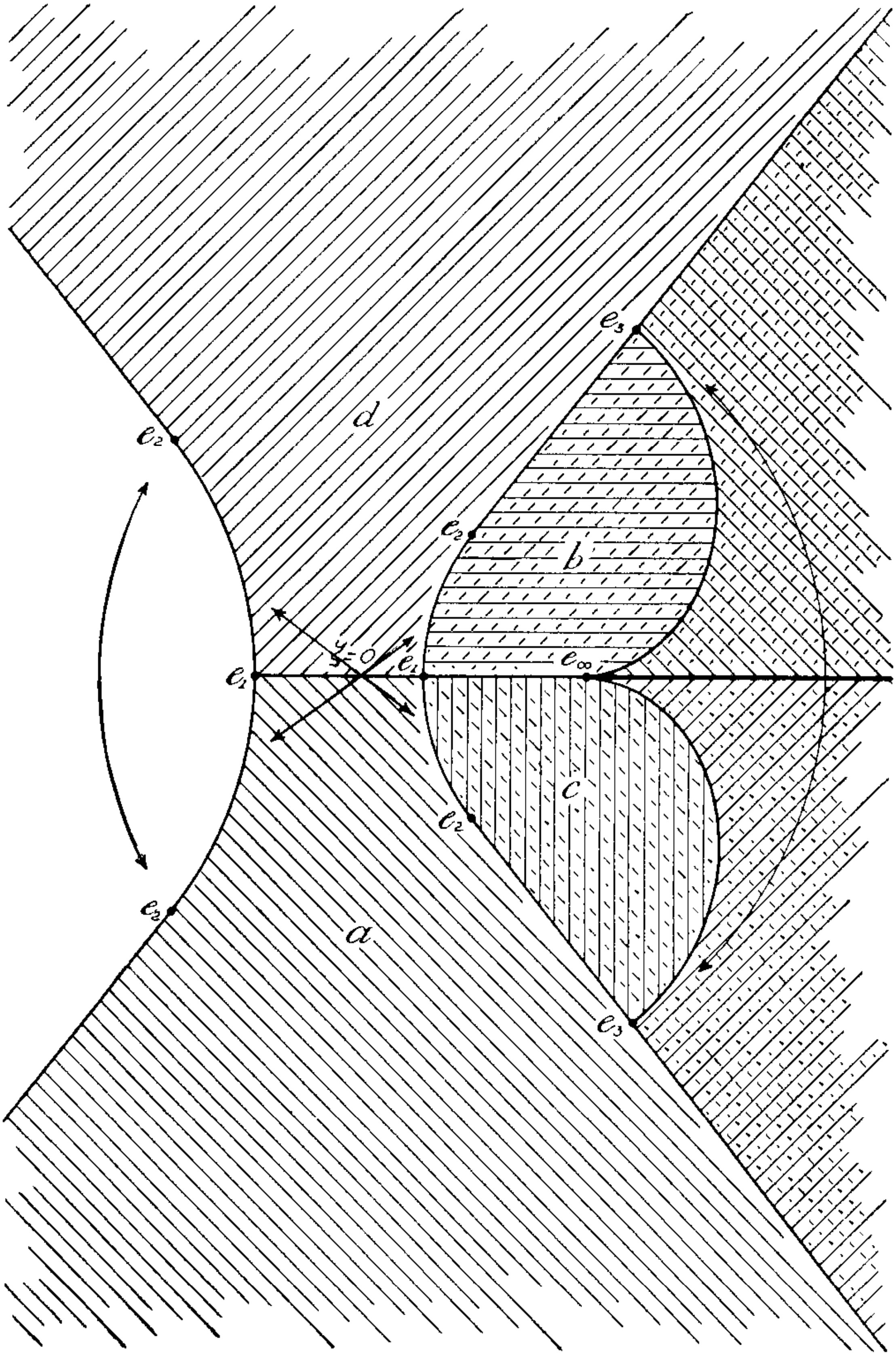


FIG. 8.

defined by the "hyperbolic substitution" $\zeta' = \kappa\zeta$, in consequence of which they are similar and symmetrically placed with respect to the centre of similitude $\zeta = 0$. In the figure we have indicated the latter transformation by the double-headed straight arrows which intersect at $\zeta = 0$. The significance of both the periods $2\omega_1$, $2i\omega_2$ for the curve traced by the apex of the top is thus made evident by our figure. And indeed we have now clearly before us for the first time the reason that the curve described in real time should be represented by elliptic functions. It is but a portion of the complete curve, or rather domain, which comes to light when we avail ourselves of the entire field of complex numbers in which the representation of both periods is alone possible.

The Riemann surface determined by $\zeta = \frac{\beta(t)}{\delta(t)}$, the curve traced by the opposite extremity of the top's axis, $\mathbf{Z} = 0$, may be constructed similarly.

For real values of t we have $\frac{\beta(t)}{\delta(t)} = -\frac{\bar{\gamma}(t)}{\bar{\alpha}(t)}$, which means simply that $\frac{\alpha(t)}{\gamma(t)}$ and $\frac{\beta(t)}{\delta(t)}$ are opposite extremities of one and the same diameter of the sphere. For complex values of t this formula is to be replaced by the more general one

$$\frac{\beta(t)}{\gamma(t)} = -\frac{\bar{\gamma}(\bar{t})}{\bar{\alpha}(\bar{t})}.$$

If now we suppose these two Riemann surfaces to be projected back again to the surface of the fixed sphere, and the points of the two which correspond to the same value of t to be joined, *the resulting system of rays will represent the* ∞^2 *positions which the axis of the top may take in the general (non-Euclidean) motion which corresponds to any motion of* t *in the parallelogram of periods.*

Of these ∞^2 "axes," only those pass through the centre of the sphere which correspond to real values of t. These are the axes which meet the curved arc $e_2e_1e_2$ of the preceding figure which lies to the left. Those axes which meet the other curved arc $e_2e_1e_2$ intersect in another point of the central line (*i.e.* of the vertical through the centre of the sphere); namely, the point into which the centre of the sphere is transformed by the hyperbolic substitution already explained. A visible representation of the possible motions of the top's axis in complex time is to be had by constructing the figures for $\frac{\alpha}{\gamma}$ and $\frac{\beta}{\delta}$ on an actual sphere and joining a number of corresponding points by straight lines.

The doubly infinite systems of the rays which are elements of the polhodes and herpolhodes of all motions possible in complex time, may be constructed in like manner, and a complete geometrical representation be thus obtained of the top's motion. The constructions are more complicated, but there is no essential difficulty in carrying them out.

In fact, the only serious difficulty in this entire method of discussion is, that all our ordinary conceptions of mechanics involve the notion that time is capable of but one sort of variation. We are so accustomed to regard the mechanical conditions which correspond to small values of t, as, so to speak, the *cause* of those which correspond to greater values, and to picture the changes of configuration as following one another in definite order with the varying time, that we find ourselves at a loss for a mechanical representation when t, by being supposed complex, becomes capable of two degrees of variation.

To avoid this difficulty as far as possible, let us suppose t no longer capable of varying in every direction in the parallelogram of periods, but only along a line parallel to the real axis. In other words, in $t = t_1 + it_2$, let us regard t_2 as constant in each particular case, and t_1 as alone varying. In this manner, by subsequently giving t_2 all possible values, we may take into account all possible complex values of t, but we conceive them as ranged along the ∞^1 parallels to the real axis. Regarded thus, the Riemann surfaces $\frac{\alpha}{\gamma}$, $\frac{\beta}{\delta}$ become carriers of certain curve systems, and the system of ∞^2 axes is distributed among ∞^1 ruled surfaces.

In this manner we separate the totality of the positions of the top in complex time into an infinite number of simply infinite sets of positions. These sets of positions are characterized not only by the initial values of t, but by the values of the constants of integration, which must have been introduced had the reckoning which we have merely sketched been actually carried out. It should perhaps have been stated earlier that in the interest of complete generality these constants must now be supposed complex, for we are now operating in the domain of complex numbers. Moreover, only by supposing them complex shall we have constants enough at our disposal to meet all the conditions of our generalized problem of motion.

So far our figures have been constructed with a view to obtaining a clear geometrical representation of the entire content of our analytical formulas. But their chief interest lies in this: that one can give them a *real* dynamical meaning, that one can find a real mechanical system by whose motions they may be generated. I assert that *one can determine a certain free mechanical system, namely, a rigid body freely moving in non-Euclidean space* *under the action of certain definite forces, which in real time carries out exactly that infinity of forms of motion which we have just been describing, the one or other of them according to the choice made of the initial conditions of motion.* The mechanical system is a generalized one, but it belongs to the domain of real dynamics.

Let us consider the general problem of the motion of a rigid body under the action of any forces, in the non-Euclidian space whose absolute is the surface:

$$x^2 + y^2 + z^2 - t^2 = 0.$$

The earliest investigation of the motion of a rigid body in non-Euclidean space was made by Clifford in 1874 — though the investigation was not published until after his death, in his collected works. The same problem has been considered also by Heath in the *Philosophical Transactions*, 1884. Both these mathematicians, however, have treated the case of the elliptic non-Euclidean geometry, not the hyperbolic, and have contented themselves with establishing the differential equations of the problem.

I shall proceed analytically, as this method is more readily understood by one who is not well versed in non-Euclidean geometry, and immediately obtain differential equations for the motion of a certain rigid body in non-Euclidean space perfectly analogous to the equations for the motion of the top in real time, but involving two sets of variables.

To have the general case before us at once, I suppose the parameters ϕ, ψ, ϑ, and the time t, all complex and set

$$\phi = \phi_1 + i\phi_2,\quad \psi = \psi_1 + i\psi_2,\quad \vartheta = \vartheta_1 + i\vartheta_2,\quad t = t_1 + it_2.$$

These parameters are connected with T and V, the kinetic and potential energy, by the well-known Lagrange equations:

$$\frac{d\left(\frac{\delta T}{\delta\vartheta'}\right)}{dt} = \frac{\delta(T-V)}{\delta\vartheta},\quad \frac{d\left(\frac{\delta T}{\delta\phi'}\right)}{dt} = \frac{\delta(T-V)}{\delta\phi},$$

$$\frac{d\left(\frac{\delta T}{\delta\psi'}\right)}{dt} = \frac{\delta(T-V)}{\delta\psi}.$$

In these equations set

$$T = T_1 + iT_2,\quad V = V_1 + iV_2.$$

Since, then,
$$\frac{\delta T}{\delta\vartheta'} = \frac{\delta T_1}{\delta\vartheta'_1} + i\,\frac{\delta T_2}{\delta\vartheta'_1}$$

$$= \frac{\delta T_1}{\delta\vartheta'_1} - i\,\frac{\delta T_1}{\delta\vartheta'_2};$$

and similarly,

$$\frac{\delta T}{\delta\phi'} = \frac{\delta T_1}{\delta\phi'_1} - i\,\frac{\delta T_1}{\delta\phi'_2} \text{ and } \frac{\delta T}{\delta\psi'} = \frac{\delta T_1}{\delta\psi'_1} - i\,\frac{\delta T_1}{\delta\psi'_2};$$

and since, furthermore, by our hypothesis, $dt = dt_1$, the first of our equations breaks up into the two equations involving real variables only,

$$\frac{d\left(\frac{\delta T_1}{\delta \vartheta'_1}\right)}{dt_1} = \frac{\delta(T_1 - V_1)}{\delta \vartheta_1}, \quad \frac{d\left(\frac{\delta T_1}{\delta \vartheta'_2}\right)}{dt_1} = \frac{\delta(T_1 - V_1)}{\delta \vartheta_2};$$

and the remaining two equations behave similarly.

Thus, every real mechanical problem again reduces to a real problem when the variables are made complex, provided the real part only of the complex t be supposed to vary, but the problem of a motion involving twice the number of variables.

Applying this general conclusion to the particular question before us, it is evident without any further discussion that the problem of the motion in complex time of a top whose point of support is fixed is changed into a problem of real dynamics; the problem of the non-Euclidean motion of a rigid body. This motion has six degrees of freedom instead of three, corresponding to the six parameters, ϑ_1, ϑ_2, ϕ_1, ϕ_2, ψ_1, ψ_2, and its kinetic and potential energy are T_1 and V_1, the real parts of the complex T and V.

But what is the rigid body, and what the force producing the motion? We shall content ourselves with simply answering these questions without entering upon the considerations appertaining to non-

Euclidean geometry by which our conclusions are reached.

The equation of the absolute being

$$x^2 + y^2 + z^2 - t^2 = 0,$$

the integral

$$\int \frac{(ux + vy + wz + \omega t)^2}{(u^2 + v^2 + w^2 - \omega^2)(x^2 + y^2 + z^2 - t^2)} dm,$$

evaluated throughout any body in the corresponding non-Euclidean space, is called the "second moment" of the body with respect to the plane whose co-ordinates are u, v, w, ω. *In the particular case before us this integral, when evaluated, will be equal to* 1, *independently of the values of* u, v, w, ω.

Remembering that u, v, w, ω are constants with respect to the integration, the result may be written

$$\frac{Au^2 + 2\,Buv + \cdots}{u^2 + v^2 + w^2 - \omega^2}, \text{ which therefore} = 1.$$

Now the surface whose equation in tangential co-ordinates is

$$Au^2 + 2\,Buv + \cdots = 0$$

is called the "null-surface." In the case before us, therefore, *the null-surface coincides with the absolute.* This is the rigid body of our non-Euclidean motion.

The force producing the motion may be defined as follows: In the figure (Fig. 9) let g represent the fixed axis of gravitation (through the point of support of the top), r the axis of the top, and p the non-Euclidean perpendicular common to g and r. The angle between g and r is then defined as $\vartheta = \vartheta_1 + i\vartheta_2$, where ϑ_1 represents the angle between the planes gp and rp, and $i\vartheta_2$ in non-Euclidean angular measure is the distance p.

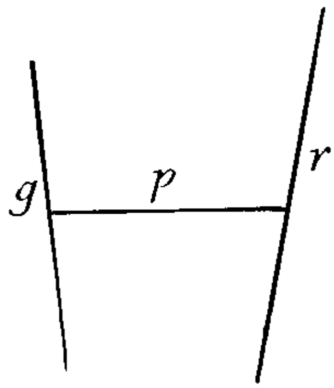


FIG. 9.

The force is then the wrench represented in intensity by $P \sin \vartheta$, of which the real part represents the rotating force acting about p and the imaginary part represents the thrust along p.

In conclusion, allow me to remark once again that this non-Euclidean geometry involves no metaphysical consideration, however interesting such considerations may be. *It is simply a geometrical theory which groups together certain geometrical relations in real space in a manner peculiarly adapted to their study.*

LECTURE IV

In the latter part of yesterday's lecture we ventured a little way into what Professor Newcomb has called the "fairyland of mathematics." Ignoring the limitation of the top's motion to real time, we gave full play to our purely mathematical curiosity. And there can be no doubt that it is proper and indeed necessary within due limits to proceed after this manner in all such investigations as that now before us. It is possible only thus to develop a strong and consistent mathematical theory. But we should not yield ourselves wholly to the charm of such speculations, but rather control them by being ever ready to return to the actual problems which nature herself proposes.

We turn again to-day, therefore, to the real top, and proceed to investigate its motion when the point of support is no longer fixed, but movable in the horizontal plane. This is the case of the *ordinary toy top*.

It has been well known since the time of Poisson that the differential equations of this motion can be integrated in terms of the hyperelliptic integrals. And it is the main purpose of my present lecture to show *that these integrals may be treated in a manner quite analogous to that in which the elliptic integrals were treated, by aid of the general "automorphic functions," of which the elliptic functions are a special class.*

The "toy top" has five degrees of freedom of motion, two of them relating to the horizontal displacement of the centre of gravity, and the other three to the motion around this centre. The horizontal motion of the centre of gravity is very simple, being, as is well known, a rectilinear motion of constant velocity. Consequently, no essential restriction of the problem is involved in assuming the horizontal projection of the centre of gravity to be a fixed point. By this assumption the problem is again reduced to one of three degrees of freedom only, and we have besides t no other variables to consider than the parameters ϕ, ψ, ϑ or α, β, γ, δ of the previous discussion — the parameters here defining the position of the top with respect to axes through its centre of gravity.

To obtain first the ordinary formulas which define the motion in terms of the astronomical parameters: let G represent the weight of the top, s the distance of its centre of gravity from the point of support, and again represent the product Gs, *i.e.* the static moment, by P. Also, for the sake of simplicity, let us again suppose that the three principal moments of inertia of the top, in this case with respect to the axes through its centre of gravity, are all equal to 1.

Then the kinetic energy, T, and the potential energy, V, are given by the following equations: viz.

$$T = \tfrac{1}{2}(\phi'^2 + \psi'^2 + 2\,\phi'\psi' \cos\vartheta + \vartheta'^2 + Ps \sin^2\vartheta \cdot \vartheta'^2),$$

$$V = P \cos\vartheta,$$

which differ from the corresponding expressions in the special case where the point of support is fixed only in the appearance of the additional term $Ps \cdot \sin^2\vartheta \cdot \vartheta'^2$ in T. As this term will disappear if $s = 0$, though we take Gs, *i.e.* P, different from zero, the elementary case may be described from the present point of view as that of a top of infinite weight whose centre of gravity coincides with its point of support.

On substituting these values for T and V in the first two Lagrange equations,

$$\frac{d\dfrac{\delta T}{\delta\phi'}}{dt} = 0, \quad \frac{d\dfrac{\delta T}{\delta\psi'}}{dt} = 0,$$

we obtain immediately, as before, the two algebraic first integrals

$$\phi' + \psi' \cos\vartheta = n,$$

$$\psi' + \phi' \cos\vartheta = l.$$

If from these last equations we reckon out ϕ' and ψ', and substitute the resulting values in the integral of energy

$$T + V = h,$$

we obtain t, ϕ, and ψ in the form of integrals in terms of the variable ϑ.

As before, we set $u = \cos\vartheta$, and

$$U = 2Pu^3 - 2hu^2 + 2(ln - P)u + (2h - l^2 - n^2),$$

when these integrals become

$$t = \int \frac{du\sqrt{(1+Ps) - Psu^2}}{\sqrt{U}},$$

$$\phi = \int \frac{n - lu}{1 - u^2} \cdot \frac{du\sqrt{(1+Ps) - Psu^2}}{\sqrt{U}},$$

$$\psi = \int \frac{l - nu}{1 - u^2} \cdot \frac{du\sqrt{(1+Ps) - Psu^2}}{\sqrt{U}}.$$

These formulas differ from the corresponding formulas for the elementary case in that the new irrational factor $\sqrt{(1+Ps) - Psu^2}$ here appears in the numerator of each integrand. In consequence, we have now to do with hyperelliptic integrals, $p = 2$. In addition to the former branch-points of the Riemann surface in the u-plane, viz. e_1, e_2, e_3, e_∞, two new real branch-points appear, viz.:

$$u = \pm\sqrt{\frac{1+Ps}{Ps}}.$$

I shall call them e_4, e_6, and assume them to be numerically greater than e_3. The Riemann surface is therefore a surface of two sheets with six branch-points e_1, e_2, e_3, e_4, e_∞, e_6, ranged along the real axis of the u-plane, as indicated in the following figure:

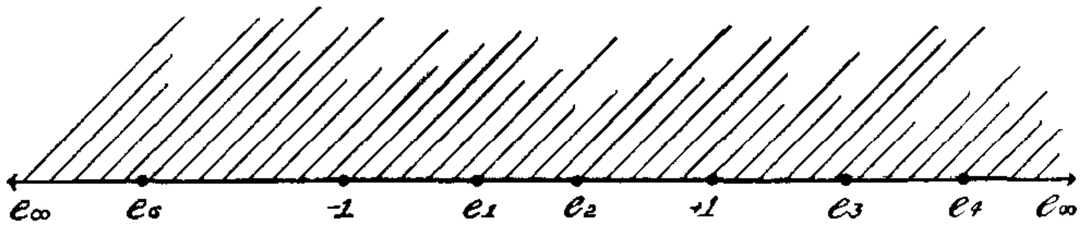


FIG. 10.

In addition to the branch-points, I have indicated the positions of the points $+1$, -1, since these particular values of u, corresponding to $\vartheta = 0$, $\vartheta = \pi$, play, as in the elementary case, a special rôle in our discussion.

The time t is no longer an integral of the first kind; that is to say, an integral which remains finite for all values of u, but an integral of the second kind, which becomes infinite for $u = \infty$, as $\sqrt{-2su}$. An integral of the second kind, it may be added, is one having a point of algebraic discontinuity only. The integrals ϕ and ψ, on the other hand, have each of them, as before, four logarithmic points of discontinuity; namely, the four points $u = \pm 1$ of the Riemann surface.

The first step to be taken is to replace the integrals ϕ and ψ by *normal* hyperelliptic integrals of the third kind; that is, by integrals possessing each but *two* logarithmic points of discontinuity with the residues $+1$ and -1. This is accomplished precisely as in the elementary case, by introducing $\log \alpha$, $\log \beta$, $\log \gamma$, $\log \delta$. As before, these prove to be normal integrals of the third kind, each having a logarithmic discontinuity (with the residue $+1$) at one of the points $u = \pm 1$, and all having a second logarithmic discontinuity in common (with the residue -1) at the point $u = \infty$. This follows at once from the result of the reckoning if it be noticed that the expression $(1 + Ps) - Psu^2$ reduces to 1 for $u = \pm 1$.

It is evident, therefore, that *the parameters* α, β, γ, δ *play the same fundamental rôle here as in the case of the top whose point of support is fixed.* And in the following discussion we shall no longer use ϕ and ψ, but α, β, γ, δ. These variables possess on the Riemann surface a 0-point each at one of the four points $u = \pm 1$, and a common ∞-point at $u = \infty$. I have not thought it necessary to enter into the details of this reduction, as it is so completely analogous to the reduction in the more elementary case.

But when we attempt to repeat the next step of the previous discussion, and endeavor, by inverting the hyperelliptic integral t, to assign to t the rôle of independent variable, we find at once that there is a profound difference between our present problem and the previous more special problem. This difference is masked when we confine our attention to the top's motion in real time. For as t varies, remaining always real, the value of u vibrates as before between the values e_1 and e_2, while ϕ and ψ are each increased by real periods. The difference comes to light, however, as soon as, allowing t to take complex values, we proceed to construct in the t-plane the image of the Riemann surface. As the image of a half-sheet of this surface, we have now, instead of the simple rectangle of the elementary case, an open hexagon with one of its angular points at infinity, as in the following figure:

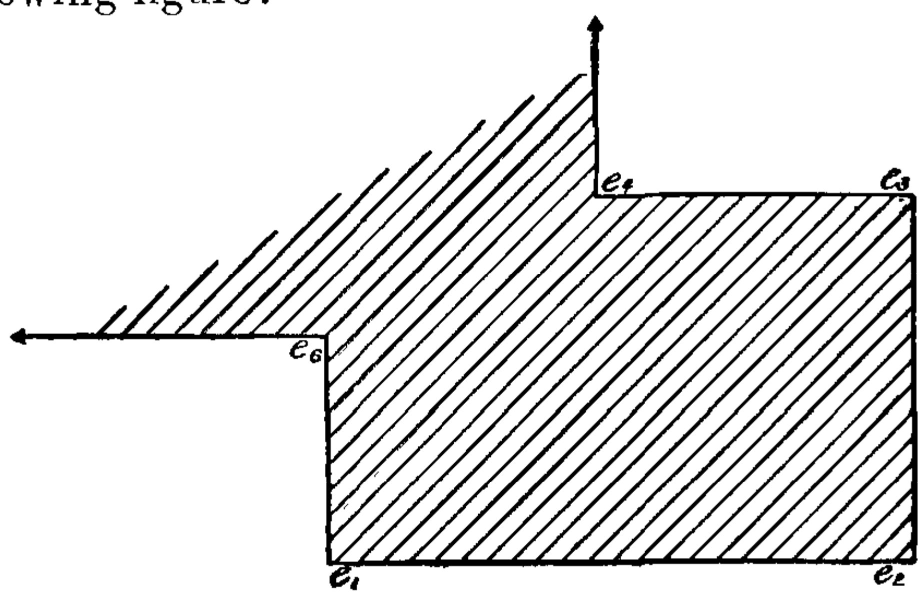


Fig. 11.

and when by the methods of symmetrical and congruent reproduction, we go on to construct from this figure the image of the entire Riemann surface, we at once encounter the difficulty that this image will cover the t-plane not simply, as in the elementary case, but rather with an infinite number of overlapping hexagonal pieces. To a single point in the t-plane, therefore, will correspond not one, but an infinite number of values of u, that is to say, u is no longer a *uniform* function of t.

I may remark that it is often said that the inversion of the hyperelliptic integrals is impossible. This is not true; it is not impossible to invert them, but to get uniform functions by the process.

There is a well known method of generalizing the result of inverting the elliptic integrals and obtaining functions, "hyperelliptic functions," as they are called, which are in a proper sense the generalization of the elliptic functions. The method is due to Jacobi, and goes by his name.

There are two hyperelliptic integrals of the first kind in the case before us:

$$v_1 = \int \frac{du}{\sqrt{U} \cdot \sqrt{1 + Ps - Psu^2}},$$

$$v_2 = \int \frac{u \cdot du}{\sqrt{U} \cdot \sqrt{1 + Ps - Psu^2}}.$$

Jacobi forms double ϑ-functions of v_1, v_2, viz. $\theta(v_1, v_2)$, in terms of which he seeks to express the other variables as uniform functions. This is, perhaps, the greatest achievement of Jacobi, and for general investigations of the highest importance, but it promises us little aid in the problem which we are considering. To avail ourselves of it, we should need first to develop a method for determining what values of v_1, v_2 correspond to the same value of t. We are therefore reduced to the direct computation of hyperelliptic integrals if we wish to avoid the complicated equation for v_1 and v_2 which results if we eliminate t.

Is it possible, then, by any means whatsoever, to obtain for the general motion of the top formulas analogous to those which we succeeded in establishing for the top whose point of support was fixed? Yes, by availing ourselves of the *theory of the uniform automorphic functions.*

A uniform automorphic function of a single variable η is a function $f(\eta)$, which satisfies the functional equation

$$f\left(\frac{a_\nu \eta + b_\nu}{c_\nu \eta + d_\nu}\right) = f(\eta),$$

where a_ν, b_ν, c_ν, d_ν have given constant values for each of the values of ν: $1, 2, 3 \cdots \infty$ — for all of which the functional equation is satisfied.

The automorphic functions, therefore, are functions which are transformed into themselves by an infinite but discontinuous group of linear substitutions. They are the generalization of the elliptic functions which consists in generalizing the periodicity of these functions, but leaving the number of the variables unchanged, while Jacobi's hyperelliptic functions are a generalization which consists in increasing the number of variables, but leaving the periodicity unchanged.

I shall present what I have to say regarding them geometrically. And, indeed, the general notion of these automorphic functions, as well as the knowledge of their most important properties, originated from geometrical considerations, and geometrical considerations only. Even now the analytical details of the theory have been only partially developed.

Our problem, as we are now to conceive of it, is this: *to define a variable* η, *of which* t, α, β, γ, δ *shall be uniform automorphic functions*, as were α, β, γ, δ of t itself in the elementary case.

To revert to the elementary case — the fact that t was itself a "uniformizing" variable, *i.e.* a variable of which u was a uniform function, was brought to light by finding that when the image in the t-plane of a single half-sheet of the Riemann surface on the u-plane was reproduced by symmetry and congruence, this image covered the t-plane *simply*. May we not, then, construct in the plane of a variable η a rectangular hexagon which shall be the image in the η-plane of a half-plane u, and which on being reproduced shall cover the η-plane or a portion of it simply, and then subsequently, from a study of the conditions which determine this hexagon, derive in definite analytical form the functional relation between η and u?

It is in fact possible, as the theory of automorphic functions shows, to construct such a rectangular hexagon, and that in essentially but one way. Its sides are not line segments, but arcs of circles which themselves cut the real axis of the η-plane at right angles. It has the following form:

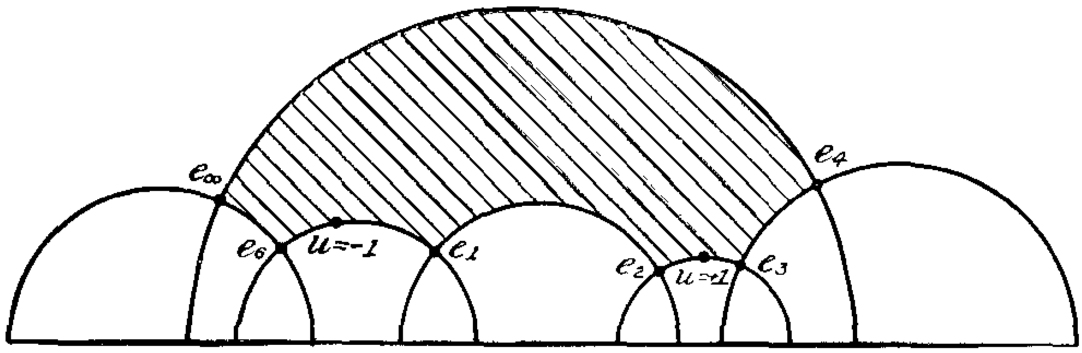


FIG. 12.

The mere geometrical requirement that the figure be made up of arcs of circles which cut the real axis orthogonally, and cut each other orthogonally also at the six points e_1, e_2, e_3, e_4, e_∞, e_6, is of course not enough to determine it completely. There are a certain number of parameters which remain undetermined, and which are to be so determined that the hexagon is an actual conformal representation of the half u-plane with the given branch-points $e_1, e_2 \cdots e_6$. The fundamental theorem of the theory of automorphic functions declares that this can be accomplished in one, and essentially but one, way.

Having determined the image of the one half-sheet of the Riemann surface on the u-plane, the infinitely many remaining images are to be had by constructing the figure into which the original image is transformed by inversion with respect to each circle of which one of its sides is an arc, by repeating the same construction for the resulting hexagons, and so on indefinitely.

By this process the entire upper half of the η-plane is simply covered without overlapping by rectangular hexagons, whose sides are circular arcs. Each of these hexagons is an image of a half-sheet of the Riemann surface. And if they be alternately shaded and left blank, the shaded ones are images of positive half-sheets, the blank ones of negative half-sheets of the surface.

Evidently, then, to a single point in the η-plane there corresponds but a single point in the Riemann surface, or *u and $\sqrt{U}$ are uniform functions* of η. On the other hand, the points in two of the hexagons which correspond to the same value of u, $\sqrt{U}$, and may be called "equivalent points," are connected by a formula of the form $\eta' = \dfrac{a_\nu \eta + b_\nu}{c_\nu \eta + d_\nu}$, as in the special elliptic case the corresponding points of two of the parallelograms of periods were connected by the formula $t'=t+2m_1\omega_1+2m_2i\omega_2$. Thus u and $\sqrt{U}$ are uniform automorphic functions of η, satisfying the equation:

$$f(\eta)=f\left(\frac{a_\nu\eta+b_\nu}{c_\nu\eta+d_\nu}\right).$$

I may remark that Lord Kelvin made use of this sort of symmetrical reproduction more than fifty years ago in his researches on electrostatic potential. But his figures were solids bounded by portions of spherical surfaces, and his aim was so to determine these that only a finite number of other distinct solids should result from them by the process of reproduction.

Not only u and $\sqrt{U}$, but also $\sqrt{1+Ps-Psu^2}$, and again t, α, β, γ, δ, are uniform functions of our new variable η, functions, it may be added, which exist only in the upper half of the η-plane. *Hence η is the uniformizing variable which we have been seeking, the variable which plays the rôle taken by t in our discussion of the special problem.*

We turn therefore to the consideration of t, α, β, γ, δ, regarded as functions of η.

The variable t is affected *additively* by the linear substitutions of η which correspond to the successive reproductions of the figure; *i.e.* with every substitution it is increased by a constant. Moreover, it becomes infinite, and that simply infinite algebraically, at all those points of the η-plane which correspond to the point e_∞ of the u-plane, the points, namely, which are equivalent to the single angular point marked e_∞ in the hexagon of our figure.

On the other hand, α, β, γ, δ, are affected multiplicatively by the linear substitutions of η. Each becomes zero in one series of equivalent points, and that simply, and each becomes infinite, and that also simply, in another series of equivalent points.

The ∞-points are the same as those for which t becomes infinite; the 0-points are the points on the perimeters of our hexagons which correspond to the four points $u = \pm 1$ of our original Riemann surface of two sheets on the u-plane. The two points corresponding to $u = +1$ we may name a', a'', and the two points corresponding to $u = -1$, b', b'', in such a manner that the series of equivalent 0-points of α, β, γ, δ, correspond respectively to a', b', b'', a''.

On this characterization of our functions $t, \alpha, \beta, \gamma, \delta$, we have now to base their analytical representation in terms of η. This is to be accomplished by means of the functions which in this more general case of the automorphic theory play the same fundamental rôle as the elliptic σ-functions in the more elementary case — the so-called *prime-forms.* The *prime-*

form is not a function of η, but a homogeneous function of the first degree of η_1, η_2 (where $\frac{\eta_1}{\eta_2}=\eta$); like the elliptic σ-function, it vanishes at all of a certain series of equivalent points, and is nowhere infinite.

I use the name prime-form because all the algebraic integral forms belonging to the Riemann surface admit of being similarly expressed as products of suitably chosen prime-forms, just as in ordinary arithmetic integers as products of prime numbers. It may be added that these prime-forms are not completely determined quantities. They may be altered by certain factors, the exact expression of which here would cause too serious a digression.

If now we represent the prime-form whose zero-points are the series of equivalent points corresponding to the point m of the Riemann surface by the symbol $\Sigma(\eta_1, \eta_2; m)$, we have the following analytical representation of our functions t, α, β, γ, δ, viz.:

$$t=\frac{\Sigma'(\eta_1, \eta_2;\ e_\infty)}{\Sigma(\eta_1, \eta_2;\ e_\infty)},$$

$$\alpha=\frac{\Sigma(\eta_1, \eta_2;\ a')}{\Sigma(\eta_1, \eta_2;\ e_\infty)}, \qquad \beta=\frac{\Sigma(\eta_1, \eta_2;\ b')}{\Sigma(\eta_1, \eta_2;\ e_\infty)},$$

$$\gamma=\frac{\Sigma(\eta_1, \eta_2;\ b'')}{\Sigma(\eta_1, \eta_2;\ e_\infty)}, \qquad \delta=\frac{\Sigma(\eta_1, \eta_2;\ a'')}{\Sigma(\eta_1, \eta_2;\ e_\infty)}.$$

And so we find here, as before, that *the functions α, β, γ, δ prove to be the simplest elements for the* *representation of the top's motion.* They are the simplest quotients of the elementary functions of the "hyperelliptic body" which has replaced the "elliptic body" of our earlier discussion.

It may be remarked that these formulas at once reduce to $t = \eta$ and the previously obtained elliptic formulas on making the hypotheses $P \gtrless 0$, $s = 0$, which are equivalent to supposing the point of support fixed.

Moreover, it must be said that these expressions for t, α, β, γ, δ are only to be understood as having a formal significance. There is altogether lacking the actual determination of the constants left at our disposal by the definitions of the Σ's, and which, it may be added, differs for the different Σ's which appear in the formulas for t, α, β, γ, δ.

And with this we come upon the point at which this theory is still incomplete. The exact determination of the formulas, and in general the means of reckoning them out by practicable methods, are for the most part wanting. The theory of the automorphic functions which for a time was a matter of principal interest in the theory of functions has in recent years not attracted the attention nor found the support which it seems to deserve. *I have therefore the more gladly laid stress here on the fact that these are not only functions possessing a theoretical* *interest, but functions which necessarily present themselves if one will completely solve even the simplest problems of mechanics.*

Had we the time, we should find it interesting to consider the geometry of this more general case of the top's motion also.

I will, however, give the equation of the curve traced on the horizontal plane by the point of support. It is $x + iy = 2\alpha\beta s$, as results from the formulas on page 8, by giving X, Y, Z the values of 0, 0, $-s$, respectively. For the values of x and y depend on α, β, γ, δ alone, these quantities, in the present case, conditioning the motion of the centre of gravity up and down its vertical, and no terms appearing in the expressions for x and y due to this motion.

And I may also make the general remark that in this geometrical study the non-Euclidean interpretation plays an important rôle. For while the curves traced by the apex, etc., have in real time a form quite similar to that in the case of the fixed point of support, the Riemann surface as described by the apex on the fixed sphere brings fully into evidence the difference between the elliptic and hyperelliptic characters of the two motions. Instead of the quadrilateral which was represented in Fig. 8 we should here have a hexagon.

GRAPHICAL METHODS

A COURSE OF LECTURES DELIVERED IN COLUMBIA UNIVERSITY, NEW YORK, OCTOBER, 1909, TO JANUARY, 1910

BY

C. RUNGE

KAISER WILHELM PROFESSOR OF GERMAN HISTORY AND INSTITUTIONS FOR THE YEAR 1909–1910
PROFESSOR OF APPLIED MATHEMATICS AT THE UNIVERSITY OF GÖTTINGEN

TABLE OF CONTENTS.

INTRODUCTION.

§ 1. A great many if not all of the problems in mathematics may be so formulated that they consist in finding from given data the values of certain unknown quantities subject to certain conditions. We may distinguish different stages in the solution of a problem. The first stage we might say is the proof that the quantities sought for really exist, that it is possible to satisfy the given conditions or, as the case may be, the proof that it is impossible. In the latter case we have done with the problem. Take for instance the celebrated question of the squaring of the circle. We may in a more generalized form state it thus: Find the integral numbers, which are the coefficients of an algebraic equation, of which π is one of the roots. Thirty years ago Lindemann showed that integral numbers subject to these conditions do not exist and thus a problem as old almost as human history came to an end. Or to give another instance take Fermat's problem, for the solution of which the late Mr. Wolfskehl, of Darmstadt, has left $25,000 in his will. Find the integral numbers x, y, z that satisfy the equation

$$x^n + y^n = z^n,$$

where n is an integral number greater than two. Fermat maintained that it is impossible to satisfy these conditions and he is probably right. But as yet it has not been shown. So the solution of the problem may or may not end in its first stage.

In many other cases the first stage of the solution may be so easy, that we immediately pass on to the second stage of finding methods to calculate the unknown quantities sought for. Or even if the first stage of the solution is not so easy, it may be expedient to pass on to the second stage. For if we succeed in finding methods of calculation that determine the unknown quantities, the proof of their existence is included. If on the other hand, we do not succeed, then it will be time enough to return to the first stage.

There are not a small number of men who believe the task of the mathematician to end here. This, I think, is due to the fact that the pure mathematician as a rule is not in the habit of pushing his investigation so far as to find something out about the real things of this world. He leaves that to the astronomer, to the physicist, to the engineer. These men, on the other hand, take the greatest interest in the actual numerical values that are the outcome of the mathematical methods of calculation. They have to carry out the calculation and as soon as they do so, the question arises whether they could not get at the same result in a shorter way, with less trouble. Suppose the mathematician gives them a method of calculation perfectly logical and conclusive but taking 200 years of incessant numerical work to complete. They would be justified in thinking that this is not much better than no method at all. So there arises a third stage of the solution of a mathematical problem in which the object is to develop methods for finding the result with as little trouble as possible. I maintain that this third stage is just as much a chapter of mathematics as the first two stages and it will not do to leave it to the astronomer, to the physicist, to the engineer or whoever applies mathematical methods, for this reason that these men are bent on the results and therefore they will be apt to overlook the full generality of the methods they happen to hit on, while in the hands of the mathematician the methods would be developed from a higher standpoint and their bearing on other problems in other scientific inquiries would be more likely to receive the proper attention.

The state of affairs today is such that in a number of cases the methods of the engineer or the surveyor are not known to the astronomer or the physicist, or vice versa, although their problems may be mathematically almost identical. It is particularly so with graphical methods, that have been invented for definite problems. A more general exposition makes them applicable to a vast number of cases that were originally not thought of.

In this course I shall review the graphical methods from a general standpoint, that is, I shall try to formulate and to teach them in their most generalized form so as to facilitate their application in any problem, with which they are mathematically connected.[1] The student is advised to do practical exercises. Nothing but the repeated application of the methods will give him the whole grasp of the subject. For it is not sufficient to understand the underlying ideas, it is also necessary to acquire a certain facility in applying them. You might as well try to learn piano playing only by attending concerts as to learn the graphical methods only through lectures.

[1] For the literature of the subject see "Encyklopädie der mathematischen Wissenschaften," Art. R. Mehmke, "Numerisches Rechnen," and Art. F Willers and C. Runge, "Graphische Integration."

CHAPTER I.

Graphical Calculation.

§ 2. *Graphical Arithmetic.*—Any quantity susceptible of mensuration can be graphically represented by a straight line, the length of the line corresponding to the value of the quantity. But this is by no means the only possible way. A quantity might also be and is sometimes graphically represented by an angle or by the length of a curved line or by the area of a square or triangle or any other figure or by the anharmonic ratio of four points in a straight line or in a variety of other ways. The representation by straight lines has some advantages over the others, mainly on account of the facility with which the elementary mathematical operations can be carried out.

What is the use of representing quantities on paper? It is a convenient way of placing them before our eye, of comparing them, of handling them. If pencil and paper were not as cheap as they are, or if to draw a line were a long and tedious undertaking, or if our eye were not as skillful and expert an assistant, graphical methods would lose much of their significance. Or, on the other hand, if electric currents or any other measurable quantities were as cheaply and conveniently produced in any desired degree and added, subtracted, multiplied and divided with equal facility, it might be profitable to use them for the representation of any other measurable quantities, not so easily produced or handled.

The addition of two positive quantities represented by straight lines of given length is effected by laying them off in the same direction, one behind the other. The direction gives each line a beginning and an end. The beginning of the second line has to coincide with the end of the first, and the resulting line representing the sum of the two runs from the beginning of the first to the end of the second. Similarly the subtraction of one positive quantity from another is effected by giving the lines opposite directions and letting the beginning of the line that is to be subtracted coincide with the end of the other. The result of the subtraction is represented by the line that runs from the beginning of the minuend to the end of the subtrahend. The result is positive when this direction coincides with that of the minuend, and negative when it coincides with that of the subtrahend. This leads to the representation of positive and negative quantities by lines of opposite direction. The subtraction of one positive quantity from another may then be looked upon as the addition of a positive and a negative quantity. I do not want to dwell on the logical explanation of this subject, but I want to point out the practical method used for adding a large number of positive and negative quantities represented by straight lines of opposite direction. Take a straight edge, say a piece of paper folded over so as to form a straight edge, mark a point on it, and assign one of the two directions as the positive one. Lay the edge in succession over the different lines and run a pointer along it through an amount equal in each case to the length of the line and in the positive or negative direction according to the sign of the quantity. The pointer is to begin at the point marked. The line running from this point to where the pointer stops represents the sum of the given quantities. The advantage of this method is that the intermediate positions of the pointer need not be marked provided only that the pointer keeps its position during the movement of the edge from one line to the next. As an example take the area, Fig. 1. A number of rectangular strips $\frac{1}{2}$ cm. wide are substituted for the area so that, measured in square centimeters, it is equal to half the sum of the lengths of the strips measured in centimeters. The straight

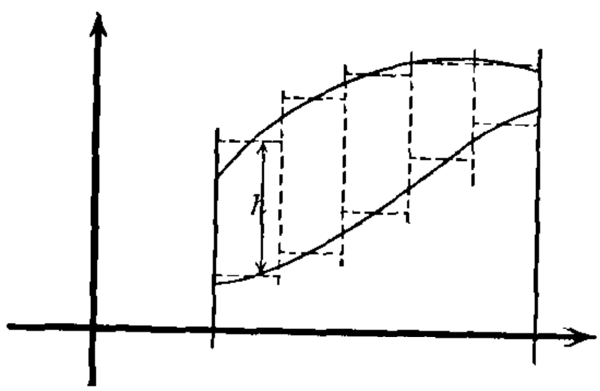


FIG 1.

edge is placed over the strips in succession and the pointer is run along them. The edge is supposed to carry a centimeter scale and the pointer is to begin at zero. The final position of the pointer gives half the value of the area in square centimeters. The drawing of the strips may be dispensed with, their lengths being estimated, only their width must be shown. If the scale should be too short for the whole length, the only thing we have to do is to break any of the lengths that range over the end of the scale and to count how many times we have gone over the whole scale. I have found it convenient to use a little pointer of paper fastened on the runner of a slide rule so that it can be moved up and down the metrical scale on one side of the

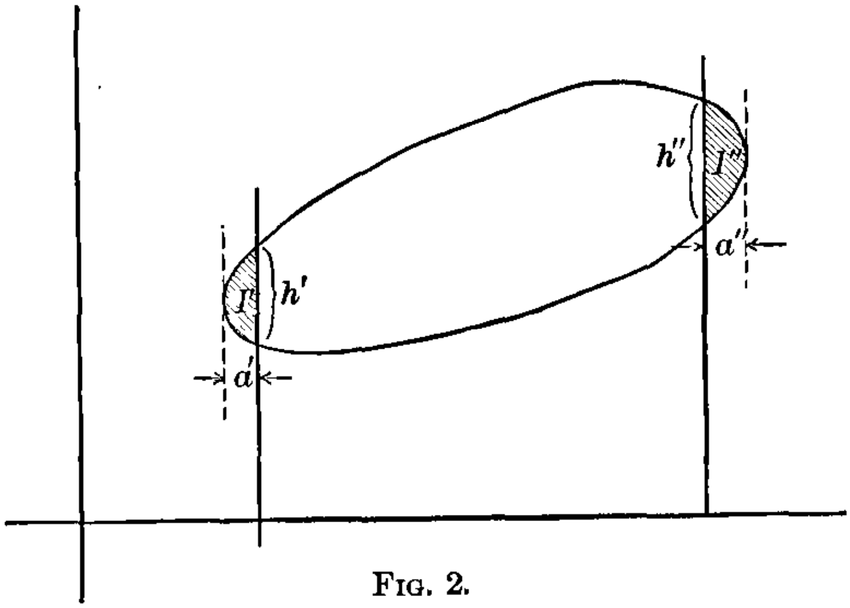


FIG. 2.

slide rule. The area is in this manner determined rapidly and with considerable accuracy, very well comparable to the accuracy of a good planimeter. If the area of any closed curve is to be found, the way to proceed is to choose two parallel lines that cut off two segments on either side (see Fig. 2), to measure the area between them by the method described above and to estimate the two segments separately. If the curves of the segments may with sufficient accuracy be regarded as arcs of parabolas the area would be two thirds the product of length and width. If not they would have to be estimated by substituting a rectangle or a number of rectangles for them.

In the same way the addition and subtraction of pure numbers may also be carried out. We need only represent the numbers by the ratios of the lengths of straight lines to a certain fixed line. The ratio of the length of the sum of the lines to the length of the fixed lines is equal to the sum of the numbers. The construction also applies to positive and negative numbers, if we represent them by the ratio of the length of straight lines of opposite directions to the length of a fixed line.

In order to multiply a given quantity c by a given number, let the number be given as the ratio of the lengths of two straight lines a/b. If the quantity c is also represented by a straight line, all we have to do is to find a straight line x whose length is to the length of c as a to b. This can be done in many ways by

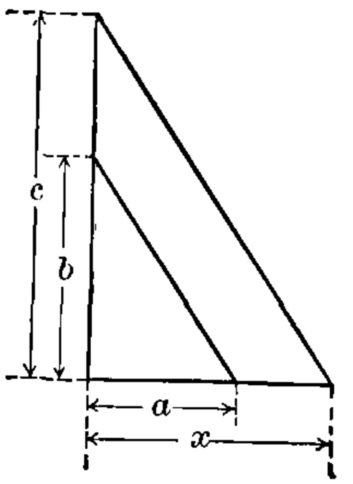


FIG. 3.

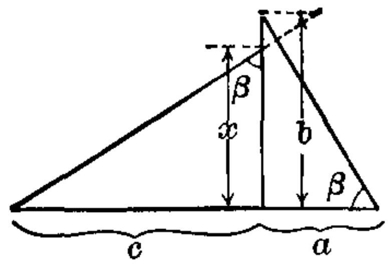


FIG. 4.

constructing any triangle with two sides equal to a and b and drawing a similar triangle with the side that corresponds to b made equal to c. As a rule it is convenient to draw a and b at right angles and the similar triangle either with its hypotenuse parallel (Fig. 3) or at right angles (Fig. 4) to the hypotenuse of the first triangle. Division by a given number is effected by the same construction; for the multiplication by the ratio a/b is equivalent to the divisions by the ratio b/a.

If a, b, c are any given numbers, we can represent them by the ratios of three straight lines to a fixed line. Then the ratio of the line constructed in the way shown in Fig. 3 and Fig. 4 to the fixed line is equal to the number

$$\frac{ac}{b}.$$

Multiplication and division are in this way carried out simultaneously. In order to have multiplication alone, we need only make b equal 1 and in order to have division alone, we need only make a or c equal 1.

In order to include the multiplication and division of positive and negative numbers we can proceed in the following way. Let the lines corresponding to a, x, Fig. 3, be drawn to the right side of the vertex to signify positive numbers and to the left side to signify negative numbers. Similarly let the lines corresponding to b, c be drawn upward to signify positive numbers and downward to signify negative numbers. Then the drawing of a parallel to the hypotenuse of the rectangular triangle a, b through the end of the line corresponding to c will always lead to the number

$$x = \frac{ac}{b}$$

whatever the signs of a, b, c may be.

The same definition will not hold for the construction of Fig. 4. If the positive direction of the line corresponding to a is to the right and the positive direction of the line corresponding to b is upwards then the positive directions of x and c ought to be such that when the right-angled triangle x, c is turned through an angle of 90° to make the positive direction of x coincident with the positive direction of a, the positive direction of c coincides with the positive direction of b. If we wish to have the positive direction of x upward, the positive direction of c would have to be to the left, or if we wish to have the positive direction of c to the right, the positive direction of x would have to be downward. If this is adhered to, the construction for division and multiplication will include the signs.

§ 3. *Integral Functions.*—We have shown how to add, subtract, multiply, divide given numbers graphically by representing them as ratios of the lengths of straight lines to the length of a fixed line and finding the result of the operation as the ratio of the length of a certain line to the same fixed line. By repeating these constructions we are now enabled to find the value of any algebraical expression built up by these four operations in any succession and repetition. Let us see for instance how the values of an integral function of x, that is to say, an expression of the form

$$a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$$

may be found by geometrical construction, where $a_0, a_1 \cdots a_n, x$ are any positive or negative numbers. We shall first assume that all the numbers are positive, but there is not the least difficulty in extending the method to the more general case.

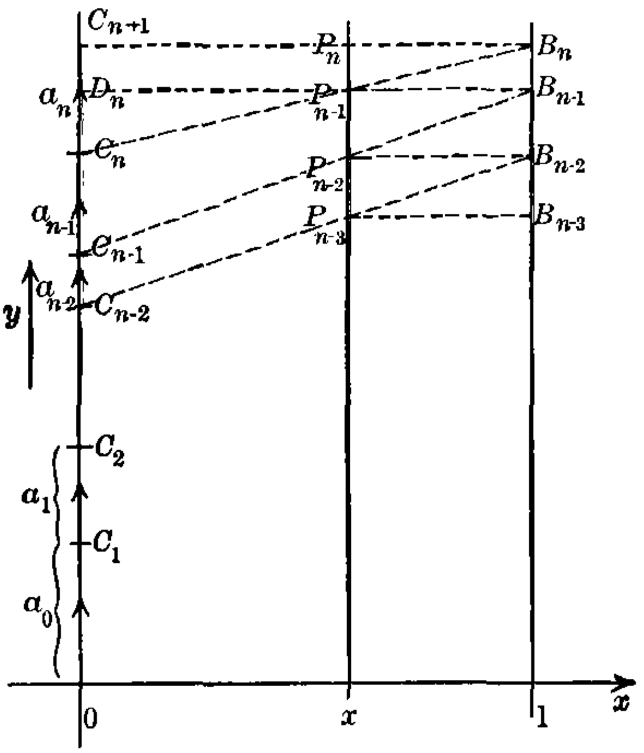


FIG. 5.

Now let $a_0, a_1, a_2, \cdots a_n$ signify straight lines laid off on a vertical line that we call the y-axis, one after the other as if to find the straight line

$$a_0 + a_1 + a_2 + \cdots + a_n.$$

The lengths of these lines measured in a conveniently chosen unit of length are equal to the numbers designated by the same letters. In Fig. 5 a_0 runs from the point O to point C_1, a_1 from C_1 to C_2, $\cdots$ a_n from C_n to C_{n+1}.

Let x be the *ratio* of the lines Ox and $O1$, Fig. 5, drawn horizontally from O to the right. The length $O1$ is chosen of convenient size independent of the unit of length that measures the lines $a_0, a_1, \cdots a_n$. The length Ox is then defined by the value of the ratio x. Through x and 1 draw lines parallel to the y-axis. Through C_{n+1} draw a line parallel to Ox, that intersects those two parallels in P_n and B_n. Draw the line B_nC_n that intersects the parallel through x in P_{n-1}. Then the height of P_{n-1} above C_n will be equal to a_nx. For if we draw a line through P_{n-1} parallel to Ox intersecting the y-axis in D_n, the triangle $C_nD_nP_{n-1}$ will be similar to $C_nC_{n+1}B_n$ and their ratio is equal to x, therefore $C_nD_n = a_nx$. Consequently the height of P_{n-1} above C_{n-1} is equal to $C_{n-1}D_n = a_nx + a_{n-1}$. Now let us repeat the same operation in letting the point D_n take the part of C_{n+1}. Through D_n draw a line parallel to Ox, that intersects the parallels through x and 1 in P_{n-1} and B_{n-1}. Draw the line $B_{n-1}C_{n-1}$ that intersects the parallel through x in P_{n-2}. Then the height of P_{n-2} above C_{n-1} will be equal to

$$C_{n-1}D_n \cdot x = (a_nx + a_{n-1})x,$$

and the height above C_{n-2} will be equal to

$$a_nx^2 + a_{n-1}x + a_{n-2}.$$

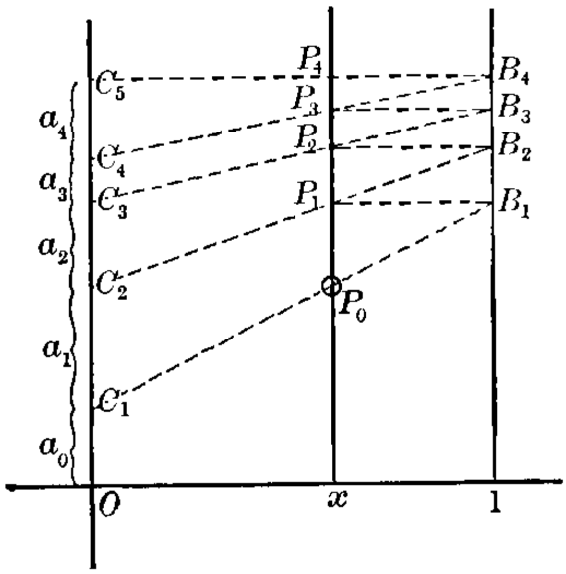


FIG. 6.

Continue in the same way. Draw $P_{n-2}B_{n-2}$ parallel to Ox, draw $B_{n-2}C_{n-2}$ and find the point P_{n-3}. Then the height of P_{n-3} above C_{n-2} will be

$$(a_nx^2 + a_{n-1}x + a_{n-2})x$$

and the height of P_{n-3} above C_{n-3}

$$a_nx^3 + a_{n-1}x^2 + a_{n-2}x + a_{n-3}.$$

Finally a point P_0 is found (see Fig. 6 for $n = 4$) by the intersection of B_1C_1 with the parallel to the y-axis through x, whose height above O is equal to

$$a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$$

Let us designate the line xP_0 by y, so that

$$y = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0,$$

in the sense that y is a vertical line of the same direction and length as the sum of the vertical lines $a_n x^n$, $a_{n-1} x^{n-1}$, $\cdots a_1 x$, a_0.

The same construction holds good for values of x greater than 1 or negative. The only difference is that the point x is beyond the interval $O1$ to the right of 1 or to the left of O. The negative sign of

$$a_n x, \; a_n x + a_{n-1}, \; a_n x^2 + a_{n-1} x, \text{ etc.},$$

will signify that the direction of the lines is downward. Nor are any alterations necessary in order to include the case that several or all of the lines a_0, a_1, $\cdots$ a_n are directed downward and correspond to negative numbers. They are laid off on the y-axis in the same way as if to find the sum

$$a_0 + a_1 + a_2 + \cdots + a_n,$$

$C_{\alpha+1}$ lying above or below C_α according to a_α being directed upward or downward. The construction can be repeated for a number of values of x. The points P_0 will then represent the curve, whose equation is

$$y = a_0 + a_1 x + \cdots + a_n x^n,$$

x and y measuring abscissa and ordinates in independent units of length.

In order to draw the curve for large values of x a modification must be introduced. It will not do to choose $O1$ small in order to keep x on your drawing board; for then the lines $B_\alpha C_\alpha$ will become too short and thus their direction will be badly defined. The way to proceed is to change the variable. Write for instance $X = x/10$, so that X is ten times as small as x and write

$$A_\alpha = a_\alpha \cdot 10^\alpha.$$

Then as

$$y = a_0 + a_1 \cdot 10 \frac{x}{10} + a_2 10^2 \frac{x^2}{10^2} + \cdots + a_n 10^n \frac{x}{10^n}$$

we find

$$y = A_0 + A_1X + A_2X^2 + \cdots + A_nX^n.$$

Lay off the lines A_0, A_1, $\cdots$ A_n in a convenient scale and let X play the part that x played before. The curve differs in scale from the first curve and the reduction of scale may be different for abscissas and ordinates but may if we choose be made the same so that it is geometrically similar to the first curve reduced to one tenth. It is evident that any other reduction can be effected in the same manner. By increasing the ratio x/X we enhance the value of A_n in comparison to the coefficients of lesser index, so that for the figure of the curve drawn in a very small scale all the terms will be insignificant except A_nX^n. In this case the points C_1, C_2, $\cdots$, C_n will very nearly coincide with O and only C_{n+1} will stand out.

It is interesting to observe that the best way of calculating an integral function

$$a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$$

for any value of x proceeds on exactly the same lines as the geometrical construction. The coefficient a_n is first multiplied with x and a_{n-1} is added Call the result a_{n-1}'. This is again multiplied by x and a_{n-2} is added. Call this result a_{n-2}'. Continuing in this way we finally obtain a value of a_0', which is equal to the value of the integral function for the value of x considered. Using a slide rule all the multiplications with x can be effected with a single setting of the instrument. The coefficients a_α and the values a_α' are best written in rows in this way

$$\begin{array}{cccccc} a_n & a_{n-1} & a_{n-2} & \cdots & a_1 & a_0 \\ & a_nx & a_{n-1}'x & \cdots & a_2'x & a_1'x \\ \hline & a_{n-1}' & a_{n-2}' & \cdots & a_1' & a_0' \end{array}$$

The accuracy of the slide rule is very nearly the same as the accuracy of a good drawing. But the rapidity is very much greater. When therefore only a few values of the integral function are required, the geometrical construction will not repay the trouble. It is different, however, when the object is to make a drawing of the curve. The values supplied by calculation would have to be plotted, while the geometrical construction furnishes the points of the curve right away and in this manner gains on the numerical method.

There is another geometrical method, which in some cases may be just as good. Let us propose to find the value of an integral function of the fourth degree.

$$y = a_0 + a_1x + a_2x^2 + a_3x^3 + a_4x^4$$

and let all coefficients in the first instance be positive.

The coefficients a_0, a_1, a_2, a_3, a_4 are supposed to be represented by straight lines, while x will be the ratio of two lines. The lines a_0, a_1, a_2, a_3, a_4 are laid off in a broken line a_0 to the right from C_0 to C_1, a_1 upward from C_1 to C_2, a_2 to the left from C_2 to C_3, a_3 downward from C_3 to C_4, a_4 again to the right from C_4 to C_5 (Fig. 7).

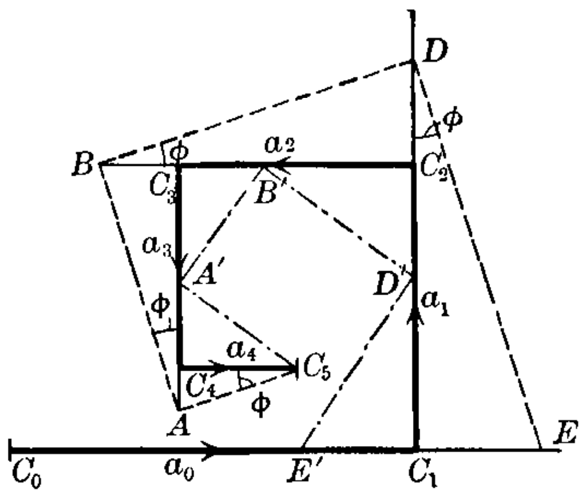


FIG. 7.

Through C_5 draw a line C_5A to a point A on C_3C_4 or its prolongation and let x be equal to the ratio $C_4A : C_4C_5$ taken positive when C_4A has the same direction as C_3C_4. Then we have

$$C_4A = a_4x,$$

and

$$C_3A = a_4x + a_3.$$

C_4A and C_3A are positive or negative according to their direction, being the same as the direction of C_3C_4 or opposite to it. Through A draw the line AB forming a right angle with C_5A to a point B on C_2C_3 or its prolongation. Then we have

$$C_3B = C_3A \cdot x = (a_4x + a_3)\,x$$

and

$$C_2B = a_4x^2 + a_3x + a_2.$$

C_3B and C_2B are positive or negative according to their direction being the same as the direction of C_2C_3 or opposite to it. Similarly we get

$$C_1D = a_4x^3 + a_3x^2 + a_2x + a_1,$$

and finally

$$C_0E = a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0.$$

C_0E is positive, when E is on the right side of C_0 and negative when on the left side. When the point A moves along the line C_3C_4, the point E will move along the line C_0C_1 and its position will determine the values of the integral function. To find the position of E for any position of A, we might use transparent squared paper, that we pin onto the drawing at C_5, so that it can freely be turned round C_5. Following the lines of the squared paper along C_5ABDE after turning it through a small angle furnishes the position of E for a new position of A (Fig. 8).

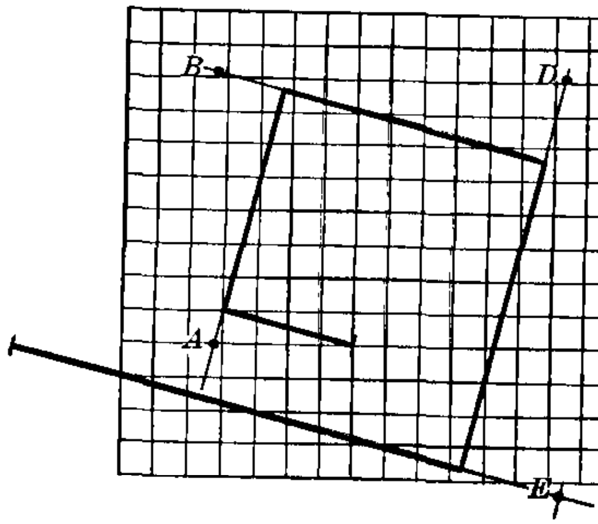


FIG. 8.

To include the case of negative coefficients we draw the corresponding line in the opposite direction. If for instance a_3 is negative C_3C_4 would have to lie above C_3; but C_3A would have to be counted in the same way as before, positive in a downward, negative in an upward direction.

The extension of the method to integral functions of any degree is obvious and need not be insisted on. It may be applied with advantage to find the real roots of an equation of any degree. For this purpose the broken line C_5ABDE would have to be drawn in such a way that E coincides with C_0. In the case of Fig. 7, for instance, it is easily seen that no real root exists. Fig. 9 shows the application to the quadratic equation. A circle is drawn over C_0C_3 as diameter. Its intersections with C_1C_2 furnish the points A and A' that correspond to the two roots. Both roots are negative in this case.

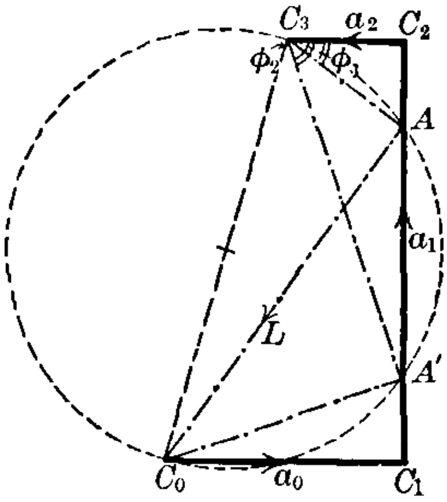


Fig. 9.

The first method of constructing the values of an integral function can be extended to the case where the function is given as the sum of a number of polynomials of the form

$$y = a_0 + a_1(x - p) + a_2(x-p)(x - q) + a_3(x - p)(x - q)(x - r) + \cdots.$$

Let us again suppose $a_0, a_1, a_2, \cdots$ to represent straight lines laid off as before on the y-axis upwards or downwards as if to find their sum. $x, p, q, r \cdots$ are meant, to be numbers represented by the ratio of certain segments on the axis of abscissas. Let us consider the case of four terms, the highest polynomial being of the third degree. The fixed distance between the points marked p and $p + 1$, q and $q + 1$, r and $r + 1$ on the axis of abscissas, Fig. 10 is chosen arbitrarily and the position

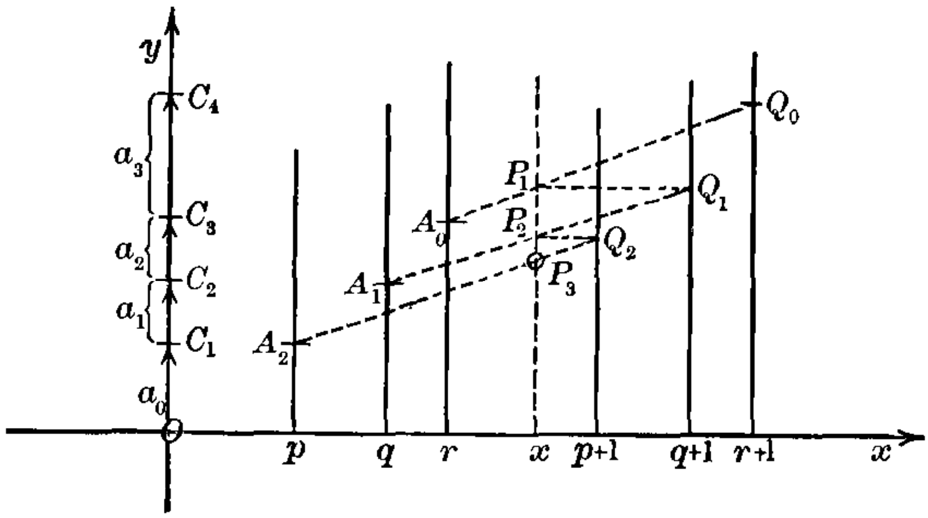


Fig. 10.

of the points marked p, q, r, x is made such that the ratio of Op, Oq, Or, Ox to that fixed distance is equal to the numbers p, q, r, x. For negative values the points are taken on the left of O.

Draw parallels to the y-axis through $p, q, r, x, p+1, q+1, r+1$. On the parallel through $r+1$ find the point Q_0 of the same ordinate as C_4 and on the parallel through r find the point A_0 of the same ordinate as C_3. Join A_0 and Q_0 by a straight line and find its intersection P_1 or that of its prolongation with the parallel through x. The height of P_1 above C_3 or A_0 is equal to $a_3(x-r)$ and the height above C_2 is equal to $a_3(x-r) + a_2$. On the parallel through $q+1$ find a point Q_1 of the same ordinate as P_1 and on the parallel through q a point A_1 of the same ordinate as C_2. Join A_1 and Q_1 by a straight line and find its intersection P_2 or that of its prolongation with the parallel through x. The height of P_2 above C_2 or A_1 is equal to

$$[a_3(x-r)+a_2](x-q),$$

and the height above C_1 is equal to

$$a_3(x-r)(x-q)+a_2(x-q)+a_1.$$

Finally find a point Q_2 on the parallel through $p+1$ of the same ordinate as P_2 and a point A_2 on the parallel through p of the same ordinate as C_1. Join A_2 and Q_2 by a straight line and find its intersection P_3 or that of its prolongation with the parallel through x. The height of P_3 above C_1 or A_2 will then be equal to

$$[a_3(x-r)(x-q)+a_2(x-q)+a_1](x-p)$$

and the ordinate of P_3 will be equal to the given integral function

$$y = a_3(x-r)(x-q)(x-p)+a_2(x-q)(x-p) + a_1(x-p)+a_0.$$

For large numbers p, q, r, x we use a similar device as before by introducing new numbers P, Q, R, X equal to one tenth, or one hundredth or any other fraction of $pqrx$. For instance

$$P = p/10, \quad Q = q/10, \quad R = r/10 \quad X = r/10.$$

We then write

$$A_0 = a_0, \quad A_1 = 10a_1, \quad A_2 = 100a_2, \quad A_3 = 1000a_3,$$

and obtain

$$y = A_0 + A_1(X - P) + A_2(X - P)(X - Q) + A_3(X - P)(X - Q)(X - R).$$

The scale for the lines A_0, A_1, A_2, A_3 and y must then be reduced conveniently and the values are constructed in the same way as before.

Now let us consider the inverse problem. The values of the integral function are given for

$$x = p,\ q,\ r,\ s;$$

find the lines a_0, a_1, a_2, a_3, so that the value of the integral function may be found for any other value of x in the way shown above.

Let us designate the given values of the integral function for $x = p, q, r, s$ by y_p, y_q, y_r, y_s and the points on the parallels through p, q, r, s with these ordinates by P, Q, R, S (see Fig. 12).

For $x = p$ the integral function

$$y = a_0 + a_1(x - p) + a_2(x - p)(x - q) + a_3(x - p)(x - q)(x - r)$$

reduces to a_0. Therefore we have $y_p = a_0$. The point C_1 is found by drawing a parallel to the axis of abscissas through P and taking its intersection with the axis of ordinates.

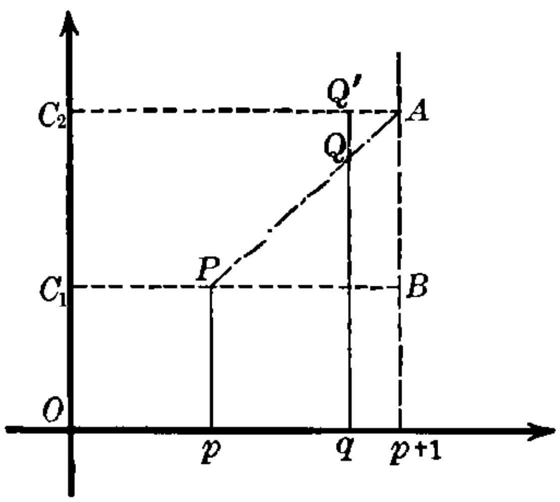


FIG. 11.

In order to find C_2 draw a straight line through P and Q and find its intersection A with the parallel through $p + 1$ (Fig. 11). A parallel to the axis of abscissas through A intersects the axis of ordinates in C_2. For the differences $y_q - y_p$ and $y_a - y_p$ (writing y_a for the ordinate of A) are proportional to the differences of the abscissas and consequently in the ratio $(q - p) : 1$. Therefore

$$y_a - y_p = \frac{y_q - y_p}{q - p} = a_1.$$

In the same way as the point Q on the parallel through q we might join any point X on a parallel through x with the point P, find the intersection with the parallel through $p + 1$ and draw a parallel to the axis of abscissas. The point of intersection of

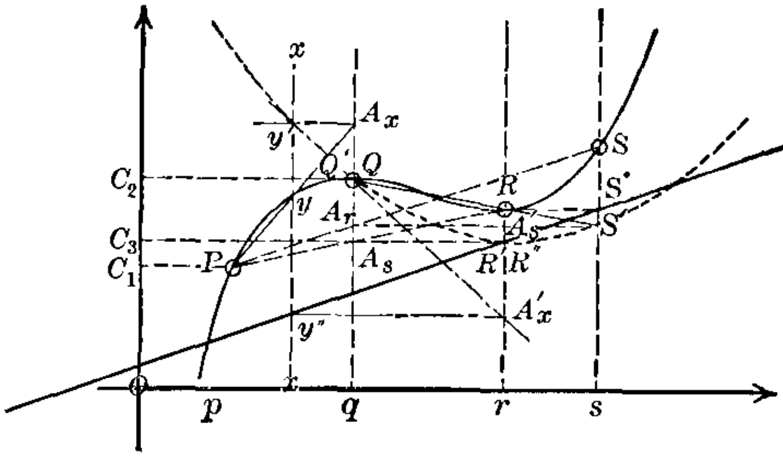


FIG. 12.

this parallel with the vertical through x let us call X' and its ordinate y'. Then we have

$$y' - y_p = \frac{y - y_p}{x - p} = a_1 + a_2(x - q) + a_3(x - q)(x - r).$$

Let us carry out this construction not only for $x = q$ but also for $x = r$ and $x = s$. This leads us to three points Q', R', S' on the verticals through q, r, s, whose ordinates are the values of the integral functions

$$y' = (a_0 + a_1) + a_2(x - q) + a_3(x - q)(x - r).$$

In this way we have reduced our problem. Instead of having to find an integral function of the third degree from four given points P, Q, R, S, we have now only to find an integral function of the second degree from three given points Q', R', S'. A second reduction is effected in exactly the same manner. Q' is joined with R' and S' by straight lines and through their intersection with the vertical through $q + 1$ parallels to the axis of abscissas are drawn that intersect the verticals through r and s in the points R'' and S'' respectively. The ordinates of these points are the values of the integral function y'' defined by

$$y'' - y_q' = \frac{y' - y_q'}{x - q} = a_2 + a_3(x - r),$$

for $x = r$ and $x = s$, or

$$y'' = a_0 + a_1 + a_2 + a_3(x - r).$$

The horizontal through R'' intersects the axis of ordinates in the point C_3. Finally we find C_4 by drawing a parallel to the axis of abscissas through the intersection of $R''S''$ or its prolongation with the vertical through $r + 1$.

Having found the points $C_1C_2C_3C_4$ we can now for any value of x construct the ordinate

$$y = a_0 + a_1(x - p) + a_2(x - p)(x - q) + a_3(x - p)(x - q)(x - r),$$

and thus draw the parabola of the third degree passing through the four points P, Q, R, S.

The construction may be somewhat simplified first by making $p + 1 = q$. Our data are the points P, Q, R, S, and we are perfectly at liberty to make the vertical through $p + 1$ coincide with the vertical through Q. In this case the point Q' will coincide with Q. The parabola of the second degree through the points $Q'R'S'$ is again independent of the distance between the verticals through q and $q + 1$ and at the same time independent of the point P. Therefore we are perfectly at liberty, for the construction of any point of this parabola, to make the vertical through $q + 1$ coincide with the vertical through R even if the distance of the verticals through P and Q is different from that of the verticals through Q and R. R'' will in this case coincide with R'. The procedure is shown in Fig. 12. Starting from the points P, Q, R, S the first step is to find R', S' by connecting R and S with P and drawing horizontals through the intersections A_r, A_s with the vertical through q. The next step is to find S'' by connecting Q (identical with Q') with S' and drawing a horizontal through the intersection with the vertical through r. Now the straight line $R''S''$ can be drawn (R'' being identical with R'). On the vertical through any point x take the intersection with $R''S''$ and pass horizontally to the point A_x' on the vertical through r. Draw the line $Q'A_x'$ and find its intersection with the vertical through x. This point is on the parabola through $Q'R'S'$. Pass horizontally to the point A_x on the vertical through q and draw the line A_xP. Its intersection with the vertical through x is a point on the parabola of the third degree through P, Q, R, S.

The method is evidently applicable to any number of given points, the degree of the parabola being one unit less than the number of points.

The methods for the construction of the values of an integral function may be applied to find the value of any rational function

$$y = R(x).$$

For a rational function can always be reduced to the form of a quotient of two integral functions

$$R(x) = g_1(x)/g_2(x).$$

Now after having constructed curves whose ordinates give the values of $g_1(x)$ and $g_2(x)$ for any abscissa x (Fig. 13), $R(x)$ is found in the following manner. Through a point P on the axis of abscissas draw a parallel to the axis of ordinates. Let G_1 and G_2 be the points whose ordinates are equal to $g_1(x)$ and $g_2(x)$. Pass horizontally from G_1 to G_1' on the vertical through P and from G_2 to G_2' on the axis of ordinates. Draw a line through P and G_2' and produce it as far as A where it intersects the horizontal through G_1. Then $R(x)$ is equal to the ratio $G_1'A$ to PO. $G_1'A$ may then be set off as ordinate on the vertical

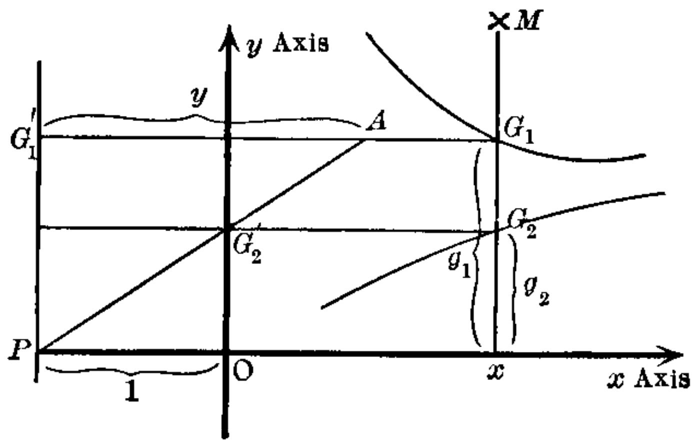


FIG. 13,

through x and defines the point M whose ordinate is equal to $R(x)$ in length, when OP is chosen as the unit of length.

§ 4. *Linear Functions of Any Number of Variables.*—Let us consider a linear function of a number of variables $x_1, x_2 \cdots x_n$,

$$a_0 + a_1x_1 + a_2x_2 + \cdots + a_nx_n,$$

where $a_0, a_1, a_2, \cdots a_n$ are given numbers positive or negative. The question is how the value of this linear function may be conveniently constructed for various systems $x_1, x_2, \cdots x_n$. Suppose $a_0, a_1, \cdots a_n$ to represent horizontal lines directed to the right or left according to the sign of the corresponding number and to be laid off on an horizontal axis in succession as if to find the sum

$$a_0 + a_1 + a_2 + \cdots + a_n,$$

a_0 begins at O and runs to C_1, a_2 begins at C_1 and runs to C_2 and so on (Fig. 14). The numbers $x_1, x_2, \cdots x_n$ let us represent

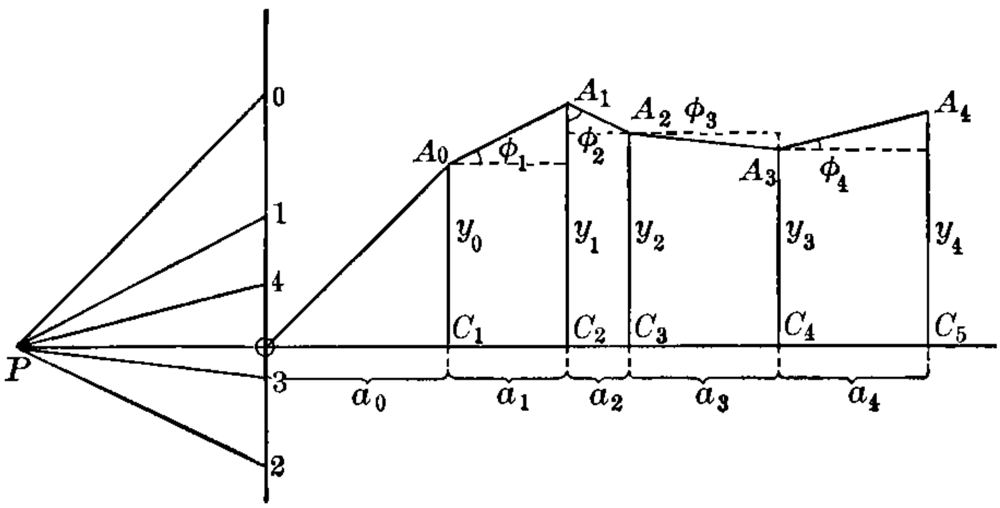


FIG. 14.

by ratios of lengths. We draw a vertical line through O and choose a point P on the horizontal axis. Then let x_1 be equal to the ratio $O1/PO$, $x_2 = O2/PO$, etc. If P is chosen on the left of O, we take the point 1 above O for a positive value of x_1 and below O for a negative one and the same for the other points. Mark a point 0 above O in the same distance from O as P. Join the point P with the points 0, 1, 2, 3, 4, $\cdots$ and draw a broken line $OA_0A_1A_2A_3A_4$ in such a manner that A_0 is on the vertical through C_1 and OA_0 is parallel to $P0$, A_1 on the vertical through C_2 and A_0A_1 parallel to $P1$, A_2 on the vertical through C_3 and A_1A_2 parallel to $P2$ and so on. Then the ordinate y_0 of A_0 will have the same length as a_0 and will be directed upward when the direction of a_0 is to the right, and downward when the direction of a_0 is to the left. The difference $y_1 - y_0$ of the ordinates of A_1 and A_0 is equal in length to a_1x_1, as $y_1 - y_0$ and a_1 have the same ratio as 01 and PO. A_1 will be above or below A_0 according to the line a_1x_1 being directed to the right or to the left and it is understood that a_1x_1 has the same direction as a_1 for positive

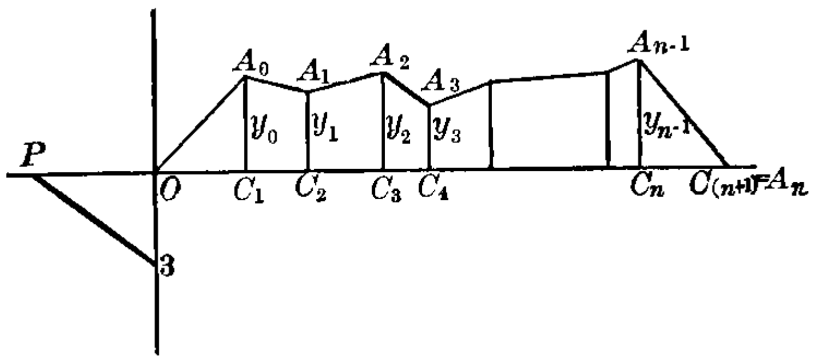


FIG. 15.

values of x_1 and a direction opposite to a_1 for negative values of x_1. Thus the ordinate y_1 has the same length as the line $a_0 + a_1x_1$ and its direction is upward or downward according to the direction of the line $a_0 + a_1x_1$ being to the right or to the left. In the same way it is shown that the ordinate y_2 of the point A_2 is equal in length to

$$a_0 + a_1x_1 + a_2x_2,$$

and y_3 to

$$a_0 + a_1x_1 + a_2x_2 + a_3x_3$$

and so on, the direction upward or downward corresponding to the positive or negative value of the linear function.

If the values of $x_1, x_2, \cdots x_n$ satisfy the equation

$$a_0 + a_1x_1 + a_2x_2 + \cdots + a_nx_n = 0$$

the ordinate y_n must vanish, that is to say, the point A_n must coincide with C_{n+1}, the end of the line a_n. And vice versa if A_n and C_{n+1} coincide the equation is satisfied. Consequently if we know all the values but one of the numbers $x_1, x_2, \cdots x_n$ the unknown value can be found graphically. For suppose x_3 to be

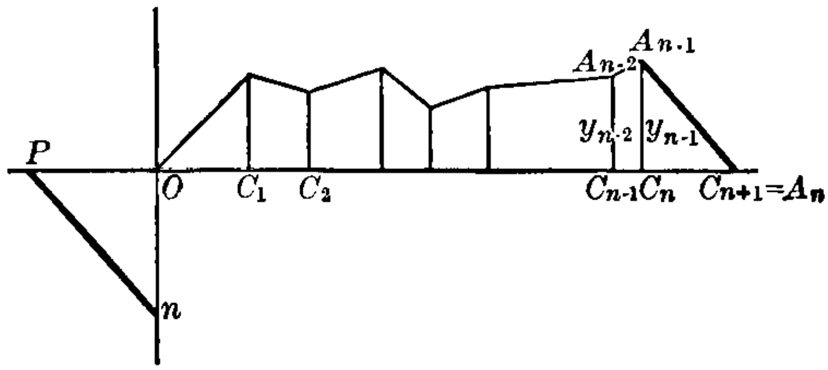


FIG. 16.

the unknown value we can, beginning from O, find the broken line as far as A_2 and beginning from the other end A_n we can find it as far as A_3 (Fig. 15). A parallel to A_2A_3 through P furnishes the point 3 on the axis of ordinates. If $x_1, x_2, \cdots x_{n-1}$ are known and only x_n not, we can draw the broken line as far as A_{n-1} and as A_n has to coincide with C_{n+1}, we can draw a parallel to $A_{n-1}A_n$ through P and find the point n on the axis of ordinates

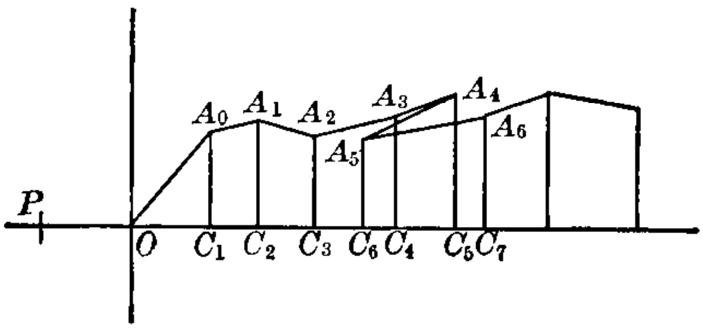


FIG. 17.

that determines the value x_n by the ratio On/PO or On/Oo. In Figs. 15 and 16 all the coefficients $a_0, a_1, \cdots$, are positive. A negative coefficient a_5 is shown in Fig. 17. The only difference is that C_6 lies to the left of C_5 and consequently the broken line passes from A_4 back to A_5.

If we keep the points 0, 1, 2, $\cdots$, in their positions but change the position of P to P' (Fig. 18) and repeat the construction of the broken line, we obtain $OA_0'A_1'A_2' \cdots$ instead of $OA_0A_1A_2 \cdots$. The ordinate y_α' of the point A_α' is evidently

$$y_\alpha' = a_0 \frac{O0}{P'O} + a_1 \frac{O1}{P'O} + \cdots + a_\alpha \frac{O\alpha}{P'O}$$

and therefore

$$y_\alpha' = \frac{PO}{P'O} y_\alpha.$$

That is to say, by changing the position of P without changing the position of the points 0, 1, 2, $\cdots$ we can change the scale of the ordinates of the broken line. They change inversely pro-

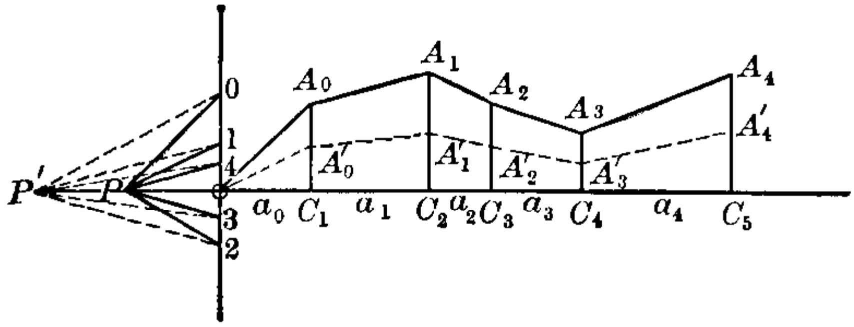


FIG. 18.

portional to PO. It may be convenient to make use of this device in order to make the ordinates a convenient size independent of the scale that we have chosen for the points 0, 1, 2, $\cdots$ that determine the values

$$x_1 = \frac{O1}{O0}, \quad x_2 = \frac{O2}{O0}, \cdots.$$

A linear equation with only one unknown quantity

$$a_0 + a_1x_1 = 0$$

is solved by drawing a parallel to A_0A_1 through P. Let a second equation be given with two unknown quantities

$$b_0 + b_1x_1 + b_2x_2 = 0.$$

The lines b_0, b_1, b_2 are laid off as before. Knowing x_1 as the solution of the first equation we can construct the broken line OB_0B_1 corresponding to the second equation and as B_2 must coincide with the end of b_2, we can draw a parallel to B_1B_2 through P and find x_2. In a similar manner we can find x_3 from a third equation

$$c_0 + c_1x_1 + c_2x_2 + c_3x_3 = 0,$$

and so we can find any number of unknown quantities, if each equation contains one unknown quantity more than those before.

In the general case when n unknown quantities are to be determined from n linear equations each equation will contain all the unknown quantities, and therefore we cannot find them one after the other as in the case just treated. But it can be shown that by means of very simple constructions the general case is reduced to a set of equations, such as has just been treated.

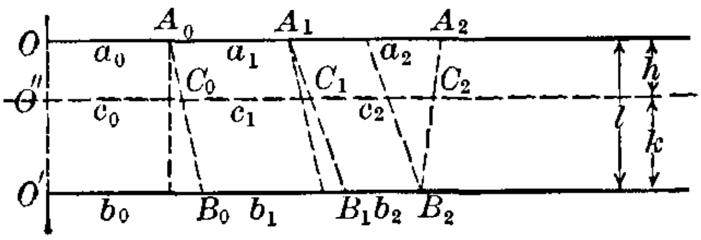


FIG. 19.

Let us begin with two equations and two unknown quantities.

$$a_0 + a_1x_1 + a_2x_2 = 0,$$
$$b_0 + b_1x_1 + b_2x_2 = 0.$$

The lines a_0, a_1, a_2 are laid off on a horizontal line $OA_0A_1A_2$ and the lines b_0, b_1, b_2 on another horizontal line $O'B_0B_1B_2$ (Fig. 19). Now let us join O and O', A_0 and B_0, A_1 and B_1, A_2 and B_2 by straight lines and let us draw a third horizontal line intersecting them in the points $O''C_0C_1C_2$. These points correspond to a certain linear function

$$c_0 + c_1x_1 + c_2x_2,$$

and it can be shown that it vanishes when x_1 and x_2 are the same values for which the first two linear functions vanish. Let the distance of the first two horizontal lines be l and the distance of the third from the first and second h and k. Then it can readily be seen that

$$c_0 = a_0 + \frac{h}{l}(b_0 - a_0) = \frac{k}{l}a_0 + \frac{h}{l}b_0.$$

For a parallel to OO' through A_0 defines with the line A_0B_0 on the third and second horizontal line segments equal to $c_0 - a_0$ and $b_0 - a_0$ and as these segments have the ratio h/l, it follows that

$$c_0 = a_0 + \frac{h}{l}(b_0 - a_0) = \frac{k}{l} a_0 + \frac{h}{l} b_0.$$

By drawing a parallel to A_0B_0 through A_1 and to A_1B_1 through A_2 or through B_2 (which comes to the same thing), we convince ourselves in the same way that

$$c_1 = a_1 + \frac{h}{l}(b_1 - a_1) = \frac{k}{l} a_1 + \frac{h}{l} b_2$$

and

$$c_2 = a_2 + \frac{h}{l}(b_2 - a_2) = \frac{k}{l} a_2 + \frac{h}{l} b_2.$$

Multiplying the equation

$$a_0 + a_1x_1 + a_2x_2 = 0$$

by k/l and the equation

$$b_0 + b_1x_1 + b_2x_2 = 0$$

by h/l and adding the two products, we obtain

$$c_0 + c_1x_1 + c_2x_2 = 0.$$

The third horizontal need not lie between the first two. If it lies below the second we have merely to give k a negative value and if it lies above the first we have to give h a negative value and the same formulæ for c_0, c_1, c_2 hold good. Consequently the conclusion remains valid, that from the first two equations the third follows.

Now as we are perfectly at liberty to draw the third horizontal line where we please, we can let it run through the intersection of the straight lines A_1B_1 and A_2B_2. In this case the points C_1 and C_2 must coincide and consequently c_2 must vanish. If c_1 does not vanish we can by what has been shown above find x_1 and with x_1 we can find x_2 from either of the two first horizontal lines. In case c_1 also vanishes, that is to say, in case the three straight lines A_2B_2, A_1B_1, A_0B_0 all pass through the same point, while OO' does not pass through it, the two given equations cannot simultaneously be satisfied. For if they were, it would follow that

$$c_0 + c_1x_1 + c_2x_2 = 0,$$

and as c_1 and c_2 are zero c_0 would have to be zero, which it is not as OO' is supposed not to pass through the intersection of A_2B_2, A_1B_1 and A_0B_0. If on the other hand all four lines A_2B_2, A_1B_1, A_0B_0, OO' pass through the same point, c_0, c_1 and c_2 will all three vanish. In this case the two given equations do not contradict one another, but $b_0b_1b_2$ will be proportional to $a_0a_1a_2$. The

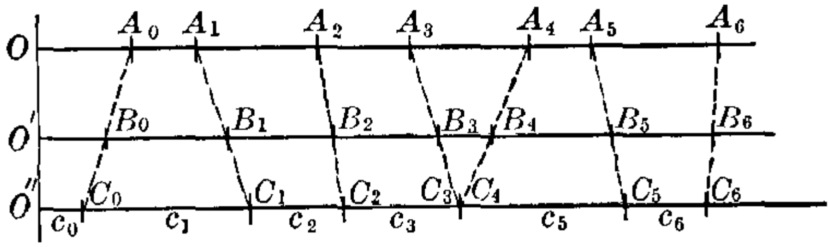


FIG. 20.

second equation will therefore contain the same relation between x_1 and x_2 as the first, so that there is only one condition for x_1 and x_2 to be satisfied. We may then assign any arbitrary value to one of them and determine the value of the other to satisfy the equation.

In the case of two linear equations of any number of quantities $x_1, x_2, \cdots x_n$ we can by the same graphical method eliminate one of the quantities. In Fig. 20 this is shown for two linear equations with six unknown quantities. The two horizontal lines $OA_0A_1A_2A_3A_4A_5A_6$ and $O'B_0B_1B_2B_3B_4B_5B_6$ represent two linear equations. Through the intersection of A_3B_3 and A_4B_4 a third horizontal line is drawn intersecting the lines OO', A_0B_0, A_1B_1, $\cdots A_6B_6$ in $O''C_0C_1 \cdots C_6$. As C_3 and C_4 coincide, the line c_4 vanishes and x_4 is eliminated, so that the equation assumes the form

$$c_0 + c_1x_1 + c_2x_2 + c_3x_3 + c_5x_5 + c_6x_6 = 0.$$

Suppose now that a set of six equations with six unknown quantities is represented geometrically on six horizontal lines. We shall keep one of these; but instead of the other five we construct five new ones from which one of the unknown quantities has been eliminated by means of the first equation. Now it may happen that at the same time another unknown quantity is eliminated, then this quantity remains arbitrary. Of the five new equations we again keep one that contains another unknown quantity and replace the four others again by four new ones from which this unknown quantity has been eliminated. Going on in this manner the general rule will be that with each step only one quantity is eliminated, so that at last one equation with one unknown quantity remains. Instead of the given six equations with six unknown quantities each, we now have one with six, one with five and so on down to one with one. The geometrical construction shows that this system is equivalent to the given system, for we can just as well pass back again to the given system. We have seen above how the unknown quantities may now be found geometrically. It may however happen in special cases that with the elimination of one unknown quantity another is eliminated at the same time. To this we may then assign an arbitrary value without interfering with the possibility of the solution. Finally all unknown quantities may be eliminated from an equation. If in this case there remains a term different from zero it shows that it is impossible to satisfy the given equations simultaneously. If no term remains, the two equations from which the elimination takes its origin contain the same relation between the unknown quantities and one of them may be ignored.

§ 5. *The Graphical Handling of Complex Numbers.*—A complex number

$$z = x + yi$$

is represented graphically by a point Z whose rectangular coördinates correspond to the numbers x and y. The units by which the coördinates are measured, we assume to be of equal length. We might also say that a complex number is nothing but an algebraical form of writing down the coördinates of a point in a plane. And the calculations with complex numbers stand for certain geometrical operations with the points which correspond to them.

By the "sum" of two complex numbers

$$z_1 = x_1 + y_1 i \quad \text{and} \quad z_2 = x_2 + y_2 i$$

we understand the complex number

$$z_3 = x_3 + y_3 i$$

where

$$x_3 = x_1 + x_2 \quad \text{and} \quad y_3 = y_1 + y_2,$$

and we write

$$z_3 = z_1 + z_2.$$

Graphically we obtain the point Z_3 representing z_3 from the points Z_1 and Z_2 representing z_1 and z_2 by drawing a parallel to OZ_2 through Z_1 and making Z_1P (Fig. 21) equal to OZ_2 in length *and direction* or by drawing a parallel through Z_2 and making Z_2P equal to OZ_1 in length and direction. The coordinates of P are evidently equal to $x_1 + x_2$ and $y_1 + y_2$.

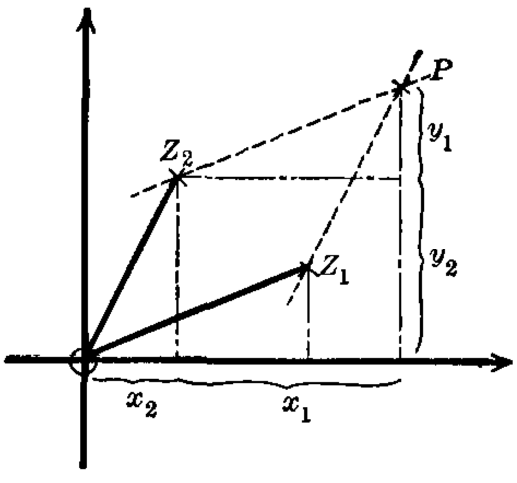


FIG. 21.

Two complex numbers z and z' are called opposite, when their sum is zero.

$$z + z' = 0 \quad \text{or} \quad x = -x' \quad \text{and} \quad y = -y' \quad \text{or} \quad z = -z'.$$

The corresponding points Z and Z' are at the same distance from the origin O but in opposite directions.

The difference of two complex numbers is that complex number, which added to the subtrahend gives the minuend

$$z_2 + (z_1 - z_2) = z_1.$$

Therefore

$$z_1 - z_2 = (x_1 - x_2) + (y_1 - y_2)i.$$

This may also be written

$$z_1 + z_2' \quad \text{where} \quad z_2' = -z_2 = -x_2 - y_2 i.$$

That is to say, the subtraction of the complex number z_2 from z_1 may be effected by adding the opposite number $-z_2$. For the geometrical construction of the point Z corresponding to $z_1 - z_2$ we have to draw a parallel to OZ_2 through Z_1 and from Z_1 in the direction from Z_2 to O we have to lay off the distance Z_2O. Or we may also draw from O a line equal in *direction* and in length to Z_2Z_1. This will also lead to the point Z representing the difference $z_1 - z_2$.

The rules for multiplication and division of complex numbers are best stated by introducing polar coördinates. Let r be the positive number measuring the distance OZ in the same unit of length in which x and y measure the abscissa and ordinate, so that

$$r = \sqrt{x^2 + y^2}$$

and let φ be the angle between OZ and the axis of x, counted in the direction from the positive axis of x toward the positive axis of y through the entire circumference (Fig. 22). Then we have

$$x = r\cos\varphi, \quad y = r\sin\varphi$$

and

$$z = x + yi = r(\cos\varphi + \sin\varphi i).$$

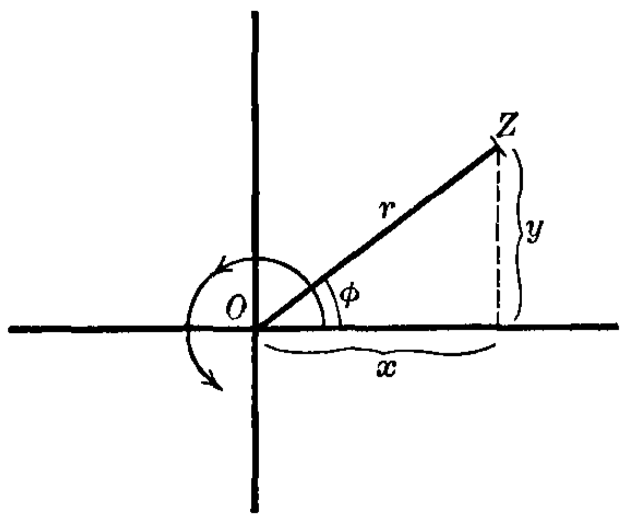


FIG. 22.

Let us call r the modulus and φ the angle of z. The angle may be increased or diminished by any multiple of four right angles without altering z, but any alteration of r necessarily implies an alteration of z.

According to Moivre's theorem, we can write

$$z = re^{\phi i}.$$

By the product of two complex numbers

$$z_1 = r_1 e^{\phi_1 i} \quad \text{and} \quad z_2 = r_2 e^{\phi_2 i}$$

we understand that complex number z_3 whose modulus r_3 is equal to the product of the moduli r_1 and r_2 and whose angle φ_3 is the sum of the angles φ_1 and φ_2 or differs from the sum only by a multiple of four right angles

$$z_3 = z_1 z_2 = r_1 r_2 e^{(\phi_1 + \phi_2)i}.$$

The definition of division follows from that of multiplication. The quotient z_1 divided by z_2 is that complex number, which multiplied by z_2 gives z_1. Therefore the product of its modulus with the modulus of z_2 must be equal to the modulus of z_1 and the sum of its angle with the angle of z_2 must be equal to the angle of z_1. Or we may also say the modulus of the quotient z_1/z_2 is equal to the quotient of the moduli r_1/r_2 and its angle is equal to the difference of the angles $\varphi_1 - \varphi_2$. An addition or subtraction of a multiple of four right angles we shall leave out of consideration as it does not affect the complex number nor the point representing it.

The geometrical construction corresponding to the multiplication and division of complex numbers is best described by considering two quotients each of two complex numbers that give the same result. Let us write

$$z_1/z_2 = z_3/z_4.$$

The geometrical meaning of this is that

$$r_1/r_2 = r_3/r_4,$$

and

$$\varphi_1 - \varphi_2 = \varphi_3 - \varphi_4.$$

That is to say, the triangles Z_1OZ_2 and Z_3OZ_4 are geometrically similar (Fig. 23). When three of the points Z_1, Z_2, Z_3, Z_4 are given the fourth can evidently be found. For instance let Z_1, Z_2, Z_4 be given. Draw a parallel to Z_1Z_2 intersecting OZ_2 at a distance r_4 from O. This point together with the intersection on OZ_1 and with O will form the three corners of a triangle congruent to the triangle Z_4Z_3O. It will be brought into

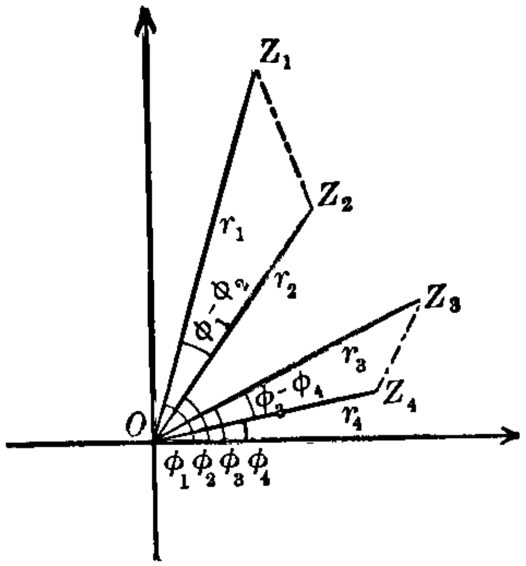


FIG. 23.

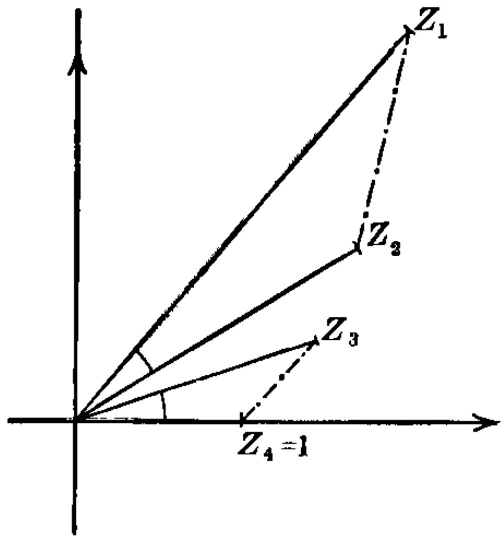


FIG. 24.

the position of Z_4Z_3O by being turned round O so as to bring the direction of the side in OZ_2 into the position of OZ_4. Thus the direction of OZ_3 and its length may be found.

This construction contains multiplication as well as division as special cases. Let Z_4 coincide with the point $x = 1$, $y = 0$, so that $z_4 = 1$ (Fig. 24), then we have

$$z_1/z_2 = z_3 \quad \text{or} \quad z_1 = z_2 z_3.$$

From any two of the points Z_1, Z_2, Z_3 a simple construction gives us the third.

The geometrical representation of complex numbers may be used to advantage to show the properties of harmonic oscillations.

Let a point P move on the axis of x, so that its abscissa at the time t is given by the formula

$$x = r \cos (nt + \alpha),$$

n, r and α being constants. We call r the amplitude and $nt + \alpha$

the phase of the motion. The point P moves backwards and forwards between the limits $x = r$ and $x = -r$. The time $T = 2\pi/n$ is called the period of the oscillation, it is the time in which one complete oscillation backwards and forwards is performed.

Now instead of x let us consider the complex number

$$z = r\cos(nt + \alpha) + r\sin(nt + \alpha)i$$

or

$$z = re^{(nt+\alpha)i},$$

of which x is the abscissa and let us follow the movement of the point Z. For $t = 0$ we have

$$z = re^{\alpha i}.$$

Designating this value by z_0, we can write

$$z = z_0 e^{nti}.$$

The geometrical meaning of the product

$$z_0 e^{nti}$$

is that the line OZ_0 is turned round O through the angle nt. For the modulus of e^{nti} being equal to 1 the modulus of z_0 is not changed by the multiplication. The movement of the point Z therefore consists in a uniform revolution of OZ round O. At the moment $t = 0$ the position is OZ_0 and after the time $T = 2\pi/n$ the same position is occupied again. The revolution goes on in the direction from the positive axis of x to the positive axis of y (Fig. 25).

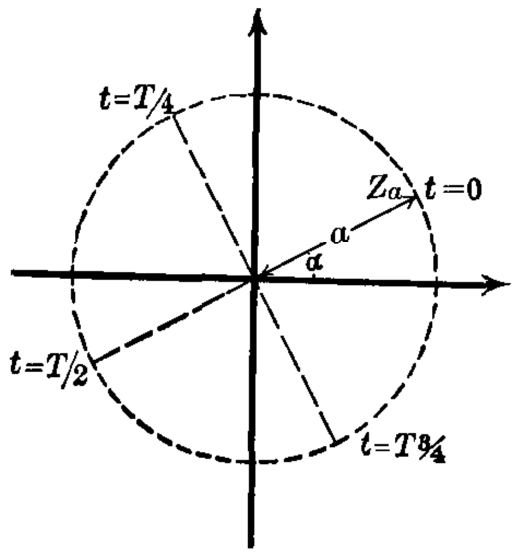


Fig. 25.

The movement of Z is evidently simpler than the movement of the projection P of Z on the axis of x.

Let us consider a motion composed of the sum of two harmonic motions of the same period but of different amplitudes and phases

$$x = r_1 \cos (nt + \alpha_1) + r_2 \cos (nt + \alpha_2),$$

and let us again substitute the motion of the point Z corresponding to the complex number

$$z = r_1 e^{(nt+\alpha_1)i} + r_2 e^{(nt+\alpha_2)i}.$$

For $t = 0$ the first term is

$$z_1 = r_1 e^{\alpha_1 i}$$

and the second term

$$z_2 = r_2 e^{\alpha_2 i}.$$

Introducing z_1 and z_2 into the expression for z we have

$$z = z_1 e^{nti} + z_2 e^{nti} = (z_1 + z_2) e^{nti} = z_3 e^{nti}$$

where

$$z_3 = z_1 + z_2.$$

This shows at once that the movement of Z is a uniform circular movement consisting in a uniform revolution of OZ round O. The position at the moment $t = 0$ is OZ_3 corresponding to the complex number

$$z_3 = z_1 + z_2.$$

The projection of Z on the axis of x has the abscissa

$$x = r_3 \cos (nt + \alpha_3)$$

where r_3 and α_3 designate modulus and angle of z_3. Thus the sum of two harmonic motions of the same period is shown also to form a harmonic motion.

The same holds for a sum of any number of harmonic motions of the same period. For the complex number

$$z = r_1 e^{(nt+\alpha_1)i} + r_2 e^{(nt+\alpha_2)i} + \cdots + r_\lambda e^{(nt+\alpha_\lambda)i}$$

where $r_1, r_2, \cdots r_\lambda; \alpha_1, \alpha_2, \cdots \alpha_\lambda$ and n are constants may be written

$$z = z_1 e^{nti} + z_2 e^{nti} + \cdots + z_\lambda e^{nti}$$

or

$$z = z_0 e^{nti},$$

where

$$z_0 = z_1 + z_2 + \cdots + z_\lambda.$$

The movement of Z therefore, excepting the case $z_0 = 0$, consists in a uniform revolution of OZ round O, OZ always keeping the same length equal to the modulus of z_0. The position of OZ at the moment $t = 0$ is OZ_0.

The motion of a point P whose abscissa is

$$x = ae^{-kt} \cos (nt + \alpha)$$

where a, k, n, α are constants (a and k positive) is called a damped harmonic motion. It may be looked upon as a harmonic motion, whose amplitude is decreasing. To study this motion let us again substitute a complex number

$$z = ae^{-kt} \cos (nt + \alpha) + ae^{-kt} \sin (nt + \alpha)i,$$

or

$$z = ae^{-kt} \cdot e^{(nt+\alpha)i},$$

or

$$z = z_0 e^{-kt} \cdot e^{nti},$$

where z_0 is written for the complex constant $ae^{\alpha i}$.

The product

$$z_0 e^{-kt}$$

is a complex number corresponding to a point Z_1 on the same radius as Z_0, coincident with Z_0 at the moment $t = 0$ but approaching O in a geometrical ratio after $t = 0$. In unit of time the distance of Z_1 from O decreases in the constant ratio $e^{-k} : 1$. The multiplication with e^{nti} turns OZ_1 round O through an angle nt. We may therefore describe the motion of Z as a uniform revolution of OZ round O, Z at the same time approaching O at a rate uniform in this sense that in equal times the distance is reduced in equal proportions (Fig. 26). At the moment $t = 0$ the position coincides with Z_0. We speak of a period of this motion meaning the time $T = 2\pi/n$ in which OZ performs an entire revolution round O, although it does not come back to its original position. Any part of the spiral curve described by Z in a given time is geometrically similar to any other part of the curve described in an interval of equal duration. For suppose the second interval of time happens τ units of time later, we shall have for the first interval

$$z = z_0 e^{-kt} \cdot e^{nti},$$

and for the second interval

$$z' = z_0 e^{-k(t+\tau)} \cdot e^{n(t+\tau)i}.$$

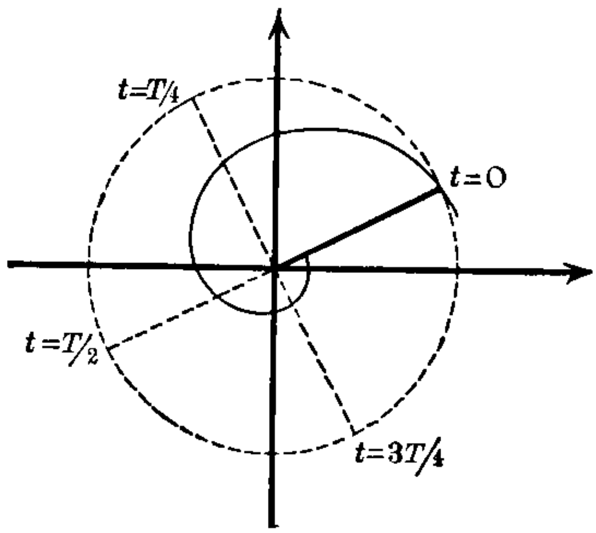


FIG. 26.

Now if z_1 and z_2 are the values of z at two moments t_1 and t_2 of the first interval and z_1' and z_2' the corresponding values of z' at the moments $t_1 + \tau$ and $t_2 + \tau$ of the second interval, we have

$$\frac{z_1}{z_2} = e^{-k(t_1-t_2)} \cdot e^{n(t_1-t_2)i} = \frac{z_1'}{z_2'}.$$

Therefore the triangle Z_1OZ_2 is geometrically similar to the triangle $Z_1'OZ_2'$. As Z_1 and Z_2 may coincide with any points of the first part of the curve, the two parts are evidently geometrically similar.

The projection of Z on the axis of x performs oscillations decreasing in amplitude. The turning-points correspond to those points of the spiral curve described by Z, where its tangent is parallel to the axis of y, that is to say, where the abscissa of dz/dt vanishes.

Now

$$\frac{dz}{dt} = z_0(-k + ni)e^{-kt}e^{nti} = (-k + ni)z$$

or

$$\frac{\frac{dz}{dt}}{z} = -k + ni = \rho e^{i\lambda}$$

where ρ and λ are the modulus and angle of the complex number $-k + ni$.

Consequently, if we represent dz/dt by a point Z', the triangle $Z'OZ$ will remain geometrically similar to itself. The turning points of the damped oscillations correspond to the moments when OZ' is directed vertically upward or downward or when the angle of dz/dt is equal to $\pi/2$ or $3\pi/2$. The angle of z will then be $\pi/2 - \lambda$ or $3\pi/2 - \lambda$ plus or minus any multiple of 2π. As the angle of z, on the other hand, is changing in time according to the formula

$$nt + \alpha,$$

we find the moments where the movement turns by the equation

$$nt + \alpha = \pi/2 - \lambda + 2N\pi,$$

or

$$nt + \alpha = 3\pi/2 - \lambda + 2N\pi,$$

N denoting any positive or negative integral number. The time between two consecutive turnings is therefore equal to π/n, that is, equal to half a period. All the points Z corresponding to turning points lie on the same straight line through the origin O forming an angle $3\pi/2 - \lambda$ with the direction of the positive axis of x. The amplitudes of the consecutive oscillations therefore decrease in the same proportion as the modulus of z, that is to say, in half a period in the ratio $e^{-\frac{k\pi}{n}}$.

Let us consider the vibrations of a system possessing one degree of freedom when the system is subjected to a force varying as a harmonic function of the time and let us limit our considerations to positions in the immediate neighborhood of a position of stable equilibrium. If the quantity x determines the position of the system the oscillations satisfy a differential equation of the form

$$m\frac{d^2x}{dt^2} + k\frac{dx}{dt} + n^2x = F\cos(pt)$$ [1]

where m, k, n, p, F are positive constants.

[1] See for instance Rayleigh, Theory of Sound, Vol. I, chap. III, § 46.

This is another case where the introduction of a complex variable

$$z = x + yi$$

and the geometrical representation of complex numbers helps to form the solution and to survey the variety of phenomena that may be produced.

In order to introduce z let us simultaneously consider the differential equation

$$m\frac{d^2y}{dt^2} + k\frac{dy}{dt} + n^2y = F\sin pt,$$

and let us multiply the second equation by i and add it to the first. We then have

$$m\frac{d^2z}{dt^2} + k\frac{dz}{dt} + n^2z = Fe^{pti}.$$

The movement of the point Z representing the complex number z then serves as well to show the movement corresponding to x. We need only consider the projection of Z on the axis of x.

A solution of the differential equation may be obtained by writing

$$z = z_0e^{pti}.$$

Introducing this expression for z and cancelling the factor e^{pti} we have

$$z_0(-mp^2 + kpi + n^2) = F,$$

or

$$z_0 = \frac{F}{-mp^2 + kpi + n^2}.$$

z_0 is a complex constant, that may be represented geometrically as we shall see later on.

This solution

$$z = z_0e^{pti}$$

is not general. If z' denotes any other solution so that

$$m\frac{d^2z'}{dt^2} + k\frac{dz'}{dt} + n^2z' = Fe^{pti},$$

we find by subtracting the two equations

$$m\frac{d^2(z'-z)}{dt^2} + k\frac{d(z'-z)}{dt} + n^2(z'-z) = 0$$

or writing

$$z' - z = u,$$

$$m\frac{d^2u}{dt^2} + k\frac{du}{dt} + n^2u = 0.$$

The general solution of this equation is

$$u = u_1e^{\lambda_1 t} + u_2e^{\lambda_2 t},$$

where u_1 and u_2 are arbitrary constants and λ_1 and λ_2 are the roots of the equation for λ

$$m\lambda^2 + k\lambda + n^2 = 0,$$

$$\left.\begin{matrix}\lambda_1\\ \lambda_2\end{matrix}\right\} = -\frac{k}{2m} \pm \sqrt{\frac{k^2}{4m^2} - n^2}.$$

If $k^2/4m^2$ is greater than n^2, so that the square root has a real value, $\sqrt{k^2/4m^2 - n^2}$ will certainly be smaller than $k/2m$. Therefore λ_1 and λ_2 will both be negative and the moduli of the complex numbers $u_1e^{\lambda_1 t}$ and $u_2e^{\lambda_2 t}$ will in time become insignificant. If, on the other hand, $k^2/4m^2$ is smaller than n^2, both complex numbers $u_1e^{\lambda_1 t}$ and $u_2e^{\lambda_2 t}$ correspond to points describing spirals that approach the origin, as we have seen above, in a constant ratio for equal intervals of time. Therefore they will also in time become insignificant.

After a certain lapse of time the expression

$$z = z_0e^{pti}$$

will therefore suffice to represent the solution.

The point Z moves uniformly in a circle round O of a radius equal to the modulus of z_0, completing one revolution in the period $2\pi/p$, the period of the force acting on the system. The movement of the projection of Z on the axis of x is given by

$$x = r_0 \cos (pt + \alpha),$$

where r_0 is the modulus and α the angle of z_0. It is a harmonic movement with the same period as that of the force: $F \cos pt$, but with a certain difference of phase and a certain amplitude depending on the values of F, m, k, n, p.

It is important to study this relation in order to survey the phenomena that may be produced. For this purpose the geometrical representation of complex numbers readily lends itself.

In the expression for z_0

$$z_0 = \frac{F}{-mp^2 + kpi + n^2},$$

let us consider the denominator

$$-mp^2 + kpi + n^2,$$

and let us suppose the period of the force acting on the system not determined, while the constants of the system m, k, n and the amplitude of the force F have given values. The quantity p is the number of oscillations of the force during an interval of 2π units of time. This quantity p we suppose to be indeterminate and we intend to show how the amplitude and phase of the forced vibrations compare with the amplitude and phase of the force for different values of p.

Let us plot the curve of the points corresponding to the complex number

$$n^2 - mp^2 + kpi,$$

where p assumes the values $p = 0$ to $+\infty$.

This curve is a parabola whose axis coincides with the axis of x and whose vertex is in the point $x = n^2$, $y = 0$. We find its equation by eliminating p from the equations

$$x = n^2 - mp^2, \quad y = kp,$$

viz.,

$$x = n^2 - \frac{m}{k^2}y^2.$$

But it is better not to eliminate p and to plot the different points for different values of p. In Fig. 27 the curve is drawn for $p = 0$ to 3 and the points for $p=0, 1, 2, 3$ are marked. The ordinates increase in proportion to p; they are equal to 0, k, $2k$, $3k$ for $p = 0, 1, 2, 3$. The distance between the projection of any point of the curve on the axis of x and the vertex is proportional to p^2. It is equal to 0, m, $4m$, $9m$ for $p = 0, 1, 2, 3$.

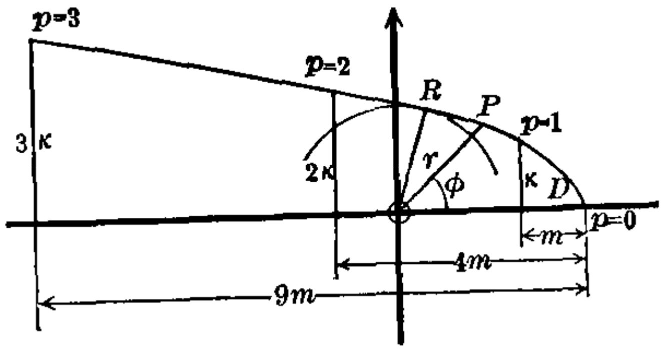


FIG. 27.

For any point P on the parabola let us denote the distance from O by r and the angle between OP and the positive axis of x by φ so that

$$n^2 - mp^2 + kpi = re^{\phi i}.$$

Then we have

$$z_0 = re^{\phi i},$$

and consequently

$$z = \frac{F}{r}e^{(pt-\phi)i},$$

and

$$x = \frac{F}{r}\cos(pt - \varphi).$$

The amplitude F/r of the forced vibration is inversely proportional to r. Thus our Fig. 27 shows us what the period of the force must be to make the forced vibrations as large as possible. It corresponds to the point on the parabola whose distance from O is smallest. It is the point where a circle round O touches the parabola. In Fig. 27 this point is marked R. It may be called the point of maximum resonance. When the constants of the system are such that the ordinate of the point, where the parabola intersects the axis of y is small in comparison with the abscissa of the vertex, then OR will lie close to the axis of y (Fig. 28). In this case the angle between OR and the positive axis of x will be very nearly equal to 90°, that is to say, the forced oscillations will lag behind the force oscillations by a little less than a quarter of a period. Keeping m and n constant, this will take place for small values of k, *i. e.*, for a small damping influence. A small deviation of p from the frequency of maximum resonance will throw the point P away from R, so that r increases considerably and φ becomes either very small (for values of p smaller than the frequency of maximum resonance) or nearly equal to 180° (for values of p larger than the frequency of maximum resonance). In other words for small values of k the maximum of resonance is very sharp. A deviation of the period of the force from the period of maximum resonance will lessen the amplitude of the forced vibration considerably. The lag of its phase behind that of the force will at the same time nearly vanish, when the frequency of the force is decreased or it will become nearly as large as half a period, when the frequency of the force is increased. For larger values of k the parabola opens out and this phenomenon becomes less marked. The minimum of the radius r becomes less pronounced. The angle between OR and the axis of x becomes smaller and smaller and for a certain value of k and all larger values the point R will coincide with the vertex of the parabola. In this case, there is no resonance. When the period of the force increases indefinitely (p becoming smaller and smaller) the amplitude of the forced vibration will increase and will approach more and more to the limit

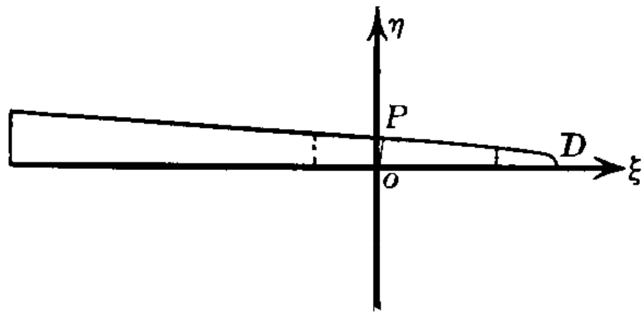


FIG. 28.

$$\frac{F}{n^2},$$

but there will be no definite period for which the forced vibrations are stronger than for all others.

CHAPTER II.

The Graphical Representation of Functions of One or More Independent Variables.

§ 6. *Functions of One Independent Variable.*—A function y of one variable x

$$y = f(x)$$

is usually represented geometrically by a curve, in such a way that the rectangular coördinates of its points measured in certain chosen units of length are equal to x and y. This graphical representation of a function is exceedingly valuable. But there is another way not less valuable for certain purposes, more used in applied than in theoretical mathematics, which here will occupy our attention.

Suppose the values of y are calculated for certain equidistant values of x, for instance:

$$x = -6, -5, -4, -3, -2, -1, 0, +1, +2, +3, +4, +5, +6,$$

and let us plot these values of y in a uniform scale on a straight line. Draw the uniform scale on one side of the straight line and mark the points that correspond to the calculated values of y on the other side of the straight line. Denote them by the numbers x that belong to them (Fig. 29). The drawing will then allow us to read off the value of y for any of the values of x with a certain accuracy depending on the size of the scale and the number of its partitions and naturally on the fine-

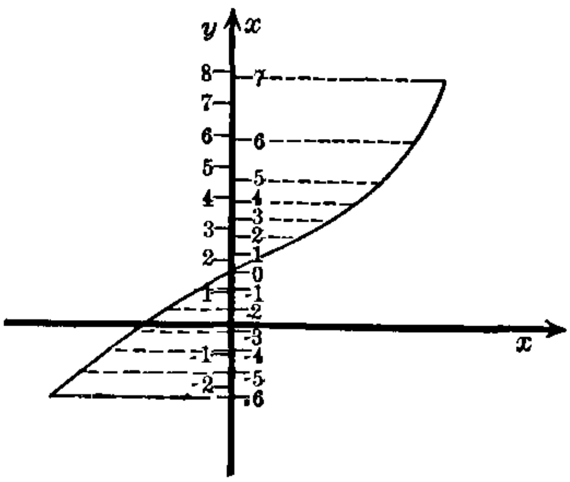


FIG. 29.

ness of the drawing. It will also allow us to read off the value of y for a value of x between those that have been marked, if the intervals between two consecutive values of x are so small that the corresponding intervals of y are nearly equal. We can with a certain accuracy interpolate values of x by sight. On the other hand, we can also read off the values of x for any of the values of y. We shall call this the representation of a function by a scale.

We can easily pass over to the representation of the same function by a curve. We need only draw lines perpendicular to the line carrying the scales through the points marked with the values of x and make their length measured in any given unit equal to the numbers x that correspond to them (Fig. 29).

In a similar way we can pass from the representation of the function by a curve to the representation by a scale.

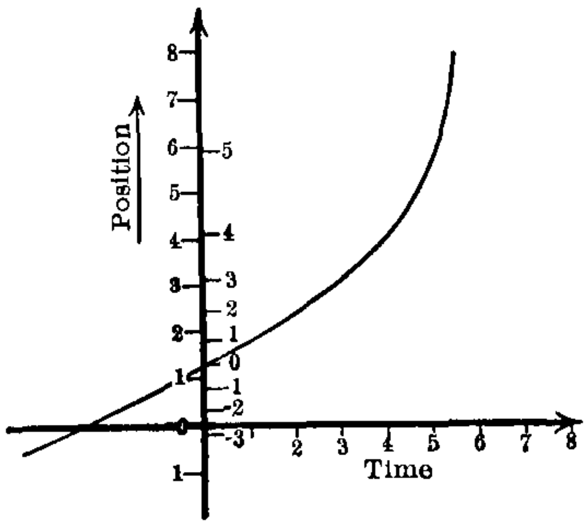


FIG. 30.

The representation by a scale may be imagined to signify the movement of a point on a straight line, the values of x meaning the time and the points marked with these values being the positions of the moving point at the times marked. By passing over to the curve the movement in the straight line is drawn out into a curve with the time as abscissa (Fig. 30).

The representation by a scale is used in connection with the representation by a curve for the purpose of drawing a function of a function.

Let y be a function of x and x a function of t. Then we wish to represent y as a function of t.

Let $y = f(x)$ be given by a curve in the usual way and let $x = \varphi(t)$ be given by a scale on the axis of x marking the points where $t = 0, 1, 2, \cdots, 12$. We then find the values of y corresponding to the values $t = 0, 1, 2, \cdots, 12$ by drawing the ordinates of the curve $y = f(x)$ for the abscissas marked $t = 0, 1, 2,$

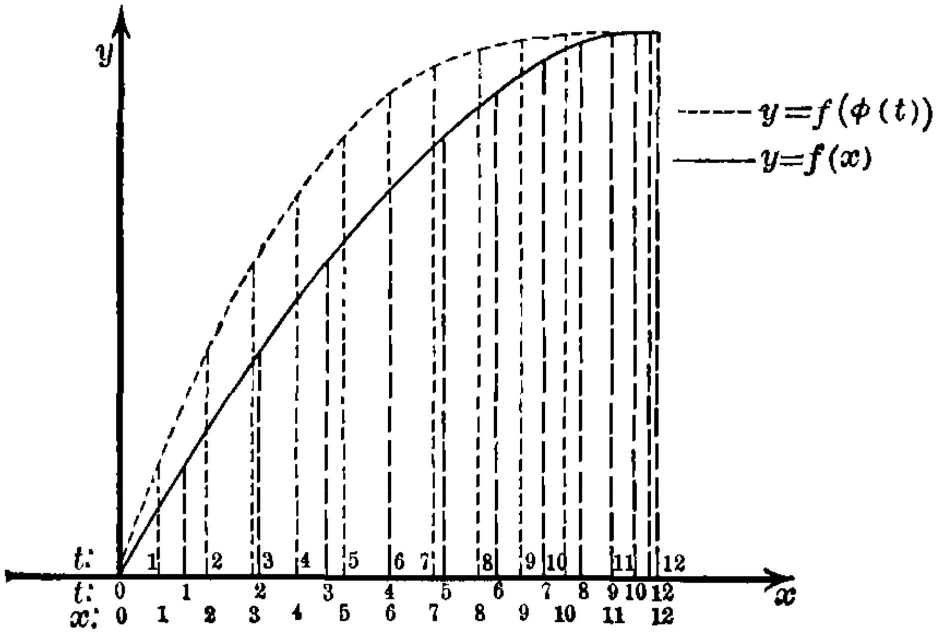


FIG. 31.

$\cdots, 12$. These ordinates as a rule will not be equidistant. But as soon as we move them so as to make them equidistant, they form the ordinates of the curve

$$y = f(\varphi(t))$$

with t as abscissa (Fig. 31).

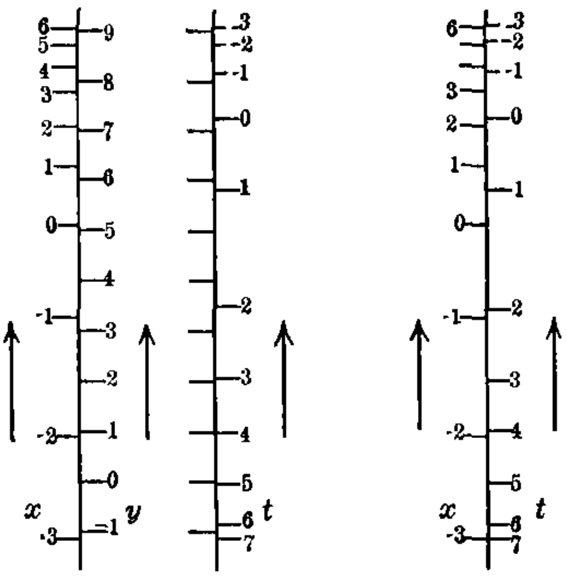


FIG. 32.

The representation of a function by a scale may be generalized in the respect that neither of the two scales facing one another on the straight line need necessarily be uniform. The intervals of both scales may vary from one side of the scale to the other. If the variation is sufficiently slow the interpolation can nevertheless be effected with accuracy. We may look at this case as composed of two cases of the first kind.

$$f(x) = y \quad \text{and} \quad y = g(t).$$

These scales are placed together, so that the scale x touches the scale t

$$f(x) = g(t),$$

while the scale y is cut out (Fig. 32).

§ 7. *The Principle of the Slide Rule.*—Let us investigate how the relation between x and t changes by sliding the x- and t-scales along one another.

If we slide the x-scale through an amount $y = c$ so that a point of the x-scale that was opposite to a certain point y of the y-scale, now is opposite $y + c$, then the relation between x and t represented by the new position of the scales will be given by the equation

$$f(x) = g(t) + c.$$

If x, t and x', t', denote two pairs of values that are placed opposite to one another, we shall have simultaneously

$$f(x) = g(t) + c,$$
$$f(x') = g(t') + c,$$

or by eliminating c

$$f(x) - g(t) = f(x') - g(t').$$

The ordinary slide rule carries two identical scales $y = \log x$ and $y = \log t$ that are able to slide along one another, x and t running through the values 1 to 100. We therefore have

$$\log x - \log t = \log x' - \log t',$$

or

$$\frac{x}{t} = \frac{x'}{t'}.$$

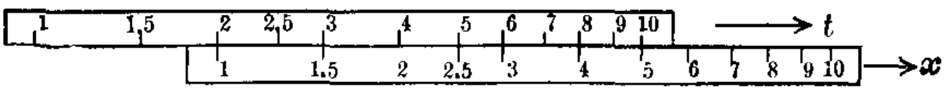


FIG. 33.

That is to say, in any position of the x- and t-scale any two values x and t opposite each other have the same ratio (Fig. 33). This is the principle on which the use of the slide rule is founded. It enables us to calculate any of the four quantities x, t, x', t' if the other three are given. Suppose, for example, x, t, x' known. We set the scales so that x appears opposite to t,

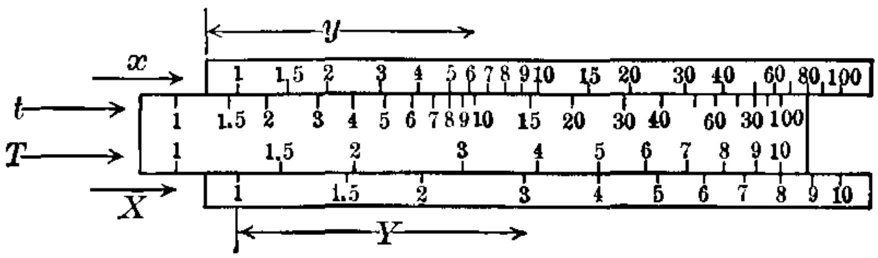


FIG. 34.

then t' is read off opposite to x'. On the other edges the slide rule carries two similar scales one double the size of the other (Fig. 34). We may write

$$y = 2 \log X \quad \text{and} \quad y = 2 \log T.$$

By means of a little frame carrying a crossline and sliding over the instrument, we can bring the scales x and T or t and X opposite each other. If, for example, for any position of the instrument x, T and x', T' are two pairs of values opposite each other, then

$$\log x - 2 \log T = \log x' - 2 \log T',$$

or

$$\frac{x}{T^2} = \frac{x'}{T'^2}.$$

If any three of the four quantities x, T, x', T' are known the fourth may be read off. Thus we find the value

$$\frac{xT'^2}{T^2},$$

by setting T opposite to x and reading off the value opposite to T'. Or we can find the value of

$$\sqrt{\frac{x'}{x}}\,T$$

by setting x opposite to T and reading off the value opposite x'.

Let us reverse the part that carries the scales t, T so that x slides along T and X along t, but in the opposite order (Fig. 35).

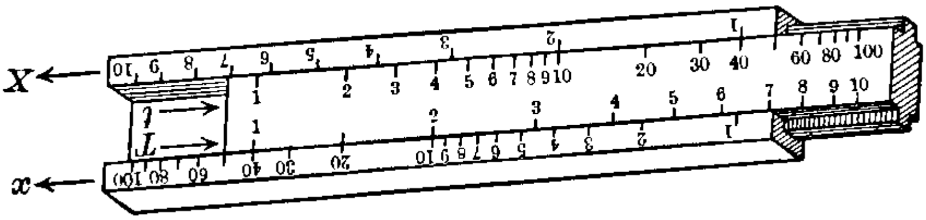


FIG. 35.

The scales t, T may then be expressed by

$$y = l - \log t \quad \text{and} \quad y = l - 2 \log T,$$

l being the entire length of the scales.

By setting the instrument to any position and considering the scales x and t or X and T by means of the cross line we have $\log x + \log t = \log x' + \log t'$ and $\log X + \log T = \log X' + \log T'$ or

$$xt = x't' \quad \text{and} \quad XT = X'T',$$

so that any two values opposite to one another have the same product.

For x and T we have

$$\log x + 2 \log T = \log x' + 2 \log T',$$

or

$$xT^2 = x'T'^2.$$

Let us apply this to find the root of an equation of the form

$$u^3 + au = b.$$

Divide by u so that

$$u^2 + a = \frac{b}{u}$$

and set $T = 1$ opposite to $X = b$. Then taking $T = u$ we find on the same cross line $t = u^2$ and $X = b/u$, so that we read the two values u^2 and b/u directly opposite to each other on the scales t and X. If b/u is positive, it decreases while u^2 increases.

Running our eye along we have to find the place where the difference $b/u - u^2$ is equal to a. Having found it the T-scale gives us the root of the equation. For example take

$$u^3 - 5u = 3,$$

or

$$u^2 - 5 = \frac{3}{u}.$$

We set $T = 1$ opposite $X = 3$ and run our eye along the scales X and t (Fig. 36), to find the place where $t - 5 = X$. We find

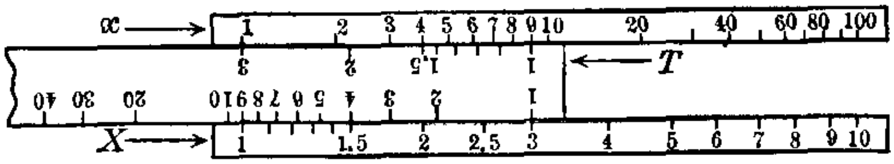


FIG. 36.

it approximately at $t = 6.2$, and on the T-scale we read off $T = 2.50$ as the approximate value of the root. This is the only positive root. But for a negative root $3/u$ is negative, and therefore the positive value of $3/u$ plus u^2 would have to be equal to 5. We run our eye along and find $t = 3.37$ opposite to $X = 1.63$, approximately corresponding to $T = 1.84$. Therefore $- 1.84$ is another root. As the coefficient of u^2 in the first form of the equations vanishes it follows that the sum of the three roots must be equal to zero. This demands a second negative root approximately equal to $- 0.66$. To make sure that it is so, we set the instrument back and take the other end of the T-scale as representing the value $T = 1$ and give it the position this end had before. Running our eye along the scales X and t, we find $t = 0.43$ opposite to $X = 4.57$, giving $X + t = 5.00$. On the T-scale we find 0.655, so that the third root is found equal to $- 0.655$.

When b is negative there is always one and only one negative root. For u running through the values $u = 0$ to $-\infty$, $u^2 - b/u$ will run from $-\infty$ to $+\infty$ without turning. When b is positive there is always one and only one positive root; for then $u^2 - b/u$

runs from $-\infty$ to $+\infty$ for $u = 0$ to $+\infty$. In the first case there may be two positive roots or none; in the second case there may be two negative roots or none. For positive values of a one root only exists in either case. This is easily seen in the first form of the equation

$$u^3 + au = b,$$

because from a positive value of a it follows that $u^3 + au$ will for $u = -\infty$ to $+\infty$, run from $-\infty$ to $+\infty$ without turning and will therefore pass any given value once only.

In order to decide whether in the case of a negative value of a there are three roots or only one let us write

$$u^2 - \frac{b}{u} = -a.$$

For negative values of b we have to investigate whether there are positive roots. For positive values of u the function $u^2 - b/u$ has a minimum, when the differential coefficient vanishes, *i. e.*, for

$$2u + \frac{b}{u^2} = 0,$$

or

$$2u^2 = -\frac{b}{u}.$$

Having set our slide rule so that t gives us u^2 and X gives us $-b/u$, we find the value u where the minimum takes place by running our eye along and looking for the values X, t opposite each other for which X is twice the value of t

$$2t = X.$$

Then $t + X$ is the minimum of $u^2 - b/u$, so that there will be two or no positive roots according to $t + X$ being smaller or larger than $-a$. For positive values of b, we have to find out whether there are negative roots. The criterion is the same. After having set $T = 1$ opposite to b and having found the positive root, we find the place where

$$2t = X.$$

Then $t + X$ is the minimum of all values that $u^2 - b/u$ assumes for negative values of u. If the minimum is smaller than $-a$ there are two negative roots; if it is larger there are none. If it is equal to $-a$ the two negative roots coincide.

For the equation

$$u^2 - 5 = \frac{3}{u},$$

for instance, we find $t = 1.31$ opposite to $X = 2.62$ (Fig. 36), so that $2t = 2.62 = X$. Now $t + X = 3.93$ is smaller than 5, therefore $u^2 - 3/u$ will assume the value 5 for two negative values of u on either side of the value $u = -T = -1.143$ for which the minimum of $u^2 - 3/u$ takes place.

On the same principle as the slide rule many other instruments may be constructed for various calculations. In all these cases we have for any position of the instrument

$$f(x) - g(t) = f(x') - g(t'),$$

where x, t are any readings of the two scales opposite each other and $x't'$ the readings at any other place. $f(x)$ and $g(t)$ may be any functions of x and t. It will only be desirable that they be limited to intervals of x and t, which contain no turning points. Else the same point of the scale corresponds to more than one value of x or t and that will prevent a rapid reading of the instrument.

Let us design an instrument for the calculation of the increase of capital at compound interest at a percentage from 2 per cent. upward. If x is the number of per cent. and t the number of years, the increase of capital at compound interest is in the proportion

$$\left(1 + \frac{x}{100}\right)^t.$$

We can evidently build an instrument for which

$$\left(1+\frac{x}{100}\right)^t=\left(1+\frac{x'}{100}\right)^{t'}.$$

For taking first the logarithm and then the logarithm of the logarithm, we obtain

$$\log t+\log\log\left(1+\frac{x}{100}\right)=\log t'+\log\log\left(1+\frac{x'}{100}\right).$$

We have only to make the x-scale

$$y=+\log\log\left(1+\frac{x}{100}\right)-\log\log\left(1+\frac{2}{100}\right),$$

and the t-scale

$$y=\log n-\log t.$$

For $x=2$ we have $y=0$ and therefore in the normal position of the instrument $t=n$. On the other end we have $t=1$ and therefore $y=\log n$. Now let us take $n=100$, so that $y=2$ for $t=1$. Say the length of the instrument is to be about 24 cm., then the unit of length for the y-scale would have to be 12 cm. In the normal position of the instrument the readings x, t opposite to each other satisfy the equation

$$\left(1+\frac{x}{100}\right)^t=\left(1+\frac{2}{100}\right)^{100}.$$

Opposite $t=1$, we read the value $x_1=624$ and this gives us

$$\left(1+\frac{2}{100}\right)^{100}=1+\frac{x_1}{100}=1+6.24=7.24.$$

A capital will increase in 100 years at two per cent. compound interest in the proportion 7.24 : 1. Or we may also say the number $x_1=624$ read off opposite $t=1$ is the amount which is added to a capital equal to 100 by double interest of 2 per cent. in 100 years. The same position of the instrument gives us the number of years that are wanted for the same increase of capital at a higher percentage. For all the values x, t opposite to each other satisfy the equation

$$\left(1 + \frac{x}{100}\right)^t = 7.24.$$

For any other given percentage x and any other given number of years t the increase of capital is found by setting x opposite to t and reading the x-scale opposite to $t = 1$. The only restriction is that the ratio is not greater than 7.24, else $t = 1$ will lie beyond the end of the x-scale.

For a given increase of capital the instrument will enable us either to find the number of years if the percentage is given, or the percentage if the number of years is given, subject only to the restriction mentioned.

We can build our instrument so as to include greater increases of capital by choosing a larger value of n. $n = 1000$, for instance, will make $y = 3$ for $t = 1$. If the instrument is not to be increased in size the scales would have to be reduced in the proportion 2 : 3.

Let us consider another instance

$$y = \frac{1}{x}, \quad y = \frac{1}{n} - \frac{1}{t}.$$

In the normal position of the instrument the scale division marked $x = \infty$ corresponds to $y = 0$ and is opposite to $t = n$. If we have $t = \infty$ on the other end, the length of the instrument will correspond to $y = 1/n$. Let us choose $n = 0.1$, so that the length of the instrument is $y = 10$. That is to say, the unit of length of the y-scale is one tenth of the length of the instrument. For any position of the instrument we have

$$\frac{1}{x} + \frac{1}{t} = \frac{1}{x'} + \frac{1}{t'}.$$

If the scale division marked $x = \infty$ is opposite to $t = c$ we can write $x' = \infty$, $t' = c$ and have

$$\frac{1}{x}+\frac{1}{t}=\frac{1}{c}.$$

The instrument will therefore enable us to read off any one of the three quantities x, t, c, if the other two are given, the only restriction being that all three lie within the limits 0.1 to ∞. The instrument may be used to determine the combined resistance of two parallel electrical resistances, for the resistances satisfy the equation

$$\frac{1}{R}=\frac{1}{R_1}+\frac{1}{R_2}.$$

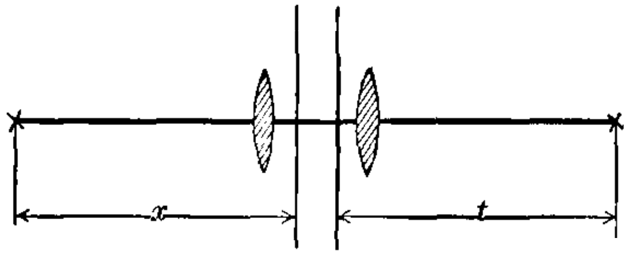


FIG. 37.

Similarly it may be used to calculate the distances of an object and its image from the principal planes of any given system of lenses. For if f is the focal length and x and t the distances of the object and its image from the corresponding principal planes (Fig. 37), the equation is

$$\frac{1}{x}+\frac{1}{t}=\frac{1}{f}.$$

On the back side of the movable part of an ordinary slide rule there generally is a scale

$$y=2+\log\sin t.$$

When this part is turned round and the scale is brought into contact with the scale

$$y=\log x,$$

we obtain for any position of the instrument

$$\log x-\log\sin t=\log x'-\log\sin t',$$

or

$$\frac{x}{\sin t}=\frac{x'}{\sin t'},$$

for any two pairs of values x, t that are opposite each other.

Given two sides of a triangle and the angle opposite the larger of the two the instrument gives at once the angle opposite the other side. Similarly when two angles and one side are given, it gives the length of the other side.

If $x' = a$ is the value opposite to $t' = 90°$, we have

$$x = a \sin t.$$

Thus we can read the position of any harmonic motion for any value of the phase.

An instrument carrying the scales

$$y = \log \sin x \quad \text{and} \quad y = \log \sin t$$

enables us to find any one of four angles x, t, x', t' for which

$$\frac{\sin x}{\sin t} = \frac{\sin x'}{\sin t'}$$

if the other three are given. Thus, knowing the declination, hour angle and height of a celestial body, we can read the azimuth on the instrument. We have only to take $x = 90° -$ height, $t =$ hour angle, $x' = 90° -$ declination, then $t' =$ azimuth or $180° -$ azimuth.

It is not necessary to carry out the subtraction $90° -$ height and $90° -$ declination. The difference may be counted on the scale by imagining 0° written in the place of 90°, 10° in the place of 80° and so on and counting the partitions of the scale backwards instead of forward.

§ 8. *Rectangular Coördinates with Intervals of Varying Size.*— The two methods of representing the relation between two variables either by a curve connecting the coördinates or by scales facing each other lead to a combination of both.

Suppose the rectangular coördinates x and y are functions of u and v,

$$x = \varphi(u) \quad \text{and} \quad y = \psi(v).$$

The function $x = \varphi(u)$ is represented by a uniform scale for x on the axis of abscissæ facing a non-uniform scale for u. The function $y = \psi(v)$ is represented by a uniform scale for y on the axis of ordinates facing a non-uniform scale for v. Through the scale-divisions u let us draw vertical lines, and through the scale-divisions v let us draw horizontal lines. These two systems of parallel lines form a network of rectangular meshes of various sizes (Fig. 38), and any equation between u and v may be represented by a curve in this plane.

The usefulness of this method will be seen by some examples. It enables us by a clever choice of the functions $\varphi(u)$ and $\psi(v)$

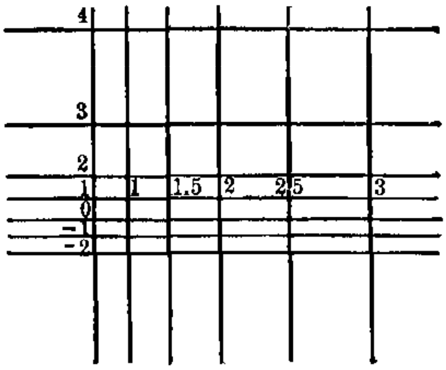


FIG. 38.

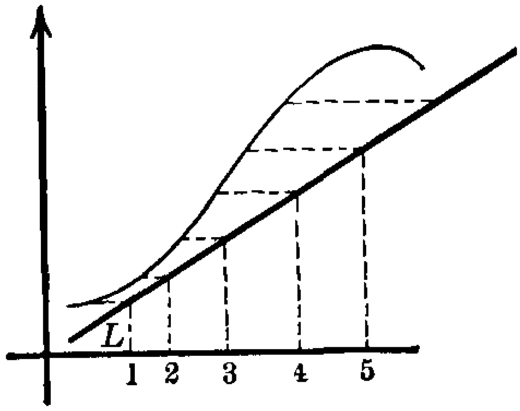


FIG. 39.

to simplify the form of the curve. It is easily seen, for instance, that a curve representing an equation $f(u, v) = 0$ may always be replaced by a straight line, if we choose the u-scale properly. For when the points $u = 1, 2, 3, 4, \cdots$ of the curve are not on a straight line, let them be moved to a straight line without altering their ordinates (Fig. 39). This will change the u-scale but it will not alter the equation $f(u, v) = 0$ now represented by the straight line.

Suppose we want to represent the relation

$$\frac{u^2}{a^2} + \frac{v^2}{b^2} = 1,$$

where a and b are given numbers. If u and v were ordinary rectangular coördinates the curve would be an ellipse. But if we make

$$x = u^2 \quad \text{and} \quad y = v^2$$

the equation of the line in rectangular coördinates becomes

$$\frac{x}{a^2} + \frac{y}{b^2} = 1,$$

and the curve will therefore be a straight line running from a point on the positive axis of x to a point on the positive axis of y. The point on the axis of x corresponds to the value $u = \pm a$ on the u-scale, and the point on the axis of y corresponds to the value $v = \pm b$ on the v-scale (Fig. 40).

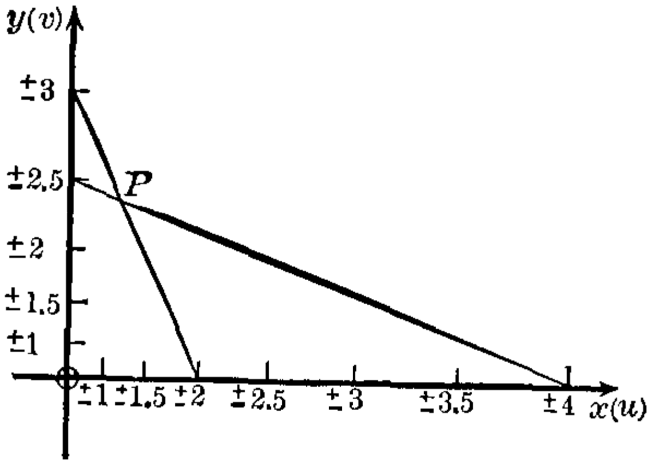


FIG. 40.

Any point on the straight line corresponds to four combinations $+u, +v; -u, +v; u, -v; -u, -v$, because x has the same values for opposite values of u and y for opposite values of v. We can read v as a function of u or u as a function of v.

If a second equation

$$\frac{u^2}{a_1^2} + \frac{v^2}{b_1^2} = 1$$

is given, we find the common solutions of the two equations by the intersection of the corresponding straight lines. Fig. 40 shows the solutions of the two equations

$$\frac{u^2}{2^2} + \frac{v^2}{3^2} = 1$$

and

$$\frac{u^2}{4^2} + \frac{2^2 v^2}{5^2} = 1,$$

approximately equal to $u = \pm 1.2$ and $v = \pm 2.4$.

Another function much used in mathematical physics

$$v = ae^{-\frac{u^2}{m^2}}$$

may also be represented by a straight line by means of the same device.

By making

$$y = \log v, \quad x = u^2,$$

we obtain

$$y = \log a - \frac{x}{m^2},$$

where $\log v$ and $\log a$ are the natural logarithms of v and a. The u-scale is laid off on the axis of x and the v-scale on the axis of y and we have to join the points $u = 0$, $v = a$ and $u = m$, $v = a/e$. The point $v = a/e$ is found by laying off the distance $v = 1$ to $v = e$ from $v = a$ downward (Fig. 41). We are not obliged to take the same units of length for x and y.

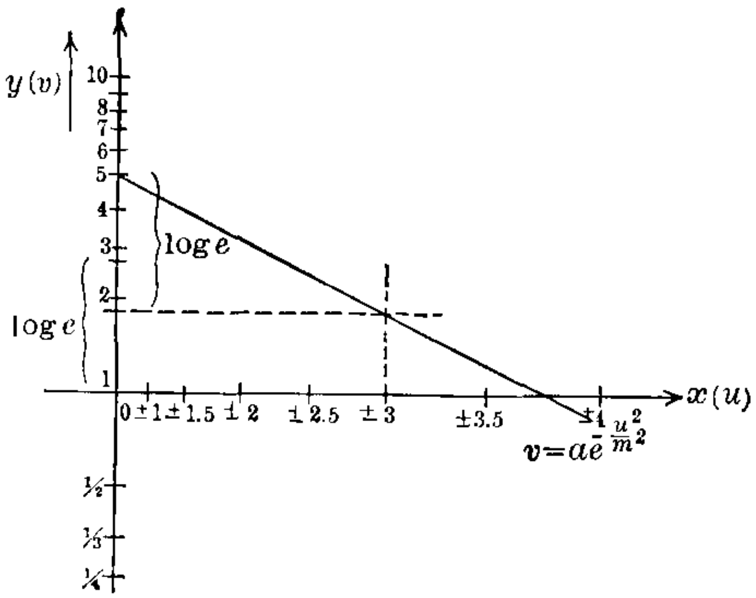


FIG. 41.

Suppose we had to find the constants a and m from two equations

$$v_1 = ae^{-\frac{u_1^2}{m^2}}$$

and

$$v_2 = ae^{-\frac{u_2^2}{m^2}}.$$

Our diagram would furnish two points corresponding to u_1, v_1 and u_2, v_2. The straight line joining these two points intersects the axis of ordinates at $v = a$ and intersects the parallel through $v = a/e$ to the axis of abscissæ at $u = m$.

In applied mathematics the problem would as a rule present itself in such a form that more than two pairs of values u, v would be given but all of them affected with errors of observation. The way to proceed would then be to plot the corresponding points and to draw a straight line through the points as best we can. A black thread stretched over the drawing may be used to advantage to find a straight line passing as close to the points as possible (Fig. 42).

In several other cases the variables u and v are connected with the rectangular coördinates x and y by the functions

$$x = \log u \quad \text{and} \quad y = \log v.$$

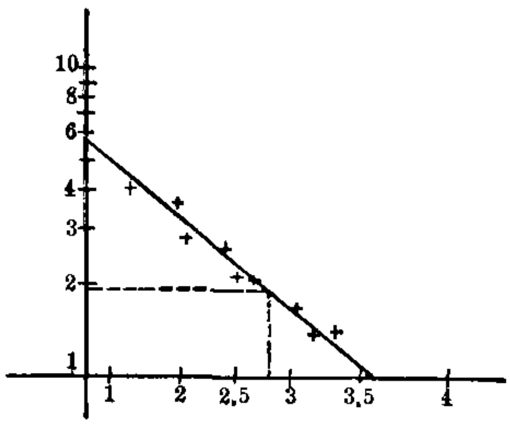


FIG. 42.

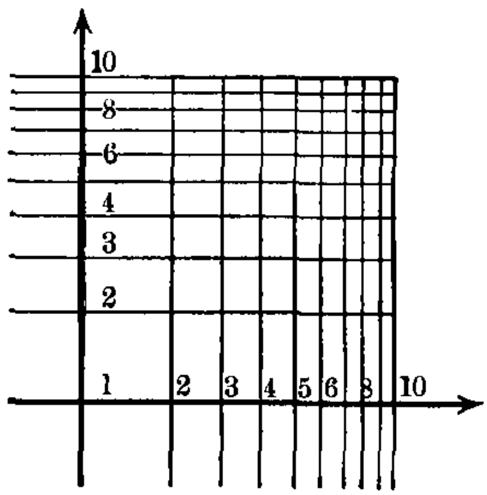


FIG. 43.

"Logarithmic paper" prepared with parallel lines for equidistant values of u and lines perpendicular to these for equidistant values of v is manufactured commercially (Fig. 43).

By this device diagrams representing the relation

$$u^r v^s = c,$$

where r, s, c are constants are given by straight lines. For by taking the logarithm we obtain

$$rx + sy = \log c.$$

The straight line connects the point $u = c^{1/r}$ on the u-scale with the point $v = c^{1/s}$ on the v-scale.

Logarithmic paper is further used to advantage in all those cases where a variety of relations between the variables u and v are considered that differ only in u and v being changed in some constant proportion. If u and v were plotted as rectangular coördinates the curves representing the different relations between u and v might all be generated from one of them by altering the scale of the abscissæ and independently the scale of the ordinates, so that the appearance of all these curves would be very different. Let us write

$$f(u, v) = 0,$$

as the equation of one of the curves. The equations of all the rest may then be written

$$f\left(\frac{u}{a}, \frac{v}{b}\right) = 0,$$

where a, b are any positive constants. The points u, v of the first curve lead to the points on one of the other curves by taking u a times as great and v b times as great. For if we write $u' = au$ and $v' = bu$ the equation $f(u, v) = 0$ leads to the equation between u' and v':

$$f\left(\frac{u'}{a}, \frac{v'}{b}\right) = 0.$$

Using logarithmic paper the diagram of all these curves becomes very much simpler. The equation $f(u, v) = 0$ is equivalent to a certain equation $\varphi(x, y) = 0$, where $x = \log u$, $y = \log v$. Now let x', y' be the rectangular coördinates corresponding to u', v' so that

$$x' = \log u' = \log u + \log a = x + \log a,$$

$$y' = \log v' = \log v + \log b = y + \log b.$$

The point x', y' is reached from the point x, y by advancing through a fixed distance $\log a$ in the direction of the axis of x and a fixed distance $\log b$ in the direction of the axis of y. The whole curve

$$f(u, v) = 0$$

drawn on logarithmic paper is therefore identical with all the curves

$$f\left(\frac{u}{a}, \frac{v}{b}\right) = 0.$$

It can be made to coincide with any one of the curves by moving it along the directions of x and y.

§ 9. *Functions of Two Independent Variables.*—When a function of one variable $y = f(x)$ is represented by a curve, the values of x are laid off on the axis of x and the values of y are represented by lines perpendicular to the axis of x. In a similar way a function of two independent variables

$$z = f(x, y)$$

may be represented by plotting x and y as rectangular coördinates and erecting lines perpendicular to the xy plane, in all the points x, y, where $f(x, y)$ is defined and making the lengths of the perpendiculars proportional to z. In this way the function corresponds to a surface in space. Now there are practical difficulties in working with surfaces in space and therefore it appears desirable to use other methods, that enable us to represent functions of two independent variables on a plane. This may be done in the following way.

Taking x, y as rectangular coördinates all the points for which $f(x, y)$ has the same value form a curve in the xy plane. Let us suppose a number of these curves drawn and marked with the value of $f(x, y)$. If the different values of $f(x, y)$ are chosen sufficiently close, so that the curves lie sufficiently close in the part of the xy plane that our drawing comprises, we are not only able to state the value of $f(x, y)$ at any point on one of the drawn curves, but we are also able to interpolate with a certain degree of accuracy the value of $f(x, y)$ at a point between two of the curves. As a rule it will be convenient to choose equidistant values of $f(x, y)$ to facilitate the interpolation of the values between. The curves may be regarded as the perpendicular projection of certain curves on the surface in space, the intersections of the surface by equidistant planes parallel to the xy plane.

The method is the generalization of the scale-representation of a function of one variable. For a relation between t and x represented by a curve with t as ordinate and x as abscissa, is transformed into a scale representation by perpendicularly projecting certain points of the curve onto the axis of x, the intersections of the curve by equidistant lines parallel to the axis of x and marking them with the value of t. A scale division in the case of a function of one variable corresponds to a curve in the case of a function of two independent variables.

This method of representing a function of two independent variables by a plane drawing or we might also say of representing a surface in space by a plane drawing, is used by naval architects to render the form of a ship and by surveyors to render the form of the earth's surface and by engineers generally. Let us apply the method to a problem of pure mathematics.

The equation

$$z^3 + pz + q = 0$$

defines z as a function of p and q. Let us represent this function by taking p and q as rectangular coördinates and drawing the lines for equidistant values of z.

For any constant value of z we have a linear equation between the variables p and q, and therefore it is represented by a straight line. This line intersects the parallels $p = 1$ and $p = -1$ at the points $q = -z^3 - z$ and $q = -z^3 + z$. Let us calculate these values for $z = 0$; ± 0.1; $\pm 0.2 \cdots \pm 1.3$ and in this way draw the lines corresponding to these values of z as far as they lie in a square comprising the values $p = -1$ to $+1$ and $q = -1$ to $+1$. Fig. 44 shows the result. On this diagram we can at once read the roots of any equation of the third degree of the form

$$z^3 + pz + q = 0,$$

where p and q lie within the limits -1 to $+1$. For $p = 0.4$ and

$q = -0.2$, for instance, we read $z = 0.37$, interpolating the value of z according to the position of the point between the lines $z = 0.3$ and $z = 0.4$. We also see that there is only one real root, for there is only one straight line passing through the point.

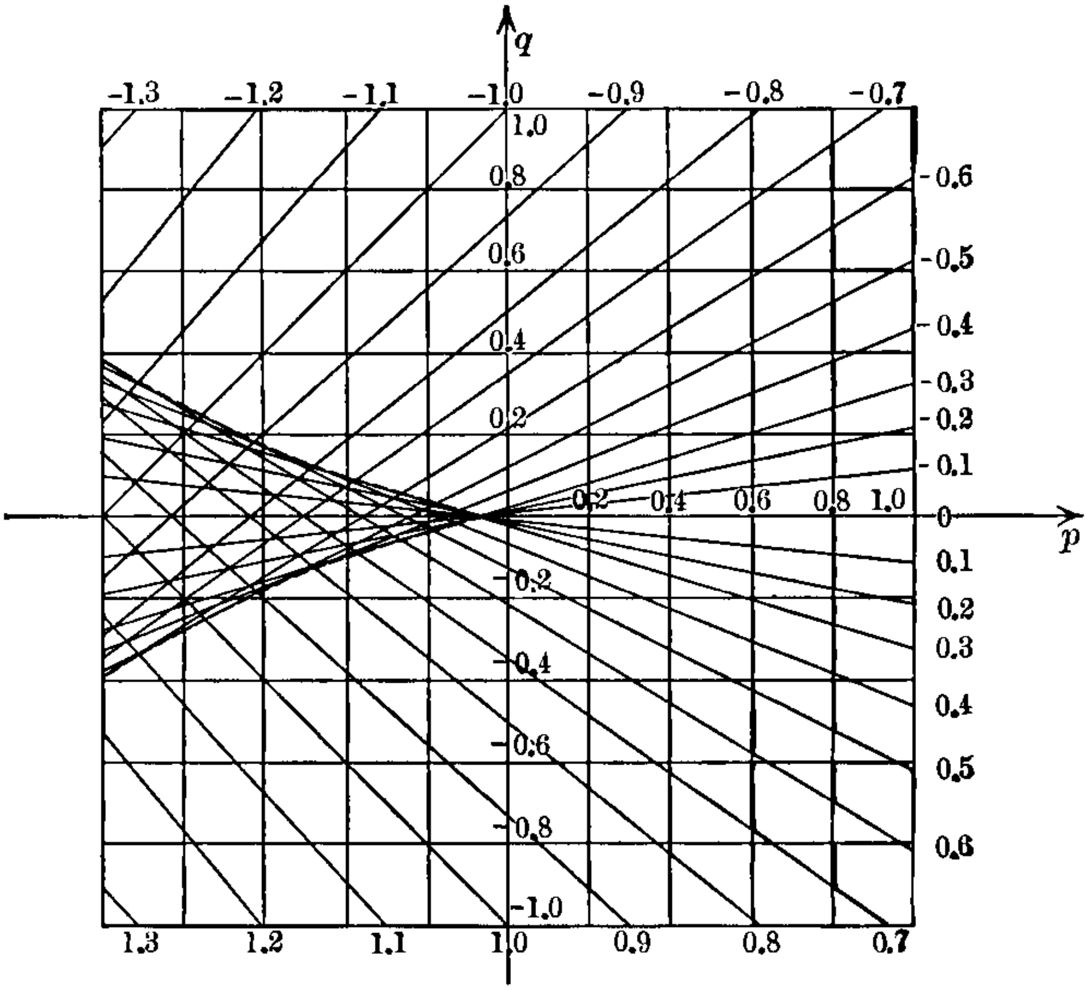


FIG. 44.

On the left side of the square there is a triangular-shaped region where the straight lines cross each other. To each point within this region corresponds an equation with three real roots. For example, at the point $p = -0.8$ and $q = +0.2$ we read $z = -1.00$; $+0.28$; $+0.72$. On the border of this region two roots coincide.

For values of p and q beyond the limits -1 to $+1$ the diagram may also be used. We only have to introduce $z' = z/m$ instead of z and to choose m sufficiently large.

Instead of

$$z^3 + pz + q = 0$$

we obtain

$$m^3z'^3 + pmz' + q = 0,$$

or dividing by m^3,

$$z'^3 + \frac{p}{m^2}z' + \frac{q}{m^3} = 0,$$

or

$$z'^3 + p'z' + q' = 0,$$

where

$$p' = \frac{p}{m^2}, \quad q' = \frac{q}{m^3}.$$

By choosing a sufficiently large value of m, p' and q' can be made to lie within the limits -1 to $+1$ so that the roots z' may be read on the diagram. Multiplying them by m we obtain the roots z of the given equation.

A function of two independent variables need not be expressed in an explicit form, but may be given in the form of an equation between three variables

$$g(u, v, w) = 0,$$

and we may consider any two of them as independent and the third as a function of the two. The graphical representation may sometimes be greatly facilitated by modifying the method described before. The curves for constant values of one of the three variables, say w, are not plotted by taking u and v as rectangular coördinates, but they are plotted after introducing new variables x and y, x a function of u and y a function of v and making x and y the rectangular coördinates.

In some cases, for instance, we can succeed by a right choice of the functions $x = \varphi(u)$ and $y = \psi(v)$ in getting straight lines for the curves $w =$ const. This will evidently be the case, when the equation $g(u, v, w) = 0$ can be brought into the form

$$a(w)\varphi(u) + b(w)\psi(v) + c(w) = 0,$$

a, b, c being any functions of w, φ any function of u and ψ any function of v.

For introducing

$$x = \varphi(u), \quad y = \psi(v)$$

the equation will become

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

where a, b, c are constants for any constant value of w.

As an example let us consider the relation between the true solar time, the height of the sun over the horizon, and the declination of the sun for a place of given latitude. Instead of the declination of the sun we might also substitute the time of the year, as the time of the year is determined by the declination of the sun. Our object then is to make a diagram for a place of given latitude from which for any time of the year and any height of the sun the true solar time may be read.

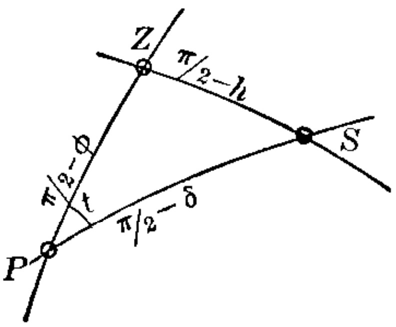


FIG. 45.

In the spherical triangle formed by the zenith Z, the north pole P (if we suppose the place to be on the northern hemisphere) and the sun S (Fig. 45), the sides are the complements of the declination δ, the height h, and the latitude φ. The angle t at the pole is the hour angle of the sun, which expressed in time gives true solar time.

The equation between these four quantities may be written in the form

$$\sin h = \sin \varphi \sin \delta + \cos \varphi \cos \delta \cos t.$$

The latitude φ is to be kept constant, so that t, h, δ are the only variables.

Now let us write

$$x = \cos t, \quad y = \sin h,$$

so that the equation takes the form

$$y = \sin \varphi \sin \delta + x \cos \varphi \cos \delta.$$

When x and y are plotted as rectangular coördinates, we obtain a straight line for any value of δ. Let us draw horizontal lines for equidistant values of $h = 0$ to $90°$ and vertical lines for equidistant values of $t = -180°$ to $+180°$ or expressed in time from midnight to midnight (Fig. 46). In order to draw the

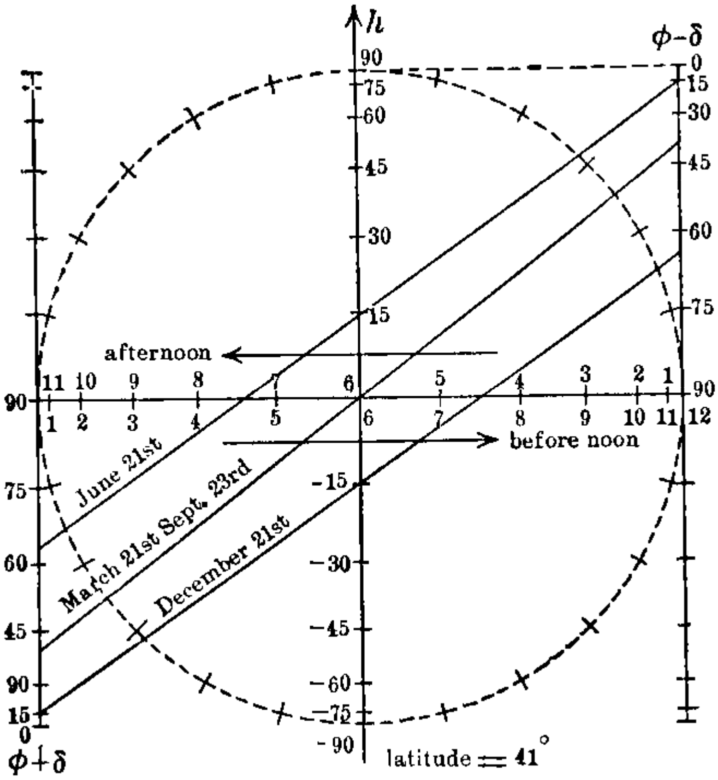


FIG. 46.

straight lines $\delta =$ const., let us calculate where they intersect the vertical lines corresponding to $x = -1$ and $x = +1$ or expressed in time corresponding to midnight and to noon. For $x = -1$ we have $y = -\cos(\varphi + \delta)$, and for $x = +1$ we have $y = \cos(\varphi - \delta)$. Let us draw a scale on the vertical $x = -1$ showing the points $y = -\cos(\varphi + \delta)$ for equidistant values of $(\varphi + \delta)$ and a scale on the vertical $x = +1$, showing the points $y = \cos(\varphi - \delta)$ for equidistant values of $\varphi - \delta$. The scale is the same as the scale for h, with the sole difference that the values of $\varphi - \delta$ are the complements of h and the values of $\varphi + \delta$ the complements of $-h$. For a latitude of 41°, for instance, we have

For	δ	$\varphi + \delta$	$\varphi - \delta$
June 21.	23.5°	64.5°	17.5°
September 23 and March 21.	0	41°	41°
December 21.	−23.5°	17.5°	64.5°

The values of $\varphi + \delta$ and $\varphi - \delta$ furnish the intersections with the verticals $x = -1$ and $x = +1$, so that the straight lines can be drawn corresponding to these days of the year. The two outward lines are parallel but the middle line is steeper. Their intersections with the horizontal line $h = 0$ show the time of sunrise and sunset.[1] Strictly speaking the straight lines do not correspond to certain days. The straight line determined by any value of δ changes its position continually as δ changes continually. But the changes of δ during one day are scarcely appreciable unless the drawing is on a larger scale.

If in the equation

$$ax + by + c = 0$$

a and b are independent of w, only c being a function of w, all the straight lines $w =$ const. are parallel. In this case we are not obliged to draw the straight lines $w =$ const. It will suffice to draw a line perpendicular to the lines $w =$ const. and a scale on it that marks the points corresponding to equidistant values of w. On the drawing we place a sheet of transparent paper or celluloid, on which three straight lines are drawn issuing from one point in the direction perpendicular to the u-scale, v-scale and w-scale (Fig. 47). If we move the transparent material without turning it and make the first two lines intersect the u-and-v scale at given points, the w-scale will be intersected at the point corresponding to the value of w. This method has the advantage

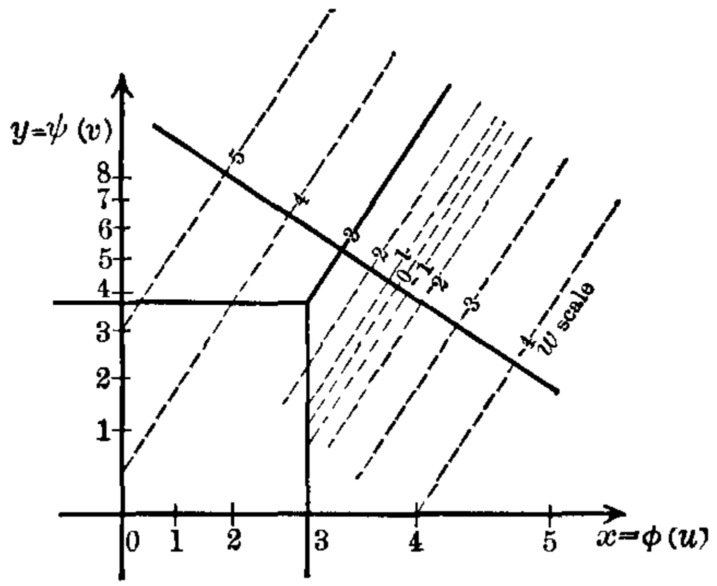


FIG. 47.

[1] That is to say, the moment when the center of the sun would be seen on the horizon, if there were no atmospherical refraction. To take account of the refraction, the line $h = -0.6°$ would have to be considered instead of $h = 0$.

that we can use the same paper for a great many relations of three variables, as we can place a great many scales side by side. Or, in the case of one relation only, we may divide the region of the values u, v, w into a number of smaller regions and draw three scales for each of them, placing all the u-scales or v-scales or w-scales side by side. The drawing will then have the same accuracy as a drawing of very much larger size in which there is only one scale for each of the three variables.

§ 10. *Depiction of One Plane on Another Plane.*—Let us now consider two quantities x and y each as a function of two other quantities u and v

$$x = \varphi(u, v),$$

$$y = \psi(u, v).$$

In order to give a geometrical meaning to this relation between two pairs of quantities let us consider x and y as rectangular coördinates of a point in a plane and u, v as rectangular coördinates of a point in another plane. We then have a correspondence between the two points. When the functions $\varphi(u, v)$ and $\psi(u, v)$ are defined for the values u, v of a certain region, they will furnish for every point u, v of this region a point in the xy plane. Let us call this a depiction of the uv plane on the xy plane. Similarly a function of one variable $x = \varphi(u)$ might be said to depict the u line on the x line. We may therefore say that the depiction of one plane on another plane is, in a certain way, the generalization of the idea of a function of one variable. Let us suppose $\varphi(u, v)$ and $\psi(u, v)$ both to have only one value for given values of u and v for which they are defined. Then there will be only one point in the xy plane corresponding to a given point in the uv plane. But to a given point in the xy plane there may very well correspond several points in the uv plane.

Let us try to explain this by a graphical representation of the depiction of planes on each other. For this purpose we draw the curves $x =$ const. and $y =$ const. in the uv plane for equidistant values of x and y. In the xy plane they correspond to equidistant lines parallel to the axis of x and to the axis of y. The point of intersection of two lines $x = a$ and $y = b$ corresponds to the points of intersection of the curves

$$\varphi(u, v) = a \quad \text{and} \quad \psi(u, v) = b,$$

in the uv plane. If in a certain region of the uv plane, that we consider, they intersect only once there is only one point in the region of the uv plane considered and one point in the xy plane corresponding to each other. Fig. 48 shows the depiction of part of the uv plane on part of the xy plane. We have a net of square-shaped meshes in the xy plane and corresponding is a net of curvilinear meshes in the uv plane.

Let us consider the curves $x =$ const. in the uv plane as the perpendicular projections of curves of equal height on a surface extended over that part of the uv plane. From any point P of the surface corresponding to the values u, v we proceed an

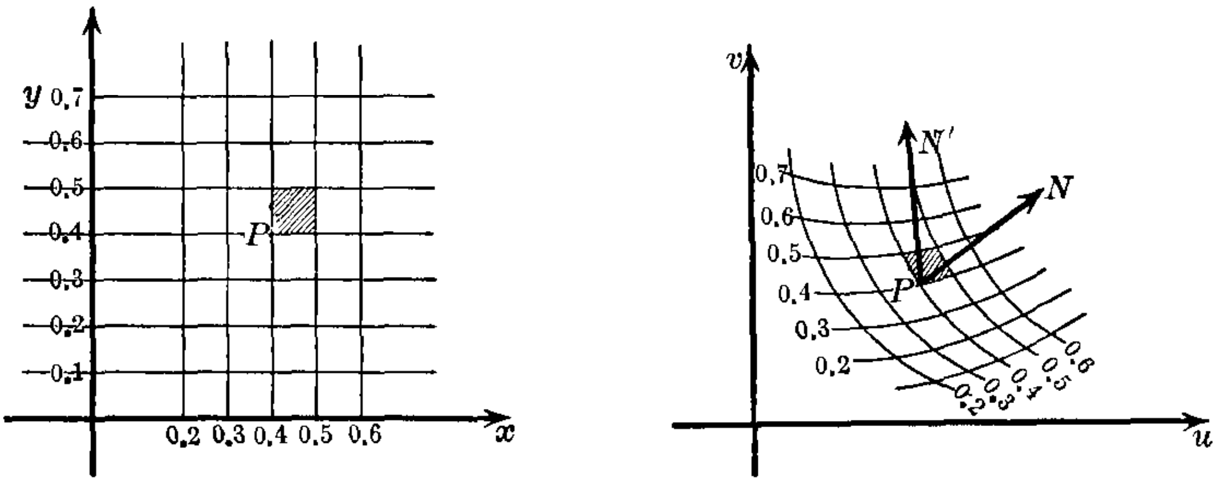


FIG. 48.

infinitely small distance, u changing to $u + du$, v to $v + dv$ and x to $x + dx$, where

$$dx = \frac{\partial \varphi}{\partial u} du + \frac{\partial \varphi}{\partial v} dv.$$

Let us write

$$du = \cos \alpha ds, \quad dv = \sin \alpha ds,$$

where ds signifies the length of the infinitely small line from u, v to $u + du, v + dv$ in the uv plane and α the angle its direction forms with the positive axis of x. Let PN be a straight line whose projections on the u and v axis are equal to $\partial\varphi/\partial u$ and $\partial\varphi/\partial v$ and let us write

$$\frac{\partial\varphi}{\partial u} = r\cos\lambda, \quad \frac{\partial\varphi}{\partial v} = r\sin\lambda,$$

r being the positive length of PN and λ the angle between its direction and the positive axis of x. Then we have

$$dx = \frac{\partial\varphi}{\partial u}du + \frac{\partial\varphi}{\partial v}dv = rds\cos(\alpha - \lambda),$$

or

$$\frac{dx}{ds} = r\cos(\alpha - \lambda).$$

dx/ds measures the steepness of the ascent. It is positive when the direction leads upward and negative when it leads downward and its value is equal to the tangent of the angle of the ascent. From the equation

$$\frac{dx}{ds} = r\cos(\alpha - \lambda)$$

we see that the ascent is steepest for $\alpha = \lambda$, where $dx/ds = r$. The line PN in the u, v-plane shows the perpendicular projection of the line of steepest ascent on the surface $x = \varphi(u, v)$ and the length of PN measured in the same unit of length in which u and v are measured is equal to the tangent of the angle of the ascent. Let us call the line PN the gradient of the function $\varphi(u, v)$ at the point u, v. The direction of the gradient is perpendicular to the curve $\varphi(u, v) =$ const. that passes through the point u, v; for in the direction of the curve we have

$$\frac{dx}{ds} = 0,$$

and therefore

$$\alpha - \lambda = \pm 90°.$$

If PN' is the gradient of the function $\psi(u, v)$ at the point u, v, the angle between PN and PN' must be equal to the angle formed by the curves $x =$ const. and $y =$ const. that intersect at the point u, v, or equal to its supplement according to the angle of intersection that we consider.

Suppose the gradients PN and PN' do not vanish in any of the points in the region of the uv plane that we consider and that their length and direction vary as continuous functions of u and v. Let us further suppose that the gradient PN' (components: $\partial\psi/\partial u$, $\partial\psi/\partial v$) is for the whole region on the left side of the gradient PN (components: $\partial\varphi/\partial u$, $\partial\varphi/\partial v$), or else for the whole region on the right side of the gradient PN, then it follows that any one of the curves $x =$ const. and any one of the curves $y =$ const. can only intersect once in the region considered.

This may be shown by considering the directions of the curves $x =$ const. and $y =$ const. in the uv plane. Let us consider *that* direction on the curve $y =$ const. in which x increases. If this direction deviates from PN the deviation must be less than 90°, because dx/ds and therefore $\cos(\alpha - \lambda)$ is positive. Let us further consider that direction on the curve $x =$ const. in which y increases. If it deviates from the direction of PN' the deviation must be less than 90°. Let us call these directions the direction of x (on the curve $y =$ const.) and the direction of y (on the curve $x =$ const.). Now if the gradient PN' is on the left of the gradient PN the y direction must also be on the left of PN (for if it were on the right of PN being perpendicular to PN it would form an obtuse angle with PN') and therefore it must be on the left of the x direction (for if it were on the right, PN' being perpendicular to the x direction would form an obtuse angle with the y direction, which we have seen to be impossible). Similarly it may be seen, that if PN' is on the right of PN, the direction of y will also be on the right of the direction of x. If therefore PN' is on the same side of PN in the whole region considered, the direction of y will also be on the same side of the direction of x for the whole region considered. This excludes the intersection of two curves $x =$ const. and $y =$ const. in more than one point. For, suppose there are two points of intersection and we pass along the curve $y =$ const. in the direction of x. At the first point of intersection we pass over the curve $x =$ const. from the side of smaller values of x to the side of larger values of x. Now if the values of x go on increasing as we go along the curve $y =$ const. we evidently cannot get back to a curve $x =$ const. corresponding to a smaller value of x. The only possibility of a second point of intersection would be that the direction in which the value of x increases on the curve $y =$ const. becomes the opposite, so that in advancing in the same direction in which we came x would decrease again.

The same holds for the curve $x =$ const. If we pass from one point of intersection with a curve $y =$ const. along a curve $x =$ const. to a second point of intersection with the same curve the only possibility is that the direction of y also becomes opposite. This is excluded as in contradiction with the direction of y being on the same side of the direction of x throughout the whole region (Fig. 49)

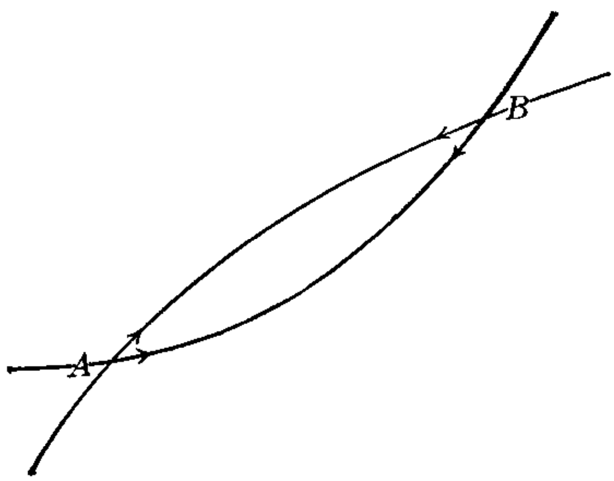


FIG. 49.

It will be useful to look at it from another point of view. Let us consider a point A in the uv plane corresponding to the values u, v and let us increase u and v by infinitely small positive amounts du and dv, so that we get four points $ABCD$, forming a rectangle corresponding to the coördinates.

$$A : u, v;\ B : u + du, v;\ C : u, v + dv;\ D : u + du, v + dv.$$

In the xy plane these points are depicted in the points A, B, C, D, the intersections of two curves u and $u + du$ with two curves v and $v + dv$ (Fig. 50).

The projections of the line AB in the xy plane on the axes of coördinates are obtained by calculating the changes of x and y for a constant value of v and a change du in the value of u

$$dx_1 = \frac{\partial\varphi}{\partial u}du, \quad dy_1 = \frac{\partial\psi}{\partial u}du.$$

Similarly the projections of AC are obtained by calculating the changes of x and y for a constant value of u and a change dv in the value of v

$$dx_2 = \frac{\partial\varphi}{dv}dv, \quad dy_2 = \frac{\partial\psi}{\partial v}dv.$$

Denoting the lengths of AB and AC by ds_1 and ds_2 and the angles that the directions of AB and AC form with the direction of the

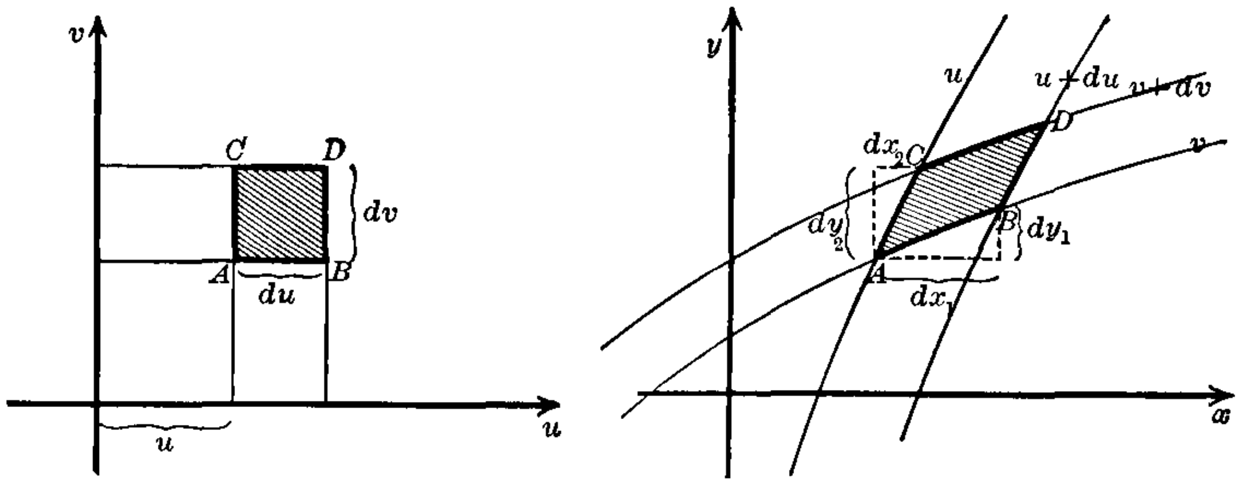


FIG. 50.

positive axis of x (the angles counted in the usual way) by γ_1 and γ_2 we have:

$$dx_1 = ds_1 \cos\gamma_1, \quad dy_1 = ds_1 \sin\gamma_1$$

and

$$dx_2 = ds_2 \cos\gamma_2, \quad dy_2 = ds_2 \sin\gamma_2,$$

or

$$\frac{\partial\varphi}{\partial u} = \cos\gamma_1 \frac{ds_1}{du}, \quad \frac{\partial\psi}{\partial u} = \sin\gamma_1 \frac{ds_1}{du}$$

and

$$\frac{\partial\varphi}{\partial v} = \cos\gamma_2 \frac{ds_2}{dv}, \quad \frac{\partial\psi}{\partial v} = \sin\gamma_2 \frac{ds_2}{dv}.$$

We may call

$$\frac{ds_1}{du} = \sqrt{\left(\frac{\partial\varphi}{\partial u}\right)^2 + \left(\frac{\partial\psi}{\partial u}\right)^2}$$

the scale of depiction at A in the direction AB and

$$\frac{ds_2}{dv} = \sqrt{\left(\frac{\partial \varphi}{\partial v}\right)^2 + \left(\frac{\partial \psi}{\partial v}\right)^2}$$

the scale of depiction at A in the direction AC. It is here understood that the uv plane is the original, which is depicted on the xy plane. If we take it the other way the scales of depiction in the directions AB and AC are the reciprocal values du/ds_1 and dv/ds_2.

The area of the parallelogram $ABCD$ in the xy plane is

$$ds_1 ds_2 \sin(\gamma_2 - \gamma_1) = \left(\frac{\partial \varphi}{\partial u}\frac{\partial \psi}{\partial v} - \frac{\partial \varphi}{\partial v}\frac{\partial \psi}{\partial u}\right) du dv.$$

According to the way in which the angles γ_2 and γ_1 are defined $\sin(\gamma_2 - \gamma_1)$ is positive, when the direction AC points to the left of the direction AB (assuming the positive axis of y to the left of the positive axis of x), and $\sin(\gamma_2 - \gamma_1)$ is negative, when AC points to the right. Now $dudv$ is equal to the area of the rectangle $ABCD$ in the uv plane. Therefore the value of

$$\frac{\partial \varphi}{\partial u}\frac{\partial \psi}{\partial v} - \frac{\partial \varphi}{\partial v}\frac{\partial \psi}{\partial u}$$

is the ratio of the areas $ABCD$ in the two planes and its positive or negative sign denotes the relative position of the directions AB and AC in the xy plane. We may call this ratio the scale of depiction of areas at the point A.

$$\frac{\partial \varphi}{\partial u}\frac{\partial \psi}{\partial v} - \frac{\partial \varphi}{\partial v}\frac{\partial \psi}{\partial u}$$

is called the functional determinant of the functions $\varphi(u, v)$ and $\psi(u, v)$.

We have found the scale of depiction of lengths in the directions AB and AC. Let us now try to find it in any direction whatever. From any point A in the uv plane, whose coördinates are u and v, we pass to a point D close by whose coördinates are $u + \Delta u$, $v + \Delta v$. In the xy plane we find the corresponding points A and D with coördinates (Fig. 51).

$$A: \begin{array}{l} x = \varphi(u, v) \\ y = \psi(u, v) \end{array} \quad D: \begin{array}{l} x + \Delta x = \varphi(u + \Delta u, v + \Delta v) \\ y + \Delta y = \psi(u + \Delta u, v + \Delta v) \end{array}$$

We expand according to Taylor's theorem, and writing for shortness

$$\varphi_u = \frac{\partial \varphi}{\partial u}, \quad \varphi_v = \frac{\partial \varphi}{\partial v}, \quad \psi_u = \frac{\partial \psi}{\partial u}, \quad \psi_v = \frac{\partial \psi}{\partial v}$$

we find

$$\Delta x = \varphi_u \Delta u + \varphi_v \Delta v + \text{terms of higher order,}$$

$$\Delta y = \psi_u \Delta u + \psi_v \Delta v + \text{terms of higher order.}$$

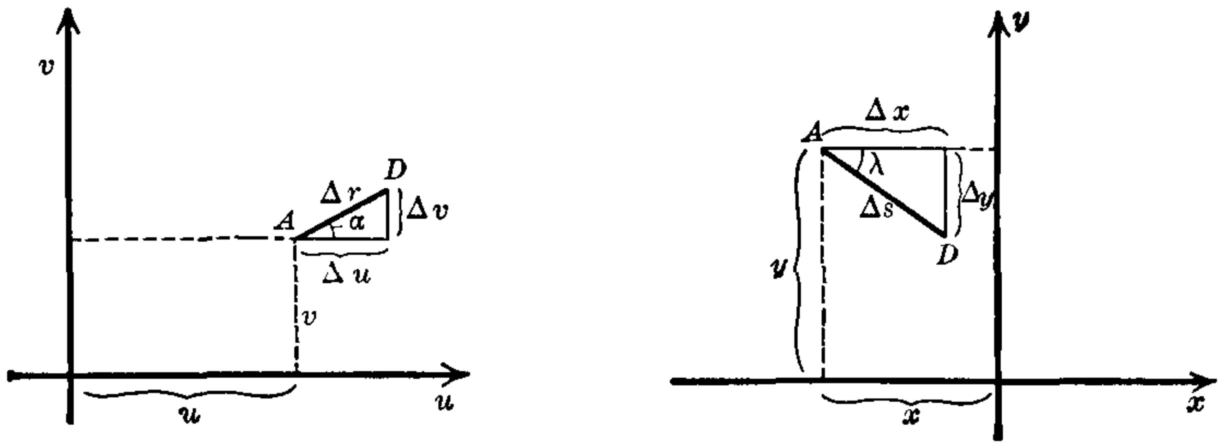


FIG. 51.

The length of AD and the angle of its direction we denote by Δr and α in the uv plane and by Δs and λ in the xy plane. The limit of the ratio $\Delta s/\Delta r$, to which it tends, when D approaches A without changing the direction AD is the scale of depiction at the point A in the direction AD.

Writing

$$\Delta u = \Delta r \cos \alpha,$$
$$\Delta v = \Delta r \sin \alpha,$$

we obtain

$$\Delta x = (\varphi_u \cos \alpha + \varphi_v \sin \alpha)\Delta r + \text{terms of higher order,}$$

$$\Delta y = (\psi_u \cos \alpha + \psi_v \sin \alpha)\Delta r + \text{terms of higher order.}$$

Dividing by Δr and letting Δr decrease indefinitely, we have in the limit

$$\frac{dx}{dr} = \varphi_u \cos \alpha + \varphi_v \sin \alpha,$$

$$\frac{dy}{dr} = \psi_u \cos \alpha + \psi_v \sin \alpha.$$

For dx/dr and dy/dr we may also write $ds/dr \cos \lambda$, $ds/dr \sin \lambda$.

$$\frac{ds}{dr} \cos \lambda = \varphi_u \cos \alpha + \varphi_v \sin \alpha,$$

$$\frac{ds}{dr} \sin \lambda = \psi_u \cos \alpha + \psi_v \sin \alpha.$$

These equations show the scale of depiction ds/dr corresponding to the different directions λ in the x, y-plane and α in the u, v-plane.

By introducing complex numbers we can show the connection still better.

Let us denote

$$z = \frac{dx}{dr} + \frac{dy}{dr} i = \frac{ds}{dr} e^{\lambda i},$$

$$z_1 = \varphi_u + \psi_u i,$$

$$z_2 = \varphi_v + \psi_v i.$$

Multiplying the second of the two equations by i and adding both they may be written as one equation in the complex form:

$$z = z_1 \cos \alpha + z_2 \sin \alpha.$$

The modulus of z is the scale of depiction of the uv plane at the point A in the direction α. The angle of z gives the direction in the xy plane corresponding to the direction α. For $\alpha = 0$ we have $z = z_1$ and for $\alpha = 90°$, $z = z_2$.

Let us substitute

$$\cos \alpha = \frac{e^{\alpha i} + e^{-\alpha i}}{2}, \quad \sin \alpha = \frac{e^{\alpha i} - e^{-\alpha i}}{2i}$$

and write

$$a = \frac{z_1 + z_2/i}{2}, \quad b = \frac{z_1 - z_2/i}{2},$$

so that the expression for z becomes

$$z = ae^{\alpha i} + be^{-\alpha i}.$$

This suggests a simple geometrical construction of the complex numbers z for different values of α. The term $ae^{\alpha i}$ is represented by the points of a circle described by turning the line that represents the complex number a round the origin through the angles $\alpha = 0 \cdots 2\pi$. The term $be^{-\alpha i}$ is represented by the points of a circle described by turning the line that represents b round the origin in the opposite direction through the angles $\alpha = 0 \cdots -2\pi$ (Fig. 52). The addition of the two complex numbers $ae^{\alpha i}$ and $be^{-\alpha i}$ for any value of α is easily performed. The points corresponding to the complex numbers z describe an ellipse, whose two principal axes bisect the angles between a and b. This is easily seen by writing

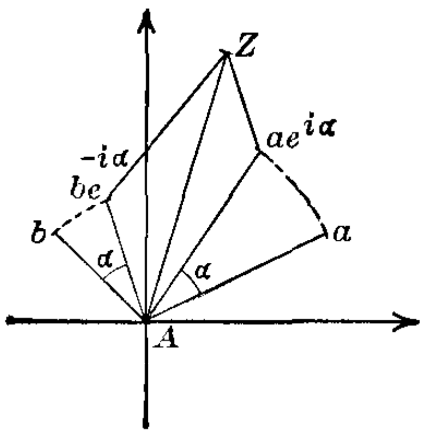


FIG. 52.

$$a = r_1 e^{(\alpha_0 - \alpha_1)i}, \quad b = r_2 e^{(\alpha_0 + \alpha_1)i}.$$

α_0 corresponds to the direction bisecting the angle between a and b and α_1 denotes half the angle between a and b (positive or negative according to the position of a and b).

$$z = r_1 e^{(\alpha_0 - \alpha_1 + \alpha)i} + r_2 e^{(\alpha_0 + \alpha_1 - \alpha)i},$$

or

$$ze^{-\alpha_0 i} = r_1 e^{(\alpha - \alpha_1)i} + r_2 e^{-(\alpha - \alpha_1)i}$$
$$= (r_1 + r_2)\cos(\alpha - \alpha_1) + (r_1 - r_2)\sin(\alpha - \alpha_1)i.$$

Denoting the coördinates of the complex number $ze^{-\alpha_0 i}$ by ξ and η we have

$$\frac{\xi}{r_1 + r_2} = \cos(\alpha - \alpha_1) \quad \text{and} \quad \frac{\eta}{r_1 - r_2} = \sin(\alpha - \alpha_1),$$

and consequently the equation of an ellipse

$$\frac{\xi^2}{(r_1 + r_2)^2} + \frac{\eta^2}{(r_1 - r_2)^2} = 1.$$

This ellipse turned round the origin through an angle equal to α_0 gives us the points corresponding to z. The principal axes are $2(r_1 + r_2)$ and $2(r_1 - r_2)$ (Fig. 53). The construction of

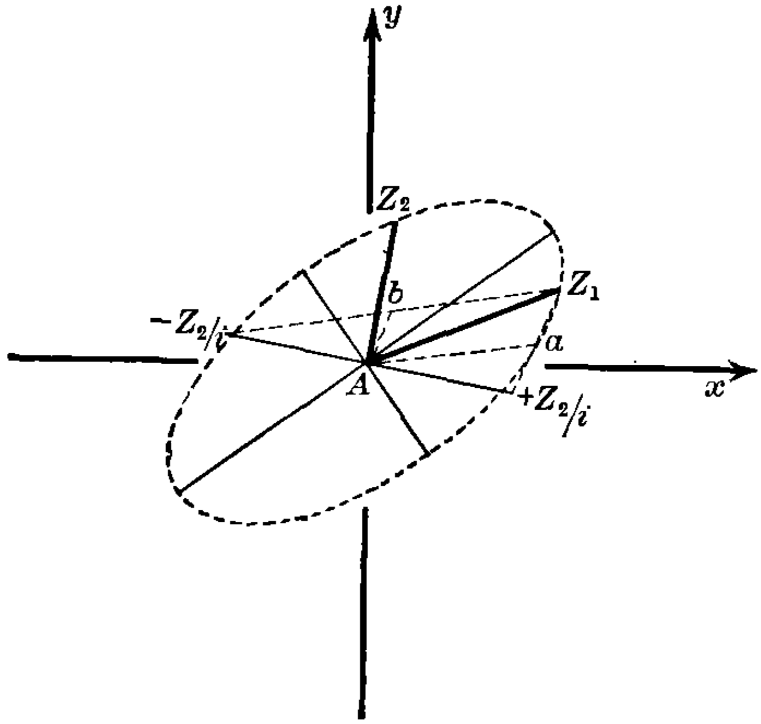


FIG. 53.

Fig. 53 is obvious. After plotting z_1 and z_2 we find z_2/i and $- z_2/i$ by turning AZ_2 through a right angle to the right and to the left. From these points lines are drawn to Z_1. The bisection of these lines give a and b.

The figure shows that in case a and b have the same modulus, the triangle $- Z_2/i$, Z_1, Z_2/i becomes equilateral and AZ_1 is perpendicular to the line joining $- Z_2/i$ and Z_2/i. In this case AZ_1 and AZ_2 would have the same or the opposite direction. But as $z_1 = \varphi_u + \psi_u i$, $z_2 = \varphi_v + \psi_v i$, this would mean that $\varphi_u\psi_v - \varphi_v\psi_u = 0$.

The radii of the ellipse (Fig. 53) measured in the unit used give the different scales of depiction corresponding to the different directions in the xy plane. We might also say the ellipse is the image in the xy plane of an infinitely small circle in the uv plane, magnified in the proportion of the infinitely small radius to 1, with its center in A.

Z_1 corresponds to $\alpha = 0$ and Z_2 to $\alpha = 90°$ and for $\alpha = 0$ to $90°$

Z moves on the ellipse from Z_1 to Z_2 through the shorter way. $-Z_1$ corresponds to $\alpha = 180°$ and $-Z_2$ to $\alpha = 270°$. Now we have shown above that a positive value of the functional determinant $\varphi_u\psi_v - \varphi_v\psi_u$ means that Z_2 is on the positive side of Z_1, so that in this case Z moves in the positive sense (that is, in the direction from the positive axis of x to the positive axis of y) with increasing values of α. With a negative value Z moves in the opposite direction.

Let us now suppose that the curves $x =$ const. and $y =$ const. in the uv plane intersect except on a certain curve where their direc-

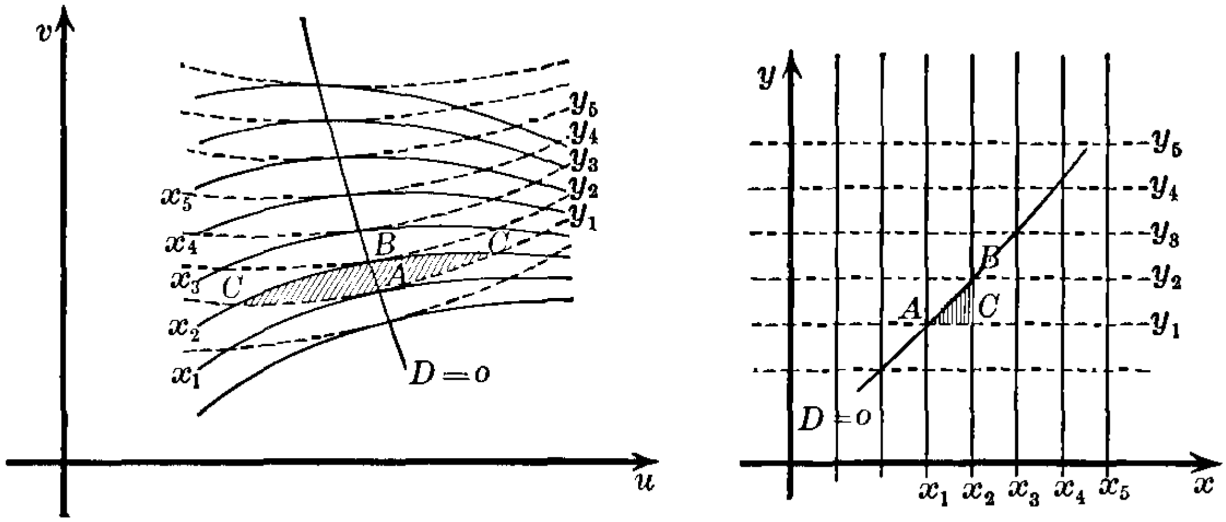


FIG. 54.

tions coincide in the way shown in Fig. 54. On this curve the functional determinant $D = \varphi_u\psi_v - \varphi_v\psi_u$ must vanish because the directions of the gradients coincide. Let us see what the depiction on the xy plane is like.

Running along one of the curves $y =$ const., say $y = y_1$, toward the curve $D = 0$ we intersect the curves $x = x_4$, x_3, x_2 until at the point A on the curve $x = x_1$ we reach the curve $D = 0$. In the xy plane the corresponding path is a parallel to the axis of x at a distance y_1 passing through x_4, x_3, x_2 and reaching a point A at x_1. If we now proceed on the curve $y = y_1$ in the uv plane beyond the curve $D = 0$, we again intersect the curves x_2, x_3, etc., but in the inverse order. Thus the corresponding path in the xy plane does not pass beyond A, but turns back through the same points x_2, y_1; x_3, y_1, etc. The same holds for any of the other lines $y =$ const. If we trace the line in the xy plane that corresponds to the points in the uv plane, where the curves $x =$ const. and $y =$ const. touch, we find the depiction of the uv plane only on one side of the curve in the xy plane. The other side has no corresponding points u, v. However to every point C on this side of the curve, there are two corresponding points C in the uv plane, one on either side of the curve $D = 0$. Imagine two sheets of paper laid on the xy plane; let them both be cut along the curve AB. Retain only the two pieces on this side of the curve and paste them together along the curve. The uv plane is in this way depicted on the paper in such a way that there is one point and one only on the paper corresponding to each point in the region of the uv plane considered. The curve $D = 0$ in the uv plane corresponds to the rim where the two pieces of paper are pasted together. Any line straight or curved passing over the curve $D = 0$ in the uv plane,corresponds to a line running from one of the sheets onto the other. It need not change its direction abruptly when it reaches the rim and passes onto the other sheet. For it may touch the rim in the direction of its tangent. This is actually the rule and the abrupt change of direction is the exception. Any line LAL (Fig. 55) in the uv plane, whose tangent as it crosses the curve $D = 0$ at A does not coincide with the common tangent of the curves $x =$ const. and $y =$ const. will correspond to a line in the xy plane, that does not change its direction abruptly when it touches the rim.

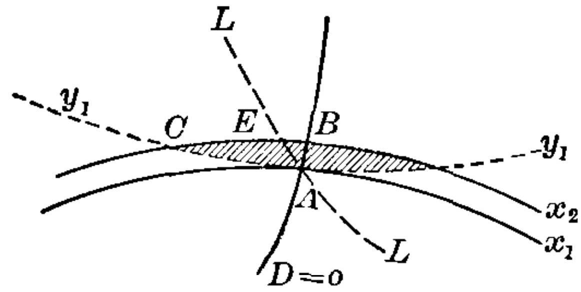


FIG. 55.

This is best understood analytically. Let us consider corresponding directions at the points A in the uv plane and in the xy plane. We have seen above that corresponding directions (Fig. 56) are connected by the equations

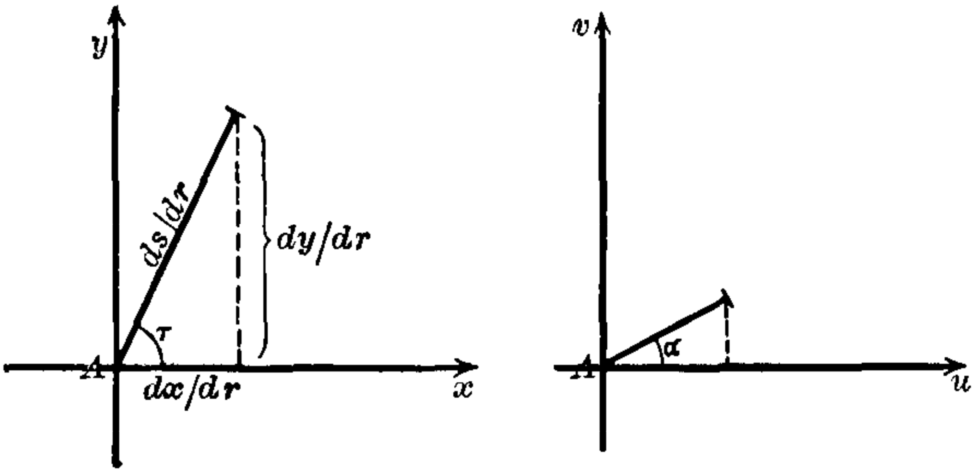


FIG. 56.

$$\cos\lambda\frac{ds}{dr} = \frac{dx}{dr} = \varphi_u \cos\alpha + \varphi_v \sin\alpha,$$

$$\sin\lambda\frac{ds}{dr} = \frac{dy}{dr} = \psi_u \cos\alpha + \psi_v \sin\alpha.$$

At the point A we have

$$\varphi_u\psi_v - \varphi_v\psi_u = 0.$$

Assuming that the gradients at A do not vanish, so that we can write

$$\varphi_u = r \cos\gamma, \quad \varphi_v = r\sin\gamma,$$

$$\psi_u = r' \cos\gamma', \quad \psi_v = r' \sin\gamma',$$

where r and r' are positive quantities, the equation $\varphi_u\psi_v - \varphi_v\psi_u = 0$ reduces to $\sin(\gamma - \gamma') = 0$, that is, $\gamma = \gamma'$ or $\gamma = \gamma' + 180°$. It follows therefore that:

$$\cos\lambda\frac{ds}{dr} = r\cos(\alpha - \gamma),$$

$$\sin\lambda\frac{ds}{dr} = r'\cos(\alpha - \gamma') = \pm r'\cos(\alpha - \gamma).$$

Consequently for all directions α in the uv plane for which $\cos(\alpha - \gamma)$ is not zero, we have

$$\operatorname{tg}\lambda = \pm\frac{r'}{r}.$$

That is to say, we have in the xy plane only one fixed direction λ and the opposite corresponding to all the different directions α except only a direction for which $\cos(\alpha - \gamma) = 0$. In the latter case, that is, when the direction α is perpendicular to the direction γ of the gradient, *i. e.*, in the direction of the curves $x =$ const. and $y =$ const., we have

$$\cos \lambda \frac{ds}{dr} = 0,$$

$$\sin \lambda \frac{ds}{dr} = 0.$$

Therefore $ds/dr = 0$ and λ remains indeterminate. Any direction λ for which $\operatorname{tg} \lambda$ differs from $+ r'/r$ corresponds to a fixed direction $\alpha = \gamma + 90°$ or $\alpha = \gamma - 90°$, while $ds/dr = 0$.

As the curve $D = 0$ is depicted on the rim of the two sheets of paper, all those lines that intersect the curve $D = 0$ in a direction different from the direction of the curves $x =$ const. and $y =$ const. are depicted in the xy plane as curves having their tangent at A in common with the rim. All lines in one of the sheets of paper that touch the rim at A in a direction different from that of the rim must be the depiction of lines in the uv plane that reach A in the direction of the lines $x =$ const. and $y =$ const. The scale of depiction is zero in the direction of the curves $x =$ const. and $y =$ const. In any other direction α we find it different from zero for:

$$\frac{ds}{dr} = \sqrt{(r^2 + r'^2) \cos^2 (\alpha - \gamma)}.$$

It is a maximum in the direction $\alpha = \gamma$ or $\gamma + 180°$ perpendicular to the curves $x =$ const. and $y =$ const.

It may help to understand all these details if we discuss an example where the depiction of the uv plane on the xy plane has a simple geometrical meaning, the planes being ground plan and elevation of a curved surface in space. The rim in the xy plane is the outline of the surface, the projection of those points where the tangential plane is perpendicular to the plane of elevation.

Suppose a cylinder of circular section cut in two half cylinders by a plane through its axis. Suppose one of the half cylinders in such a position that its axis forms an angle δ with the ground plan, the plan of elevation being parallel to its axis, Fig. 57. Let us introduce rectangular coördinates u, v in the ground plan and rectangular coördinates x, y in the plan of elevation. A point P on the cylinder is defined by certain values u, v which define its ground plan and certain values x, y which define its elevation. It is easily seen from Fig. 57 that we have

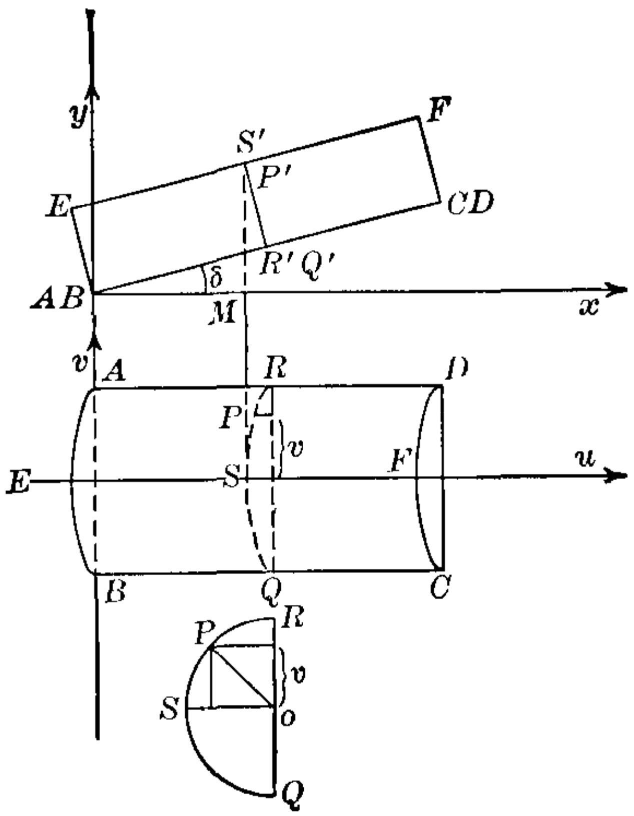


FIG. 57.

$$x = u$$

and

$$y = u \operatorname{tg}\delta + \frac{1}{\cos\delta}\sqrt{a^2 - v^2},$$

where a is the radius of the section. Now let us consider the elevation of the points P as a depiction of their ground plan. The functions $\varphi(u, v)$ and $\psi(u, v)$ in this case are

$$\varphi(u, v) = u,$$
$$\psi(u, v) = u \operatorname{tg}\delta + \frac{1}{\cos\delta}\sqrt{a^2 - v^2},$$

and

$$\varphi_u = 1, \quad \varphi_v = 0; \quad \psi_u = \operatorname{tg}\delta, \quad \psi_v = -\frac{v}{\cos\delta\sqrt{a^2 - v^2}},$$

$$\varphi_u\psi_v - \varphi_v\psi_u = -\frac{v}{\cos\delta\sqrt{a^2 - v^2}}.$$

The functional determinant vanishes for $v = 0$ on the line EF. The lines $y =$ const. are the intersections of the cylinder with horizontal planes. In the plan of elevation they are straight horizontal lines; in the ground plan they are ellipses (Fig. 58). As we pass along one of these curves we cross the line EF in the ground plan but we only touch it in the plan of elevation, retracing the horizontal line back again. The lines $x =$ const. are straight lines in both planes, but in space they correspond to ellipses. Again as we cross EF in the ground plan we only touch it in the plan of elevation and retrace the vertical line down again. Any curve on the cylinder that crosses EF in a direction not perpendicular to the plan of elevation is projected in the plan of elevation with EF as its tangent. For the real tangent in space lying in the tangential plane of the cylinder can have no other projection, if not perpendicular to the plan of elevation. In this latter case the projection of the tangent is a point and the tangent of the elevation is determined by the inclination of the osculatory plane.

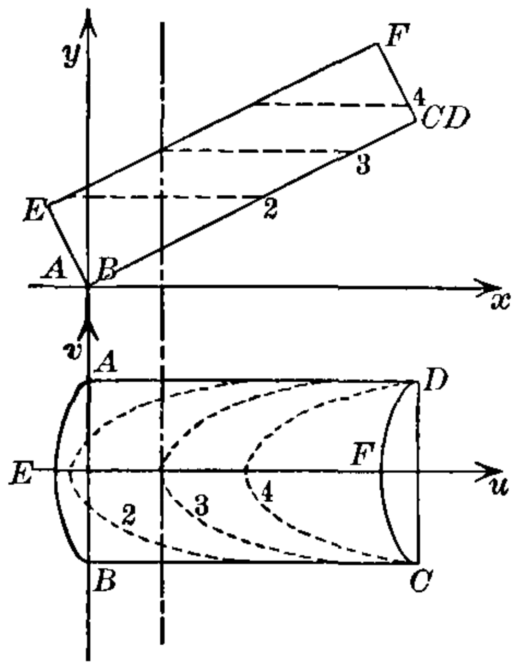


FIG. 58.

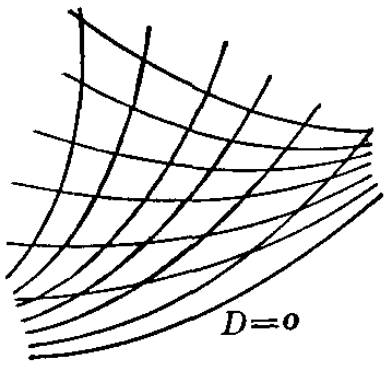


FIG. 59.

There is a particular case to be considered, when the curve $D = 0$ in the uv plane coincides with one of the curves $x =$ const. or $y =$ const. (Fig. 59), assuming the gradients of the functions $\varphi(u, v)$ and $\psi(u, v)$ not to vanish at the points of this curve. We have seen that at a point where $D = 0$ the scale of depiction must vanish in the directions of the curve $x =$ const. or $y =$ const. Let the curve $D = 0$ coincide with a line $x =$ const., then it follows that the length of the depiction of this curve is zero and the depiction must be contracted in a point. For the length of the depiction of a curve $x =$ const. is given by an integral

$$\int \frac{ds}{dr} dr,$$

where dr denotes an element of the curve and ds/dr the scale of depiction in the direction of the curve. As ds/dr is zero all along the curve the integral must necessarily vanish.

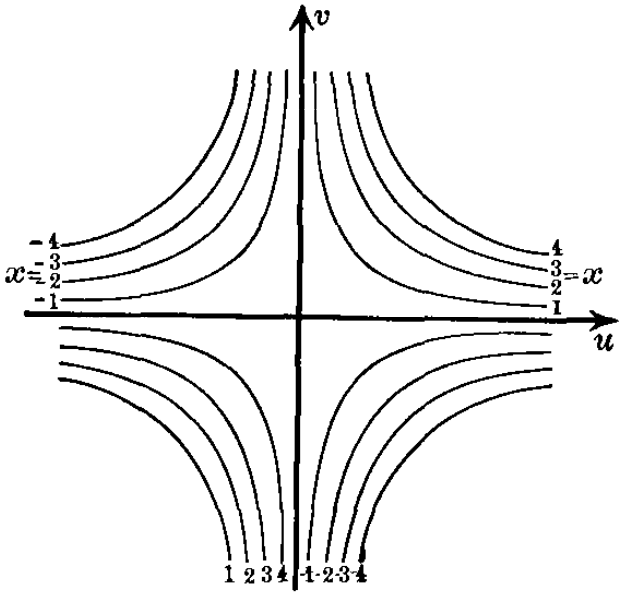


FIG. 60.

As an example let us consider

$$x = uv,$$

$$y = v.$$

The lines $x =$ const. in the uv plane are equilateral hyperbolas, the lines $y =$ const. are parallels to the axis of u (Fig. 60). Along the axis of u we have at the same time $y = 0$, $x = 0$ and $D = v = 0$. The whole axis of u is depicted in the point $x = 0$, $y = 0$ of the xy plane.

Let us finally consider the case where the scale of depiction at any point is the same in all directions, though it need not be the same at different points.

Writing as before

$$z_1 = \varphi_u + \psi_u i, \quad z_2 = \varphi_v + \psi_v i,$$

$$z = \frac{dx}{dr} + \frac{dy}{dr} i = \frac{ds}{dr} e^{\lambda i},$$

the connection between the scale of depiction ds/dr and the angles λ, α determining corresponding directions in the xy plane and in the uv plane is given by the equation

$$z = z_1 \cos \alpha + z_2 \sin \alpha,$$

or

$$z = ae^{i\alpha} + be^{-i\alpha},$$

where

$$a = \tfrac{1}{2}(z_1 + z_2/i), \quad b = \tfrac{1}{2}(z_1 - z_2/i).$$

In the case where the scale of depiction ds/dr, that is to say, the modulus of z, is independent of α, one of the constants a or b must vanish, as we see at once from the construction of z (Fig. 52). Let us consider the case $b = 0$,

$$z = ae^{\alpha i} = \frac{ds}{dr} e^{\lambda i}.$$

The complex number a may be written $|a|\ e^{\alpha_0 i}$, where $|a|$ denotes the modulus of a and α_0 the angle. Both may vary from point to point, but at every point they have fixed values.

Consequently we have

$$\frac{ds}{dr} = |a| \quad \text{and} \quad \lambda = \alpha + \alpha_0.$$

That is to say, from an angle α determining a direction in the uv plane, we find the angle λ determining the corresponding direction in the xy plane by the addition of a fixed value α_0. Any two directions α, α' will therefore form the same angle as the corresponding directions λ, λ' in the xy plane. The same is true when $a = 0$ and $z = be^{-\alpha i}$. The only difference is that in this latter case the direction of z rotates in the opposite sense with increasing values of α.

Analytically depictions of this kind are represented by functions of complex numbers,

$$x + yi = f(u + vi) \quad \text{or} \quad x + yi = f(u - vi).$$

Assuming the function to possess a differential coefficient we have

$$z_1 = \frac{\partial x}{\partial u} + \frac{\partial y}{\partial u} i = f'(u \pm vi),$$

$$z_2 = \frac{\partial x}{\partial v} + \frac{\partial y}{\partial v} i = \pm f'(u \pm vi) i,$$

and therefore either

$$z_1 = z_2/i \quad \text{or} \quad z_1 = -z_2/i.$$

Hence in the first case

$$a = \tfrac{1}{2}(z_1 + z_2/i) = z_1, \quad b = \tfrac{1}{2}(z_1 - z_2/i) = 0$$

and in the second case

$$a = 0, \quad b = z_1.$$

§ 11. *Other Methods of Representing Relations between Three Variables.*—The depiction of one plane on another may be used to generalize the graphical representation of a function of two variables or a relation between three variables, as we prefer to say.

As we have seen before, an equation

$$g(x, y, z) = 0$$

between three variables x, y, z can be represented by taking x and y as rectangular coördinates and plotting the curves $z =$ const. (Fig. 61) for equidistant values of z. Suppose now the xy plane to be depicted on another plane. The lines $x =$ const., $y =$ const. and $z =$ const. will be represented by three sets of curves. The fact that three values x, y, z satisfy the equation $g(x, y, z) = 0$ is shown geometrically by the intersection of the three corresponding curves in one point.

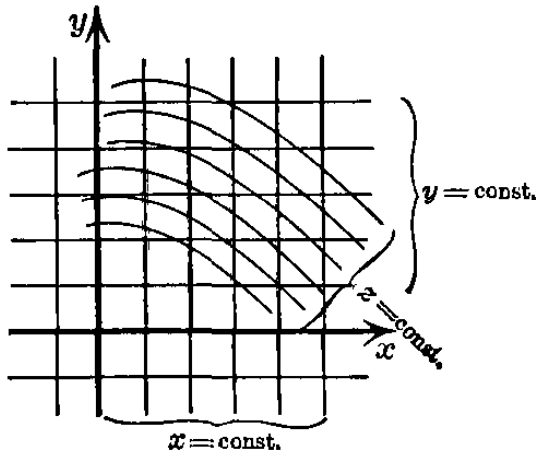


FIG. 61.

Another method for representing certain relations between three variables u, v, w consists in drawing three curves, each curve carrying a scale. The values of u, v, w are read each on one of the three scales. The relation between three values u, v, w is represented geometrically by the condition that the corresponding points lie on a straight line (Fig. 62). This method is far more convenient than the one using three sets of curves. It is less trouble to place a ruler over two points u, v of two curves and read the value w on the scale of the third than to find the intersection of two curves u = const. and v = const. among sets of others, pick out the curve w = const. that passes through the

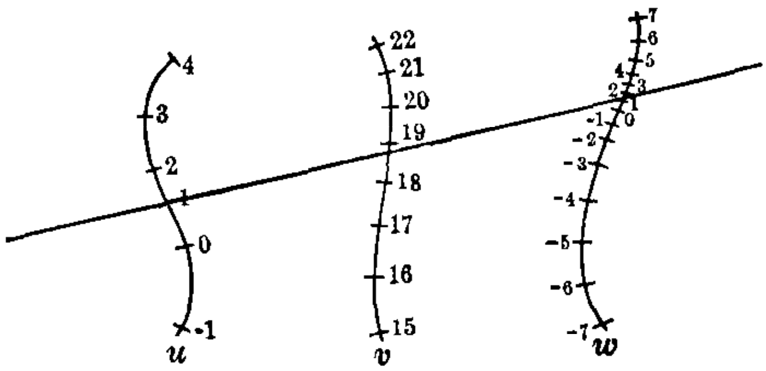


Fig. 62.

same point and read the value of w corresponding to it. For we must consider that the curves corresponding to certain values of u and v are generally not drawn, but must be interpolated and so must the curve w = const. It is true that interpolations are necessary with both methods, but the interpolation on scales like those in Fig. 62 is easily done.

It must however be understood that while the three sets of curves form a perfectly general method for representing any relation between three variables, the other method is restricted to certain cases. In order to investigate this subject more fully we shall have to explain the use of line coördinates.

When we apply rectangular coördinates x, y to define a certain point in a plane, we may say that x determines one of a set of straight lines (parallel to the axis of ordinates) and y determines one of another set of straight lines (parallel to the axis of abscissas) and the point is the intersection of the two (Fig. 63, *I*). A similar method may be used to determine a certain straight line in a plane. Let x determine a *point* on a certain straight line, x being its distance from a fixed point A on the line measured in a certain unit and counted positive on one side and negative on the other. Let y define a *point* on another straight line parallel to the first, y being its distance from a fixed point B on the line measured in the same way as x. The straight line passing through the two points is thus determined by the values

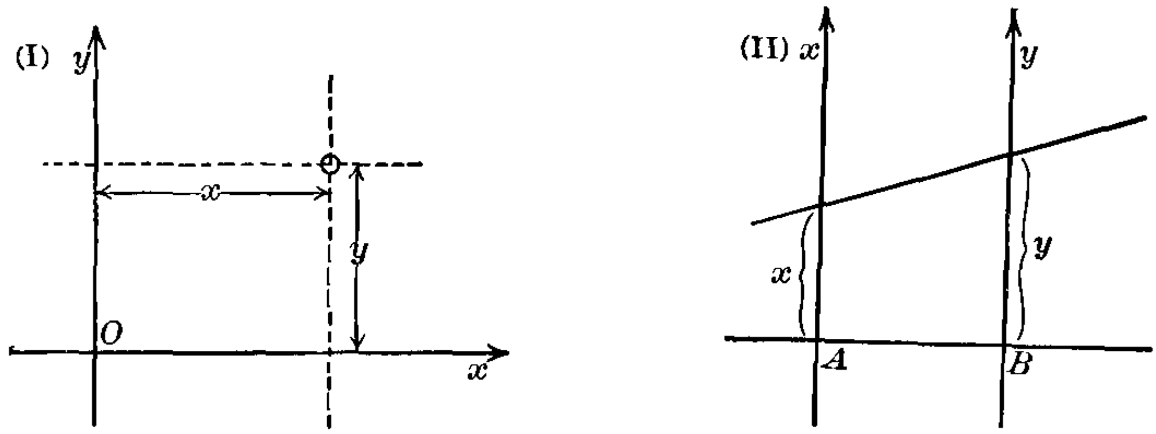


FIG. 63.

x and y and for all possible values of x and y we obtain all the straight lines of the plane except those parallel to the lines on which x and y are measured. For simplicity we choose AB perpendicular to the two lines (Fig. 63, *II*). Let us call x and y the line coördinates of the line connecting the two points x and y in Fig. 63, *II*, in the same way as x and y in Fig. 63, *I*, are called the point coördinates of the point where the two lines x and y intersect.

A linear equation between point coördinates

$$y = mx + \mu$$

is the equation of a straight line. That is to say, all the points whose coördinates satisfy the equation lie on a certain straight line. If, on the other hand, we regard x and y as line coördinates we find the analogous theorem: all the straight lines whose line coördinates satisfy the equation

$$y = mx + \mu$$

pass through a certain point. The equation is therefore called the equation of the point.

In order to show this let us first draw the line $x = 0$, $y = \mu$ (APO in Fig. 64). If now for any value of x we make $AR = x$

and $PQ = mx$, the point of intersection of RQ and AP must be independent of x, for

$$\frac{PO}{AO} = \frac{mx}{x} = m.$$

The ratio PO/AO determines the position of O and as it is independent of x and the positions of A and P are also independent of x, the same is true for O. For negative values of m, PO and AO have opposite directions so that O lies between A and P.

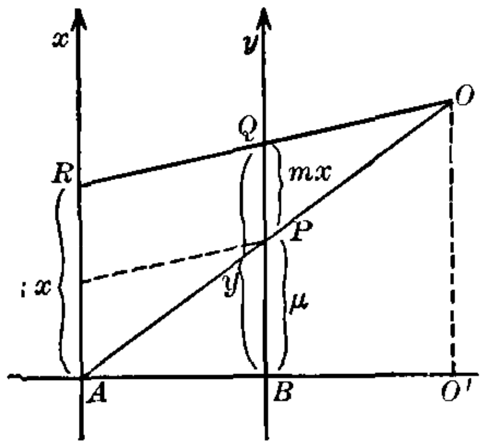


FIG. 64.

For a given point O, we can find the corresponding values of m and μ by joining O with the points A and the point corresponding to $x = 1$. If P and Q are the intersections of these lines with the line on which y is measured, we have $BP = \mu$ and $PQ = m$. Any point in the plane thus leads to an equation

$$y = mx + \mu,$$

except the points on the line on which x is measured. For $m = 0$ the equation reduces to

$$y = \mu,$$

that is, the equation of a point on the line on which y is measured.

Instead of $y = mx + \mu$, we might also write $x = m'y + \mu'$, and go through similar considerations changing the parts of x and y. This form does not include the points on the line on which y is measured, but it does include the points on the line on which x is measured. For these we have $m' = 0$.

The general equation of a point in line coördinates is given in the form

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

from which we may derive either of the first-mentioned forms dividing it by a or b.

Dividing by c another convenient form is obtained,

$$\frac{ax}{-c} + \frac{by}{-c} = 1,$$

or writing

$$\frac{-c}{a} = x_0, \quad \frac{-c}{b} = y_0,$$

$$\frac{x}{x_0} + \frac{y}{y_0} = 1,$$

x_0 determining the point of intersection of the line BO (Fig. 64) and the x-line, while y_0 determines the point of intersection of the line AO with the y-line.

A curve may be given by an equation

$$a_1(u)x + b_1(u)y + c_1(u) = 0,$$

in which $a_1(u)$, $b_1(u)$, $c_1(u)$ are functions of a variable u. Any value of u furnishes the equation of a certain point and as u changes the point describes the curve. Let us suppose the curve drawn and a scale marked on it giving the values of u in certain intervals sufficiently close to interpolate the values of u between them. Two other curves are in the same way given by the equations

$$a_2(v)x + b_2(v)y + c_2(v) = 0,$$

$$a_3(w)x + b_3(w)y + c_3(w) = 0,$$

and scales on these curves mark the values of v and w.

Now we are enabled to formulate the condition which must be satisfied by the values u, v, w in order that the three corresponding points lie in one straight line. If x and y are the line coördinates of the line passing through the three points, x and y must satisfy all three equations simultaneously.

Consequently the determinant of the three equations must vanish

$$a_1(b_2c_3 - b_3c_2) + a_2(b_3c_1 - b_1c_3) + a_3(b_1c_2 - b_2c_1) = 0,$$

and, vice versa, if the equation between u, v, w may be brought into this form where a_1, b_1, c_1 are any functions of u, a_2, b_2, c_2 any functions of v and a_3, b_3, c_3 any functions of w, we can form the equations

$$a_1x + b_1y + c_1 = 0,$$

$$a_2x + b_2y + c_2 = 0,$$

$$a_3x + b_3y + c_3 = 0,$$

and represent them graphically by curves carrying scales for u, v, w. The relation between u, v, w is then equivalent to the condition that the corresponding points on the three curves lie on a straight line. But it must be remembered that only a restricted class of relations can be brought into the required form, so that the method cannot be applied to any given relation.

The equation of a point

$$ax + by + c = 0$$

remains of the same form, when the units of length are changed for x and y. If x' denotes the number measuring the same length as the number x but in another unit, the two numbers must have a constant ratio equal to the inverse ratio of the two units. Therefore, by changing the units independently, we have

$$x = \lambda x', \quad y = \mu y',$$

and the equation of the point may be written

$$a\lambda x' + b\mu y' + c = 0,$$

or

$$a'x' + b'y' + c = 0,$$

where $a' = \lambda a$ and $b' = \mu b$.

It is sometimes convenient to define the line coördinates in another way. Let ξ and η denote rectangular coördinates measured in the same unit, then the equation of a straight line can be written

$$\eta = \operatorname{tg} \varphi \xi + \eta_0,$$

where φ is the angle between the line and the axis of ξ and η_0, the ordinate of the point of intersection with the axis of η. Now let us call tg φ and η_0 the line coördinates of the straight line represented by the equation and let us denote them by x and y. Thus the values of x and y define a certain straight line and any straight line not parallel to the axis of ordinates may be defined in this manner. The condition that a straight line x, y passes through a point ξ, η is expressed by the equation

$$\eta = x\xi + y,$$

or

$$y = -\xi x + \eta.$$

If we fix the values of x and y, all the values ξ, η that satisfy this equation represent the points of the straight line x, y and we therefore call it the equation of the straight line. If, on the other hand, we fix the values of ξ and η, all the values x, y that satisfy the equation represent the straight lines that pass through the given point ξ, η, and therefore we call it the equation of the point.

The more general form

$$ax + by + c = 0$$

can be reduced to

$$y = -\frac{a}{b}x - \frac{c}{b}.$$

It therefore represents the equation of the point, whose rectangular coördinates are $\xi = a/b$ and $\eta = -c/b$. The case where $b = 0$ or

$$ax + c = 0$$

represents the equation of a point infinitely far away in the direction φ or the opposite direction $\varphi + 180°$, φ being defined by

$$\text{tg } \varphi = x = -\frac{c}{a}.$$

All the straight lines, whose coördinates x, y satisfy the equation

$$ax + c = 0$$

correspond to the same value of x but to any value of y. That is to say, they are all parallel and all the straight lines of this direction belong to them.

Let us now discuss some of the applications of line coördinates to the graphical representation of relations between three variables.

The relation

$$uv = w$$

may be written in the form

$$\log u + \log v = \log w,$$

or

$$x + y = \log w,$$

when

$$x = \log u \quad \text{and} \quad y = \log v.$$

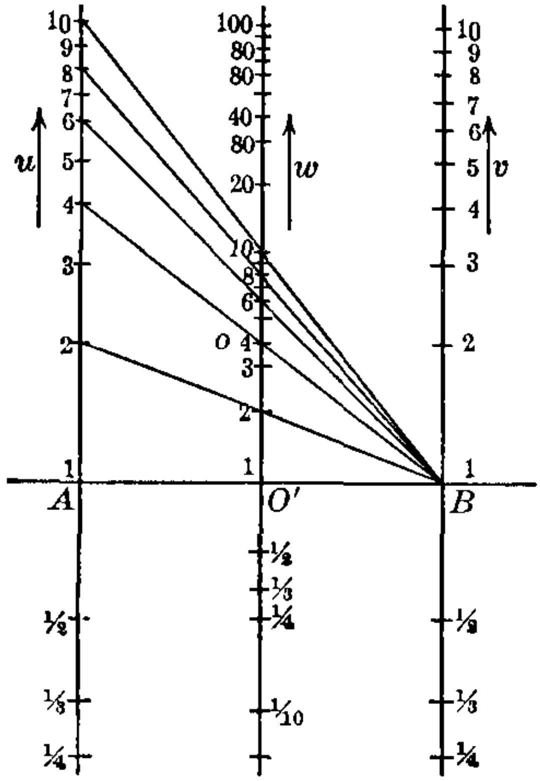


FIG. 65.

Let us plot x and y as line coördinates on two parallel lines (Fig. 65), with scales for the values of u and v. The equations $x = \log u$ and $y = \log v$ may be regarded as the equations of the points of these two scales. The equation

$$x + y = \log w$$

for any value of w is the equation of a point. It can easily be constructed as the intersection of any lines x, y satisfying its equation. For instance, the line $x = \log w$, $y = 0$ and the line $x = 0$, $y = \log w$. The first line is found by connecting the scale division $u = w$ of the u-scale with the point B, the second by connecting the scale division $v = w$ of the v-scale with the point A. If the units of x and y are taken of the same length, the point of intersection will lie in the middle between the two lines carrying the u and v scales on a line parallel to the two other lines and the w-scale will be half the size of the other two (Fig. 65).

The relation

$$uv = w$$

or

$$\log u + \log v = \log w$$

expresses the condition that the three equations

$$x = \log u, \quad y = \log v, \quad x + y = \log w$$

are satisfied simultaneously by the same values of x and y, that is to say, that the three points on the u, v, w scales corresponding to the values of u, v, w lie on the same straight line x, y.

The more general relation

$$u^\alpha v^\beta = w,$$

where α and β are any given values, can be treated in the same manner. Thus the pressure and volume of a gas undergoing adiabatic changes may be represented. In this case we have

$$pv^k = w,$$

where p denotes the pressure, v the volume and k and w constants.

For a given gas k has a given value, but w depends on the quantity of the gas considered.

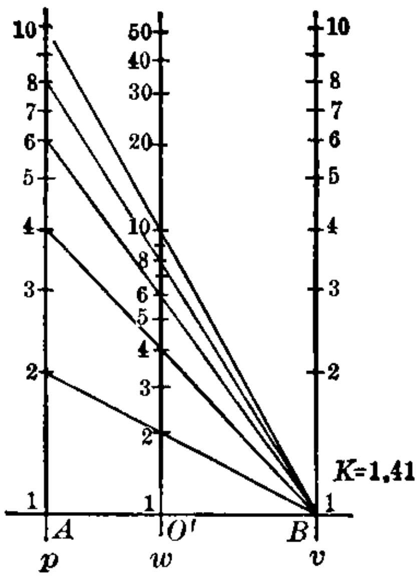


FIG. 66.

We write

$$x = \log p, \quad y = \log v.$$

The relation then takes the form

$$x + ky = \log w,$$

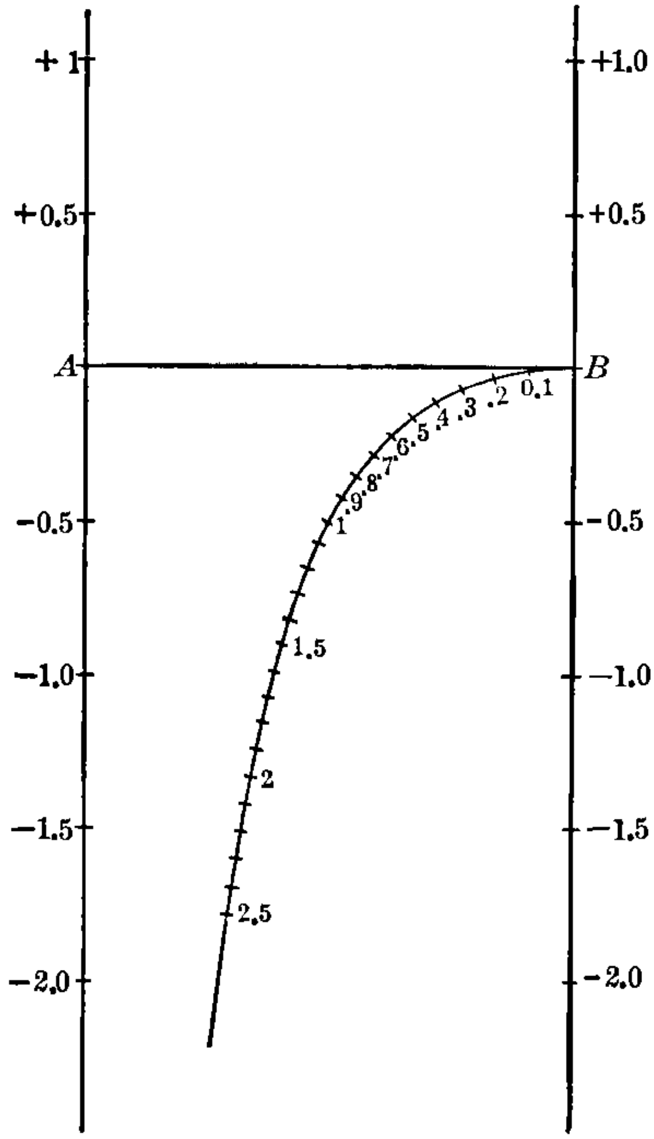
and represents a point which may be constructed by the intersection of any two straight lines x, y, whose coördinates satisfy the equation, for instance

$$x = \log w, \quad y = 0$$

and

$$x = 0, \quad y = \frac{1}{k} \log w.$$

The first line connects the point B (Fig. 66) with the scale division $p = w$ of the p scale and the second line connects the point A with the scale division of the v scale for which $y = k \log w$. A perpendicular from the point of intersection on AB meets it in O' and as the ratio $AO'/O'B$ is equal to the ratio of the segments on the p and v scales $\log w/k \log w = 1/k$ it is independent of w. All the points corresponding to different values of w lie on the same parallel to the p and v scales and the w scale may be obtained by a central projection of the p scale on this parallel from the center B (Fig. 66). We might dispense with the construction of the w scale as long as the straight line for the w scale is drawn. For in using the diagram we generally start with values p_0, v_0 and want to find other values p, v, for which



$$pv^k = p_0v_0^k.$$

FIG. 67.

The straight line connecting the scale divisions p and v intersects the w scale at the same point as the straight line connecting the scale divisions p_0 and v_0, so that we need not know the value of $p_0v_0^k$. It suffices to mark the point of intersection in order to find the value of p, when v is given or the value of v when p is given.

Another example is furnished by the equation

$$w^2 + xw + y = 0.$$

If we regard x and y as line coördinates any value of w determines the equation of a point. We plot the curve formed by these points with a scale on it indicating the corresponding values of w. Any values of x and y determine a straight line whose intersections with the w scale furnish the roots of the equation. Each point of the w scale may be constructed by the intersection of two straight lines, whose coördinates x, y satisfy the equation, for instance

$$x = 0, \quad y = -w^2 \quad \text{and} \quad x = -w, \quad y = 0.$$[1]

In Fig. 67 the w scale is shown for the positive values $w = 0$ to $w = 2.5$.

In the same manner a diagram for the solution of the cubic equation

$$w^3 + xw + y = 0.$$

or of any equation of the form

$$w^\lambda + xw^\mu + y = 0$$

may be constructed.

§ 12. *Relations between Four Variables.*—The method can be generalized for relations between four variables.

Suppose four variables u, v, w, t are connected by the equation

$$g(u, v, w, t) = 0,$$

and let us assume that for any particular value $t = t_0$ the resulting relation between u, v, w can be given by a diagram of the form considered consisting of three curves carrying scales for u, v and w. Let us further suppose that for other values of t the scales for u and v remain the same, but the scale for w changes. Then we shall have a set of w scales corresponding to different values of t. Connecting the points that correspond to the same value of w we obtain a network of curves $t =$ const. and $w =$ const. (Fig. 68). Any two values u, v furnish a straight line intersecting

[1] For small values of w, this combination is not good because the angle of intersection is small. One might substitute $x = 2$, $y = -w^2 - 2w$ for the first line.

the network of curves. The points of intersection correspond to values of t and w that satisfy the given relation.

Any relation of the form

$$\varphi(u)f(t, w) + \psi(v)g(t, w) + h(t, w) = 0$$

may be represented in this way, $\varphi(u)$ denoting any function of u, $\psi(v)$ any function of v and $f(t, w)$, $g(t, w)$, $h(t, w)$ any functions of t and w.

In this case we need only introduce the line coördinates x, y, writing

$$x = \varphi(u), \quad y = \psi(v).$$

We then obtain a linear equation between x and y,

$$f(t, w)x + g(t, w)y + h(t, w) = 0,$$

which for any given values of t and w represents the equation of a point.

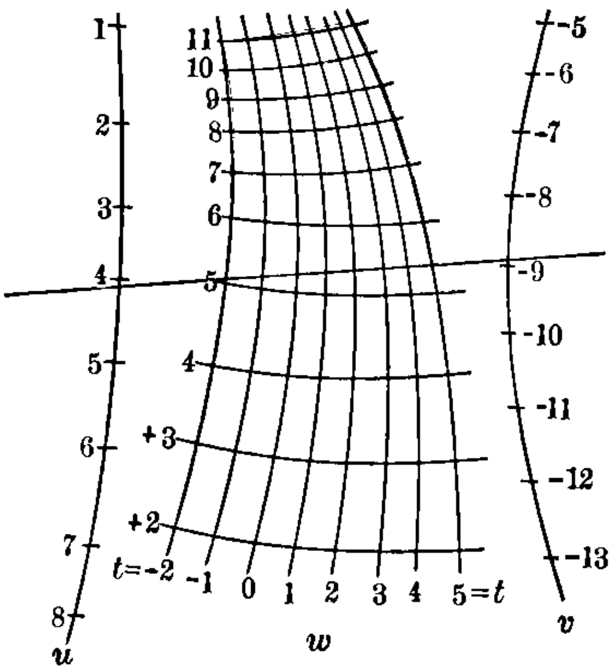


FIG. 68.

For a given value of t and variable values of w we obtain a curve $t =$ const. carrying a scale for w and for a series of values of t we obtain a set of curves $t =$ const. Similarly for a given value of w and variable values of t the equation furnishes a curve $w =$ const., carrying a scale for t and a series of values of w furnishes a set of curves $w =$ const. From any given values of u and v the line coördinates x and y are calculated and the points where this straight line defined by x and y intersects the network of the curves $t =$ const. and $w =$ const. furnish the values t, w that satisfy the relation together with the given values of u and v. The relation between the height, azimuth, declination of a celestial body and the latitude of the point of observation may serve as an example. Let h, a, δ denote the height, azimuth and declination and φ the latitude. The angles $\pi/2 - \varphi$, $\pi/2 - h$, $\pi/2 - \delta$ are the three sides of a spherical triangle PZS (Fig. 69) formed by the pole P, the zenith Z and the celestial body S. The azimuth is defined as the supplement of the angle PZS.

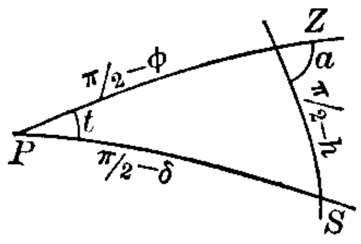


FIG. 69.

The equation is

$$\sin \delta = \sin \varphi \sin h - \cos \varphi \cos h \cos a.$$

We write

$$x = \cos a, \quad y = \sin \delta,$$

so that the equation becomes

$$y = \sin \varphi \sin h - x \cos \varphi \cos h.$$

We shall in this case use the second system of line coördinates where x is the slope of the line measured by the tangent of the angle formed with the axis of abscissas and y is the ordinate of the intersection with the axis of ordinates. If ξ, η denote the rectangular coördinates of the point, the equation of the points takes the form

$$\eta = x\xi + y \quad \text{or} \quad y = \eta - \xi x,$$

so that in our case we have

$$\xi = \cos \varphi \cos h, \quad \eta = \sin \varphi \sin h.$$

The curves $\varphi =$ const. and $h =$ const. can be drawn by means of these formulas. It is easily seen that they are ellipses and that the curves $\varphi =$ const. are the same as the curves $h =$ const. For a definite value of φ and a variable value of h we find

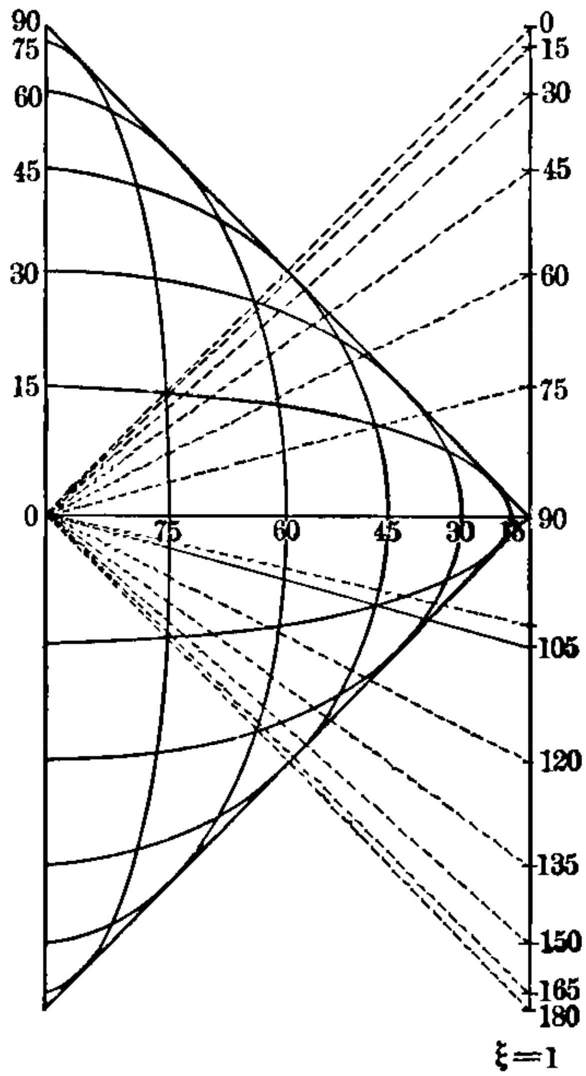


FIG. 70.

$$\frac{\xi^2}{\cos^2 \varphi} + \frac{\eta^2}{\sin^2 \varphi} = 1,$$

and for a definite value of h and a variable value of φ

$$\frac{\xi^2}{\cos^2 h} + \frac{\eta^2}{\sin^2 h} = 1.$$

Any of the ellipses intersects all the others and in this way they form a network. A point of intersection of the ellipse $\varphi = c_1$ and the ellipse $h = c_2$ also corresponds to the values $h = c_1$ and $\varphi = c_2$, as the ellipse $\varphi = c_1$ is identical with the ellipse $h = c_1$ and $\varphi = c_2$ identical with $h = c_2$ (Fig. 70). The easiest way to find this network consists in drawing the straight lines

$$\xi + \eta = \cos(\varphi - h),$$

and perpendicular to them the straight lines

$$\xi - \eta = \cos(\varphi + h),$$

for equidistant values of $\varphi + h$ and $\varphi - h$. The ellipses run diagonally through the rectangular meshes formed by the two systems of straight lines. The scales for φ and h are written on the axis of coördinates, both scales being available for both variables. The scale for δ is written on the axis of ordinates and is identical with the scale for t and h on this axis. For the ordinate corresponding to a given value $\delta = c$ is $\sin c$, and this is also the ordinate of the point where the ellipse $\varphi = c$ or $h = c$ intersects the axis of ordinates. The scale for the azimuth cannot be laid down in exactly the same way as that for φ, h and δ because $\cos a$ determines the slope of the straight line x, y. Let us draw a parallel to the axis of ordinates through the point $\xi = 1$, $\eta = 0$ and mark a scale for the azimuth on it, making $\eta = \cos a$ (Fig. 70). A line connecting the origin with any scale division of this scale has the slope of the line $x = \cos a$, $y = \sin \delta$. To bring it into the position of the line x, y it must be moved parallel to itself, until its point of intersection with the axis of ordinates coincides with the scale division δ. This suggests another way of using the diagram. Let a pencil of rays be drawn from the origin to the scale divisions of the azimuth scale (Fig. 70), and let it be drawn on a sheet of transparent paper placed over the drawing of the ellipses. For any given value of δ it is moved up or down as the case may be so that the center of the pencil coincides with the scale division δ. As long as the celestial body does not materially alter its declination the diagram in this position will enable us to find any of the three values φ, h, a from the other two.

As a second example let us consider the relation between the declination δ, the azimuth a, the hour angle t of a celestial body and the latitude φ of the point of observation.

The relation is found by eliminating the height h from the equation

$$\sin\delta = \sin\varphi\sin h - \cos\varphi\cos h\cos a.$$

For this purpose we express $\sin h$ and $\cos h$ by the other angles and substitute these expressions for $\sin h$ and $\cos h$.

We have

$$\cos h = \cos\delta\sin t/\sin a,$$

$$\sin h = \sin\varphi\sin\delta + \cos\varphi\cos\delta\cos t.$$

Substituting these values we find

$\sin\delta = \sin^2\varphi\sin\delta + \sin\varphi\cos\varphi\cos\delta\cos t - \cos\varphi\cos\delta\sin t\,\mathrm{ctg}\,a$, or

$$\cos^2\varphi\sin\delta = \sin\varphi\cos\varphi\cos\delta\cos t - \cos\varphi\cos\delta\sin t\,\mathrm{ctg}\,a.$$

Dividing by $\cos^2\varphi\cos\delta$ we finally obtain

$$\mathrm{tg}\,\delta = \mathrm{tg}\,\varphi\cos t - \frac{\sin t}{\cos\varphi}\,\mathrm{ctg}\,a.$$

In order to represent this relation graphically we introduce line coördinates

$$x = \mathrm{ctg}\,a \quad \text{and} \quad y = \mathrm{tg}\,\delta$$

and find

$$y = \mathrm{tg}\,\varphi\cos t - \frac{\sin t}{\cos\varphi}\,x.$$

Let us use the second system of line coördinates. The rectangular coördinates ξ, η of the point represented by the equation are found from it equal to:

$$\xi = \frac{\sin t}{\cos \varphi}, \quad \eta = \operatorname{tg} \varphi \cos t.$$

The curves $\varphi =$ const. are ellipses,

$$\cos^2 \varphi \xi^2 + \frac{\eta^2}{\operatorname{tg}^2 \varphi} = 1.$$

The curves $t =$ const. are hyperbolas,

$$\frac{\xi^2}{\sin^2 t} - \frac{\eta^2}{\cos^2 t} = 1.$$

The ellipses and hyperbolas are confocal, the foci coinciding with the points $\xi = \pm 1$, $\eta = 0$, so that the curves intersect at right angles.

The scale for φ may be written on the axis of ordinates at the points where it intersects the ellipses. It is identical with the scale for δ, the ordinate in both cases being the tangent of the angle with the only difference that δ is negative on the negative part of the axis and φ is not. The scale for t may be written on one of the ellipses corresponding to the largest value of φ that is to be taken account of. This ellipse forms the boundary of the diagram, so that larger values of φ are not represented. Corresponding to the azimuth we draw a pencil of rays on a sheet of transparent paper, which is laid on the drawing of the curves. The center of the pencil is placed on the scale division δ and the azimuth is equal to the angles that the rays form with the positive direction of the axis of ordinates (Fig. 71). It suffices to draw the curves and the rays only on one side of the axis of ordinates. At the apex of the

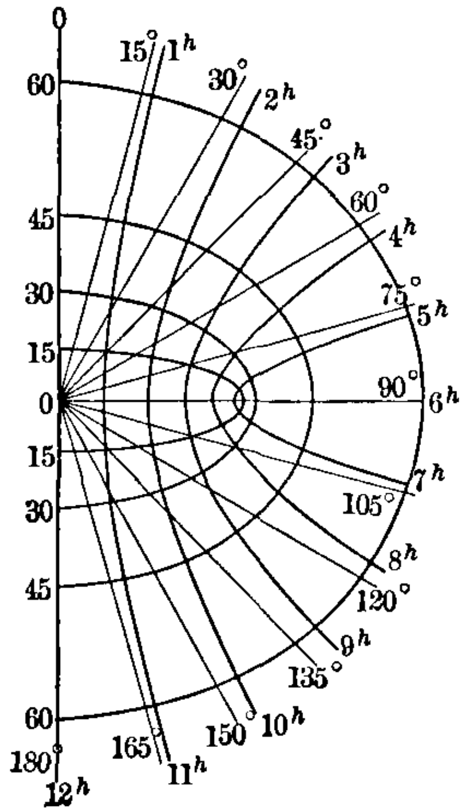


FIG. 71.

hyperbolas the value of t changes abruptly. The line $t = 6^h$ is meant to start from the focus $\xi = 1, \eta = 0$. When the center of the pencil of rays is in the origin the rays form the asymptotic lines of the hyperbolas, $a = 15°$ corresponding to $t = 1^h$, $a = 30°$ to $t = 2^h$ and so on.

CHAPTER III.

THE GRAPHICAL METHODS OF THE DIFFERENTIAL AND INTEGRAL CALCULUS.

§ 13. *Graphical Integration.*—We have shown how the elementary mathematical operations of adding, subtracting, multiplying and dividing and the inverse operation of finding the root of an equation can be carried out by graphical methods and how functions of one or more variables may be represented and handled. But the graphical methods would lack generality and would be of very limited use, if they were not applicable to the infinitesimal operations of differentiation and integration. Indeed it is here that they are found of the greatest value. In many cases, where the calculus is applied to problems of natural science or of engineering, the functions concerned are given in a graphical form. Their true analytical structure is not known and as a rule an approximation by analytical expressions is not easily calculated nor easily handled. In these cases it is of vital importance that the operations of the calculus can be performed, although the functions are only given graphically.

Let us begin with integration, because it is easier than differentiation and of more general application.

Suppose a function $y = f(x)$ given by a curve whose ordinate is y and whose abscissa is x. The problem is to find a curve, whose ordinate Y is an integral of the function $f(x)$,

$$Y = \int_a^x f(x)dx.$$

Let us assume the unit of length for the abscissas independent of the unit of length for the ordinates. The value of Y measures the area between the ordinates corresponding to a and x, the curve $y = f(x)$ and the axis of x in units equal to the rectangle formed by the units of x and y.

In the simple case where $f(x)$ is a constant the equation $y = f(x) = c$ is represented by a line parallel to the axis of x and

$$Y = \int_a^x c dx = c(x - a).$$

Y is the ordinate of a straight line intersecting the axis of x at the point $x = a$. The constant c is the change of Y for an increase of x equal to 1. If P is the point on the axis of x for $x = -1$ and Q the point where the line $y = c$ intersects the axis of ordinates (Fig. 72) the desired line is parallel to PQ. It is constructed by drawing a parallel to PQ through the point $x = a$ on the axis of x (Fig. 72, where $a = 0$).

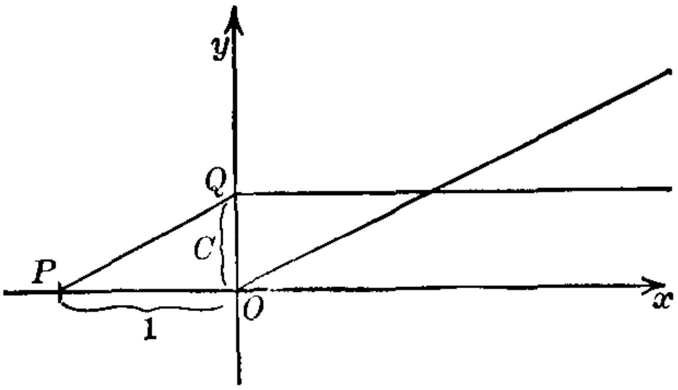


FIG. 72.

When a given value c_1 is added, so that the equation becomes

$$Y = c\,(x - a) + c_1$$

it amounts to the same as when the straight line is moved in the direction of the axis of ordinates through a distance c_1. For $x = a$ we then have $Y = c_1$, so that we obtain the line

$$Y = c(x - a) + c_1,$$

by drawing a parallel to PQ through the point $x = a$, $y = c_1$.

In the second place let us assume that the line $y = f(x)$ consists of a number of steps, that is to say, that the function has different constant values in a number of intervals $x = x_1$ to x_2, x_2 to x_3, etc., while it changes its value abruptly at x_2, x_3, etc. The line presenting the integral

$$Y = \int_{x_1}^x f(x)dx$$

does not change its ordinate abruptly. It consists of a continuous broken line, whose corners have the abscissas x_2, x_3, etc.

The directions of the different parts are found in the way just described by the pencil of rays from P to the points α, β, γ, etc. (Fig. 73), where the horizontal lines intersect the axis of ordinates.

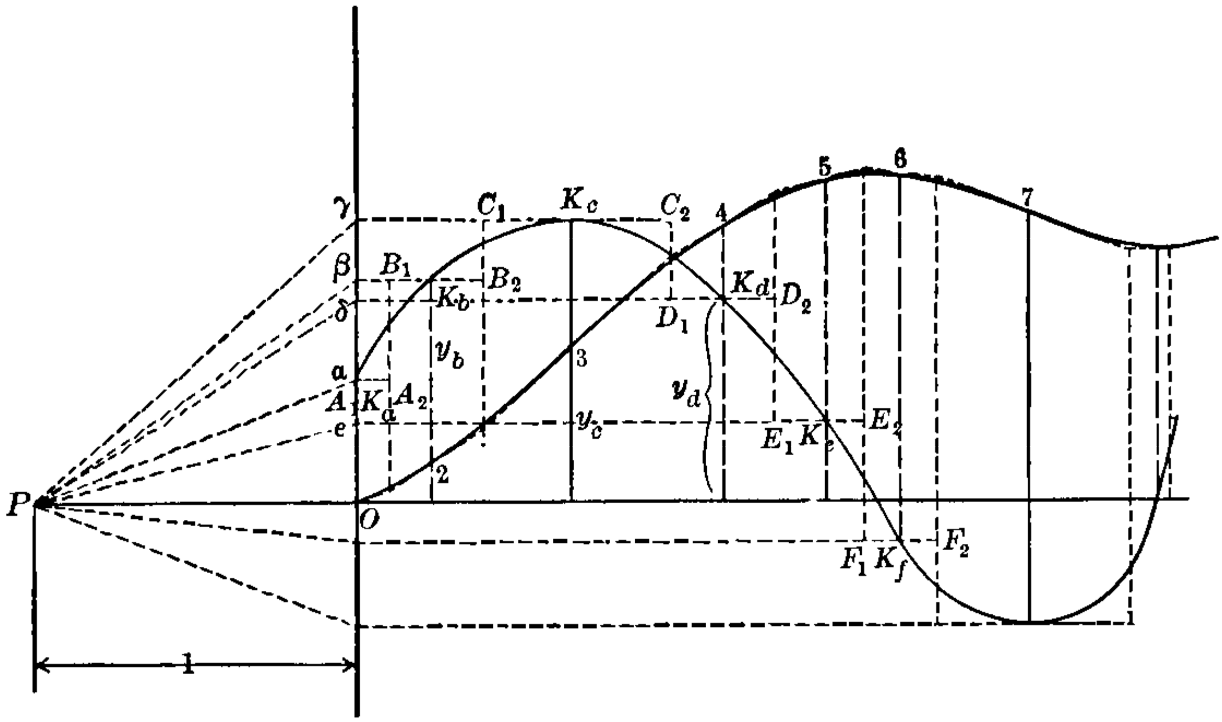


FIG. 73.

To construct the broken line we draw a parallel to $P\alpha$ through the point $x = x_1$ (in Fig. 73 x_1 is equal to 0) as far as the vertical $x = x_2$. Through the point of intersection with the vertical $x = x_2$ we draw a parallel to $P\beta$ as far as the vertical $x = x_3$. Through the point of intersection with the vertical $x = x_3$ we draw a parallel to $P\gamma$ and so on.

Finally let us consider the case of an arbitrary function $y = f(x)$ represented by any curve. In order to find the curve

$$Y = \int_a^x f(x)dx$$

we substitute for $y = f(x)$ a function consisting of different constant values in different intervals and changing its value abruptly when x passes from one interval to the next, so that the line representing this function consists of a number of steps leading up or down according to the increase or decrease of $f(x)$. These steps are arranged in the following way. The horizontal part A_1A_2 of the first step (Fig. 73) starts from any point A_1 of the given curve. The vertical part A_2B_1 and the following horizontal part B_1B_2 are then drawn in such a manner that B_1B_2 intersects the curve and that the integral of the given function as far as the point of intersection K_b is equal to the integral of the stepping line as far as the same point. That is to say, the areas between the stepping line and the given curve on both sides of the vertical part A_2B_1 have to be equal. When K_b is fixed the right position of A_2B_1 may be found by eye estimate. The eye is rather sensitive for differences of small areas. Besides a shift of A_2B_1 to the right or to the left enlarges one area and diminishes the other so that even a slight deviation from the correct position makes itself felt. In the same way the next step $B_2C_1C_2$ is drawn with its vertical part B_2C_1 in such a position that the areas on both sides are equal. The integral of the given curve as far as K_c will again have the same value as that of the stepping line as far as K_c. And so on for the other steps. The integral of the stepping line is constructed in the way shown. It is represented by a broken line beginning at the foot of the ordinate of A_1. The corners lie on the vertical parts of the steps or their prolongations. It is readily seen that the broken line consists of a series of tangents of the integral curve

$$Y = \int_a^x f(x)dx,$$ [1]

and that their points of contact with the integral curve lie on the same verticals as the points A_1, K_b, K_c, etc. (In Fig. 73 these points are denoted 0, 2, 3, $\cdots$.) That these points lie on the integral curve follows from the arrangement of the steps which make the integral of the given function at $K_b, K_c, \cdots$ equal to the integral of the stepping line. Now in the points A_1, K_b, K_c $\cdots$ the ordinates of the given curve coincide with those of the stepping line. Hence both integral lines must for these abscissas have the same direction.

[1] In Fig. 73 the lower limit is 0.

Having constructed the broken line and marked the points 2, 3, 4, ⋯ (Fig. 73), the integral curve is drawn with a curved ruler so as to touch the broken line in the points, 0, 2, 3, ⋯. As the given curve does not change its ordinate abruptly the integral curve does not change its direction abruptly. The drawing shows how well the integral curve is determined by the broken line. There is practically no choice in drawing it any other way without violating the conditions.

The ordinate of the integral curve is measured in the same unit as the ordinate of the given curve $y = f(x)$. It may sometimes be convenient to draw the ordinates of the integral curve in a scale different from that of the ordinates of the given curve. For instance the value of the integral may become so large that measured in the same unit the ordinates of the integral curve would pass the boundaries of the drawing board, or else they may be so small that their changes cannot be measured with sufficient accuracy. In the first case the scale is diminished, in the latter case it is enlarged. This is done by altering the position of the point P, the center of the pencil of rays that define the directions of the broken line. If P approaches O the directions $P\alpha$, $P\beta$, ⋯ become steeper to the same degree as if keeping P unchanged we had increased the ordinates of A_1A_2, B_1B_2, ⋯ in the inverse proportion of the two distances PO. Hence by diminishing the distance PO the ordinates of the resulting broken line are enlarged in the inverse proportion. On the other hand, by increasing the distance PO the ordinates of the resulting broken line are diminished in the inverse proportion of the distances, because the change of the directions $P\alpha$, $P\beta$, ⋯ caused by a longer distance PO is the same as if the ordinates of A_1A_2, B_1B_2, ⋯ were diminished in the inverse proportion. The broken line constructed by means of the longer distance $P'O$ will therefore be the same as if the ordinates of the stepping line were diminished. It therefore leads to an integral curve whose ordinates are diminished in the same proportion (Fig. 74).

The graphical integration of

$$Y = \int_a^x f(x)dx$$

is not limited to values $x > a$. The method is just as well applicable to the continuation of the integral curve for $x < a$. The

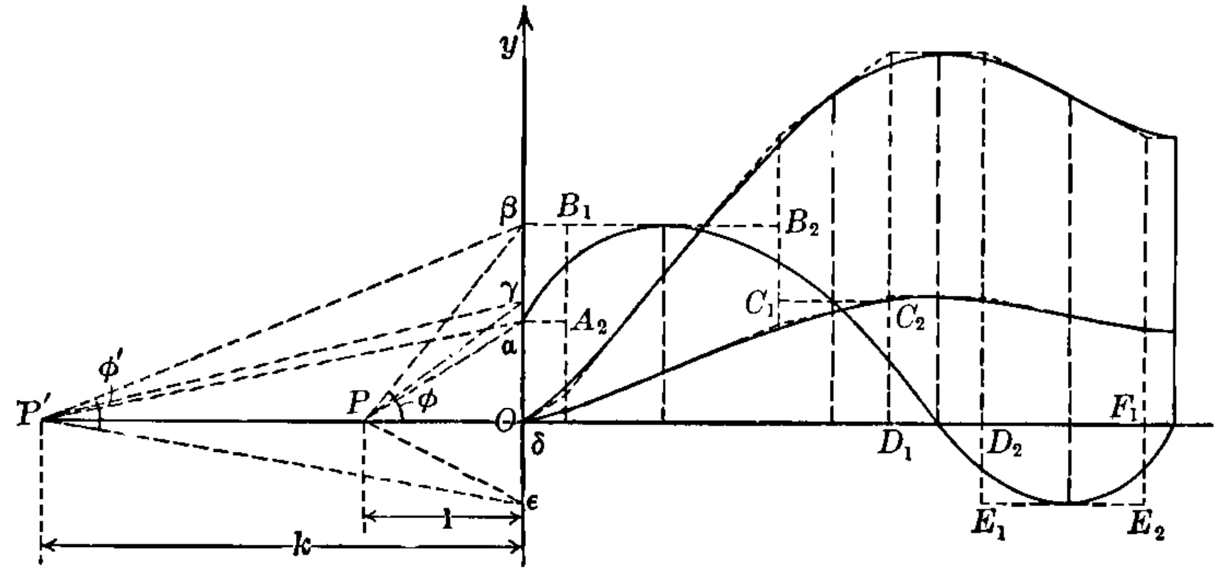


Fig. 74.

steps have only to be drawn from right to left. The lower limit a determines the point where the integral curve intersects the axis of x.

There is a method for the construction of the vertical parts of the steps, which may in some cases be useful, though as a rule we may dispense with it and fix their position by estimation.

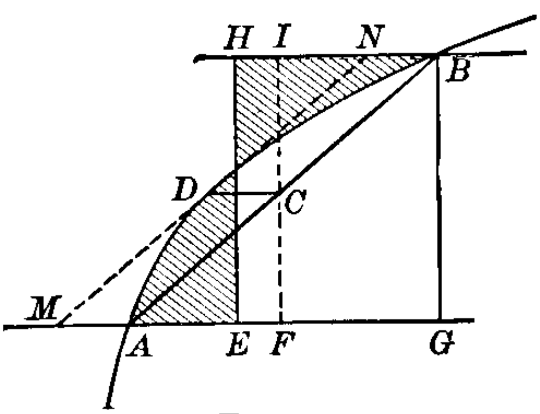


Fig. 75.

Suppose that A and B (Fig. 75) are two points where the curve is intersected by the horizontal parts of two consecutive steps and that the curve between A and B is a parabola whose axis is parallel to the axis of x. The position of the vertical part of the step between A and B can be then found by a simple construction. Through the center C of the chord AB (Fig. 75) draw a parallel CD to the axis of x, D being the point of intersection with the parabola. The vertical part EH of the step intersects CD in a point whose distance from C is twice the distance from D. That this is the right position of EH is shown as soon as we can prove that the area $ADBGA$ is equal to the rectangle $EHBG$. The area $ADGBA$ can be divided in two parts, the triangle ABG and the part $ADBCA$ between the curve and the chord. The triangle is equal to the rectangle $FIBG$, while $ADBCA$ is equal to two thirds of the parallelogram $MNBA$, and hence equal to the rectangle $EHIF$. Both together are therefore equal to the rectangle $EHBG$, and the two areas between the stepping line and the curve on both sides of EH are thus equal.

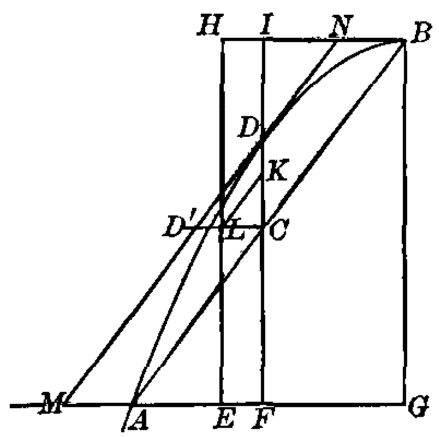


FIG. 76.

If the curve between A and B is supposed to be a parabola with its axis parallel to the axis of ordinates the construction has to be modified a little. Through the center C of the chord AB (Fig. 76) draw a vertical line CD as far as the parabola. On CD find the point K whose distance from C is double the distance from D and draw through it a parallel to the chord AB. This parallel intersects a horizontal line through C at a point L. Then EH must pass through L. This may be shown in the following way. The area between the parabola ADB and the chord AB is equal to two thirds of the parallelogram $MNBA$, MN being the tangent to the parabola at the point D. If D' is the point of intersection of NN and the horizontal line through C, we have evidently

$$CL = \tfrac{2}{3}CD'.$$

Therefore the rectangle $EHIF$ is equal to the area $ADBA$ between the parabola and the chord and $EHBG$ is equal to $ADGBA$.

Any part of a curve can be approximated by the arc of a parabola with sufficient accuracy if the part to be approximated is sufficiently small. When the direction of the curve is nowhere parallel to the axis of coördinates, both kinds of parabolas may be used for approximation, those whose axes are parallel to the axis of x and those whose axes are parallel to the axis of y. But when the direction in one of the points is horizontal (Fig. 76), we can only use those with vertical axes and when the direction in one of the points is vertical we can only use those with horizontal axes. Accordingly we have to use either of the two constructions to find the position of the vertical part of the step.

Do not draw your steps too small. For, although the difference between the broken line and the integral curve becomes smaller, the drawing is liable to an accumulation of small errors owing to the considerable number of corners of the broken line and little errors of drawing committed at the corners. Only practical experience enables one to find the size best adapted to the method.

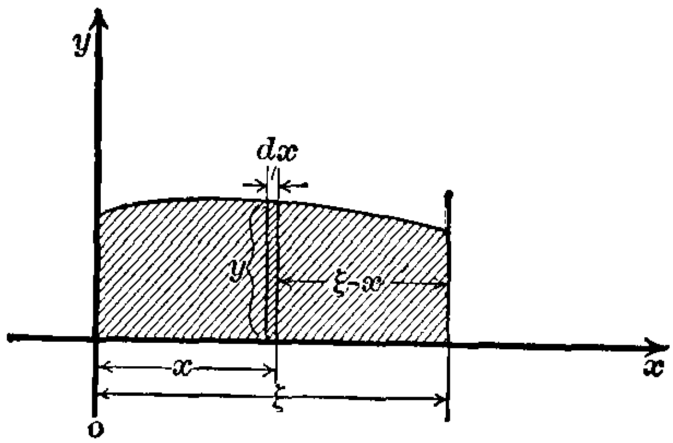


FIG. 77.

Statical moments of areas may be found by a double graphical integration. Let us consider the area between the curve $y = f(x)$ (Fig. 77), the axis of x and the ordinates corresponding to $x = 0$ and $x = \xi$. The statical moment with respect to the vertical through $x = \xi$ is the integral of the products of each element ydx and its distance $\xi - x$ from the vertical

$$M = \int_0^\xi (\xi - x)ydx.$$

Let us regard M as a function of ξ and differentiate it:

$$\frac{dM}{d\xi} = ((\xi - x)y)_{x=\xi} + \int_0^\xi \frac{d}{d\xi}(\xi - x)ydx$$
$$= 0 + \int_0 ydx.$$

That is to say, a graphical integration of the curve $y = f(x)$ beginning at $x = 0$ furnishes the curve whose ordinate is

$$\frac{dM}{d\xi}.$$

Hence a second integration of this latter curve will furnish the curve M as a function of ξ. As M vanishes for $\xi = 0$ the second integration must also begin at the abscissa $x = 0$.

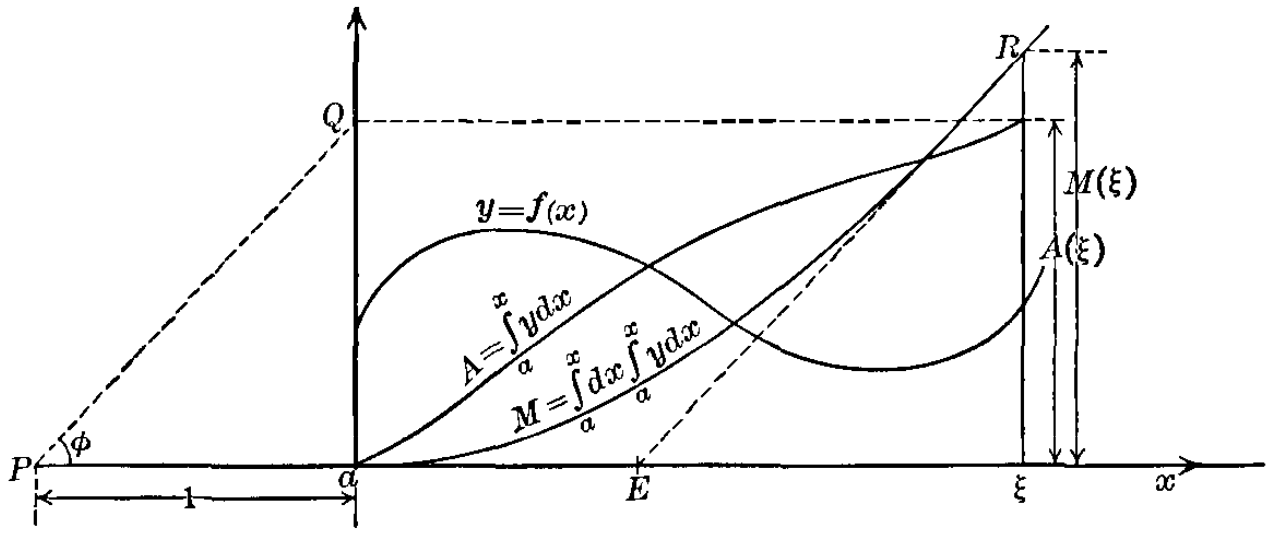


FIG. 78.

Fig. 78 shows an example. Each ordinate of the curve found by the second integration is the statical moment of the area on the left side of it with respect to the vertical through this same ordinate. The ordinate furthest to the right is the statical moment of the whole area with respect to the vertical on the right. The statical moment of the whole area with respect to a vertical line through any point x_1 is the integral

$$\int_0^\xi (x_1 - x)ydx.$$

Considered as a function of x_1 its differential coefficient is

$$\int_0^\xi \frac{d}{dx_1}(x_1 - x)ydx = \int_0^\xi ydx.$$

That is to say, the differential coefficient is independent of x_1, hence the statical moment is represented by a straight line. As its differential coefficient is represented by a horizontal line through the last point on the right of the curve

$$\int_0^\xi ydx,$$

the direction of the straight line is found by drawing a line through P and through the point of intersection Q of the horizontal line and the axis of ordinates (Fig. 78). The position of the straight line is then determined by the condition that

$$\int_0^\xi (x_1 - x)y\,dx$$

for $x_1 = \xi$ is equal to the statical moment

$$M(\xi) = \int_0^\xi (\xi - x)y\,dx.$$

We have therefore only to draw a parallel to PQ through the last point R of the curve for $M(\xi)$ found by the second integration. The ordinates of this straight line for any abscissa x_1 represent the values of

$$\int_0^\xi (x_1 - x)y\,dx$$

measured in the unit of length of the ordinates. The point of intersection E with the axis of x determines the position of the vertical in regard to which the statical moment is zero, that is to say, the vertical through the center of gravity.

The moment of inertia of the area

$$\int_0^\xi y\,dx$$

about the axis $x = \xi$ is found in a similar way. It is expressed by the integral

$$T = \int_0^\xi (\xi - x)^2 y\,dx.$$

Considered as a function of ξ we find by differentiation

$$\begin{aligned}\frac{dT}{d\xi} &= [(\xi - x)^2 y]_{x=\xi} + \int_0^\xi \frac{d}{d\xi}(\xi - x)^2 y\,dx \\ &= 0 + 2\int_0^\xi (\xi - x)y\,dx.\end{aligned}$$

That is to say, the differential coefficient is equal to double the statical moment about the same axis. This holds for every value of ξ. Hence we obtain $\frac{1}{2}T$ as a function of ξ by integrating the curve for $M(\xi)$. For $\xi = 0$ we have $T = 0$, so that the curve begins on the axis of x at $\xi = 0$.

The integral

$$\int_a^x ydx$$

is zero for $x = a$. The curve representing the integral has to intersect the axis of x at $x = a$ (admitting values of $x > a$ and $x < a$), and it is there that we begin the construction of the broken line. If instead we begin it at the point $x = a$, $y = c$, the only difference is that the whole integral curve is shifted parallel to the axis of ordinates by an amount equal to c upwards if c is positive, downwards if it is negative. But the form of the curve remains the same. It is different when this curve is integrated a second time. For instead of

$$\int_a^x ydx$$

we now integrate

$$\int_a^x ydx + c.$$

The ordinate of the integral curve is therefore changed by an amount equal to $c(x - a)$ and besides if the second integral curve is begun at $x = a$, $y = c_1$ instead of $x = a$, $y = 0$ the change amounts to

$$c(x - a) + c_1,$$

so that the difference between the ordinates of the new integral curve and the ordinates of the straight line

$$y = c(x - a) + c_1$$

is equal to the ordinates of the first integral curve (Fig. 79).

This effect of adding a linear function to the ordinates of the integral curve is also attained by shifting the pole P upward or downward. For it evidently comes to the same thing whether the curve to be integrated is shifted upward by the amount c or whether the point P is moved downward by the same amount, so that the relative position of P and the curve to be integrated is the same as before. Changing the ordinate of P by $-c$ adds

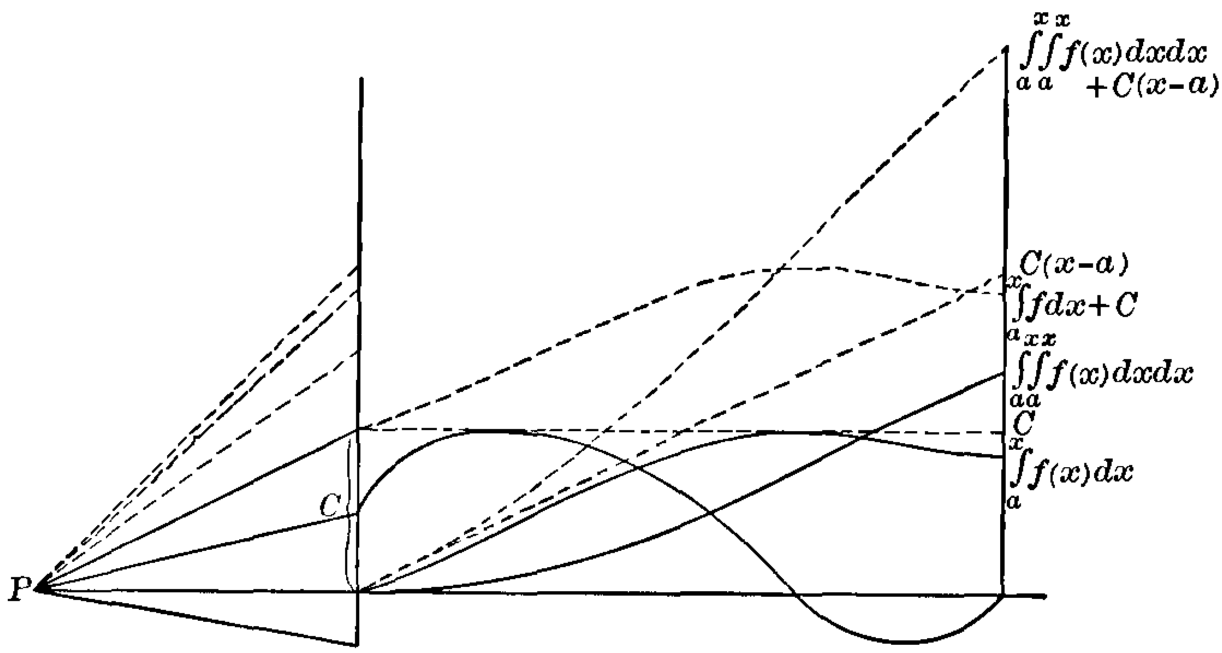


FIG. 79.

$c(x-a)$ to the ordinates of the integral curve. $c(x-a)$ is the ordinate of a straight line parallel to the straight line from the new position of P to the origin.

By this device of shifting the position of P upward or downward the integral curve may sometimes be kept within the boundaries of the drawing without any reduction of the scale of ordinates. A good rule is to choose the ordinate of P about equal to the mean ordinate of the curve to be integrated. The ordinates of the integral curve will then be nearly the same at both ends. The value of the integral

$$\int_a^x ydx$$

is equal to the difference between the ordinates of the integral curve and the ordinates of a straight line parallel to PO through the point of the integral curve whose abscissa is a.

When the ordinate of P is accurately equal to the mean ordinate of the curve to be integrated for the interval $x = a$ to b the ordinates of the integral curve will be accurately the same at the two ends. But we do not know the mean ordinate before having integrated the curve.

After having integrated we find the mean ordinate for the interval $x = a$ to b by drawing a straight line through P parallel to the chord AB of the integral curve, A and B belonging to the abscissas $x=a$ and $x=b$. This line intersects the axis of ordinates at a point whose ordinate is the mean ordinate.

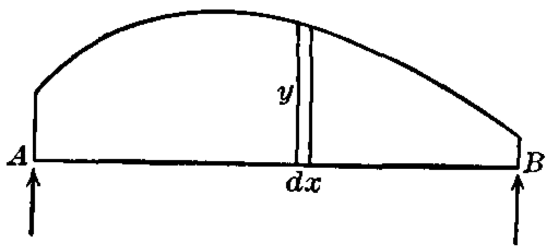


FIG. 80.

Suppose a beam AB is supported at both ends and loaded by a load distributed over the beam as indicated by Fig. 80. That is to say, the load on dx is measured by the area ydx. Let us integrate this curve graphically, beginning at the point A with P on the line AB. The final ordinate at B

$$\int_a ydx$$

gives the whole load and is therefore equal to the sum of the two reactions at A and B that equilibrate the load. Integrating this curve again we obtain the curve whose ordinate is equal to

$$\int_a^\xi Ydx,$$

Y being written for

$$\int_a ydx$$

The ordinate of this curve at any point $x = \xi$ represents the statical moment of the load between the verticals $x = a$ and $x = \xi$ about the axis $x = \xi$. Its final ordinate BM, Fig. 81, is the moment of the whole load about the point B, and as the reactions equilibrate the load it must be equal to the moment of the reactions about the same point and therefore opposite to the moment of the reaction at A about B. If the reaction at A is denoted by F_a we therefore have

$$F_a(b - a) = \int_a^b Y dx.$$

That is to say, F_a is equal to the mean ordinate of the curve

$$Y = \int_a^\xi y dx$$

in the interval $x = a$ to b. The mean ordinate is found by drawing a parallel to AM through P which intersects the vertical through A at the point F so that $AF = F_a$. As DB is equal to

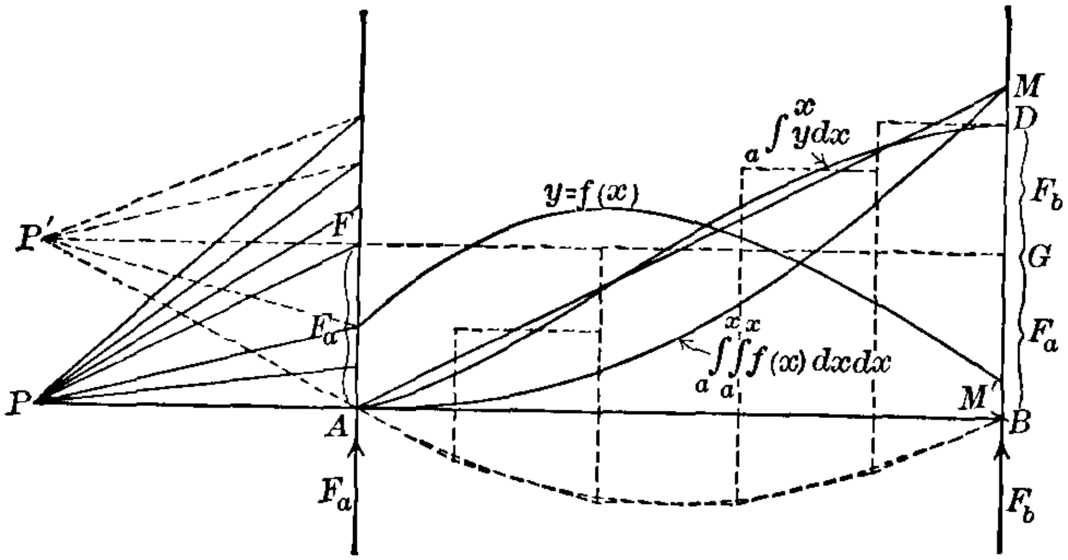


FIG. 81.

the sum of the two reactions a horizontal line through F will divide BD into the two parts $BG = F_a$ and $GD = F_b$.

Shifting the position of P to P' on the horizontal line FG and repeating the integration

$$\int_a^\xi Y dx,$$

we obtain a curve with equal ordinates at both ends. If we begin at A it must end in B. Its ordinates are equal to the difference between the ordinates of the chord AM and the curve AM (Fig. 81), and represent the moment about any point of the beam of all the forces on one side of the point (load and reaction).

The area of a closed curve may be found by integrating over the whole boundary. Suppose $x = a$ and $x = b$ to be the limits of the abscissas of the closed curve, the vertical $x = a$ touching the curve at A and the vertical $x = b$ at B (Fig. 82). By A and B the closed curve is cut in two, both parts connecting A and B. Let us denote the upper part by $y = f_1(x)$ and the lower part by $y = f_2(x)$. The whole area is then equal to the difference

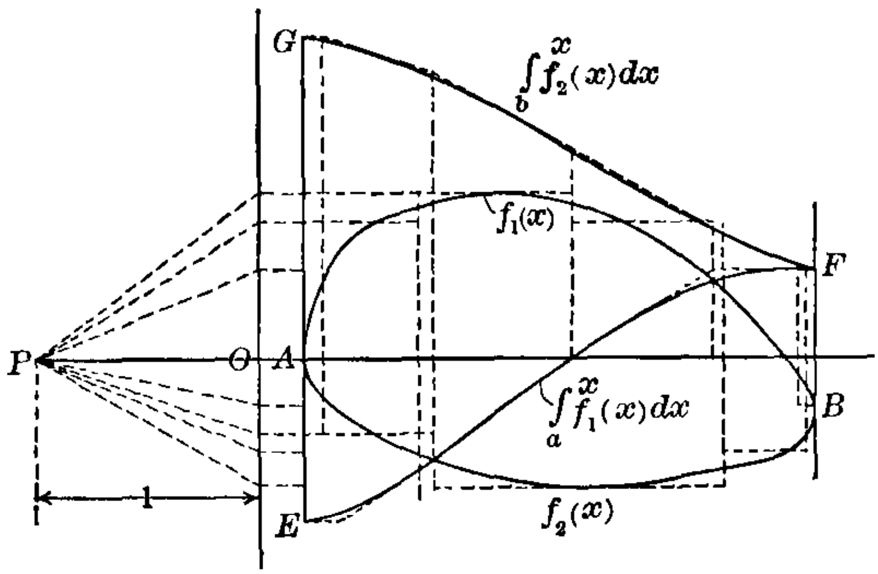


FIG. 82.

$$\int_a^b f_1(x)dx - \int_a^b f_2(x)dx,$$

or equal to

$$\int_a^b f_1(x)dx + \int_b^a f_2(x)dx.$$

We begin the integral curve over the upper part at the vertical $x = a$ at a point E, the ordinate of which is arbitrary, and draw the broken line as far as F on the vertical $x = b$ (Fig. 82). Then we integrate back again over the lower part, continuing the broken line from F to G. The line EG measured in the unit of length set down for the ordinates is equal to the area measured in units of area, this unit being a rectangle formed by PO and the unit of ordinates. That is to say, the area is equal to the area of a rectangle whose sides are PO and EG.

The method is not limited to the case drawn in Fig. 82, where the closed curve intersects any vertical not more than twice. A more complicated case is shown in Fig. 83. But in all those cases

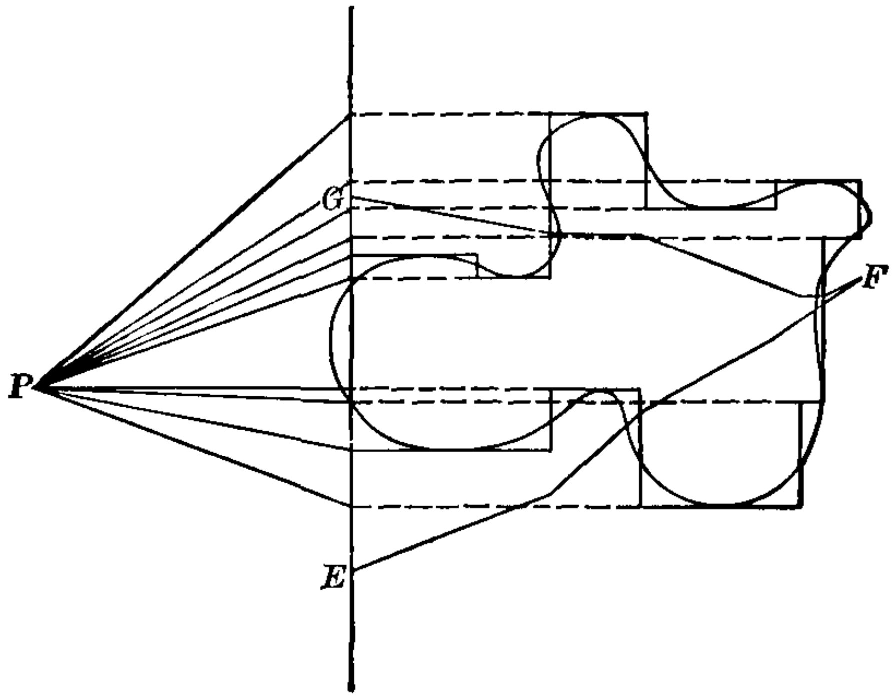


FIG. 83.

where the object is not to find the integral curve but only to find the value of the last ordinate the method, cannot claim to be of much use, because it cannot compete with the planimeter.

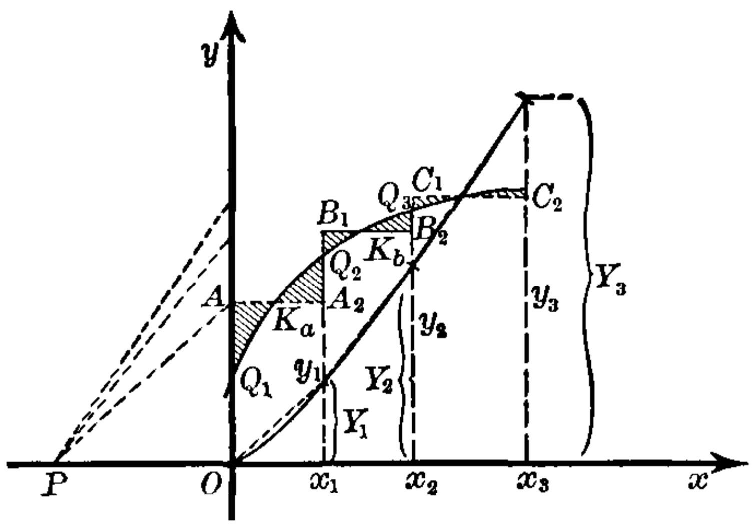


FIG. 84.

For the construction of the broken line we have drawn the steps in such a manner that the areas on both sides of the vertical part of a step between the curve and the stepping line are equal.

It would have also been admissible to construct the stepping line in such a way that the areas on both sides of the *horizontal* part of a step are equal (Fig. 84). Only the broken line would consist of a series of chords instead of a series of tangents of the integral curve. The points K_a, K_b, $\cdots$, where the horizontal parts of the steps intersect the curve would determine the abscissas of the points of the integral curve, where its direction is parallel to the direction of the broken line. But this forms very little help for drawing the integral curve. That is the reason why the former method where the broken line consists of a series of tangents is to be preferred. However where the object is only to find the last ordinate of the integral curve the two methods are equivalent.

§ 14. *Graphical Differentiation.*—The graphical differentiation of a function represented by a curve is not so satisfactory as the graphical integration because the values of the differential coefficient are generally not very well defined by the curve. The operation consists in drawing tangents to the given curve and drawing parallels through P to the tangents (Fig. 85). The points of intersection of these parallels with the axis of ordinates furnish the ordinates of the curve representing the derivative.

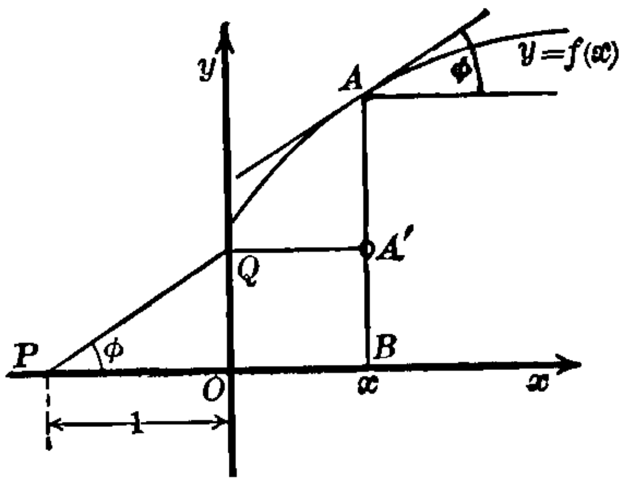


FIG. 85.

The abscissa to each ordinate coincides with the abscissa of the point of contact of the corresponding tangent. The principal difficulty is to draw the tangent correctly. As a rule it can be recommended to draw a tangent of a given direction and then mark its point of contact instead of trying to draw the tangent for a given point of contact. A method of finding the point of contact more accurately than by mere inspection consists in drawing a number of chords parallel to the tangent and to bisect them. The points of bisection form a curve that intersects the given curve at the point of contact (Fig. 86). When a number of tangents are drawn, their points of contact marked and the points representing the differential coefficient constructed, the derivative curve has to be drawn through these points. This may be done more accurately by means of the stepping line. The horizontal parts of the steps pass through the points while the vertical parts lie in the same vertical as the point of intersection of two consecutive tangents. The derivative curve connects the points in such a way that the areas between it and the stepping line are equal on both sides of the vertical parts of each step. Thus the result of the graphical differentiation is exactly the same

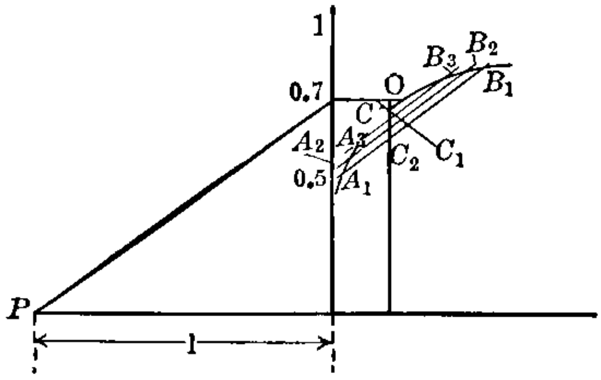


FIG. 86.

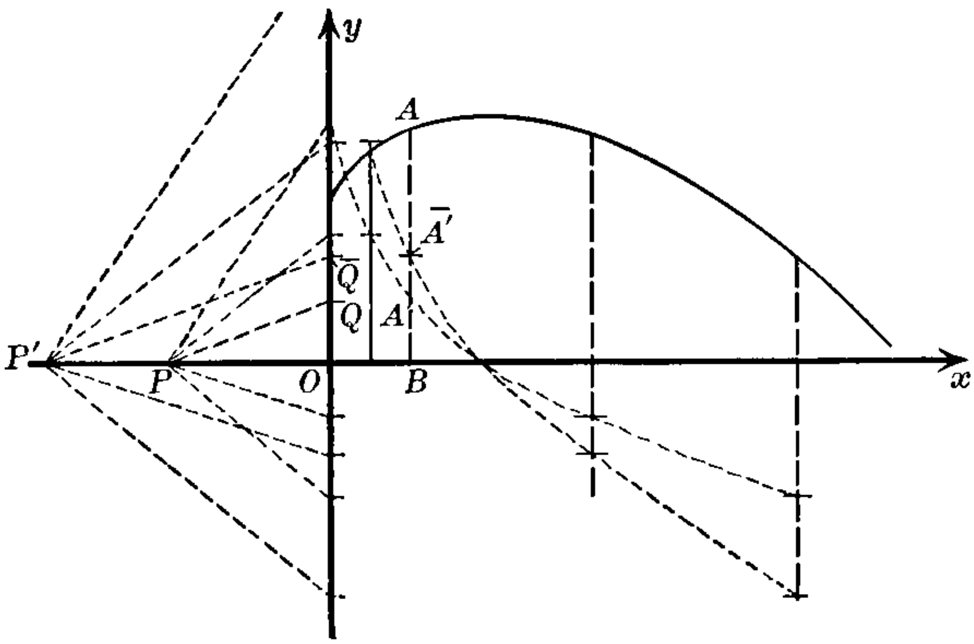


FIG. 87.

figure that we get by integration, only the operations are carried out in the inverse order.

A change of the distance PO (Fig. 87) changes the ordinates of the derivative curve in the same proportion and for the same reason that it changes the ordinates of the integral curve when we are integrating, but in the inverse ratio. Any change of the ordinate of P only shifts the curve up or down by an equal amount, so that if we at the same time change the axis of x and draw it through the new position of P the ordinates of the curve will remain the same and will represent the differential coefficient.

When a function $f(x, y)$ of two variables is given by a diagram showing the curves $f(x, y) =$ const. for equidistant values of $f(x, y)$ the partial differential coefficients can be found at any point x_0, y_0 by means of drawing curves whose ordinates represent $f(x, y_0)$ to the abscissa x or $f(x_0, y)$ to the abscissa y and applying the methods explained above. For this purpose a parallel is drawn to the axis of x, for instance, through the point x_0, y_0 and at the points where it intersects the curves $f(x, y) =$ const. ordinates are erected representing the values of $f(x, y_0)$ in any convenient scale. A smooth curve is then drawn though the points so found and the tangent of the curve at the point x_0 furnishes the differential coefficient $\partial f/\partial x$ for $x = x_0$, $y = y_0$.

The differential coefficients $\partial f/\partial x$, $\partial f/\partial y$ are best represented graphically by a straight line starting from the point x, y to which the differential coefficients correspond, and of such length and direction that its orthogonal projections on the axis of x and y are equal to $\partial f/\partial x$ and $\partial f/\partial y$. This line represents the gradient of the function $f(x, y)$ at the point x, y.[1] It is normal to the curve $f(x, y) =$ const. that passes through the point x, y, its direction being the direction of steepest ascent. Its length measures the slope of the surface $z = f(x, y)$ in the direction of steepest ascent. This is shown by considering the slope in any other direction. Let us change x and y by

$$r \cos \alpha, \quad r \sin \alpha$$

and consider the corresponding change

$$\Delta z = f(x + r \cos \alpha, y + r \sin \alpha) - f(x, y)$$

of the function. By Taylor's theorem we can write it

[1] See Chap. II, § 10.

$$\frac{\partial f}{\partial x} r \cos \alpha + \frac{\partial f}{\partial y} r \sin \alpha + \text{terms of higher order in } r,$$

α is the direction from the point x, y to the new point $x + r \cos \alpha$, $y + r \sin \alpha$ and r is the distance of the two points. Dividing Δz by r and letting r approach to zero we find

$$\lim \frac{\Delta z}{r} = \frac{\partial f}{\partial x} \cos \alpha + \frac{\partial f}{\partial y} \sin \alpha.$$

This expression measures the slope of the surface $z = f(xy)$ in the direction α. Now let us introduce the length l and the angle λ of the gradient, and write

$$\frac{\partial f}{\partial x} = l \cos \lambda, \quad \frac{\partial f}{\partial y} = l \sin \lambda.$$

Then we have

$$\frac{\partial f}{\partial x} \cos \alpha + \frac{\partial f}{\partial y} \sin \alpha = l \cos (\alpha - \lambda).$$

That is to say, the slope in any direction α is proportional to $\cos (\alpha - \lambda)$, it is a maximum in the direction of the gradient $(\alpha = \lambda)$ and zero in a direction perpendicular to it and negative in all directions that form an obtuse angle with it. When all three coördinates are measured in the same unit, the length of l measured in this unit is equal to the tangent of the angle of steepest ascent. Hence the length of the gradient varies with the unit of length. When the unit of length in which the values of $f(xy)$ are plotted is kept unaltered, while we change the unit of length corresponding to the values x and y, the length of the gradient varies with the square of the unit of length.

§ 15. *Differential Equations of the First Order.*—In the problem of solving a differential equation of the first order

$$\frac{dy}{dx} = f(x, y)$$

by graphical methods the first question is how to represent the differential equation graphically. If x and y are meant to be the values of rectangular coördinates, the geometrical meaning of the differential equation is that at every point x, y, where $f(x, y)$ is defined, the equation prescribes a certain direction for the curve that satisfies it. Let us suppose curves drawn through all those points for which $f(x, y)$ has certain constant values. Each curve then corresponds to a certain direction or the opposite direction. Let us distinguish the curves by different numbers or letters and let us draw a pencil of rays together with the curves and mark the rays with the same numbers or letters in such a way that each of them shows the direction corresponding to the

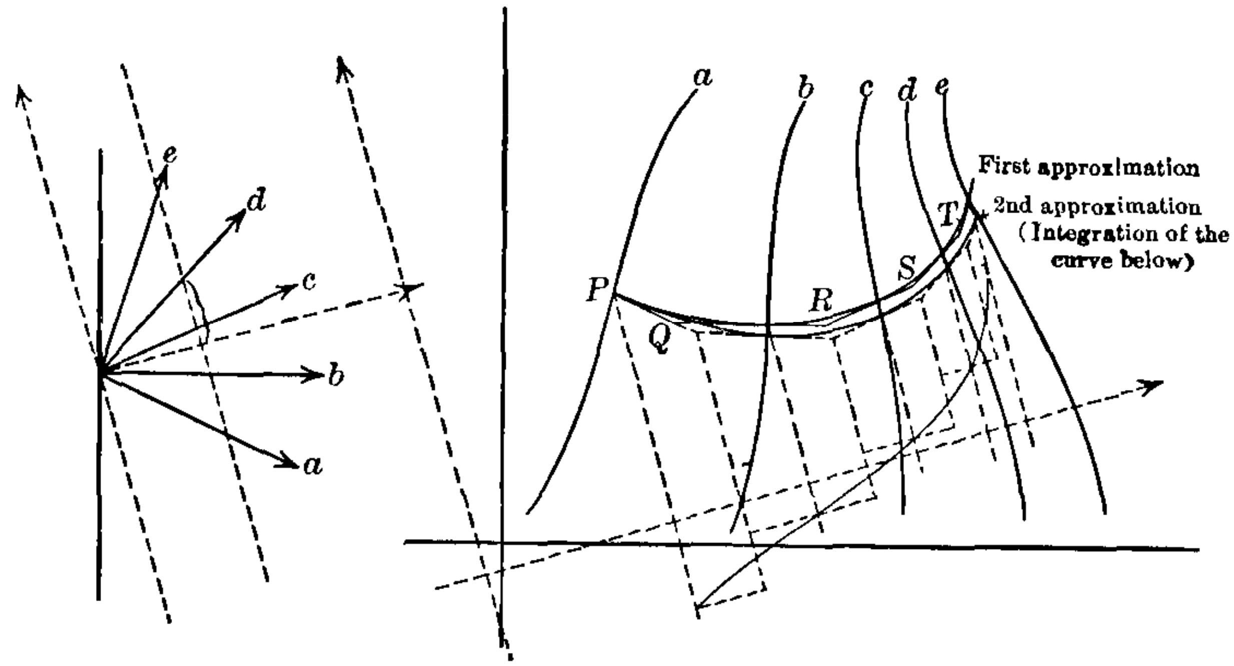


FIG. 88.

curve marked with that particular number or letter (Fig. 88). Our drawing of course only comprises a certain region in which we propose to find the curves satisfying the differential equation. It may be that $f(xy)$ is defined beyond the boundaries of our drawing. Those regions have to be dealt with separately.

The graphical representation of the differential equation in the region considered consists in the correspondence between the curves and the rays. It is important to observe that this representation is independent of the system of coördinates by means of which we have deduced the curves from the equation

$$\frac{dy}{dx} = f(xy).$$

We can now introduce any system of coördinates ξ, η and find from our drawing the equation

$$\frac{d\eta}{d\xi} = \varphi(\xi\eta),$$

that is to say, we can find the value of $\varphi(\xi, \eta)$ at any point ξ, η of our drawing. If, for instance, the unit of length is the same for ξ and η we draw a line through the center of the pencil of rays in the direction of the positive axis of ξ and a line perpendicular to it at the distance 1 from the center. The segment on the second line between the first line and the point of intersection with one of the rays measured in units of length and counted positive in the direction of positive η furnishes the value of $\varphi(\xi, \eta)$ for all the points ξ, η corresponding to that particular ray. In this respect the graphical representation of a differential equation is superior to the analytical form, in which certain coördinates are used and the transformation to another system of coördinates requires a certain amount of calculation.

Now let us try to find the curve through a given point P on the curve marked (a) (Fig. 88) that satisfies the differential equation. We begin by drawing a series of tangents of a curve that is meant to be a first approximation. Through P we draw a parallel to the ray (a) as far as the point Q somewhere in the middle between the curves (a) and (b). Through Q we draw a parallel to the ray (b) as far as R somewhere in the middle between the curves (b) and (c). Through R we again draw a parallel to the ray (c) and so on. The curve touching this broken line at the points of intersection with the curves (a), (b), $\cdots$ is a first approximation. But we need not draw this curve. In order to find a better approximation we introduce a rectangular system of coördinates x, y, laying the axis of x somewhat in the mean direction of the broken line. Let us denote by y_1 the function of x that corresponds to the curve forming the first approximation. The second approximation y_2 is then obtained as an integral curve of $f(x, y_1)$, that is, of dy_1/dx

$$y_2 = y_p + \int_{x_p}^{x} f(x, y_1)dx,$$

denoting by x_p, y_p, the coördinates of P. For this purpose the curve whose ordinates are equal to $f(x, y_1)$ or dy_1/dx has to be constructed first. The values of $f(x, y_1)$ are found immediately at the points where the first approximation intersects the curve (a), (b) $\cdots$ by differentiation in the way described above. A line is drawn through the center of the pencil of rays parallel to the axis of x and a line perpendicular to it at a convenient distance from the center. This distance is chosen as the unit of length. The points of intersection of this line with the rays determine segments whose lengths are equal to the values of $f(x, y_1)$ on the corresponding curves. These values are plotted as ordinates to the abscissas of the points where the first approximation intersects the curves (a), (b), $\cdots$ and a curve

$$Y = f(x, y_1)$$

is drawn (Fig. 88). This curve is integrated graphically beginning at the point P and the integral curve is a second approximation. Again we need not draw the curve. The broken line suffices, if we intend to construct a third approximation. In this case we have to repeat the foregoing operation. This can now be performed much quicker than in the first case because the values of $f(x, y)$ on the curves (a), (b), $\cdots$ have already been constructed and are at our disposal. In order to find the curve

$$Y = f(x, y_2)$$

we have only to shift the same ordinates to new abscissas and make these coincide with the abscissas of the points where the second approximation intersects the curves (a), (b), $\cdots$. The curve

$$Y = f(x, y_2)$$

is then drawn and integrated graphically, beginning at the point P.

Suppose now the integral curve did not differ from the second approximation, it would mean that

$$y_2 = y_p + \int_{x_p}^{x} f(x, y_2)dx,$$

or that

$$\frac{dy_2}{dx} = f(x, y_2),$$

that is to say, that y_2 satisfies the differential equation.

If there is a perceptible difference the integral curve represents a third approximation. It has been shown by Picard that proceeding in this way we find the approximations (under a certain condition to be discussed presently) converging to the true solution of the differential equation, so that after a certain number of operations the error of the approximation must become imperceptible.

Denoting by y_n the function of the nth approximation we have

$$y_{n+1} = y_p + \int_{x_p}^{x} f(x, y_n)dx.$$

The true solution with the same initial conditions $y = y_p$ for $x = x_p$ satisfies the equation

$$y = y_p + \int_{x_p}^{x} f(x, y)dx.$$

Hence

$$y_{n+1} - y = \int_{x_p}^{x} [f(x, y_n) - f(x, y)]dx,$$

or

$$y_{n+1} - y = \int_{x_p}^{x} \frac{f(x, y_n) - f(x, y)}{y_n - y}(y_n - y)dx.$$

Let us now suppose that the absolute value of

$$\frac{f(x, y_n) - f(x, y)}{y_n - y},$$

for all the values of x, y, y_n within the considered region does not surpass a certain limit M, then it follows that a certain relation must exist between the maximum error of y_n, which we denote by e_n and the maximum error of y_{n+1}, which we denote by e_{n+1}. The absolute value of the integral not being larger than

$$Me_n \mid x - x_n \mid$$

($\mid x - x_n \mid$ denoting the absolute value of $x - x_n$) we have

$$e_{n+1} \leqq M \mid x - x_n \mid e_n.$$

Hence as long as the distance $x - x_n$ over which the integration is performed is so small that

$$M \mid x - x_n \mid \leqq k < 1,$$

k being a constant smaller than one, the error of y_{n+1} cannot be larger than a certain fraction of the maximum error of y_n. But in the same way it follows that the error of y_n cannot be larger than the same fraction of the maximum error of y_{n-1}, and so on, so that

$$e_{n+1} \leqq ke_n \leqq k^2 e_{n-1} \cdots \leqq k^n e_1.$$

But as e_1 is a constant and k a constant smaller than one, $k^n e_1$ must be as small as we please for a sufficient large value of n. That is to say, the approximations converge to the true solution.

M being a given constant the condition of convergence

$$M \mid x - x_p \mid \leqq k < 1$$

limits the extent of our integration in the direction of the axis of x. But it does not limit our progress. From any point P' that we have reached with sufficient accuracy we can make a fresh start, choosing a new axis of x suited to the new situation. As a rule it does not pay to trouble about the value of M and to try to find the extent of the convergence by the help of this value. The actual construction of the approximations will show clearly enough how far to extend the integration. As far as two consecutive approximations show no difference they represent the true curve.

Suppose that

$$\frac{f(x, y_n) - f(x, y)}{y_n - y}$$

has the same sign for all values x, y, y_n concerned. Say it is negative. Suppose further that $y_n - y$ is of the same sign for the whole extent of the integration

$$y_{n+1} - y = \int_{x_p}^{x} \frac{f(x, y_n) - f(x, y)}{y_n - y} (y_n - y) dx;$$

that is to say, the approximative curve y_n is all on one side of the true curve. Then if $x - x_p$ is positive, $y_{n+1} - y$ must evidently be of the opposite sign from $y_n - y$, or the approximative curve y_{n+1} is all on the other side of the true curve from y_n. For these and all following approximations the true curve must lie between two consecutive approximations. If the first approximation y_1 is all on one side of the true curve the theorem holds for any two consecutive approximations. This is very convenient for the estimation of the error.

In Fig. 88

$$\frac{f(x, y_n) - f(x, y)}{y_n - y}$$

is negative from the point P as far as somewhere near S. The first approximation is all on the upper side of the true curve. Therefore the second approximation must be below the true curve at least as far as somewhere near S.

When the sign is positive the same theorem holds for negative values of $x - x_p$. If the integration has been performed in the positive direction of x, it may be a good plan to check the result by integrating backwards, starting from a point that has been reached and to try if the curve gets back to the first starting point. In this direction we profit from the advantage of the true curve lying between consecutive approximations and are better able to estimate the accuracy of our drawing.

We have seen that the convergence depends on the maximum absolute value of

$$\frac{f(x, y_n) - f(x, y)}{y_n - y}$$

for all values of x, y, y_n concerned. In order to find the maximum value we may as well consider

$$\frac{\partial f}{\partial y}$$

for all values of x, y within the region considered. For if we assume $\partial f/\partial y$ to be a continuous function of y, it follows that the quotient of differences

$$\frac{f(x, y_n) - f(x, y)}{y_n - y}$$

must be equal to $\partial f/\partial y$ taken for the same value of x and a value of y between y and y_n. This is immediately seen by plotting $f(x, y)$ as ordinate to the abscissa y for a fixed value of x. The value of the quotient of differences is determined by the slope of the chord between the two points of abscissas y and y_n. The slope of the chord is equal to the slope of the curve at a certain point between the ends of the chord. The value of $\partial f/\partial y$ at this point is equal to the value of

$$\frac{f(x, y_n) - f(x, y)}{y_n - y}.$$

Now let us consider how the coördinate system may be chosen in order to make $\partial f/\partial y$ as small as possible and thus obtain the best convergence. For this purpose let us investigate how the value of $\partial f/\partial y$ changes at a certain point, when the system of coördinates is changed.

Let us start with a given system of rectangular coördinates ξ, η with which the differential equation is written

$$\frac{d\eta}{d\xi} = \varphi(\xi, \eta).$$

The direction of the curve satisfying the differential equation forms a certain angle α with the positive axis of ξ determined by

$$\operatorname{tg} \alpha = \frac{d\eta}{d\xi} = \varphi(\xi, \eta)$$

(assuming the coördinates to be measured in the same unit). Now let us introduce a new system of rectangular coördinates x, y connected with the system ξ, η by the equations

$$x = \xi \cos \omega + \eta \sin \omega,$$

$$y = -\xi \sin \omega + \eta \cos \omega,$$

which are equivalent to

$$\xi = x \cos \omega - y \sin \omega,$$

$$\eta = x \sin \omega + y \cos \omega,$$

ω being the angle between the positive direction of x and the positive direction of ξ, counted from ξ towards x in the usual way.

The angle formed by the direction of the curve with the positive direction of the axis of x is $\alpha - \omega$, and therefore

$$\frac{dy}{dx} = \operatorname{tg} (\alpha - \omega) = f(x, y).$$

Consequently we obtain for a given value of ω

$$\frac{\partial f}{\partial y} = \frac{1}{\cos^2 (\alpha - \omega)} \frac{\partial \alpha}{\partial y},$$

or remembering that α is given as a function of ξ and η,

$$\frac{\partial f}{\partial y} = \frac{1}{\cos^2 (\alpha - \omega)} \cdot \left(- \frac{\partial \alpha}{\partial \xi} \sin \omega + \frac{\partial \alpha}{\partial \eta} \cos \omega \right).$$

For simplicity's sake we shall assume that the axis of ξ is the tangent of the curve $\varphi(\xi, \eta) =$ const. that passes through the given point, so that $\partial\alpha/\partial\xi = 0$.

We then have

$$\frac{\partial f}{\partial y} = \frac{1}{\cos^2 (\alpha - \omega)} \frac{\partial \alpha}{\partial \eta} \cos \omega,$$

and our object is to find how $\partial f/\partial y$ varies for different values of

ω. The value of $\partial\alpha/\partial\eta$ is independent of ω; it denotes the value of the gradient of α, which we represent by a straight line drawn from the origin A (Fig. 89) perpendicular to the curve $\alpha =$ const. or $\varphi(\xi, \eta) =$ const.

It is no restriction to assume the value of $\partial\alpha/\partial\eta$ positive; it only means that the direction of the positive axis of η is chosen

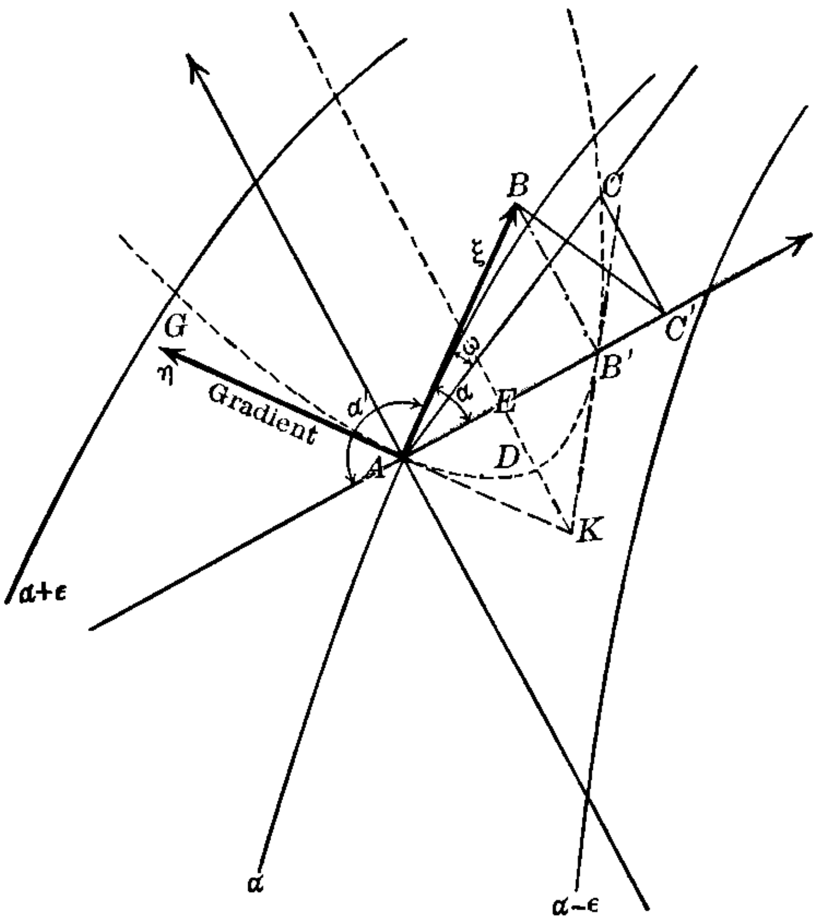


FIG. 89.

in the direction of the gradient. Let us draw the line AB (Fig. 89) in the direction of the positive axis of ξ and of the same length as the gradient.

In order to show the values of $\partial f/\partial y$ for the different positions of the axis of x let us lay off the value of $\partial f/\partial y$ as an abscissa. For instance for $\omega = \alpha$, $\partial f/\partial y$ assumes the value

$$\frac{\partial\alpha}{\partial\eta}\cos\alpha.$$

The abscissa corresponding to this value is AB' (Fig. 89), the orthogonal projection of AB on the axis of x. For any other position AC (Fig. 89) corresponding to some other value of ω, we find $\partial\alpha/\partial\eta \cos\omega$ by orthogonal projection of AB on AC. Then the division by $\cos(\alpha - \omega)$ furnishes AC' and a second division by $\cos(\alpha - \omega)$ leads to AC. Thus a certain curve can be constructed whose polar coördinates are $r = \partial f/\partial y$ and ω, the equation in polar coördinates being

$$r = \frac{\partial\alpha}{\partial\eta} \cdot \frac{\cos\omega}{\cos^2(\alpha - \omega)} \quad \text{or} \quad [r\cos(\alpha - \omega)]^2 = \frac{\partial\alpha}{\partial\eta} r\cos\omega.$$

In rectangular coördinates ξ, η the equation assumes the form

$$(\cos\alpha\xi + \sin\alpha\eta)^2 = \frac{\partial\alpha}{\partial\eta}\,\xi.$$

This shows that the equation is a parabola, the axis of which is perpendicular to the direction α. AB' is a chord and the gradient

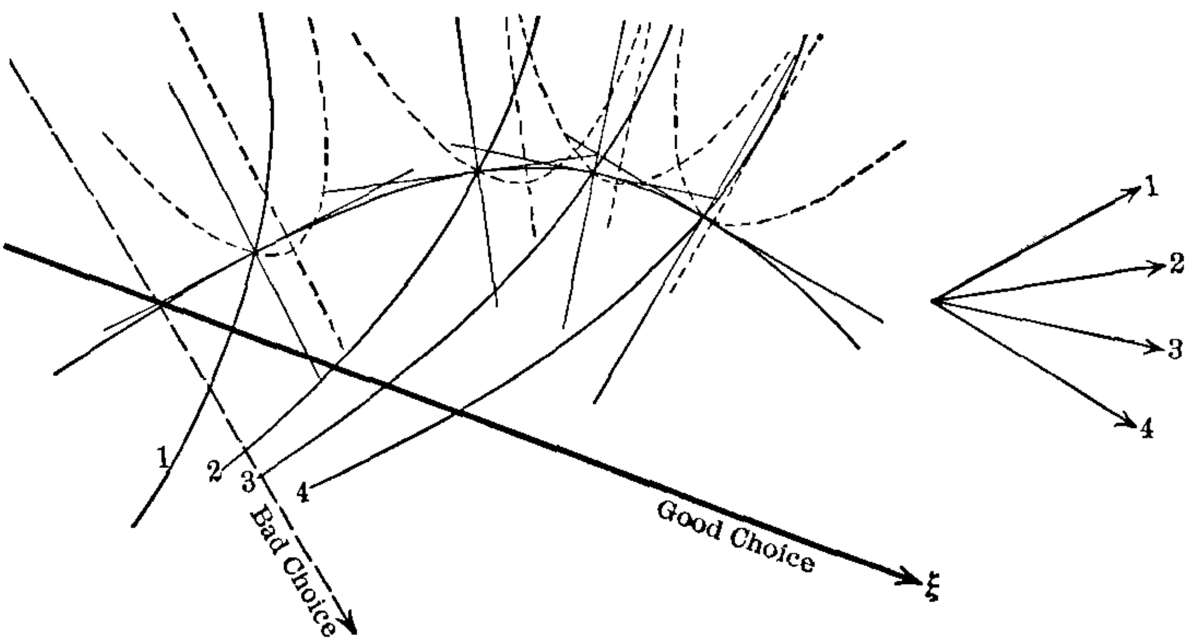


FIG. 90.

AG is a tangent of the parabola. Bisecting AB' in E, drawing EK perpendicular to AB' as far as the axis of η and bisecting EK in D, we find D the apex of the parabola. The three points A, B', D together with the gradient will suffice to give us an idea of the size and sign of $\partial f/\partial y$ for the different positions of the positive axis of x.

$\partial f/\partial y$ vanishes when the axis of x is perpendicular to the curve $\alpha =$ const., so that it seems as if this were the most favorable position. We must, however, bear in mind that the axis of x is kept unaltered for a certain interval of integration. When we pass on to other points the axis of x is no longer perpendicular to the curve $\alpha =$ const. there. The position of the axis of x is good when the average value of $\partial f/\partial y$ is small. In Fig. 90 the parabolas are constructed for a number of points on the first approximation of a curve satisfying the differential equation.

If we want to make use of the parabolas to give us the numerical values of $\partial f/\partial y$ the unit of length must also be marked in which the coördinates are measured. The numerical value of $\partial f/\partial y$ varies as the unit of length and therefore the length of the line representing it must vary as the square of the unit of length. But if we draw a line whose length measured in the same unit is equal to $\frac{1}{\partial f/\partial y}$, this line would be independent of the unit of length. For if l is the line representing the unit of length and l', l'' the lines representing the values $\partial f/\partial y$ and $\frac{1}{\partial f/\partial y}$, $\partial f/\partial y$ would be the ratio l'/l and $\frac{1}{\partial f/\partial y}$ the ratio l''/l; hence $l'' = l^2/l'$. Since l' varies as l^2 with the change of the unit of length l'' is independent of the unit of length. This line l'' represents the limit beyond which the product

$$\frac{\partial f}{\partial y}\cdot l''$$

becomes greater than 1. If $\partial f/\partial y$ remained the same this would mean the limit beyond which the convergence of the process of approximation ceases. We might lay off the length of $\frac{1}{\partial f/\partial y}$ in the different directions in the same way as $\partial f/\partial y$ has been laid off. The result is a curve corresponding, point by point, to the parabola, the image of the parabola according to the relation of reciprocal radii. But all these preparations as a rule would not pay. It is better to attack the integration at once with an axis of x somewhat perpendicular to the curves $\alpha =$ const. as long as the direction of the curve forms a considerable angle with the curve $\alpha =$ const. and to lose no time in troubling about the very best position. The convergence will show itself, when the operations are carried out. When the angle between the direction of the curve that satisfies the differential equation and the curve $\alpha =$ const. becomes small the apex of the parabola moves far away and when the direction coincides with that of the curve $\alpha =$ const. the parabola degenerates into two parallel lines perpendicular to the direction of the curve $\alpha =$ const. In this case the best position for the axis of x is in the direction of the curve $\alpha =$ const. Without going into any detailed investigation about the best position of the axis of x we can establish the general rule not to make the axis of x perpendicular to the direction of the curve satisfying the differential equation, that is to say, not to make it parallel to the axis of the parabola. But we hardly need pronounce this rule. In practice it would enforce its own observance, because for that position of the axis of x not only $\partial f/\partial y$ but also $f(x, y)$ are infinite and it would become impossible to plot the curve $Y = f(x, y_1)$.

There is another graphical method of integrating a differential equation of the first order

$$\frac{dy}{dx} = f(x, y),$$

which in some cases may well compete with the first method. Like the first it is the analogue of a certain numerical method.

The numerical method starts from given values x, y and calculates the change of y corresponding to a certain small change of x. Let h be the change of x and k the change of y, so that $x + h$, $y + k$ are the coördinates of a point on the curve satisfying the differential equation and passing through the point x, y. k is calculated in the following manner. We calculate in succession four values k_1, k_2, k_3, k_4 by the following equations—

$$k_1 = f(x, y)h,$$

$$k_2 = f\left(x + \frac{h}{2}, y + \frac{k_1}{2}\right)h,$$

$$k_3 = f\left(x + \frac{h}{2}, y + \frac{k_2}{2}\right)h,$$

$$k_4 = f(x + h, y + k_3)h.$$

We then form the arithmetical means

$$p = \frac{k\ + k_3}{2} \quad \text{and} \quad q = \frac{k_1 + k_4}{2},$$

and find with a high degree of approximation as long as h is not too large

$$k = p + \tfrac{1}{3}(q - p).^{1}$$

The new values

$$X = x + h, \quad Y = y + k$$

are then substituted for x and y and in the same way the coördinates of a third point are calculated and so on.

This calculation may be performed graphically in a profitable manner, if the function $f(x, y)$ is represented in a way suited to

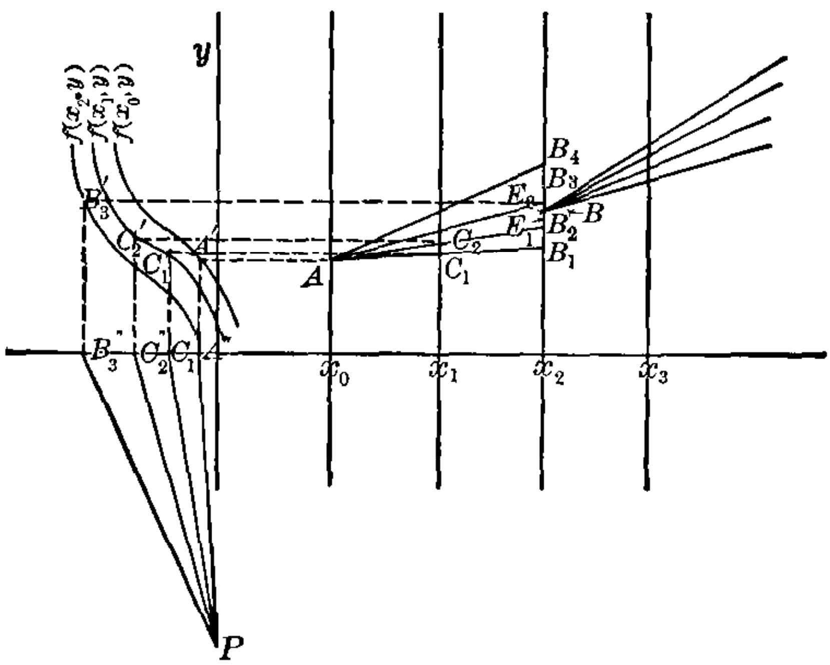


FIG. 91.

[1] See W. Kutta, *Zeitschrift für Mathematik und Physik*, Vol. 46, p. 443.

the purpose. Let us suppose a number of equidistant parallels to the axis of ordinates: $x = x_0$, $x = x_1$, $x = x_2$, $x = x_3$, $\cdots$. Along these lines $f(x, y)$ is a function of y. Let us lay off the values of $f(x, y)$ as ordinates to the abscissa y, the axis of y being taken as the axis of abscissas. We thus obtain a number of curves representing the functions $f(x_0, y)$, $f(x_1, y)$, $f(x_2, y)$, $\cdots$. Starting from a point $A(x_0, y_0)$ on the first vertical $x = x_0$ (Fig. 91) we proceed to a point B_1 on the vertical $x = x_2$ in the following way. By drawing a horizontal line through A we find the point A' on the curve representing $f(x_0, y)$. Its ordinate is equal to $f(x_0, y_0)$. Projecting the point A' onto the axis of x we find A'' and draw the line PA''. P is a point on the negative side of the y-axis and PO is equal to the unit of length by which the lines representing $f(x, y)$ are measured. Thus

$$OA''/PO = f(x_0, y_0).$$

Now we draw AB_1 perpendicular to PA'', so that if h and k_1 denote the differences of the coördinates of A and B, we have

$$k_1/h = OA''/PO,$$

$$k_1 = f(x_0, y_0)h.$$

From C_1 the point of intersection of the line AB_1 and the vertical $x = x_1$ we find C_1' and C_1'' in the same way as we found A' and A'' from A, only that C_1' is taken in the curve representing the values of $f(x_1, y)$, and draw the line AB_2 perpendicular to PC_1''. Denoting the difference of the ordinates of A and B_2 by k_2 we have

$$\frac{k_2}{h} = \frac{OC_1''}{PO} = f\left(x_0 + \frac{h}{2}, y_0 + \frac{k_1}{2}\right),$$

or

$$k_2 = f\left(x_0 + \frac{h}{2}, y_0 + \frac{k_1}{2}\right)h.$$

From C_2 the point of intersection of the line AB_2 and the vertical $x = x_1$ we find in the same way a point B_3 on the vertical

$x = x_2$ and the difference k_3 between the ordinate of B_3 and that of A is

$$k_3 = f\left(x_0 + \frac{h}{2}, y_0 + \frac{k_2}{2}\right)h.$$

From B_3 we pass horizontally to B_3' on the curve representing $f(x_2 y)$ and vertically down to B_3''. The line AB_4 is then drawn perpendicular to PB_3'', so that the difference k_4 between the ordinates of B_4 and A is

$$k_4 = f(x_0 + h, y + k_3)h.$$

The bisection of B_2B_3 and of B_1B_4 gives us the points E_1 and E_2 and the point B is taken between E_1 and E_2, so that its distance from E_1 is half its distance from E_2. The point B is with a high degree of approximation a point of the curve that passes through A and satisfies the differential equation.

B is then taken as a new point of departure instead of A, and in this manner a series of points of the curve are found.

In order to get an idea of the accuracy attained the distance of the vertical lines is altered. For instance, we may leave out the verticals $x = x_1$ and $x = x_3$, and reach the point on the vertical $x = x_4$ in one step instead of two. The error of this point should then be about sixteen times as large as the error on the same vertical reached by two steps, so that the error of the latter should be about one-fifteenth of the distance of the two. If their distance is not appreciable the smaller steps are evidently unnecessarily small.

The values of $f(x, y)$ may become so large that an inconveniently small unit of length must be applied to plot them. In this case x and y have to change parts and the differential equation is written in the form

$$\frac{dx}{dy} = \frac{1}{f(x, y)}.$$

The values of $1/f(x, y)$ are then plotted for equidistant values of

y as ordinates to the abscissa x and the constructions are changed accordingly.

§ 16. *Differential Equations of the Second and Higher Orders.*— Differential equations of the second order may be written in the form

$$\frac{d^2y}{dx^2} = f\left(x, y, \frac{dy}{dx}\right).$$

Let us introduce the radius of curvature instead of the second differential coefficient. Suppose we pass along a curve that satisfies the equation and the direction of our motion is determined by the angle α it forms with the positive axis of x (counted in the usual way from the positive axis of x through ninety degrees to the positive axis of y and so on), s being the length of the curve counted from a certain point from which we start. We then have

$$\frac{dy}{dx} = \operatorname{tg}\alpha, \quad \frac{dx}{ds} = \cos\alpha.$$

Consequently

$$\frac{d^2y}{dx^2} = \frac{1}{\cos^2\alpha}\cdot\frac{d\alpha}{dx} = \frac{1}{\cos^3\alpha}\cdot\frac{d\alpha}{ds},$$

or

$$\frac{d\alpha}{ds} = \cos^3\alpha\,\frac{d^2y}{dx^2}.$$

$d\alpha/ds$ measures the "curvature," the rate of change of direction as we pass along the curve, counted positive when the change takes place to the side of greater values of α (if the positive axis of x is drawn to the right and the positive axis of y upwards a positive value of $d\alpha/ds$ means that the path turns to the left). Let us count the radius of curvature with the same sign as $d\alpha/ds$ and let us denote it by ρ. Then we have

$$\frac{1}{\rho} = \cos^3\alpha\, f(x, y, \operatorname{tg}\alpha).$$

Thus the differential equation of the second order may be said to give the radius of curvature as a function of x, y, α, that is to say, as a function of place and direction.

Let us assume that this function of three variables is represented by a diagram, so that the length and sign of ρ may quickly be obtained for any point and any direction.

Starting from any given point in any given direction we can then approximate the curve satisfying the differential equation by a series of circular arcs. Let A (Fig. 92) be the starting point. We make M_aA perpendicular to the given direction and equal to ρ in length. For positive values of ρ, M_a must be on the positive side of the given direction, for negative values on the negative side. M_a is the center of curvature for the curve at A. With M_a as center and M_aA as radius we draw a circular arc AB and draw the line BM_a. On this line or on its production we mark the point M_b at a distance from B equal to the value of ρ that corresponds to B and to the direction in which the circular arc reaches B. With M_b as center and M_bB as radius we draw a circular arc BC and so on.

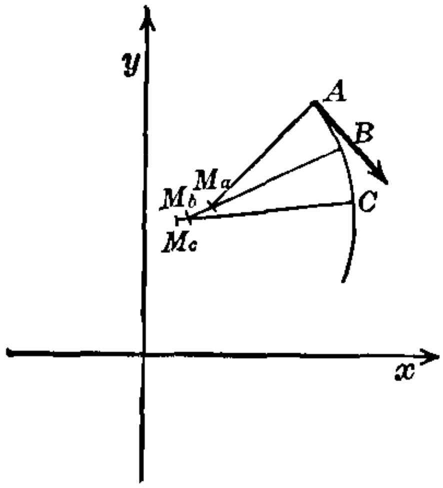


FIG. 92.

The true curve changes its radius of curvature continuously, while our approximation changes it abruptly at the points $A, B, C, \cdots$. The smaller the circular arcs the less will accurately-drawn circular arcs deviate from the curve. But it must be kept in mind that small errors cannot be avoided, when passing from one arc to the next. Hence, if the arcs are taken very small so that their number for a given length of curve increases unduly, the accuracy will not be greater than with somewhat longer arcs. The best length cannot well be defined mathematically; it must be left to the experience of the draughtsman.

Some advantage may be gained by letting the centers and the radii of the circular arcs deviate from the stated values. The circular arc AB (Fig. 92) is evidently drawn with too small a radius because the radius of the curve increases towards B. If we had taken the radius equal to M_bB it would have been too large. A better approximation is evidently obtained by making the radius of the first circular arc equal to the mean of M_aA and M_bB, and the direction with which it reaches B will also be closer to the right direction.

To facilitate the plotting an instrument may be used consisting of a flat ruler with a hole on one end for a pencil or a capillary tube or any other device for tracing a line. A straight line with a scale is marked along the middle of the ruler and a little tripod of sewing needles is placed with one foot on the line and two feet on the paper. Thus the pencil traces a circular arc. When the radius is changed, the ruler is held in its position by pressing it against the paper until the tripod is moved to a new position. By this device the pencil must continue its path in exactly the same direction, while with the use of ordinary compasses it is not easy to avoid a slight break in the curve at the joint of two circular arcs.

Another method consists in a generalization of the method for the graphical solution of a differential equation of the first order.

A differential equation of the second order

$$\frac{d^2y}{dx^2} = g\left(x, y, \frac{dy}{dx}\right)$$

may be written in the form of two simultaneous equations of the first order:

$$\frac{dy}{dx} = z,$$

$$\frac{dz}{dx} = g(x, y, z).$$

Let us consider the more general form, in which the differential coefficients of two functions y, z of x are given as functions of x, y, z:

$$\frac{dy}{dx} = f(x, y, z),$$

$$\frac{dz}{dx} = g(x, y, z).$$

We may interpret x, y, z as the coördinates of a point in space and the differential equation as a law establishing a certain direction or the opposite at every point in space where $f(x, y, z)$ and $g(x, y, z)$ are defined. A curve in space satisfies the differential equation, when it never deviates from the prescribed direction. Its projection in the xy plane represents the function y and its projection in the xz plane represents the function z.

Let us represent y and z as ordinates and x as abscissa in the same plane with the same system of coördinates. Any point in

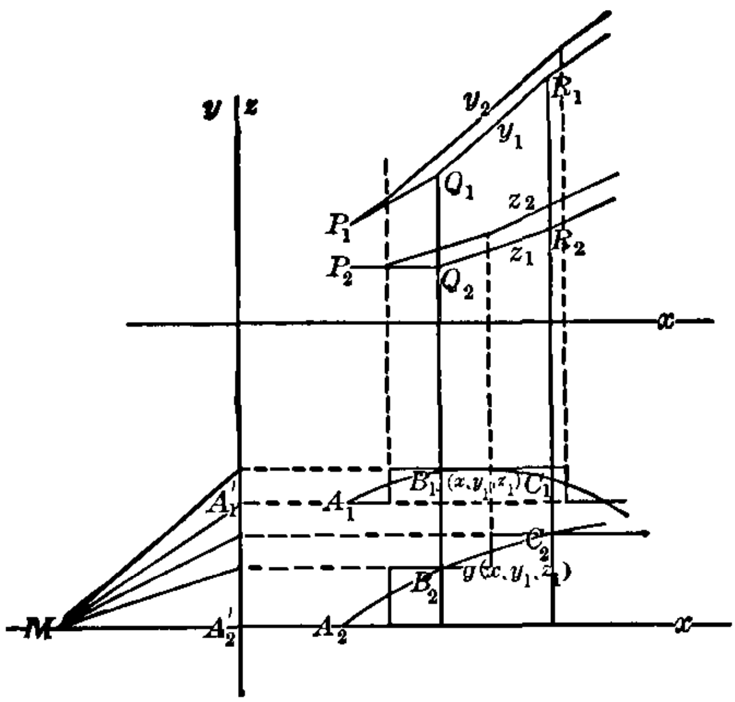


FIG. 93.

space is represented by two points with the same abscissa. The functions $f(x, y, z)$ and $g(x, y, z)$ we suppose to be given either by diagrams or by certain methods of construction or calculation. For any point that we have to deal with, the values of $f(x, y, z)$ and $g(x, y, z)$ are plotted as ordinates to the abscissa x, but for clearness sake not in the same system of coördinates as y and z, but in another system with the same axis of ordinates and an axis of x parallel to the first and removed far enough so that the drawings in the two systems do not interfere with one another.

Starting from a certain point $P(x_p, y_p, z_p)$ in space we represent it by the two points $P_1(x_p, y_p)$ and $P_2(x_p, z_p)$ in the first system and the values of $f(x_p, y_p, z_p)$ and $g(x_p, y_p, z_p)$ by the two points A_1 and A_2 in the second system of coördinates (Fig. 93). The points A_1 and A_2 determine certain directions MA_1', and MA_2' of the curves x, y and x, z, the point M (Fig. 93) being placed at a distance from the axis of ordinates equal to the unit of length by which the ordinates representing $f(x, y, z)$ and $g(x, y, z)$ are measured. Through P_1 and P_2 we draw parallels to MA_1' and MA_2' as far as Q_1 and Q_2 with the coördinates x_q, y_q and x_q, z_q. With these coördinates the values $f(x_q, y_q, z_q)$ and $g(x_q, y_q, z_q)$ are determined, which we represent by the ordinates of the points B_1, B_2. These points again determine certain directions parallel to which the lines Q_1R_1 and Q_2R_2 are drawn, etc. In this manner we find first approximations y_1 and z_1 for the functions y and z and corresponding to these approximations we find curves representing $f(x, y_1, z_1)$ and $g(x, y_1, z_1)$. These curves are now integrated graphically, the integral curve of $f(x, y_1, z_1)$ beginning at P_1 and the integral curve of $g(x, y_1, z_1)$ at P_2 and lead to second approximations y_2 and z_2:

$$y_2 = y_p + \int_{x_p}^{x} f(x, y_1, z_1)dx,$$

$$z_2 = z_p + \int_{x_p}^{x} g(x, y_1, z_1)dx.$$

For these second approximations the values of $f(x, y_2, z_2)$ and $g(x, y_2, z_2)$ are determined at a number of points along the curves x, y_2 and x, z_2 sufficiently close to construct the curves representing $f(x, y_2, z_2)$ and $g(x, y_2, z_2)$. By their integration a third approximation y_3, z_3 is obtained

$$y_3 = y_p + \int_{x_p}^{x} f(x, y_2, z_2)dx,$$

$$z_3 = z_p + \int_{x_p}^{x} g(x, y_2, z_2)dx,$$

and so on as long as a deviation of an approximation from the one before can still be detected. As soon as there is no deviation for a certain distance $x - x_p$ the curve represents the true solution (as far as the accuracy of the drawing goes). The curve is continued by taking its last point as a new starting point for a similar operation.

The distance over which the integral is taken can in general not surpass a certain limit where the convergence of the approximations ceases. But we are free to make it as small as we please and accordingly increase the number of operations to reach a given distance. It is evidently not economical to make it too small. On the contrary, we shall choose it as large as possible without unduly increasing the number of approximations.

In the case of a differential equation

$$\frac{d^2y}{dx^2} = g\left(x, y, \frac{dy}{dx}\right)$$

we have $f(x, y, z) = z$, and the curve z, x is identical with the curve representing the values of $f(x, y, z)$. We shall therefore draw it only once.

The proof of the convergence of the approximations is almost the same as in the case of the differential equation of the first order.

For the $n + 1^{st}$ approximation we have

$$y_{n+1} = y_p + \int_{x_p}^{x} f(x, y_n, z_n)dx; \quad z_{n+1} = z_p + \int_{x_p}^{x} g(x, y_n, z_n)dx.$$

For the true curve that passes through the point x_p, y_p, z_p we find by integration

$$y = y_p + \int_{x_p}^{x} f(x, y, z)dx; \quad z = z_p + \int_{x_p}^{x} g(x, y, z)dx;$$

hence

$$y_{n+1} - y = \int_{x_p}^{x} [f(x, y_n, z_n) - f(x, y, z)]dx;$$

$$z_{n+1} - z = \int_{x_p}^{x} [g(x, y_n, z_n) - g(x, y, z)]dx.$$

Now let us write

$$f(x, y_n, z_n) - f(x, y, z) = \frac{f(x, y_n, z_n) - f(x, y, z_n)}{y_n - y}(y_n - y) + \frac{f(x, y, z_n) - f(x, y, z)}{z_n - z}(z_n - z),$$

and similarly

$$g(x, y_n, z_n) - g(x, y, z) = \frac{g(x, y_n, z_n) - g(x, y, z_n)}{y_n - y}(y_n - y) + \frac{g(x, y, z_n) - g(x, y, z)}{z_n - z}(z_n - z).$$

The quotients of differences

$$\frac{f(x, y_n, z_n) - f(x, y, z_n)}{y_n - y}$$

and the three others are equal to certain values of $\partial f/\partial y$, $\partial f/\partial z$, $\partial g/\partial y$, $\partial g/\partial z$ for values of y, z between y and y_n and between z and z_n (y, y_n, z, z_n not excluded). Let us assume that for the region of all the values of x, y, z concerned the absolute value of $\partial f/\partial y$ and $\partial f/\partial z$, is not greater than M_1, and that of $\partial g/\partial y$ and $\partial g/\partial z$ not greater than M_2, and that δ_n, ϵ_n denote the maximum of the absolute values of $y - y_n$ and $z - z_n$ in the interval x_p to x. Then it follows that the absolute values of

$$f(x, y_n, z_n) - f(x, y, z) \quad \text{and} \quad g(x, y_n, z_n) - g(x, y, z)$$

are not greater than

$$M_1(\delta_n + \epsilon_n) \quad \text{and} \quad M_2(\delta_n + \epsilon_n).$$

Hence for the maximum values of $y_{n+1} - y$ and $z_{n+1} - z$, which are denoted by δ_{n+1} and ϵ_{n+1} we obtain the limits

$$\delta_{n+1} \leqq M_1(\delta_n + \epsilon_n)\,|\,x - x_p\,|, \qquad \epsilon_{n+1} \leqq M_2(\delta_n + \epsilon_n)\,|\,x - x_p\,|,$$

and

$$\delta_{n+1} + \epsilon_{n+1} \leqq (M_1 + M_2)\,|\,x - x_p\,|\,(\delta_n + \epsilon_n).$$

If therefore the interval $x - x_p$ of the integration is so far reduced that

$$(M_1 + M_2)\,|\,x - x_p\,| \leqq k < 1,$$

$\delta_{n+1} + \epsilon_{n+1}$ is not larger than the fraction k of $(\delta_n + \epsilon_n)$, but from the same reason

$$(\delta_n + \epsilon_n) \leqq k(\delta_{n-1} + \epsilon_{n-1}), \quad (\delta_{n-1} + \epsilon_{n-1}) < k(\delta_{n-2} + \epsilon_{n-2}), \text{ etc.};$$

therefore

$$\delta_{n+1} + \epsilon_{n+1} \leqq k^n(\delta_1 + \epsilon_1).$$

That is to say, for a sufficiently large value of n δ_{n+1} and ϵ_{n+1} will both become as small as we please.

As in the case of the differential equation of the first order it is not worth while, as a rule, to investigate the convergence for the purpose of finding a sufficiently close approximation by graphical methods. It is better at once to tackle the task of drawing the approximations and to repeat the operations until no further improvement is obtained. The curve will then satisfy the differential equation as far as the graphical methods allow it to be recognized.

When the values of $f(x, y, z)$ or $g(x, y, z)$ become too large we can have recourse to the same device that we found useful with the differential equation of the first order. Instead of x, one of the other two variables y or z may be considered as independent, so that the equations take the form

$$\frac{dx}{dy} = \frac{1}{f(x, y, z)}, \quad \frac{dz}{dy} = \frac{g(x, y, z)}{f(x, y, z)},$$

or

$$\frac{dx}{dz} = \frac{1}{g(x, y, z)}, \quad \frac{dy}{dz} = \frac{f(x, y, z)}{g(x, y, z)},$$

or we may introduce a new system of coördinates x', y', z' and consider the resulting differential equations.

The second method for the integration of differential equations of the first order can also be generalized to include the second order. Let us again consider the more general case

$$\frac{dy}{dx} = f(x, y, z), \quad \frac{dz}{dx} = g(x, y, z).$$

Starting from a point x, y, z the changes of y and z (denoted by

k and l) can be calculated for a small change h of x by the following formulas analogous to those used for one differential equation of the first order:

$$k_1 = f(x, y, z)h; \qquad l_1 = g(x, y, z)h;$$

$$k_2 = f\left(x+\frac{h}{2},\ y+\frac{k_1}{2},\ z+\frac{l_1}{2}\right)h; \quad l_2 = g\left(x+\frac{h}{2},\ y+\frac{k_1}{2},\ z+\frac{l_1}{2}\right)h;$$

$$k_3 = f\left(x+\frac{h}{2},\ y+\frac{k_2}{2},\ z+\frac{l_2}{2}\right)h; \quad l_3 = g\left(x+\frac{h}{2},\ y+\frac{k_2}{2},\ z+\frac{l_2}{2}\right)h;$$

$$k_4 = f(x + h,\ y + k_3,\ z + l_3)h; \quad l_4 = g(x + h,\ y + k_3,\ z + l_3)h;$$

$$p = \frac{k_2 + k_3}{2},\ q = \frac{k_1 + k_4}{2}; \qquad p' = \frac{l_2 + l_3}{2},\ q' = \frac{l_1 + l_4}{2};$$

and with a high degree of approximation,

$$k = p + \tfrac{1}{3}(q - p); \quad l = p' + \tfrac{1}{3}(q' - p').$$

These calculations may be performed graphically. For this purpose the functions $f(x, y, z)$ and $g(x, y, z)$ must be given in some handy form. We notice that in our formulas the first argument assumes the values x, $x + h/2$, $x + h$. In the next step where $x + h$, $y + k$, $z + l$ are the coördinates of the starting point that play the same part that x, y, z played in the first step, we are free to make the change of the first argument the same as in the first step, so that in the formulas of the second step it assumes the values $x + h$, $x + \frac{3}{2}h$, $x + 2h$ and so on for the following steps. All the values of the first argument can thus be assumed equidistant. Let us denote these equidistant values by

$$x_0,\ x_1,\ x_2,\ x_3,\ \cdots.$$

The values of $f(x, y, z)$ and $g(x, y, z)$ appear in all our formulas only for the constant values

$$x = x_0,\ x_1,\ x_2,\ \cdots.$$

For each of these constants f and g are functions of two independent variables and as such may be represented graphically by drawings giving the curves $f =$ const. and $g =$ const., each value of x corresponding to a separate drawing. These drawings we must consider as the graphical form in which the differential equations are given. It may of course sometimes be very tiresome to translate the analytical form of a differential equation into a graphical form, but this trouble ought not to be laid to the account of the graphical method.

The method now is similar to that used for the differential equation of the first order. y and z are plotted as ordinates in the same system in which x is the abscissa. Equidistant parallels to the axis of ordinates are drawn

$$x = x_0, \ x = x_1, \ x = x_2, \text{ etc.}$$

On the first $x = x_0$ we mark two points with ordinates y_0 and z_0, and from the drawing that gives the values of $f(x_0, y, z)$ and

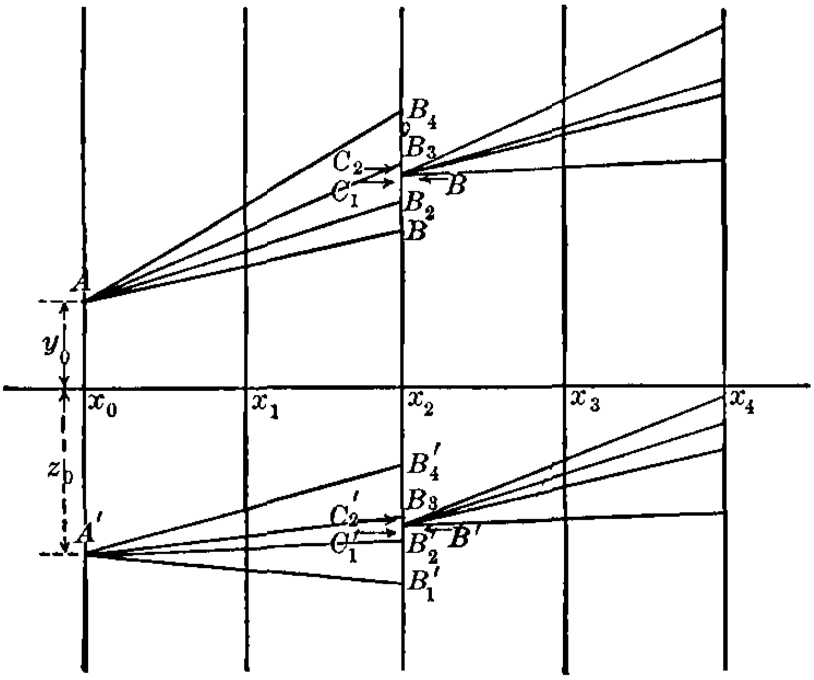


FIG. 94.

$g(x_0, y, z)$ as functions of y and z we read the values $f(x_0, y_0, z_0)$ and $g(x_0, y_0, z_0)$ and draw the lines from x_0, y_0, and x_0, z_0 to the points

$$x_2, y_0 + k_1 \quad \text{and} \quad x_2, z_0 + l_1.$$

The intersections of these lines with the parallel $x = x_1$ furnishes the points

$$x_1, y_0 + \frac{k_1}{2} \quad \text{and} \quad x_1, z_0 + \frac{l_1}{2}.$$

With these ordinates we find from the second drawing the values

$$f\left(x_1, y_0 + \frac{k_1}{2}, z_0 + \frac{l_1}{2}\right) \quad \text{and} \quad g\left(x_1, y_0 + \frac{k_1}{2}, z_0 + \frac{l_1}{2}\right),$$

and by their help we can draw the lines from x_0, y_0 and x_0, z_0 to the points

$$x_2, y_0 + k_2 \quad \text{and} \quad x_2, y_0 + l_2.$$

The intersections of these lines with the line $x = x_1$ furnishes the points

$$x_1, y_0 + \frac{k_2}{2} \quad \text{and} \quad x_1, z_0 + \frac{l_2}{2},$$

and with these ordinates we find the values

$$f\left(x_1, y_0 + \frac{k_2}{2}, z_0 + \frac{l_2}{2}\right), \quad g\left(x_1, y_0 + \frac{k_2}{2}, z_0 + \frac{l_2}{2}\right),$$

which enable us to draw the lines from x_0, y_0 and x_0, z_0 to x_2, $y_0 + k_3$ and x_2, $z_0 + l_3$.
With these two ordinates we find from the third diagram ($x = x_2$) the values

$$f(x_2, y_0 + k_3, z_0 + l_3) \quad \text{and} \quad g(x_2, y_0 + k_3, z_0 + l_3),$$

which finally enable us to draw the lines from x_0y_0 and x_0z_0 to x_2, $y_0 + k_4$ and x_2, $z_0 + l_4$.

On the vertical line $x = x_2$ we thus obtain four points, B_1, B_2, B_3, B_4, corresponding to $y_0 + k_1$, $y_0 + k_2$, $y_0 + k_3$, $y_0 + k_4$ and four points, B_1', B_2', B_3', B_4', corresponding to $z_0 + l_1$, $z_0 + l_2$, $z_0 + l_3$, $z_0 + l_4$ (Fig. 94).

B_2B_3 and B_1B_4 are bisected by the points C_1 and C_2; $B_2'B_3'$ and $B_1'B_4'$ by the points C_1', C_2'. Finally C_1C_2 and $C_1'C_2'$ are divided into three equal parts and the points B and B' are found in the dividing points nearest to C_1 and C_1'.

The same construction is then repeated with B and B' as starting points and furnishes two new points on the vertical

$x = x_4$ and so on. To test the accuracy the construction is repeated with intervals of x of double the size. The difference in the values of y and of z found for $x = x_4$ enables us to estimate the errors of the first construction—they are about one-fifteenth of the observed differences.

Both methods are without difficulty generalized for the integration of differential equations of any order. We can write a differential equation of the nth order in the form

$$\frac{d^n x}{dt^n} = f\left(t, x, \frac{dx}{dt}, \cdots, \frac{dx^{n-1}}{dt^{n-1}}\right),$$

or in the form of n simultaneous equations of the first order

$$\frac{dx}{dt} = x_1,$$

$$\frac{dx_1}{dt} = x_2,$$

$$\cdots\cdots$$

$$\frac{dx_{n-2}}{dt} = x_{n-1},$$

$$\frac{dx_{n-1}}{dt} = f(t, x, x_1, x_2, \cdots x_{n-1}).$$

A more general and more symmetrical form is

$$\frac{dx}{dt} = f_1(t, x, x_1, \cdots x_{n-1}),$$

$$\frac{dx_1}{dt} = f_2(t, x, x_1, \cdots x_{n-1}),$$

$$\cdots\cdots\cdots\cdots$$

$$\frac{dx_{n-1}}{dt} = f_n(t, x, x_1, \cdots x_{n-1}).$$

The functions $x, x_1, x_2, \cdots x_{n-1}$ are then represented as ordinates to the abscissa t, so that we have n different curves. When the function $f(t, x, x_1, x_2, \cdots x_{n-1})$ is given in a handy form, so that its value may be quickly found for any given values of t, x, x_1, $\cdots$ x_{n-1}, there is no difficulty in constructing n curves whose ordinates represent the functions x, x_1, x_2, $\cdots$ x_{n-1}. Starting from given values of t, x, x_1, x_2, $\cdots$ x_{n-1} we have only to apply the same methods that have been explained for the first and the second order.

INTRODUCTION TO THE

THEORY OF ALGEBRAIC EQUATIONS.

BY

LEONARD EUGENE DICKSON, Ph.D.,

ASSISTANT PROFESSOR OF MATHEMATICS IN
THE UNIVERSITY OF CHICAGO.

PREFACE.

THE solution of the general quadratic equation was known as early as the ninth century; that of the general cubic and quartic equations was discovered in the sixteenth century. During the succeeding two centuries many unsuccessful attempts were made to solve the general equations of the fifth and higher degrees. In 1770 Lagrange analyzed the methods of his predecessors and traced all their results to one principle, that of rational resolvents, and proved that the general quintic equation cannot be solved by rational resolvents. The impossibility of the algebraic solution of the general equation of degree n $(n>4)$, whether by rational or irrational resolvents, was then proved by Abel, Wantzel, and Galois. Out of these algebraic investigations grew the theory of substitutions and groups. The first systematic study of substitutions was made by Cauchy (*Journal de l'école polytechnique*, 1815).

The subject is here presented in the historical order of its development. The First Part (pp. 1–41) is devoted to the Lagrange-Cauchy-Abel theory of general algebraic equations. The Second Part (pp. 42–98) is devoted to Galois' theory of algebraic equations, whether with arbitrary or special coefficients. The aim has been to make the presentation strictly elementary, with practically no dependence upon any branch of mathematics beyond elementary algebra. There occur numerous illustrative examples, as well as sets of elementary exercises.

In the preparation of this book, the author has consulted, in addition to various articles in the journals, the following treatises:

Lagrange, *Réflexions sur la résolution algébrique des équations*; Jordan, *Traité des substitutions et des équations algébriques*; Serret, *Cours d'Algèbre supérieure*; Netto-Cole, *Theory of Substitutions and its Applications to Algebra*; Weber, *Lehrbuch der Algebra*; Burnside, *The Theory of Groups* Pierpont, *Galois' Theory of Algebraic Equations*, Annals of Math., 2d ser., vols. 1 and 2; Bolza, *On the Theory of Substitution-Groups and its Applications to Algebraic Equations*, Amer. Journ. Math., vol. XIII.

The author takes this opportunity to express his indebtedness to the following lecturers whose courses in group theory he has attended: Oscar Bolza in 1894, E. H. Moore in 1895, Sophus Lie in 1896, Camille Jordan in 1897.

But, of all the sources, the lectures and publications of Professor Bolza have been of the greatest aid to the author. In particular, the examples (§ 65) of the group of an equation have been borrowed with his permission from his lectures.

The present elementary presentation of the theory is the outcome of lectures delivered by the author in 1897 at the University of California, in 1899 at the University of Texas, and twice in 1902 at the University of Chicago.

CHICAGO, *August*, 1902

TABLE OF CONTENTS.

APPENDIX.

THEORY OF ALGEBRAIC EQUATIONS.

FIRST PART.

THE LAGRANGE-ABEL-CAUCHY THEORY OF GENERAL ALGEBRAIC EQUATIONS.

CHAPTER I.

SOLUTION OF THE GENERAL QUADRATIC, CUBIC, AND QUARTIC EQUATIONS. LAGRANGE'S THEOREM* ON THE IRRATIONALITIES ENTERING THE ROOTS.

1. Quadratic equatiou. The roots of $x^2+px+q=0$ are

$$x_1=\tfrac{1}{2}(-p+\sqrt{p^2-4q}), \quad x_2=\tfrac{1}{2}(-p-\sqrt{p^2-4q}).$$

By addition, subtraction, and multiplication, we get

$$x_1+x_2=-p, \quad x_1-x_2=\sqrt{p^2-4q}, \quad x_1x_2=q.$$

Hence the irrationality $\sqrt{p^2-4q}$, which occurs in the expressions for the roots, is rationally expressible in terms of the roots, being equal to x_1-x_2. Unlike the last function, the functions x_1+x_2 and x_1x_2 are *symmetric* in the roots and are rational functions of the coefficients.

2. Cubic equation. The general cubic equation may be written

$$x^3-c_1x^2+c_2x-c_3=0. \tag{1}$$

Setting $x=y+\tfrac{1}{3}c_1$, the equation (1) takes the simpler form

$$y^3+py+q=0, \tag{2}$$

* *Réflexions sur la résolution algébrique des équations*, Œuvres de Lagrange, Paris, 1869, vol. 3; first printed by the Berlin Academy, 1770–71.

if we make use of the abbreviations

(3) $$p=c_2-\tfrac{1}{3}c_1^{\,2},\quad q=-c_3+\tfrac{1}{3}c_1c_2-\tfrac{2}{27}c_1^{\,3}.$$

The cubic (2), lacking the square of the unknown quantity, is called the *reduced cubic equation.* When it is solved, the roots of (1) are found by the relation $x=y+\frac{1}{3}c_1$.

The cubic (2) was first solved by Scipio Ferreo before 1505. The solution was rediscovered by Tartaglia and imparted to Cardan under promises of secrecy. But Cardan broke his promises and published the rules in 1545 in his *Ars Magna*, so that the formulæ bear the name of Cardan. The following method of deriving them is essentially that given by Hudde in 1650. By the transformation

(4) $$y=z-\frac{p}{3z},$$

the cubic (2) becomes $z^3-\dfrac{p^3}{27z^3}+q=0$, whence

(5) $$z^6+qz^3-\frac{p^3}{27}=0.$$

Solving the latter as a quadratic equation for z^3, we get

$$z^3=-\tfrac{1}{2}q\pm\sqrt{R},\quad R\equiv\tfrac{1}{4}q^2+\tfrac{1}{27}p^3.$$

Denote a definite one of the cube roots of $-\frac{1}{2}q+\sqrt{R}$ by

$$\sqrt[3]{-\tfrac{1}{2}q+\sqrt{R}}.$$

The other two cube roots are then

$$\omega\sqrt[3]{-\tfrac{1}{2}q+\sqrt{R}},\quad \omega^2\sqrt[3]{-\tfrac{1}{2}q+\sqrt{R}},$$

where ω is an imaginary cube root of unity found as follows. The three cube roots of unity are the roots of the equation

$$r^3-1=0,\quad \text{or}\quad (r-1)(r^2+r+1)=0.$$

The roots of $r^2+r+1=0$ are $-\frac{1}{2}+\frac{1}{2}\sqrt{-3}\equiv\omega$ and $-\frac{1}{2}-\frac{1}{2}\sqrt{-3}=\omega^2$. Then

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

In view of the relation

$$(-\tfrac{1}{2}q+\sqrt{R})(-\tfrac{1}{2}q-\sqrt{R})=\tfrac{1}{4}q^2-R=-\tfrac{1}{27}p^3,$$

a particular cube root $\sqrt[3]{-\tfrac{1}{2}q-\sqrt{R}}$ may be chosen so that

$$\sqrt[3]{-\tfrac{1}{2}q+\sqrt{R}}\cdot\sqrt[3]{-\tfrac{1}{2}q-\sqrt{R}}=-\tfrac{1}{3}p.$$

$$\therefore\quad \omega\sqrt[3]{-\tfrac{1}{2}q+\sqrt{R}}\cdot\omega^2\sqrt[3]{-\tfrac{1}{2}q-\sqrt{R}}=-\tfrac{1}{3}p,$$

$$\omega^2\sqrt[3]{-\tfrac{1}{2}q+\sqrt{R}}\cdot\omega\sqrt[3]{-\tfrac{1}{2}q-\sqrt{R}}=-\tfrac{1}{3}p.$$

Hence the six roots of equation (5) may be separated into pairs in such a way that the product of two in any pair is $-\tfrac{1}{3}p$. The root paired with z is therefore $-\dfrac{p}{3z}$, and their sum $z-\dfrac{p}{3z}$ is, in view of (4), a root y of the cubic (2). In particular, the two roots of a pair lead to the same value of y, so that the *six* roots of (5) lead to only *three* roots of the cubic, thereby explaining an apparent difficulty. Since the sum of the two roots of any pair of roots of (5) leads to a root of the cubic (2), we obtain Cardan's formulæ for the roots y_1, y_2, y_3 of (2):

$$(7)\qquad \begin{cases} y_1=\sqrt[3]{-\tfrac{1}{2}q+\sqrt{R}}+\sqrt[3]{-\tfrac{1}{2}q-\sqrt{R}},\\ y_2=\omega\sqrt[3]{-\tfrac{1}{2}q+\sqrt{R}}+\omega^2\sqrt[3]{-\tfrac{1}{2}q-\sqrt{R}},\\ y_3=\omega^2\sqrt[3]{-\tfrac{1}{2}q+\sqrt{R}}+\omega\sqrt[3]{-\tfrac{1}{2}q-\sqrt{R}}. \end{cases}$$

Multiplying these expressions by $1, \omega^2, \omega$ and adding, we get, by (6),

$$\sqrt[3]{-\tfrac{1}{2}q+\sqrt{R}}=\tfrac{1}{3}(y_1+\omega^2y_2+\omega y_3).$$

Using the multipliers $1, \omega, \omega^2$, we get, similarly,

$$\sqrt[3]{-\tfrac{1}{2}q-\sqrt{R}}=\tfrac{1}{3}(y_1+\omega y_2+\omega^2y_3).$$

Cubing these two expressions and subtracting the results, we get

$$\sqrt{R}=\tfrac{1}{54}\{(y_1+\omega^2y_2+\omega y_3)^3-(y_1+\omega y_2+\omega^2y_3)^3\}$$

$$=\frac{\sqrt{-3}}{18}(y_1-y_2)(y_2-y_3)(y_3-y_1),$$

upon applying the Factor Theorem and the identity $\omega-\omega^2=\sqrt{-3}$. Hence all the irrationalities occurring in the roots (7) are rationally expressible in terms of the roots, a result first shown by Lagrange.

The function

$$(y_1-y_2)^2(y_2-y_3)^2(y_3-y_1)^2=-27q^2-4p^3$$

is called the *discriminant* of the cubic (2).

The roots of the general cubic (1) are

$$x_1=y_1+\tfrac{1}{3}c_1, \quad x_2=y_2+\tfrac{1}{3}c_1, \quad x_3=y_3+\tfrac{1}{3}c_1.$$

$$\therefore\ x_1-x_2=y_1-y_2, \quad x_2-x_3=y_2-y_3, \quad x_3-x_1=y_3-y_1,$$

$$(8) \qquad (x_1-x_2)(x_2-x_3)(x_3-x_1)=(y_1-y_2)(y_2-y_3)(y_3-y_1)$$

$$=\frac{18}{\sqrt{-3}}\sqrt{R}=-6\sqrt{-3}\sqrt{\tfrac{1}{4}q^2+\tfrac{1}{27}p^3}.$$

EXERCISES.

1. Show that $x_1+\omega^2x_2+\omega x_3=y_1+\omega^2y_2+\omega y_3$, $x_1+\omega x_2+\omega^2x_3=y_1+\omega y_2+\omega^2y_3$.

2. The cubic (2) has one real root and two imaginary roots if $R>0$; three real roots, two of which are equal, if $R=0$; three real and distinct roots if $R<0$ (the so-called irreducible case).

3. Show that the discriminant $(x_1-x_2)^2(x_2-x_3)^2(x_3-x_1)^2$ of the cubic (1) equals

$$c_1^2c_2^2+18c_1c_2c_3-4c_2^3-4c_1^3c_3-27c_3^2.$$

Hint: Use formula (8) in connection with (3).

4. Show that the nine expressions $\sqrt[3]{-\tfrac{1}{2}q+\sqrt{R}}+\sqrt[3]{-\tfrac{1}{2}q-\sqrt{R}}$, where all combinations of the cube roots are taken, are the roots of the cubics

$$y^3+py+q=0, \qquad y^3+\omega py+q=0, \qquad y^3+\omega^2py+q=0.$$

5. Show that $y_1+y_2+y_3=0$, $y_1y_2+y_1y_3+y_2y_3=p$, $y_1y_2y_3=-q$.

6 Show that $x_1+x_2+x_3=c_1$, $x_1x_2+x_1x_3+x_2x_3=c_2$, $x_1x_2x_3=c_3$, using Ex. 5. How may these results be derived directly from equation (1)?

3. Aside from the factor $\frac{1}{3}$, the roots of the sextic (5) are

$$\psi_1=x_1+\omega x_2+\omega^2x_3, \qquad \psi_4=x_1+\omega x_3+\omega^2x_2,$$
$$\psi_2=\omega^2\psi_1=x_2+\omega x_3+\omega^2x_1, \qquad \psi_5=\omega^2\psi_4=x_3+\omega x_2+\omega^2x_1,$$
$$\psi_3=\omega\psi_1=x_3+\omega x_1+\omega^2x_2, \qquad \psi_6=\omega\psi_4=x_2+\omega x_1+\omega^2x_3.$$

These functions differ only in the permutations of x_1, x_2, x_3. As there are just six permutations of three letters, these functions give all that can be obtained from ψ_1 by permuting x_1, x_2, x_3. For this reason, ψ_1 is called a *six-valued* function.

Lagrange's *à priori* solution of the general cubic (1) consists in determining these six functions $\psi_1, \ldots, \psi_6$ directly. They are the roots of the sextic equation $(t-\psi_1)\ldots(t-\psi_6)=0$, whose coefficients are symmetric functions of $\psi_1, \ldots, \psi_6$ and consequently symmetric functions of x_1, x_2, x_3 and hence * are rationally expressible in terms of c_1, c_2, c_3. Since $\psi_2=\omega^2\psi_1$, $\psi_3=\omega\psi_1$, etc., we have by (6)

$$(t-\psi_1)(t-\psi_2)(t-\psi_3)=t^3-\psi_1^3,$$
$$(t-\psi_4)(t-\psi_5)(t-\psi_6)=t^3-\psi_4^3.$$

Hence the *resolvent* sextic becomes

$$t^6-(\psi_1^3+\psi_4^3)t^3+\psi_1^3\psi_4^3=0. \tag{9}$$

But
$$\psi_1\psi_4=x_1^2+x_2^2+x_3^2+(\omega+\omega^2)(x_1x_2+x_1x_3+x_2x_3)$$
$$=(x_1+x_2+x_3)^2-3(x_1x_2+x_1x_3+x_2x_3)=c_1^2-3c_2,$$

in view of Ex. 6, page 4. Also, $\psi_1^3+\psi_4^3$ equals

$$2(x_1^3+x_2^3+x_3^3)-3(x_1^2x_2+x_1x_2^2+x_1^2x_3+x_1x_3^2+x_2^2x_3+x_2x_3^2)+12x_1x_2x_3$$
$$=3(x_1^3+x_2^3+x_3^3)-(x_1+x_2+x_3)^3+18x_1x_2x_3$$
$$=2c_1^3-9c_1c_2+27c_3.$$

Hence equation (9) becomes

$$t^6-(2c_1^3-9c_1c_2+27c_3)t^3+(c_1^2-3c_2)^3=0.$$

Solving it as a quadratic equation for t^3, we obtain two roots θ and θ', and then obtain

$$\psi_1=\sqrt[3]{\theta}, \qquad \psi_4=\sqrt[3]{\theta'}.$$

Here $\sqrt[3]{\theta}$ may be chosen to be an arbitrary one of the cube roots of θ, but $\sqrt[3]{\theta'}$ is then that definite cube root of θ' for which

$$\sqrt[3]{\theta}\cdot\sqrt[3]{\theta'}=c_1^2-3c_2. \tag{10}$$

We have therefore the following known expressions:

$$x_1+\omega x_2+\omega^2x_3=\sqrt[3]{\theta}, \qquad x_1+\omega^2x_2+\omega x_3=\sqrt[3]{\theta'}, \qquad x_1+x_2+x_3=c_1.$$

---

* The fundamental theorem on symmetric functions is proved in the Appendix.

Multiplying them by 1, 1, 1; then by $\omega^2, \omega, 1$; and finally by $\omega, \omega^2, 1$; and adding the resulting equations in each case, we get

$$\text{(11)} \qquad \begin{cases} x_1 = \tfrac{1}{3}(c_1 + \sqrt[3]{\theta} + \sqrt[3]{\theta'}), \\ x_2 = \tfrac{1}{3}(c_1 + \omega^2\sqrt[3]{\theta} + \omega\,\sqrt[3]{\theta'}), \\ x_3 = \tfrac{1}{3}(c_1 + \omega\,\sqrt[3]{\theta} + \omega^2\,\sqrt[3]{\theta'}). \end{cases}$$

4. Quartic equation. The general equation of degree four,

$$\text{(12)} \qquad x^4 + ax^3 + bx^2 + cx + d = 0,$$

may be written in the form

$$(x^2 + \tfrac{1}{2}ax)^2 = (\tfrac{1}{4}a^2 - b)x^2 - cx - d.$$

With Ferrari, we add $(x^2 + \frac{1}{2}ax)y + \frac{1}{4}y^2$ to each member. Then

$$\text{(13)} \qquad (x^2 + \tfrac{1}{2}ax + \tfrac{1}{2}y)^2 = (\tfrac{1}{4}a^2 - b + y)x^2 + (\tfrac{1}{2}ay - c)x + \tfrac{1}{4}y^2 - d.$$

We seek a value y_1 of y such that the second member of (13) shall be a perfect square. Set

$$\text{(14)} \qquad a^2 - 4b + 4y_1 = t^2.$$

The condition for a perfect square requires that

$$\text{(15)} \qquad \tfrac{1}{4}t^2x^2 + (\tfrac{1}{2}ay_1 - c)x + \tfrac{1}{4}y_1^{\,2} - d = \left(\tfrac{1}{2}tx + \frac{\frac{1}{2}ay_1 - c}{t}\right)^2.$$

$$\therefore\ \tfrac{1}{4}y_1^{\,2} - d = \left(\frac{\frac{1}{2}ay_1 - c}{t}\right)^2 = \frac{(\frac{1}{2}ay_1 - c)^2}{a^2 - 4b + 4y_1}.$$

Hence y_1 must be a root of the cubic, called the *resolvent*,

$$\text{(16)} \qquad y^3 - by^2 + (ac - 4d)y - a^2d + 4bd - c^2 = 0.$$

In view of (15), equation (13) leads to the two quadratic equations

$$\text{(17)} \qquad x^2 + (\tfrac{1}{2}a - \tfrac{1}{2}t)x + \tfrac{1}{2}y_1 - (\tfrac{1}{2}ay_1 - c)/t = 0,$$

$$\text{(18)} \qquad x^2 + (\tfrac{1}{2}a + \tfrac{1}{2}t)x + \tfrac{1}{2}y_1 + (\tfrac{1}{2}ay_1 - c)/t = 0.$$

Let x_1 and x_2 be the roots of (17), x_3 and x_4 the roots of (18). Then

$$x_1 + x_2 = -\tfrac{1}{2}a + \tfrac{1}{2}t, \quad x_1x_2 = \tfrac{1}{2}y_1 - (\tfrac{1}{2}ay_1 - c)/t,$$

$$x_3 + x_4 = -\tfrac{1}{2}a - \tfrac{1}{2}t, \quad x_3x_4 = \tfrac{1}{2}y_1 + (\tfrac{1}{2}ay_1 - c)/t.$$

By addition and subtraction, we get

$$(19) \qquad x_1+x_2-x_3-x_4=t, \quad x_1x_2+x_3x_4=y_1.$$

In solving (17) and (18), two radicals are introduced, one equal to x_1-x_2 and the other equal to x_3-x_4 (see § 1). Hence all the irrationalities entering the expressions for the roots of the general quartic are rational functions of its roots.

If, instead of y_1, another root of the resolvent cubic (16) be employed, quadratic equations different from (17) and (18) are obtained, such, however, that their four roots are x_1, x_2, x_3, x_4, but paired differently. It is therefore natural to expect that the three roots of (16) are

$$(20) \qquad y_1=x_1x_2+x_3x_4, \quad y_2=x_1x_3+x_2x_4, \quad y_3=x_1x_4+x_2x_3.$$

It is shown in the next section that this inference is correct.

5. Without having recourse to Ferrari's device, the two quadratic equations whose roots are the four roots of the general quartic equation (12) may be obtained by an *à priori* study of the rational functions $x_1x_2+x_3x_4$ and $x_1+x_2-x_3-x_4=t$. The three quantities (20) are the roots of $(y-y_1)(y-y_2)(y-y_3)=0$, or

$$(21) \qquad y^3-(y_1+y_2+y_3)y^2+(y_1y_2+y_1y_3+y_2y_3)y-y_1y_2y_3=0.$$

Its coefficients may be expressed * as rational functions of a, b, c, d:

$$y_1+y_2+y_3=x_1x_2+x_3x_4+x_1x_3+x_2x_4+x_1x_4+x_3x_4=b,$$

$$\begin{aligned} y_1y_2+y_1y_3+y_2y_3 &= -4x_1x_2x_3x_4 \\ &\quad +(x_1+x_2+x_3+x_4)(x_1x_2x_3+x_1x_2x_4+x_1x_3x_4+x_2x_3x_4) \\ &= ac-4d, \end{aligned}$$

$$\begin{aligned} y_1y_2y_3 &= (x_1x_2x_3+x_1x_2x_4+x_1x_3x_4+x_2x_3x_4)^2 \\ &\quad +x_1x_2x_3x_4\{(x_1+x_2+x_3+x_4)^2-4(x_1x_2+x_1x_3+\dots+x_3x_4)\} \\ &= c^2+d(a^2-4b). \end{aligned}$$

---

* This is due to the fact (shown in § 29, Ex. 2, and § 30) that any permutation of x_1, x_2, x_3, x_4 merely permutes y_1, y_2, y_3, so that any symmetric function of y_1, y_2, y_3 is a symmetric function of x_1, x_2, x_3, x_4 and hence rationally expressible in terms of a, b, c, d.

Hence equation (21) is identical with the resolvent (16). Next,

$$\begin{aligned} t^2 &= (x_1+x_2+x_3+x_4)^2-4(x_1+x_2)(x_3+x_4) \\ &= a^2-4(x_1x_2+x_1x_3+\dots+x_3x_4)+4x_1x_2+4x_3x_4 \\ &= a^2-4b+4y_1. \end{aligned}$$

Again, $x_1+x_2+x_3+x_4=-a$. Hence

$$x_1+x_2=\tfrac{1}{2}(t-a), \quad x_3+x_4=\tfrac{1}{2}(-t-a).$$

To find x_1x_2 and x_3x_4, we note that their sum is y_1, while

$$-c=x_1x_2(x_3+x_4)+x_3x_4(x_1+x_2)=x_1x_2\left(\frac{-t-a}{2}\right)+x_3x_4\left(\frac{t-a}{2}\right).$$

$$\therefore\ x_1x_2=(c-\tfrac{1}{2}ay_1+\tfrac{1}{2}ty_1)/t, \qquad x_3x_4=(-c+\tfrac{1}{2}ay_1+\tfrac{1}{2}ty_1)/t.$$

Hence x_1 and x_2 are the roots of (17), x_3 and x_4 are the roots of (18).

6. Lagrange's *à priori* solution of the quartic (12) is quite similar to the preceding. A root $y_1=x_1x_2+x_3x_4$ of the cubic (16) is first obtained. Then $x_1x_2\equiv z_1$ and $x_3x_4\equiv z_2$ are the roots of

$$z^2-y_1z+d=0.$$

Then x_1+x_2 and x_3+x_4 are found from the relations

$$(x_1+x_2)+(x_3+x_4)=-a,$$

$$z_2(x_1+x_2)+z_1(x_3+x_4)=x_3x_4x_1+x_3x_4x_2+x_1x_2x_3+x_1x_2x_4=-c.$$

$$\therefore\ x_1+x_2=\frac{-az_1+c}{z_1-z_2}, \quad x_3+x_4=\frac{az_2-c}{z_1-z_2}.$$

Hence x_1 and x_2 are given by a quadratic, as also x_3 and x_4.

7. In solving the auxiliary cubic (16), the first irrationality entering (see § 2) is

$$\Delta\equiv(y_1-y_2)(y_2-y_3)(y_1-y_3).$$

But
$$y_1-y_2=(x_1-x_4)(x_2-x_3),$$

$$y_2-y_3=(x_1-x_2)(x_3-x_4), \quad y_1-y_3=(x_1-x_3)(x_2-x_4),$$

in view of (20). Hence

(22) $$\Delta=(x_1-x_2)(x_1-x_3)(x_1-x_4)(x_2-x_3)(x_2-x_4)(x_3-x_4).$$

By § 2, the reduced form of (16) is $\eta^3+P\eta+Q=0$, where

(23)
$$\begin{cases} P=ac-4d-\frac{1}{3}b^2, \\ Q=-a^2d+\frac{1}{3}abc+\frac{8}{3}bd-c^2-\frac{2}{27}b^3. \end{cases}$$

Applying (8), with a change of sign, we get

(24)
$$\Delta=6\sqrt{-3}\sqrt{\tfrac{1}{4}Q^2+\tfrac{1}{27}P^3}.$$

CHAPTER II.

SUBSTITUTIONS; RATIONAL FUNCTIONS.

8. The operation which replaces x_1 by x_α, x_2 by x_β, x_3 by x_γ, . . . , x_n by x_ν, where $\alpha, \beta, \ldots, \nu$ form a permutation of $1, 2, \ldots, n$, is called a **substitution** on $x_1, x_2, x_3, \ldots, x_n$. It is usually designated

$$\begin{pmatrix} x_1 & x_2 & x_3 & \ldots & x_n \\ x_\alpha & x_\beta & x_\gamma & \ldots & x_\nu \end{pmatrix}.$$

But the order of the columns is immaterial; the substitution may also be written

$$\begin{pmatrix} x_2 & x_1 & x_3 & \ldots & x_n \\ x_\beta & x_\alpha & x_\gamma & \ldots & x_\nu \end{pmatrix}, \quad \text{or} \quad \begin{pmatrix} x_n & x_1 & x_2 & x_3 & \ldots \\ x_\nu & x_\alpha & x_\beta & x_\gamma & \ldots \end{pmatrix}, \ldots$$

The substitution which leaves every letter unaltered,

$$\begin{pmatrix} x_1 & x_2 & x_3 & \ldots & x_n \\ x_1 & x_2 & x_3 & \ldots & x_n \end{pmatrix},$$

is called the **identical substitution** and is designated I.

9. THEOREM. *The number of distinct substitutions on n letters is $n! \equiv n(n-1) \ldots 3 \cdot 2 \cdot 1$.*

For, to every permutation of the n letters there corresponds a substitution.

EXAMPLE. The $3! = 6$ substitutions on $n = 3$ letters are:

$$I = \begin{pmatrix} x_1 & x_2 & x_3 \\ x_1 & x_2 & x_3 \end{pmatrix}, \quad a = \begin{pmatrix} x_1 & x_2 & x_3 \\ x_2 & x_3 & x_1 \end{pmatrix}, \quad b = \begin{pmatrix} x_1 & x_2 & x_3 \\ x_3 & x_1 & x_2 \end{pmatrix},$$
$$c = \begin{pmatrix} x_1 & x_2 & x_3 \\ x_1 & x_3 & x_2 \end{pmatrix}, \quad d = \begin{pmatrix} x_1 & x_2 & x_3 \\ x_3 & x_2 & x_1 \end{pmatrix}, \quad e = \begin{pmatrix} x_1 & x_2 & x_3 \\ x_2 & x_1 & x_3 \end{pmatrix}.$$

Applying these substitutions to the function $\psi \equiv x_1 + \omega x_2 + \omega^2 x_3$, we obtain the following six distinct functions (cf. § 3):

$$\psi_I = x_1 + \omega x_2 + \omega^2 x_3 \equiv \psi, \quad \psi_a = x_2 + \omega x_3 + \omega^2 x_1 = \omega^2 \psi, \quad \psi_b = x_3 + \omega x_1 + \omega^2 x_2 = \omega \psi,$$
$$\psi_c = x_1 + \omega x_3 + \omega^2 x_2, \quad \psi_d = x_3 + \omega x_2 + \omega^2 x_1 = \omega^2 \psi_c, \quad \psi_e = x_2 + \omega x_1 + \omega^2 x_3 = \omega \psi_c.$$

Applying them to the function $\phi \equiv (x_1-x_2)(x_2-x_3)(x_3-x_1)$, we obtain

$$\phi_I=\phi_a=\phi_b=\phi, \qquad \phi_c=\phi_d=\phi_e=-\phi.$$

Hence ϕ remains unaltered by I, a, b, but is changed by c, d, e.

10. Product. Apply first a substitution s and afterwards a substitution t, where

$$s=\begin{pmatrix} x_1 & x_2 & \dots & x_n \\ x_\alpha & x_\beta & \dots & x_\nu \end{pmatrix}, \quad t=\begin{pmatrix} x_\alpha & x_\beta & \dots & x_\nu \\ x_{\alpha'} & x_{\beta'} & \dots & x_{\nu'} \end{pmatrix}.$$

The resulting permutation $x_{\alpha'}, x_{\beta'}, \dots, x_{\nu'}$ can be obtained directly from the original permutation $x_1, x_2, \dots, x_n$ by applying a *single* substitution, namely,

$$u=\begin{pmatrix} x_1 & x_2 & \dots & x_n \\ x_{\alpha'} & x_{\beta'} & \dots & x_{\nu'} \end{pmatrix}.$$

We say that u is the **product** of s by t and write $u=st$.

Similarly, stv denotes the substitution w which arises by applying first s, then t, and finally v, so that $stv=uv=w$. The order of applying the factors is from left to right.*

EXAMPLES. For the substitutions on three letters (§ 9),

$$ab=ba=I, \quad ac=d, \quad ca=e, \quad ad=e, \quad da=c,$$
$$aa=b, \quad bb=a, \quad abc=Ic=c, \quad aca=da=c.$$

Applying the substitution a to the function ψ, we get ψ_a; applying the substitution c to ψ_a, we get ψ_d. Hence $\psi_{ac}=\psi_d$. Likewise $\psi_{ab}=\psi_I=\psi$, $\psi_{ba}=\psi$.

11. Multiplication of substitutions is **not commutative** in general.

Thus, in the preceding example, $ac\neq ca$, $ad\neq da$. But $ab=ba$, so that a and b are said to be **commutative.**

12. Multiplication of substitutions is **associative**: $st\cdot v=s\cdot tv$.

Let s, t, and their product $st=u$ have the notations of § 10. If

$$v=\begin{pmatrix} x_{\alpha'} & x_{\beta'} & \dots & x_{\nu'} \\ x_{\alpha''} & x_{\beta''} & \dots & x_{\nu''} \end{pmatrix}, \quad \text{then } tv=\begin{pmatrix} x_\alpha & x_\beta & \dots & x_\nu \\ x_{\alpha''} & x_{\beta''} & \dots & x_{\nu''} \end{pmatrix}.$$

$$\therefore\ st\cdot v=uv=\begin{pmatrix} x_1 & x_2 & \dots & x_n \\ x_{\alpha''} & x_{\beta''} & \dots & x_{\nu''} \end{pmatrix}=\begin{pmatrix} x_1 & x_2 & \dots & x_n \\ x_\alpha & x_\beta & \dots & x_\nu \end{pmatrix}\begin{pmatrix} x_\alpha & \dots & x_\nu \\ x_{\alpha''} & \dots & x_{\nu''} \end{pmatrix}=s\cdot tv.$$

EXAMPLE. For 3 letters, $ac\cdot a=da=c$, $a\cdot ca=ae=c$.

---

* This is the modern use. The inverse order ts, vts was used by Cayley and Serret.

13. Powers. We write s^2 for ss, s^3 for sss, etc. Then

(25) $$s^m s^n = s^{m+n} \qquad (m \text{ and } n \text{ positive integers}).$$

For, by the associative law, $s^m s^n = s^m \cdot s s^{n-1} = s^{m+1} s^{n-1} = \ldots$

14. Period. Since there is only a finite number $n!$ of distinct substitutions on n letters, some of the powers

$$s,\ s^2,\ s^3,\ \ldots \textit{ ad infinitum}$$

must be equal, say $s^m = s^{m+n}$, where m and n are positive integers. Then $s^m = s^m s^n$, in view of (25). Hence s^n leaves unaltered each of the n letters, so that $s^n = I$.

The *least* positive integer σ such that $s^\sigma = I$ is called the **period** of s. It follows that

(26) $$s,\ s^2,\ \ldots\ s^{\sigma-1},\ s^\sigma \equiv I$$

are all distinct; while $s^{\sigma+1}$, $s^{\sigma+2}, \ldots,$ $s^{2\sigma-1}$, $s^{2\sigma}$ are repetitions of the substitutions (26). Hence the first σ powers are repeated periodically in the infinite series of powers.

EXAMPLES. From the example in § 10, we get

$a^2 = b$, $a^3 = a^2 a = ba = I$, whence a is of period 3;
$b^2 = a$, $b^3 = b^2 b = ab = I$, whence b is of period 3;
c, d, e are of period 2; I is of period 1.

15. Inverse substitution. To every substitution s there corresponds one and only one substitution s' such that $ss' = I$. If

$$s = \begin{pmatrix} x_1 & x_2 & \ldots & x_n \\ x_\alpha & x_\beta & \ldots & x_\nu \end{pmatrix}, \text{ then } s' = \begin{pmatrix} x_\alpha & x_\beta & \ldots & x_\nu \\ x_1 & x_2 & \ldots & x_n \end{pmatrix}.$$

Evidently $s's = I$. We call s' the **inverse** of s and denote it henceforth by s^{-1}. Hence

$$ss^{-1} = s^{-1}s = I, \quad (s^{-1})^{-1} = s.$$

If s is of period σ, then $s^{-1} = s^{\sigma-1}$. Since s replaces a rational function $f \equiv f(x_1, \ldots, x_n)$ by $f_s \equiv f(x_\alpha, \ldots, x_\nu)$, s^{-1} replaces f_s by f.

EXAMPLES For the substitutions on 3 letters (§ 9),

$$a = \begin{pmatrix} x_1 & x_2 & x_3 \\ x_2 & x_3 & x_1 \end{pmatrix}, \quad a^{-1} = \begin{pmatrix} x_2 & x_3 & x_1 \\ x_1 & x_2 & x_3 \end{pmatrix} \equiv \begin{pmatrix} x_1 & x_2 & x_3 \\ x_3 & x_1 & x_2 \end{pmatrix} = b,$$

$$b^{-1} = a, \quad c^{-1} = c, \quad d^{-1} = d, \quad e^{-1} = e, \quad I^{-1} = I.$$

These results also follow from those of the examples in § 14. For the functions of § 9 the substitution a replaces ψ by ψ_a; $a^{-1}=b$ replaces ψ_a by ψ.

16. THEOREM. *If* $st=sr$, *then* $t=r$.

Multiplying st and sr on the left by s^{-1}, we get

$$s^{-1}st=t, \quad s^{-1}sr=r.$$

17. THEOREM. *If* $ts=rs$, *then* $t=r$.

18. Abbreviated notation for substitutions. Substitutions like

$$a=\begin{pmatrix}x_1 & x_2 & x_3\\ x_2 & x_3 & x_1\end{pmatrix}, \quad b=\begin{pmatrix}x_1 & x_3 & x_2\\ x_3 & x_2 & x_1\end{pmatrix}, \quad q=\begin{pmatrix}x_2 & x_3 & x_1 & x_4\\ x_3 & x_1 & x_4 & x_2\end{pmatrix},$$

which replace the first letter in the upper row by the second letter in the upper row, the second by the third letter in the upper row, and so on, finally, the last letter of the upper row by the first letter of the upper row, are called **circular substitutions** or **cycles.** Instead of the earlier double-row notation, we employ a single-row notation for cycles. Thus

$$a=(x_1x_2x_3), \quad b=(x_1x_3x_2), \quad q=(x_2x_3x_1x_4).$$

Evidently $(x_1x_2x_3)=(x_2x_3x_1)=(x_3x_1x_2)$, since each replaces x_1 by x_2, x_2 by x_3, and x_3 by x_1. *A cycle is not altered by a cyclic permutation of its letters.*

Any substitution can be expressed as a product of circular substitutions affecting different letters. Thus

$$\begin{pmatrix}x_1 & x_2 & x_3\\ x_1 & x_3 & x_2\end{pmatrix}=(x_1)(x_2x_3), \quad \begin{pmatrix}x_1 & x_2 & x_3 & x_4 & x_5 & x_6\\ x_3 & x_6 & x_5 & x_4 & x_1 & x_2\end{pmatrix}=(x_1x_3x_5)(x_2x_6)(x_4).$$

A cycle of a single letter is usually suppressed, with the understanding that a letter not expressed is unaltered by the substitution. Thus $(x_1)(x_2x_3)$ is written (x_2x_3).

A circular substitution of two letters is called a **transposition.**

19. Tables of all substitutions on n letters, for $n=3$, 4, 5.

For $n=3$, the $3!=6$ substitutions are (compare § 9):

$I=$identity, $\quad a=(x_1x_2x_3), \quad b=(x_1x_3x_2),$
$c=(x_2x_3), \quad d=(x_1x_3), \quad e=(x_1x_2).$

For $n=4$, the 24 substitutions are (only the indices being written):

I = identity;

6 transpositions: (12), (13), (14), (23), (24), (34);

8 cycles of 3 letters: (123), (132), (124), (142), (134), (143), (234), (243);

6 cycles of 4 letters: (1234), (1243), (1324), (1342), (1423), (1432);

3 products of 2 transpositions: (12)(34), (13)(24), (14)(23).

For $n=5$ the $5!=120$ substitutions include

I = identity;

$\frac{5\cdot 4}{2}=10$ transpositions of type (12);

$\frac{5\cdot 4\cdot 3}{3}=20$ cycles of type (123);

$\frac{5\cdot 4\cdot 3\cdot 2}{4}=30$ cycles of type (1234);

$\frac{5\cdot 4\cdot 3\cdot 2\cdot 1}{5}=24$ cycles of type (12345);

$5\cdot 3=15$ * products of type (12)(34);

20 † products of type (123)(45).

EXERCISES.

1. The period of $(1\ 2\ 3\ \ldots\ n)$ is n; its inverse is $(n\ n-1\ \ldots\ 3\ 2\ 1)$.

2. The period of any substitution is the least common multiple of the periods of its cycles. Thus (123)(45) is of period 6.

3. Give the number of substitutions on 6 letters of each type.

4. Show that the function $x_1x_2+x_3x_4$ is unaltered by the substitutions I, (x_1x_2), (x_3x_4), $(x_1x_2)(x_3x_4)$, $(x_1x_3)(x_2x_4)$, $(x_1x_4)(x_2x_3)$, $(x_1x_3x_2x_4)$, $(x_1x_4x_2x_3)$.

5. Show that $x_1x_2+x_3x_4$ is changed into $x_1x_3+x_2x_4$ by (x_2x_3), (x_1x_4), $(x_1x_3x_2)$, $(x_1x_2x_4)$, $(x_1x_4x_3)$, $(x_2x_3x_4)$, $(x_1x_2x_4x_3)$, $(x_1x_3x_4x_2)$.

6. Write down the eight substitutions on four letters not given in Exs. 4 and 5, and show that each changes $x_1x_2+x_3x_4$ into $x_1x_4+x_2x_3$.

---

* Since the omitted letter may be any one of five, while one of the four chosen letters may be associated with any one of the other three letters.

† The same number as of type (123), since (45) = (54).

CHAPTER III.

SUBSTITUTION GROUPS; RATIONAL FUNCTIONS.

20. A set of distinct substitutions $s_1, s_2, \ldots, s_m$ forms a **group** if the product of any two of them (whether equal or different) is a substitution of the set. The number m of distinct substitutions in a group is called its **order**, the number n of letters operated on by its substitutions is called its **degree**. The group is designated $G_m^{(n)}$.

All the $n!$ substitutions on n letters form a group, called the **symmetric group on** n **letters** $G_{n!}^{(n)}$. In fact, the product of any two substitutions on n letters is a substitution on n letters. The name of this group is derived from the fact that its substitutions leave unaltered any rational symmetric function of the letters.

EXAMPLE 1. For the six substitutions on $n=3$ letters, given in § 9, the *multiplication table* is as follows:*

$G_6^{(3)}$:

	I	a	b	c	d	e
I	I	a	b	c	d	e
a	a	b	I	d	e	c
b	b	I	a	e	c	d
c	c	e	d	I	b	a
d	d	c	e	a	I	b
e	e	d	c	b	a	I

Thus $ad=e$ is given in the intersection of row a and column d.

EXAMPLE 2. The substitutions I, a, b form a group with the multiplication table

	I	a	b
I	I	a	b
a	a	b	I
b	b	I	a

* It was partially established in the example of § 10.

If s is a substitution of period m, the substitutions

$$I, s, s^2, \ldots, s^{m-1}$$

form a group of order m called **a cyclic group.**

EXAMPLE 3. I, $a=(123)$, $b=a^2=(132)$ form a cyclic group (Ex. 2).

EXAMPLE 4. I, $s=(123)(45)$, $s^2=(132)$, $s^3=(45)$, $s^4=(123)$, $s^5=(132)(45)$ form a cyclic group of order 6 and degree 5.

21. FUNDAMENTAL THEOREM. *All the substitutions on x_1, $x_2, \ldots, x_n$ which leave unaltered a rational function $\phi(x_1, x_2, \ldots, x_n)$ form a group G.*

Let ϕ_s denote the function obtained by applying to ϕ the substitution s. If a and b are two substitutions which leave ϕ unaltered, then $\phi_a \equiv \phi$, $\phi_b \equiv \phi$. Hence

$$(\phi_a)_b = (\phi)_b = \phi_b = \phi, \quad \text{or} \quad \phi_{ab} = \phi.$$

Hence the product ab is one of the substitutions which leave ϕ unaltered. Hence the set has the group property.

The group G is called the **group of the function** ϕ, while ϕ is said to **belong to the group** G.

EXAMPLE 1. The only substitutions on 3 letters which leave unaltered the function $(x_1-x_2)(x_2-x_3)(x_3-x_1)$ are (by § 9) I, $a=(x_1x_2x_3)$, $b=(x_1x_3x_2)$. Hence they form a group (compare Ex. 2, § 20). Another function belonging to this group is

$$(x_1+\omega x_2+\omega^2 x_3)^3, \quad \omega \text{ an imaginary cube root of unity.}$$

EXAMPLE 2. The only substitution on 3 letters which leaves unaltered $x_1+\omega x_2+\omega^2 x_3$ is the identity I (§ 9). Thus the substitution I alone forms a group G_1 of order 1.

EXAMPLE 3. The rational functions occurring in the solution of the quartic equation (§ 4) furnish the following substitution groups on four letters:

a) The symmetric group G_{24} of all the substitutions on 4 letters.

b) The group to which the function $y_1=x_1x_2+x_3x_4$ belongs (Exs. 4–6, p. 14):

$$G_8=\{I, (12), (34), (12)(34), (13)(24), (14)(23), (1324), (1423)\}.$$

c) Since $y_2 \equiv x_1x_3+x_2x_4$ is derived from $y_1 \equiv x_1x_2+x_3x_4$ by interchanging x_2 and x_3, the group of y_2 is derived from G_8 by interchanging x_2 and x_3 within its substitutions. Hence the group of y_2 is

$$G_8'=\{I, (13), (24), (13)(24), (12)(34), (14)(32), (1234), (1432)\}.$$

d) The group of $y_3 \equiv x_1x_4 + x_2x_3$, derived from G_8 by interchanging x_2 and x_4, is:

$$G_8'' = \{I, (14), (32), (14)(32), (13)(42), (12)(43), (1342), (1243)\}.$$

e) The function $x_1 + x_2 - x_3 - x_4$ belongs to the group

$$H_4 = \{I, (12), (34), (12)(34)\}.$$

Since all the substitutions of H_4 are contained in the group G_8, H_4 is called a **subgroup** of G_8. But H_4 is not a subgroup of G_8'.

f) The function $\psi \equiv y_1 + \omega y_2 + \omega^2 y_3$, or

$$\psi \equiv x_1x_2 + x_3x_4 + \omega(x_1x_3 + x_2x_4) + \omega^2(x_1x_4 + x_2x_3),$$

remains unaltered by the substitutions which leave y_1, y_2, and y_3 simultaneously unaltered and by no other substitutions. Hence the group of ψ is composed of the substitutions common to the three groups G_8, G_8', G_8'', forming their **greatest common subgroup**:

$$G_4 = \{I, r = (12)(34), s = (13)(24), t = (14)(23)\}$$

That these four substitutions form a group may be verified directly:

$$r^2 = I,\ s^2 = I,\ t^2 = I,$$

$$rs = sr = t,\ rt = tr = s,\ st = ts = r.$$

Hence any two of its substitutions are commutative. This **commutative group** G_4 is therefore a subgroup of G_8, G_8', and G_8''.

22. THEOREM. *Every substitution can be expressed as a product of transpositions in various ways.*

Any substitution can be expressed as a product of cycles on different letters (§ 18). A single cycle on n letters can be expressed as a product of $n-1$ transpositions:

$$(1234 \ldots n) = (12)(13)(14) \ldots (1n).$$

EXAMPLES. $(123)(456) = (12)(13)(45)(46)$,
$(132) = (13)(12) = (12)(23) = (12)(23)(45)(45)$.

23. THEOREM. *Of the various decompositions of a given substitution s into a product of transpositions, all contain an even number of transpositions (whence s is called an* **even substitution**), *or all contain an odd number of transpositions (whence s is called an* **odd substitution**).

A single transposition changes the sign of the **alternating function** *

$$\phi = (x_1 - x_2)(x_1 - x_3)(x_1 - x_4) \dots (x_1 - x_n)$$
$$\cdot (x_2 - x_3)(x_2 - x_4) \dots (x_2 - x_n)$$
$$\dots\dots\dots$$
$$\cdot (x_{n-1} - x_n).$$

Thus $(x_1 x_2)$ affects only the terms in the first and second lines of the product, and replaces them by

$$(x_2 - x_1)(x_2 - x_3)(x_2 - x_4) \dots (x_2 - x_n)$$
$$\cdot (x_1 - x_3)(x_1 - x_4) \dots (x_1 - x_n).$$

Hence, if s is the product of an even number of transpositions, it leaves ϕ unaltered; if s is the product of an odd number of transpositions, it changes ϕ into $-\phi$.

Corollary. The totality of even substitutions on n letters forms a group, called the **alternating group on n letters.**

Example 1. The alternating group on 3 letters is (§§ 9, 19)

$$G_3^{(3)} = \{I, \quad (123), \quad (132)\}.$$

Example 2. The alternating group on 4 letters is (§ 19)

$$G_{12}^{(4)} = \{I,\ (12)(34),\ (13)(24),\ (14)(23), \text{ and the 8 cycles of three letters}\}.$$

24. Theorem. *The order of the alternating group on n letters is $\frac{1}{2} \cdot n!$*

Denote the distinct *even* substitutions by

$$(e) \qquad e_1,\ e_2,\ e_3,\ \dots,\ e_k.$$

Let t be a transposition. Then the products

$$(o) \qquad e_1 t,\ e_2 t,\ e_3 t,\ \dots,\ e_k t$$

are all distinct (§ 17) and being *odd* are all different from the substitutions (e). Moreover, every odd substitution s occurs in

* It may be expressed as the determinant

$$\begin{vmatrix} 1 & x_1 & x_1^2 & \dots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \dots & x_2^{n-1} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 1 & x_n & x_n^2 & \dots & x_n^{n-1} \end{vmatrix}.$$

the set (o), since st is even and hence identical with a certain e_i, so that

$$s=e_i t^{-1}=e_i t.$$

Hence the $2k$ substitutions given by (e) and (o) furnish all the $n!$ substitutions on n letters without repetitions. Hence $k=\frac{1}{2}\cdot n!$

25. As shown in § 21, every rational function $\phi(x_1, \ldots, x_n)$ *belongs* to a certain group G of substitutions on $x_1, \ldots, x_n$, namely, is unaltered by the substitutions of G and changed by all other substitutions on $x_1, \ldots, x_n$. We next prove the inverse theorem:

Given a group G of substitutions on $x_1, \ldots, x_n$, we can construct a rational function $\phi(x_1, \ldots, x_n)$ belonging to G.

Let $G=\{a\equiv I, b, c, \ldots, l\}$ and consider the function

$$V=m_1x_1+m_2x_2+\ \ldots\ +m_nx_n,$$

where $m_1, m_2, \ldots, m_n$ are all distinct. Then V is an $n!$-valued function. Applying to V the substitutions of G, we get

(27) $$V_a\equiv V, V_b, \ldots, V_l.$$

all of which are distinct. Applying to (27) any substitution c of G, we get

(28) $$V_{ac}, V_{bc}, \ldots. V_{lc}.$$

These values are a permutation of the values (27). since $ac, bc, \ldots, lc$ all belong to the *group* G and are all distinct (§ 17). Hence any symmetric function of $V_a, V_b, \ldots, V_l$ is unaltered by all the substitutions of G. By suitable choice of the parameter ρ, the symmetric function

$$\phi\equiv(\rho-V)(\rho-V_b)(\rho-V_c)\ \ldots\ (\rho-V_l)$$

will be altered by every substitution s not in G. Indeed,

$$\phi_s\equiv(\rho-V_s)(\rho-V_{bs})(\rho-V_{cs})\ \ldots\ (\rho-V_{ls})$$

is not identical with ϕ since V_s is different from $V, V_b, V_c, \ldots, V_l$.

EXAMPLE 1. For $G=\{I, a=(x_1x_2x_3), b=(x_1x_3x_2)\}$, take

$$V=x_1+\omega x_2+\omega^2x_3.$$

Then $V_a=\omega^2V$, $V_b=\omega V$. Hence

$$V+V_a+V_b=(1+\omega+\omega^2)V=0,\ VV_a+VV_b+V_aV_b=0,\ VV_aV_b=V^3.$$

The function V^3 belongs to G (see Ex. 1, § 21).

EXAMPLE 2. For $G=\{I, c=(x_2x_3)\}$, take the V of Ex. 1. Then

$$VV_c=(x_1+\omega x_2+\omega^2x_3)(x_1+\omega x_3+\omega^2x_2)=c_1{}^2-3c_2$$

is unaltered by all six substitutions on the three letters. But

$$\phi=(\rho-V)(\rho-V_c)=\rho^2-(2x_1-x_2-x_3)\rho+c_1{}^2-3c_2,$$

for $\rho\neq 0$, is changed by every substitution on the letters not in G. Hence, for any $\rho\neq 0$, ϕ belongs to G.

EXERCISES.

Ex. 1. If ω is a primitive μth root of unity,

$$(x_1+\omega x_2+\omega^2x_3+\ \ldots\ +\omega^{\mu-1}x_\mu)^\mu$$

belongs to the cyclic group $\{I,\ a,\ a^2, \ldots,\ a^{\mu-1}\}$, where $a\equiv(x_1x_2\ldots x_\mu)$.

Ex. 2. Taking $V=x_1+ix_2-x_3-ix_4$ and $s=(x_1x_2)(x_3x_4)$, show that $VV_s\equiv i(x_1-x_3)^2+i(x_2-x_4)^2$ belongs to G_8 of § 21, that $V+V_s$ belongs to H_4 of § 21, while $(\rho-V)(\rho-V_s)$, for $\rho\neq 0$, belongs to the group $\{I, s\}$

Ex 3. Taking $V=x_1+ix_2-x_3-ix_4$ and $t=(x_1x_3)(x_2x_4)$, show that VV_t belongs to the group $\{I, t\}$

Ex. 4. If $a_1, a_2, \ldots, a_n$ are any distinct numbers, the function

$$V=x_1{}^{a_1}x_2{}^{a_2}\ldots x_n{}^{a_n}$$

is $n!$-valued, and $V+V_b+V_c+\ \ldots\ +V_l$ belongs to $\{I, b, c, \ldots, l\}$.

Ex. 5. If ϕ belongs to G and ϕ' belongs to G', constants a and a' exist such that $a\phi+a'\phi'$ belongs to the greatest common subgroup of G and G'.

26. THEOREM. *The order of a subgroup is a divisor of the order of the group.*

Consider a group G of order N and a subgroup H composed of the substitutions

(29) $$h_1=I,\ h_2,\ h_3, \ldots,\ h_P.$$

If G contains no further substitutions. $N=P$, and the theorem is true. Let next G contain a substitution g_2 not in H. Then G contains the products

(30) $$g_2,\ h_2g_2,\ h_3g_2, \ldots,\ h_Pg_2.$$

The latter are all distinct (§ 17), and all different from the substitutions (29), since $h_\alpha g_2=h_\beta$ requires that $g_2=h_\alpha^{-1}h_\beta=$ a substitution of H contrary to hypothesis. Hence the substitutions (29) and (30) give $2P$ distinct substitutions of G. If there are no other substitutions in G, $N=2P$ and the theorem is true. Let next G contain a substitution g_3 not in one of the sets (29) and (30). Then G contains

$$(31) \qquad g_3, h_2g_3, h_3g_3, \ldots, h_Pg_3.$$

As before, the substitutions (31) are all distinct and all different from the substitutions (29). Moreover, they are all different from the substitutions (30), since $h_\alpha g_3 = h_\beta g_2$ requires that $g_3 = h_\alpha^{-1}h_\beta g_2$ shall belong to the set (30), contrary to hypothesis. We now have $3P$ distinct substitutions of G. Either $N=3P$ or else G contains a substitution g_4 not in one of the sets (29), (30) (31) In the latter case, G contains the products

$$(32) \qquad g_4, h_2g_4, h_3g_4, \ldots, h_Pg_4,$$

all of which are distinct and all different from the substitutions (29), (30), (31), so that we have $4P$ distinct substitutions. Proceeding in this way, we finally reach a last set of P substitutions

$$(33) \qquad g_\nu, h_2g_\nu, h_3g_\nu, \ldots, h_Pg_\nu,$$

since the order of H is finite (§ 9). Hence $N=\nu P$.

DEFINITION. The number $\nu = \frac{N}{P}$ is called the **index** of the subgroup H under G, and the relation is exhibited in the adjacent scheme.

$$\begin{array}{c} G \\ \nu \big| \\ H \end{array}$$

COROLLARY. The order of any group H of substitutions on n letters is a divisor of $n!$ Indeed H is a subgroup of the symmetric group $G_{n!}$ on n letters.

27. THEOREM. *The period of any substitution contained in a group G of order N is a divisor of N.*

If the group G contains a substitution s of period P, it contains the cyclic subgroup H of order P:

$$H = \{s, s^2, \ldots, s^{P-1}, s^P \equiv I\}.$$

Then, by § 26, P is a divisor of N.

COROLLARY.* If the order N of a group G is a *prime* number, G is a cyclic group composed of the first N powers of a substitution of period N.

28. As shown in § 26, the N substitutions of a group G can be arranged in a **rectangular array** with the substitutions of any subgroup H in the first row:

$$\begin{array}{lllll} h_1=I & h_2 & h_3 & \dots & h_P \\ g_2 & h_2g_2 & h_3g_2 & \dots & h_Pg_2 \\ g_3 & h_2g_3 & h_3g_3 & \dots & h_Pg_3 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ g_\nu & h_2g_\nu & h_3g_\nu & \dots & h_Pg_\nu \end{array}$$

Here $g_1=I$, g_2, g_3, ..., g_ν are called the right-hand **multipliers.** They may be chosen in various ways: g_2 is any substitution of G not in the first row; g_3 any substitution of G not in the first and second rows; g_4 any substitution of G not in the first, second, and third rows; etc.

Similarly, a rectangular array for the substitutions of G may be formed by employing left-hand multipliers.

29. THEOREM. *If ψ is a rational function of x_1. ..., x_n belonging to a subgroup H of index ν under G, then ψ is ν-valued under G.*

Apply to ψ all the N substitutions of G arranged in a rectangular array, as in § 28. All the substitutions belonging to a row give the same value since

$$\psi_{h_ig_a}=(\psi_{h_i})_{g_a}=(\psi)_{g_a}=\psi_{g_a}.$$

Hence there result at most ν values. But, if

$$\psi_{g_a}=\psi_{g_\beta} \qquad (\beta<a),$$

then $\psi_{g_ag_\beta^{-1}}=\psi$, so that $g_ag_\beta^{-1}$ is a substitution h_i leaving ψ

* This result is a special case of the following theorems, proved in any treatise on groups:

If the order of a group is divisible by a *prime* number p, the group contains a subgroup of order p (Cauchy)

If p^t is the highest power of the prime number p dividing the order of a group, the group contains a subgroup of order p^t (Sylow).

unaltered. Hence $g_\alpha = h_i g_\beta$, contrary to the assumption made in forming the rectangular array.

DEFINITION. The ν distinct functions $\psi, \psi_{g_2}, \psi_{g_3}, \ldots, \psi_{g_\nu}$ are called the **conjugate values** of ψ under the group G.

Taking G to be the symmetric group $G_{n!}$, we obtain Lagrange's result:

The number of distinct values which a rational function of n letters takes when operated on by all n! substitutions is a divisor of n!

EXAMPLE 1. To find the distinct conjugate values of the functions

$$\Delta \equiv (x_1 - x_2)(x_2 - x_3)(x_3 - x_1), \quad \theta \equiv (x_1 + \omega x_2 + \omega^2 x_3)^3$$

under the symmetric group G_6 on 3 letters, we note that they belong to the subgroup $G_3 = \{I, a = (x_1x_2x_3), b = (x_1x_3x_2)\}$, as remarked in § 21, Ex. 1. The rectangular array and the conjugate values are:

$$\begin{array}{ccc} I, & a = (x_1x_2x_3), & b = (x_1x_3x_2) \\ c = (x_2x_3), & ac = (x_3x_1), & bc = (x_1x_2) \end{array} \left\| \begin{array}{c} \Delta \\ -\Delta \end{array} \right| \begin{array}{c} \theta \\ \theta_c \end{array} \Bigg| .$$

EXAMPLE 2. To obtain the conjugate values of $x_1x_2 + x_3x_4$ under the symmetric group G_{24} on 4 letters, we rearrange the results of Exs. 4, 5, 6, page 14, and exhibit a rectangular array of the substitutions of G_{24} with those of G_8 in the first row:

I,	(12),	(34),	(12)(34),	(13)(24),	(14)(23),	(1324),	(1423)	$x_1x_2 + x_3x_4$
(234),	(1342),	(23),	(132),	(143),	(124),	(14),	(1243)	$x_1x_3 + x_2x_4$
(243),	(1432),	(24),	(142),	(123),	(134),	(1234),	(13),	$x_1x_4 + x_2x_3$

30. THEOREM. *The ρ distinct values which a rational function $\phi(x_1, \ldots, x_n)$ takes when operated on by all n! substitutions are the roots of an equation of degree ρ whose coefficients are rational functions of the elementary symmetric functions*

$$(34) \quad c_1 = x_1 + x_2 + \ldots + x_n, \quad c_2 = x_1x_2 + x_1x_3 + \ldots + x_{n-1}x_n, \ldots,$$
$$c_n = x_1x_2 \ldots x_n.$$

Let the ρ distinct values of $\phi(x_1, \ldots, x_n)$ be designated

$$(35) \qquad \phi_1 \equiv \phi, \quad \phi_2, \quad \phi_3, \quad \ldots, \quad \phi_\rho.$$

They are the roots of an equation $(y - \phi_1)(y - \phi_2) \ldots (y - \phi_\rho) = 0$ whose coefficients $\phi_1 + \phi_2 + \ldots + \phi_\rho, \ldots, \pm \phi_1\phi_2 \ldots \phi_\rho$ are symmetric functions of $\phi_1, \phi_2, \ldots, \phi_\rho$. After proving that they are symmetric functions of $x_1, x_2, \ldots, x_n$, we may conclude (Appendix) that they are rational functions of the expressions (34). We have therefore only to prove that any substitution s on $x_1, \ldots, x_n$ merely interchanges the functions (35). Let s replace the functions (35) by respectively

$$(36) \qquad \phi'_1, \phi'_2, \phi'_3, \ldots, \phi'_\rho.$$

In the first place, each ϕ' is identical with a function (35). For, there exists a substitution t which replaces ϕ_1 by ϕ_i, and s replaces ϕ_i by ϕ'_i, so that ts replaces ϕ_1 by ϕ'_i. Hence there is a substitution on $x_1, \ldots, x_n$ which replaces ϕ_1 by ϕ'_i, so that ϕ'_i occurs in the set (35).

In the second place, the functions (36) are all distinct. For, if $\phi'_i \equiv \phi'_j$, we obtain, upon applying the substitution s^{-1}, $\phi_i \equiv \phi_j$ contrary to assumption.

DEFINITION. The equation having the roots (35) is called the **resolvent equation** for ϕ.

Compare the solution of the general cubic (§ 3) and general quartic (§ 5).

31. LAGRANGE'S THEOREM. *If a rational function $\phi(x_1, x_2, \ldots, x_n)$ remains unaltered by all the substitutions which leave another rational function $\psi(x_1, x_2, \ldots, x_n)$ unaltered, then ϕ is a rational function of ψ and $c_1, c_2, \ldots, c_n$.*

The function ψ belongs to a certain group

$$H = \{h_1 \equiv I, h_2, h_3, \ldots, h_P\}.$$

Let ν be the index of H under the symmetric group $G_{n!}$. Consider a rectangular array of the substitutions of $G_{n!}$ with those of H in the first row:

$$\begin{array}{llll|l|l} I & h_2 & \ldots & h_P & \psi \;\;\equiv \psi_1 & \phi \equiv \phi_1 \\ g_2 & h_2 g_2 & \ldots & h_P g_2 & \psi_{g_2} \equiv \psi_2 & \phi_{g_2} \equiv \phi_2 \\ \cdot & \cdot & \cdot & \cdot & \cdot\;\;\cdot\;\;\cdot & \cdot\;\;\cdot\;\;\cdot \\ g_\nu & h_2 g_\nu & \ldots & h_P g_\nu & \psi_{g_\nu} \equiv \psi_\nu & \phi_{g_\nu} \equiv \phi_\nu \end{array}$$

Then $\psi_1, \psi_2, \ldots, \psi_\nu$ are all distinct (§ 29); but $\phi_1, \phi_2, \ldots, \phi_\nu$ need not be distinct since ϕ belongs to a group G which may be larger than H. Under any substitution s on $x_1, x_2, \ldots, x_n$, the functions

$\psi_1, \psi_2, \ldots, \psi_\nu$ are merely permuted (§ 30). Moreover, if s replaces ψ_i by ψ_j, it replaces ϕ_i by ϕ_j. Set

$$g(t) \equiv (t-\psi_1)(t-\psi_2)\ldots(t-\psi_\nu),$$

$$\lambda(t) \equiv g(t)\left(\frac{\phi_1}{t-\psi_1}+\frac{\phi_2}{t-\psi_2}+\ldots+\frac{\phi_\nu}{t-\psi_\nu}\right),$$

so that $\lambda(t)$ is an integral function of degree $\nu-1$ in t. Since $\lambda(t)$ remains unaltered under every substitution s, its coefficients are rational symmetric functions of $x_1, x_2, \ldots, x_n$ and hence are rational functions of the expressions (34). Taking $\psi_1 \equiv \psi$ for t, we get *

$$\lambda(\psi_1) = (\psi_1-\psi_2)(\psi_1-\psi_3)\ldots(\psi_1-\psi_\nu)\cdot\phi_1 = g'(\psi_1)\cdot\phi_1,$$

(37) $$\phi = \frac{\lambda(\psi)}{g'(\psi)}.$$

The theorem may be given the convenient symbolic form:

$$\textit{If}\ \begin{array}{c} G:\phi \\ | \\ H:\psi \end{array},\ \textit{then}\ \phi = \textit{Rat. Func.}\ (\psi;\ c_1, \ldots, c_n).$$

Taking first $H=G$ and next $H=I$, we obtain the corollaries:

COROLLARY 1. *If two rational functions belong to the same group, either is a rational function of the other and* $c_1, c_2, \ldots, c_n$.

COROLLARY 2. *Every rational function of* $x_1, x_2, \ldots, x_n$ *is a rational function of any* $n!$*-valued function (such as V of* § 25) *and* $c_1, c_2, \ldots, c_n$.

EXAMPLE 1. The functions Δ and θ of Ex. 1, § 29, belong to the same group $G_3^{(3)}$. We may therefore express Δ in terms of θ. By §§ 2, 3,

$$3\sqrt{-3}\,\Delta = (x_1+\omega^2x_2+\omega x_3)^3-(x_1+\omega x_2+\omega^2x_3)^3 = \frac{(c_1^2-3c_2)^3}{\theta}-\theta.$$

The expression for $\theta \equiv \psi_1^3$ in terms of Δ is given in § 34 below.

---

* The relation (37) is valid as long as $x_1, x_2, \ldots, x_n$ denote indeterminate quantities, since $\psi_1, \ldots, \psi_\nu$ are algebraically distinct so that $g'(\psi)$ is not identically zero. In case special values are assigned to $x_1, \ldots, x_n$ such that two or more of the functions $\psi_1, \ldots, \psi_\nu$ become numerically equal, then $g'(\psi)=0$, and ϕ is not a rational function of $\psi, c_1, \ldots, c_n$. In this case, see Lagrange, *Œuvres*, vol. 3, pp. 374-388; Serret, *Algèbre*, II, pp. 434-441. But this subject is considered in Part II.

Example 2. The function $y_1 \equiv x_1x_2+x_3x_4$ belongs to the group G_8 and $t \equiv x_1+x_2-x_3-x_4$ belongs to the subgroup H_4 (§ 21). Hence y_1 is a rational function of t and the coefficients a, b, c, d of the equation whose roots are x_1, x_2, x_3, x_4. By § 5, $y_1 = \frac{1}{4}(t^2-a^2+4b)$.

Example 3. The function $\psi_1 \equiv x_1+\omega x_2+\omega^2 x_3$ has $3!=6$ values. Hence every rational function of x_1, x_2, x_3 is a rational function of ψ_1 and c_1, c_2, c_3. The expressions for x_1, x_2, x_3 themselves follow from the formulæ (11) of § 3. Thus

$$x_1 = \frac{1}{3}\left(c_1+\psi_1+\frac{c_1{}^2-3c_2}{\psi_1}\right).$$

32. Theorem. *If* $\nu \,\Big|\, \begin{matrix} G:\phi \\ H:\psi \end{matrix}$, *then* ψ *satisfies an equation of degree* ν *whose coefficients are rational functions of* ϕ, $c_1, \ldots, c_n$.

As in § 29, we consider the ν conjugate values of ψ under G:

$$\psi,\ \psi_{g_2},\ \psi_{g_3},\ \ldots,\ \psi_{g_\nu}.$$

Under any substitution of the group G, these values are merely permuted amongst themselves. Hence any symmetric function of them is unaltered under every substitution of G and therefore, by Lagrange's Theorem, is a rational function of $\phi, c_1, \ldots, c_n$. The same is therefore true of the coefficients of the equation

$$(w-\psi)(w-\psi_{g_2})\ldots(w-\psi_{g_\nu})=0.$$

CHAPTER IV.

THE GENERAL EQUATION FROM THE GROUP STANDPOINT.

33. In the light of the preceding theorems, we now reconsider Cardan's solution (§ 2) of the reduced cubic equation $y^3+py+q=0$. The determination of its roots y_1, y_2, y_3 depends upon the chain of resolvent equations:

$$\xi^2=\frac{q^2}{4}+\frac{p^3}{27}, \quad \text{where } \xi\equiv\frac{\sqrt{-3}}{18}(y_1-y_2)(y_2-y_3)(y_3-y_1);$$

$$z^3=-\frac{q}{2}+\xi, \quad \text{where } z\equiv\tfrac{1}{3}(y_1+\omega y_2+\omega^2 y_3);$$

$$y_1=z-\frac{p}{3z}, \quad y_2=\omega z-\frac{\omega^2 p}{3z}, \quad y_3=\omega^2 z-\frac{\omega p}{3z}.$$

Initially given are the elementary symmetric functions

$$y_1+y_2+y_3=0, \quad y_1y_2+y_1y_3+y_2y_3=p, \quad -y_1y_2y_3=q,$$

belonging to the symmetric group G_6 on y_1, y_2, y_3. Solving a quadratic resolvent equation, we find the two-valued function ξ, which belongs to the subgroup G_3 of G_6 (§ 21, Ex. 1). Solving next a cubic resolvent equation, we find the six-valued function z, which belongs to the subgroup G_1 of G_3 (§ 21, Ex. 2). Then y_1, y_2, y_3 are rational functions of z, p, q, since they belong to the respective groups

$$G_2'=\{I, (y_2y_3)\}, \quad G_2''=\{I, (y_1y_3)\}, \quad G_2'''=\{I, (y_1y_2)\},$$

each containing G_1 (also direct from § 31, Cor. 2). From the group standpoint, the solution is therefore expressed by the scheme:

$$\begin{array}{llll}
G_6: p,\, q & & & \\
2\,| & & & \\
G_3: \xi & G_2': y_1 & G_2'': y_2 & G_2''': y_3 \\
3\,| & | & | & | \\
G_1: z & G_1: z & G_1: z & G_1: z
\end{array}$$

34. The same method leads to a solution of the general cubic

$$x^3 - c_1 x^2 + c_2 x - c_3 = 0.$$

To the symmetric group G_6 on x_1, x_2, x_3 belong the functions

$$x_1 + x_2 + x_3 = c_1, \quad x_1x_2 + x_1x_3 + x_2x_3 = c_2, \quad x_1x_2x_3 = c_3.$$

To the subgroup $G_3 = \{I, (x_1x_2x_3), (x_1x_3x_2)\}$ belongs the function

$$\Delta = (x_1 - x_2)(x_2 - x_3)(x_3 - x_1).$$

In view of Ex. 3, page 4, Δ is a root of the binomial resolvent

$$\Delta^2 = c_1^2 c_2^2 + 18 c_1 c_2 c_3 - 4 c_2^3 - 4 c_1^3 c_3 - 27 c_3^2.$$

By § 3 and § 2, we have for $\psi_1 = x_1 + \omega x_2 + \omega^2 x_3$. $\psi_4 = x_1 + \omega^2 x_2 + \omega x_3$,

$$\psi_1^3 + \psi_4^3 = \quad 2c_1^3 - 9c_1c_2 + 27c_3,$$

$$\psi_1^3 - \psi_4^3 = -3\sqrt{-3}(x_1 - x_2)(x_2 - x_3)(x_3 - x_1) = -3\sqrt{-3}\,\Delta.$$

$$\therefore \; \psi_1^3 = \tfrac{1}{2}(2c_1^3 - 9c_1c_2 + 27c_3 - 3\sqrt{-3}\,\Delta),$$

$$\psi_4^3 = \tfrac{1}{2}(2c_1^3 - 9c_1c_2 + 27c_3 + 3\sqrt{-3}\,\Delta).$$

After determining* ψ_1 by extracting a cube root, the value of ψ_4 is (§ 3)

$$\psi_4 = (c_1^2 - 3c_2) \div \psi_1.$$

Then, as in § 3, x_1, x_2, x_3 are rationally expressible in terms of ψ_1:

$$x_1 = \tfrac{1}{3}(c_1 + \psi_1 + \psi_4), \quad x_2 = \tfrac{1}{3}(c_1 + \omega^2\psi_1 + \omega\psi_4), \quad x_3 = \tfrac{1}{3}(c_1 + \omega\psi_1 + \omega^2\psi_4).$$

35. The solution given in § 5 of the general quartic equation

(12) $$x^4 + ax^3 + bx^2 + cx + d = 0$$

may be exhibited from the group standpoint by the scheme:

$G_{24}: a, b, c, d$

|

$G_8 \;: y_1 = x_1x_2 + x_3x_4, \quad t^2 = (x_1 + x_2 - x_3 - x_4)^2$

|

$H_4 \;: t, \; x_1 + x_2, \; x_3 + x_4, \; x_1x_2, \; x_3x_4$

/ \

$H_2 : x_1 - x_2 \qquad H_2' : x_3 - x_4.$

Here $H_2 = \{I, (x_3x_4)\}$, $H_2' = \{I, (x_1x_2)\}$, G_8 and H_4 being given in § 21.

---

* For another method see Ex. 4, page 41.

36. Lagrange's second solution of (12) is based upon the direct computation of the function $x_1+x_2-x_3-x_4$. Its six conjugate values under G_{24} are $\pm t_1$, $\pm t_2$, $\pm t_3$, where

$$t_1=x_1+x_2-x_3-x_4,\quad t_2=x_1+x_3-x_2-x_4,\quad t_3=x_1+x_4-x_2-x_3.$$

The resolvent sextic is therefore

$$(\tau^2-t_1^2)(\tau^2-t_2^2)(\tau^2-t_3^2)=0.$$

Its coefficients may be computed * easily by observing that

$$t_1^2=a^2-4b+4y_1,\quad t_2^2=a^2-4b+4y_2,\quad t_3^2=a^2-4b+4y_3,$$

as follows from § 5. Using the results there established, we get

$$t_1^2+t_2^2+t_3^2=3a^2-12b+4(y_1+y_2+y_3)=3a^2-8b,$$

$$\begin{aligned}t_1^2t_2^2+t_1^2t_3^2+t_2^2t_3^2&=3(a^2-4b)^2+8(a^2-4b)(y_1+y_2+y_3)\\&\quad+16(y_1y_2+y_1y_3+y_2y_3)\\&=3a^4-16a^2b+16b^2+16ac-64d,\end{aligned}$$

$$\begin{aligned}t_1^2t_2^2t_3^2&=(a^2-4b)^3+4(a^2-4b)^2(y_1+y_2+y_3)\\&\quad+16(a^2-4b)(y_1y_2+y_1y_3+y_2y_3)+64y_1y_2y_3\\&=\{8c+a(a^2-4b)\}^2.\end{aligned}$$

The resolvent becomes a cubic equation upon setting $\tau^2=\sigma$. Denote its roots by $\sigma_1=t_1^2$, $\sigma_2=t_2^2$, $\sigma_3=t_3^2$. Then

$$x_1+x_2-x_3-x_4=\sqrt{\sigma_1},\quad x_1+x_3-x_2-x_4=\sqrt{\sigma_2},$$
$$x_1+x_4-x_2-x_3=\sqrt{\sigma_3},\quad x_1+x_2+x_3+x_4=-a.$$

From these we get

$$(38)\quad\begin{cases}x_1=\tfrac14(-a+\sqrt{\sigma_1}+\sqrt{\sigma_2}+\sqrt{\sigma_3}),\ x_2=\tfrac14(-a+\sqrt{\sigma_1}-\sqrt{\sigma_2}-\sqrt{\sigma_3}),\\ x_3=\tfrac14(-a-\sqrt{\sigma_1}+\sqrt{\sigma_2}-\sqrt{\sigma_3}),\ x_4=\tfrac14(-a-\sqrt{\sigma_1}-\sqrt{\sigma_2}+\sqrt{\sigma_3}).\end{cases}$$

The signs of $\sqrt{\sigma_1}$ and $\sqrt{\sigma_2}$ may be chosen arbitrarily, while that of $\sqrt{\sigma_3}$ follows from

$$(39)\qquad \sqrt{\sigma_1}\sqrt{\sigma_2}\sqrt{\sigma_3}=t_1t_2t_3=4ab-8c-a^3.$$

Indeed, we may determine the sign in

$$t_1t_2t_3=\pm\{8c+a(a^2-4b)\}$$

---

* Compare Ex. 5, page 41.

by taking $x_1=1$, $x_2=x_3=x_4=0$, whence $a=-1$, $b=c=d=0$, $t_1t_2t_3=1$.

37. The following solution of the quartic is of greater interest as it leads directly to a 24-valued function V, in terms of which all the roots are expressed rationally. As in § 5, we determine y_1 and t, belonging to G_8 and H_4 respectively, by solving a cubic and a quadratic equation. To the subgroup

$$G_2=\{I, (x_1x_2)(x_3x_4)\}$$

of H_4 belongs the function $\psi=V^2$, while to G_1 belongs V, where

$$V=(x_1-x_2)+i(x_3-x_4).$$

Under H_4, ψ takes a second value $\psi_1=\{(x_1-x_2)-i(x_3-x_4)\}^2$. Then

$$z^2-(\psi+\psi_1)z+\psi\psi_1=0$$

is the resolvent equation for ψ. But

$$\psi\psi_1=\{(x_1-x_2)^2+(x_3-x_4)^2\}^2=\{a^2-2b-2y_1\}^2=\tfrac{1}{4}\{3a^2-8b-t^2\}^2,$$

$$\begin{aligned}\psi+\psi_1=2\{(x_1-x_2)^2-(x_3-x_4)^2\}&=2(x_1-x_2+x_3-x_4)(x_1-x_2-x_3+x_4)\\&=2(4ab-8c-a^3)\div t,\end{aligned}$$

in view of (39). After finding ψ and ψ_1, we get

$$V=\sqrt{\psi}.\quad V_1=\sqrt{\psi_1}=(x_1-x_2)-i(x_3-x_4),$$

(40) $$V_1=\tfrac{1}{2}(3a^2-8b-t^2)\div V.$$

Having the four functions t, V, V_1, and $x_1+x_2+x_3+x_4=-a$, we get

(41) $$\begin{cases} x_1=\tfrac{1}{4}(-a+t+V+V_1), & x_2=\tfrac{1}{4}(-a+t-V-V_1),\\ x_3=\tfrac{1}{4}(-a-t-iV+iV_1), & x_4=\tfrac{1}{4}(-a-t+iV-iV_1).\end{cases}$$

38. The solution of the general cubic (§ 34) and the solution of the general quartic (§ 37) each consists essentially in finding the value of a function which is altered by every substitution on the roots and which therefore belongs to the identity group G_1. Likewise, the general equation of degree n,

(42) $$x^n-c_1x^{n-1}+c_2x^{n-2}-\ldots+(-1)^nc_n=0,$$

could be completely solved if we could determine *one* value of a function belonging to the group G_1; for example,

(43) $\quad V=m_1x_1+m_2x_2+\ldots+m_nx_n \qquad$ (m's all distinct).

In fact, each x_i is a rational function of $V, c_1, \ldots, c_n$ by § 31. For the cubic and quartic, the scheme for determining such a function V was as follows:

$$\begin{array}{ll}
G_6: c_1,\ c_2,\ c_3 & G_{24}: a, b, c, d \\
2\ | & 3\ | \\
G_3: (x_1+\omega x_2+\omega^2x_3)^3 & G_8: x_1x_2+x_3x_4 \\
3\ | & 2\ | \\
G_1: x_1+\omega x_2+\omega^2x_3 & H_4: x_1+x_2-x_3-x_4 \\
 & 2\ | \\
 & G_2: (x_1-x_2+ix_3-ix_4)^2 \\
 & 2\ | \\
 & G_1: x_1-x_2+ix_3-ix_4
\end{array}$$

The same plan of solution applied to (42) gives the following scheme:

$$\begin{array}{ll}
G_{n!}: c_1, c_2, \ldots, c_n & \\
\lambda\ | & \\
H: \xi, & \xi^\lambda+R_1(c_1, \ldots, c_n)\xi^{\lambda-1}+\ldots=0 \\
\mu\ | & \\
K: \eta, & \eta^\mu+R_2(\xi, c_1, \ldots, c_n)\eta^{\mu-1}+\ldots=0 \\
\ \ | & \\
\ \ \vdots & \\
M: \psi & \\
\rho\ | & \\
G_1: V, & V^\rho+R(\psi\ c_1, \ldots, c_n)V^{\rho-1}+\ldots=0.
\end{array}$$

Such resolvent equations would exist in view of the theorem of § 32. In case the resolvent equations were all binomial, the function V (and hence $x_1, \ldots, x_n$) would be found by the extraction of roots of known quantities, so that the equation would be solvable by radicals. We may limit the discussion to binomial equations of *prime* degree, since $z^{pq}=A$ may be replaced by the chain of equations $z^p=u$, $u^q=A$. The following question therefore arises:

If $\begin{array}{l} G: \phi \\ \nu\ | \\ H: \psi \end{array}$, when will the resolvent equation for ψ take the form

(44) $$\psi^\nu=\text{Rat. Func. }(\phi, c_1, \ldots, c_n).$$

Since ν is assumed to be prime, there exists a primitive νth root of unity, namely a number ω having the properties

$$\omega^\nu=1, \quad \omega^k \neq 1 \text{ for any positive integer } k<\nu.$$

Hence the roots of (44) may be written

$$(45) \qquad \psi,\ \omega\psi,\ \omega^2\psi, \ldots,\ \omega^{\nu-1}\psi.$$

Let $\psi_1 \equiv \psi, \psi_2, \ldots, \psi_\nu$ denote the conjugate functions to ψ under G (their number is ν by § 29). Now ψ belongs to the group H by hypothesis. Let ψ_2 belong to the group H_2, ψ_3 to $H_3, \ldots, \psi_\nu$ to H_ν. Since the roots (45) differ only by constant factors, they belong to the same group. Hence a *necessary* condition is that

$$H=H_2=H_3=\ldots=H_\nu.$$

39. The first problem is to determine the group to which belongs the function ψ_s into which ψ is changed by a substitution s, when it is given that ψ belongs to the group

$$H=\{h_1 \equiv I,\ h_2, \ldots,\ h_P\}.$$

If a substitution σ leaves ψ_s unaltered, so that $\psi_{s\sigma}=\psi_s$, then

$$\psi_{s\sigma s^{-1}}=\psi_{ss^{-1}}=\psi.$$

Hence $s\sigma s^{-1}=h$, where h is a substitution of H. Then

$$\sigma=s^{-1}hs.$$

Inversely, every substitution $s^{-1}hs$ leaves ψ_s unaltered. Hence ψ_s belongs to the group

$$\{s^{-1}h_1s=I,\ s^{-1}h_2s, \ldots,\ s^{-1}h_Ps\},$$

which will be designated $s^{-1}Hs$. We may state the theorem:

If ψ belongs to the subgroup H of index ν under G, the conjugates

$$\psi,\ \psi_{g_2}, \ldots,\ \psi_{g_\nu},$$

of ψ under G, belong to the respective groups

$$H,\ g_2^{-1}Hg_2, \ldots,\ g_\nu^{-1}Hg_\nu.$$

DEFINITIONS. The latter groups are said to form a **set of conjugate subgroups** of G. In case they are all identical, H is called a **self-conjugate subgroup** of G (or an **invariant subgroup** of G).

Hence a necessary condition that the general equation of degree n shall be solvable by radicals under the plan of solution proposed in § 38 is that each group in the series shall be a self-conjugate subgroup of prime index under the preceding group.

Note that the group $G_1=\{I\}$ is self-conjugate under every group G since $g^{-1}Ig=I$.

EXAMPLE 1. Let G be the symmetric group G_6 on 3 letters and let H be the group $G_3=\{I,\ (x_1x_2x_3),\ (x_1x_3x_2)\}$. Let $g_2=(x_2x_3)$. Then

$$\psi=(x_1+\omega x_2+\omega^2x_3)^3,\quad \psi_{g_2}=(x_1+\omega^2x_2+\omega x_3)^3$$

form a set of conjugate functions under G. Now ψ belongs to H and ψ_2 belongs to the group $\{I,\ (x_1x_3x_2),\ (x_1x_2x_3)\}$, whose substitutions are derived from those of H by interchanging the letters x_2 and x_3, since that interchange replaces ψ by ψ_{g_2}. To proceed by the general method, we would compute

$$(x_2x_3)^{-1}(x_1x_2x_3)(x_2x_3)=(x_1x_3x_2),\quad (x_2x_3)^{-1}(x_1x_3x_2)(x_2x_3)=(x_1x_2x_3).$$

By either method we find that the group of ψ and ψ_{g_2} are identical, so that G_3 is self-conjugate under G_6 Also, G_1 is self-conjugate under G_3. Hence the necessary condition that the general cubic shall be solvable by radicals is satisfied.

EXAMPLE 2. Consider the conjugate values x_1, x_2, x_3 of x_1 under G_6:

$$\begin{array}{ll|l} I, & (x_2x_3) & x_1 \\ g_2=(x_1x_2), & (x_2x_3)g_2=(x_1x_2x_3) & x_2 \\ g_3=(x_1x_3), & (x_2x_3)g_3=(x_1x_3x_2) & x_3 \end{array}$$

Hence $H=\{I,\ (x_2x_3)\}$ is not self-conjugate under G_6. Here

$$g_2^{-1}Hg_2=\{I,\ (x_1x_3)\}\neq H,\quad g_3^{-1}Hg_3=\{I,\ (x_1x_2)\}\neq H.$$

40. DEFINITIONS. Two substitutions a and a' of a group G are called **conjugate under** G if there exists a substitution g belonging to G such that $g^{-1}ag=a'$. Then a' is called the **transform** of a by g.

There is a simple method of finding $g^{-1}ag$ without performing the actual multiplication. Suppose first that a is a circular substitution, say $a=(\alpha\beta\gamma\delta)$, while g is any substitution, say

$$g=\begin{pmatrix}\alpha & \beta & \gamma & \delta & \ldots & \lambda \\ \alpha' & \beta' & \gamma' & \delta' & \ldots & \lambda'\end{pmatrix}.$$

$$\therefore\ g^{-1}=\begin{pmatrix}\alpha' & \beta' & \gamma' & \delta' & \ldots & \lambda' \\ \alpha & \beta & \gamma & \delta & \ldots & \lambda\end{pmatrix},\quad g^{-1}ag=\begin{pmatrix}\alpha' & \beta' & \gamma' & \delta' & \epsilon' & \ldots & \lambda' \\ \beta' & \gamma' & \delta' & \alpha' & \epsilon' & \ldots & \lambda'\end{pmatrix}.$$

Hence $g^{-1}ag=(a'\beta'\gamma'\delta')$ may be obtained by applying the substitution g to the letters of the cycle $a=(a\beta\gamma\delta)$.

Let next $a=a_1a_2a_3\ldots$, where $a_1, a_2, \ldots$ are circular substitutions. Then

$$g^{-1}ag=g^{-1}a_1g\cdot g^{-1}a_2g\cdot g^{-1}a_3g\ldots$$

Hence $g^{-1}ag$ is obtained by applying g within the cycles of a.

Thus $$(123)^{-1}\cdot(12)(34)\cdot(123)=(23)(14).$$

Corollary. Since any substitution transforms an even substitution into an even substitution, the alternating group $G_{\frac{1}{2}n!}$ is a self-conjugate subgroup of the symmetric group $G_{n!}$.

41. Theorem. *Of the following groups on four letters:*

$$G_{24},\ G_{12},\ G_4=\{I,\ (12)(34),\ (13)(24),\ (14)(23)\},$$
$$G_2=\{I,\ (12)(34)\},\ G_1=\{I\},$$

each is a self-conjugate subgroup of the preceding group.

By the Corollary of § 40, G_{12} is self-conjugate under G_{24}. To show that G_4 is self-conjugate under G_{12} (as well as under G_{24}), we observe that G_4 contains all the substitutions of the type $(a\beta)(\gamma\delta)$, while the latter is transformed into a substitution of the form $(a'\beta')(\gamma'\delta')$ by any given substitution on four letters. That G_2 is self-conjugate under G_4 follows from the fact that (12)(34), (13)(24), (14)(23) all transform (12)(34) into itself.*

42. The necessary condition (§ 39) that the general quartic

$$x^4+ax^3+bx^2+cx+d=0$$

shall be solvable by radicals is satisfied in view of the preceding theorem. We proceed to determine a chain of *binomial* resolvent equations of *prime* degree which leads to a 24-valued function

$$V=x_1-x_2+ix_3-ix_4,$$

* This also follows from § 21, Ex. (*f*), since $rs=sr$ gives $s^{-1}rs=r$.

in terms of which the roots x_1, x_2, x_3, x_4 are rationally expressible. Let

(20) $$y_1=x_1x_2+x_3x_4,\quad y_2=x_1x_3+x_2x_4,\quad y_3=x_1x_4+x_2x_3,$$

as in § 4. The scheme for the solution is the following:

$$\begin{array}{l} G_{24}: a,\ b,\ c,\ d \\ 2\ | \\ G_{12}: \Delta\ =(x_1-x_2)(x_1-x_3)(x_1-x_4)(x_2-x_3)(x_2-x_4)(x_3-x_4) \\ 3\ | \\ G_4\ : \phi_1=y_1+\omega y_2+\omega^2 y_3 \\ 2\ | \\ G_2\ : \lambda\ =\phi_1 \div (x_1+x_2-x_3-x_4) \\ 2\ | \\ G_1\ : V\ =x_1-x_2+ix_3-ix_4 \end{array}$$

Referring to formulæ (22), (23), (24) of § 7, and setting $P=-4I$, $Q=16J$, we get

$$\Delta=16\sqrt{I^3-27J^2},$$

$$I\equiv d-\frac{ac}{4}+\frac{b^2}{12},\quad J\equiv\frac{bd}{6}-\frac{c^2}{16}-\frac{a^2d}{16}+\frac{abc}{48}-\frac{b^3}{216}.$$

Hence Δ is a root of the binomial resolvent $\Delta^2=256(I^3-27J^2)$. The resolvent for ϕ_1 is the binomial equation

$$(\phi-\phi_1)(\phi-\omega\phi_1)(\phi-\omega^2\phi_1)\equiv\phi^3-\phi_1{}^3=0.$$

By Lagrange's Theorem, $\phi_1{}^3$ is a rational function of Δ, a, b, c, d. To determine this function, set $\phi_2=y_1+\omega^2y_2+\omega y_3$. Then (§§ 2, 7)

$$\phi_2{}^3-\phi_1{}^3=3\sqrt{-3}(y_1-y_2)(y_2-y_3)(y_3-y_1)=-3\sqrt{-3}\,\Delta,$$
$$\phi_2{}^3+\phi_1{}^3=2(y_1{}^3+y_2{}^3+y_3{}^3)+12y_1y_2y_3+3(\omega+\omega^2)\delta,$$

where $\delta\equiv y_1{}^2y_2+y_1y_2{}^2+y_1{}^2y_2+y_1y_3{}^2+y_2{}^2y_3+y_2y_3{}^2$ satisfies the relations

$$(y_1+y_2+y_3)(y_1y_2+y_1y_3+y_2y_3)=\delta+3y_1y_2y_3,$$
$$(y_1+y_2+y_3)^3=3\delta+6y_1y_2y_3+y_1{}^3+y_2{}^3+y_3{}^3.$$

$$\therefore\ \phi_2{}^3+\phi_1{}^3=2(y_1+y_2+y_3)^3-9(y_1+y_2+y_3)(y_1y_2+y_1y_3+y_2y_3)+27y_1y_2y_3$$
$$=2b^3-9b(ac-4d)+27(c^2+a^2d-4bd)=-432J.$$

upon applying the relations in § 5. Hence

$$\phi_1^3 = \tfrac{1}{2}3\sqrt{-3}\,\Delta - 216J.$$

In view of Lagrange's Theorem, y_1, y_2, and y_3 are rational functions of ϕ_1. These functions may be determined as follows:

$$\begin{aligned}\phi_1\phi_2 &= y_1^2+y_2^2+y_3^2+(\omega+\omega^2)(y_1y_2+y_1y_3+y_2y_3)\\ &=(y_1+y_2+y_3)^2-3(y_1y_2+y_1y_3+y_2y_3)\\ &=b^2-3ac+12d\equiv H.\end{aligned}$$

From $y_1+y_2+y_3=b,\quad y_1+\omega y_2+\omega^2 y_3=\phi_1,\quad y_1+\omega^2 y_2+\omega y_3=\dfrac{H}{\phi_1}$,

$$y_1=\tfrac{1}{3}\left(b+\phi_1+\frac{H}{\phi_1}\right),\quad y_2=\tfrac{1}{3}\left(b+\omega^2\phi_1+\frac{\omega H}{\phi_1}\right),\quad y_3=\tfrac{1}{3}\left(b+\omega\phi_1+\frac{\omega^2 H}{\phi_1}\right).$$

Setting $t\equiv x_1+x_2-x_3-x_4$, we obtain for $\lambda=\phi_1/t$ the binomial resolvent

$$\lambda^2=\phi_1^2\div(a^2-4b+4y_1),$$

upon replacing t^2 by its value given in § 5. Next, we have (§ 37)

$$\begin{aligned}V^2 &= (x_1-x_2)^2-(x_3-x_4)^2+2i(x_1-x_2)(x_3-x_4)\\ &=\frac{4ab-8c-a^3}{t}+2i(y_2-y_3)\\ &=\frac{\lambda}{\phi_1}(4ab-8c-a^3)+\tfrac{2}{3}\sqrt{3}\left(\phi_1-\frac{H}{\phi_1}\right).\end{aligned}$$

The values of x_1, x_2, x_3, x_4 are then given by (41) in connection with (40).

SERIES OF COMPOSITION OF THE SYMMETRIC GROUP ON n LETTERS.

43. DEFINITIONS. Let a given group G have a maximal self-conjugate subgroup H, namely, a self-conjugate subgroup of G which is not contained in a larger self-conjugate subgroup of G. Let H have a maximal self-conjugate subgroup K. Such a series of groups, terminating with the identity group G_1,

$$G,\quad H,\quad K,\quad \ldots,\quad M,\quad G_1,$$

in which each group is a maximal self-conjugate subgroup of the preceding group, forms a **series of composition** of G. The numbers λ (the index of H under G), μ (the index of K under H), . . . , ρ (the index of G_1 under M) are called the **factors of composition** of G.

If the series is composed of the groups G and G_1 alone, the group G is called **simple.** Thus a simple group is one containing no self-conjugate subgroup other than itself and the identity group. A group which is not simple is called a **composite group.**

EXAMPLE 1. For the symmetric group on 3 letters, a series of composition is G_6, G_3, G_1 (see Ex. 1, § 39). Since the indices 2, 3 are prime numbers, the self-conjugate subgroups are maximal (see § 26).

EXAMPLE 2. A series of composition of the symmetric group on 4 letters is G_{24}, G_{12}, G_4, G_2, G_1 (§ 41), the indices being prime numbers.

EXAMPLE 3. A cyclic group of prime order is a simple group (§ 26).

44. LEMMA. *If a group on n letters contains all circular substitutions on 3 of the n letters, it is either the symmetric group $G_{n!}$ or else the alternating group $G_{\frac{1}{2}n!}$.*

It is required to show that every *even* substitution s can be expressed as a product of circular substitutions on 3 letters. Let

$$s = t_1 t_2 \dots t_{2\nu-1} t_{2\nu},$$

where $t_1, \dots, t_{2\nu}$ are transpositions (§§ 22, 23), and $t_1 \neq t_2$. If t_1 and t_2 have one letter in common, then

$$t_1 t_2 = (a\beta)(a\gamma) = (a\beta\gamma).$$

If, however, t_1 and t_2 have no letter in common, then

$$t_1 t_2 = (a\beta)(\gamma\delta) = (a\beta)(a\gamma)(\gamma a)(\gamma\delta) = (a\beta\gamma)(\gamma a\delta).$$

Similarly, $t_3 t_4$ is either the identity or else equivalent to one cycle on 3 letters or to a product of two such cycles.

Hence the group contains all *even* substitutions on the n letters.

45. THEOREM. *The symmetric group on $n > 4$ letters contains no self-conjugate subgroup besides itself, the identity G_1, and the alternating group $G_{\frac{1}{2}n!}$, so that the latter is the only maximal self-conjugate subgroup of $G_{n!}$ ($n > 4$).*

That the alternating group is self-conjugate under the symmetric group was shown in § 40.

Let $G_{n!}$ have a self-conjugate subgroup H which contains a substitution s not the identity I.

Suppose first that s contains cycles of more than 2 letters:

$$s=(abc\ldots d)(ef\ldots)\ldots$$

Let α, β, δ be any three of the n letters and $\gamma, \epsilon, \ldots, \phi, \ldots$ the remaining $n-3$ letters. Then H contains the substitutions

$$s_1=(\alpha\beta\gamma\ldots\delta)(\epsilon\phi\ldots)\ldots, \quad s_2=(\beta\alpha\gamma\ldots\delta)(\epsilon\phi\ldots)\ldots,$$

the letters indicated by dots in s_1 being the same as the corresponding letters in s_2. The fact that s_1 (and likewise s_2) belongs to H follows since

$$\sigma=\begin{pmatrix} a & b & c & \ldots & d & e & f & \ldots \\ \alpha & \beta & \gamma & \ldots & \delta & \epsilon & \phi & \ldots \end{pmatrix}$$

is a substitution on the n letters which transforms s into s_1 (§ 40), while any substitution σ of $G_{n!}$ transforms a substitution s of the *self-conjugate* subgroup H into a substitution belonging to H (§ 39). Since H is a group, it contains the product $s_2 s_1^{-1}$, which reduces to $(\alpha\beta\delta)$. Hence H contains a circular substitution on 3 letters chosen arbitrarily from the n letters. Hence H is either $G_{n!}$ or $G_{\frac{1}{2}n!}$ (§ 44).

Suppose next that s contains only transpositions and at least two transpositions. The case $s=(ab)(ac)\ldots=(abc)\ldots$ has been treated. Let therefore

$$s=(ab)(cd)(ef)\ldots(lm).$$

Let $\alpha, \beta, \gamma, \delta$ be any four of the n letters, and $\epsilon, \phi, \ldots, \lambda, \mu$ the others. Then the self-conjugate subgroup H contains the substitutions

$$s_1=(\alpha\beta)(\gamma\delta)(\epsilon\phi)\ldots(\lambda\mu), \quad s_2=(\alpha\gamma)(\beta\delta)(\epsilon\phi)\ldots(\lambda\mu)$$

and therefore also the product $s_2 s_1^{-1}$, which reduces to $(\alpha\delta)(\beta\gamma)$.

Since $n>4$, there is a letter ρ different from a, β, γ, δ. Hence H contains $(a\rho)(\beta\gamma)$ and therefore the product

$$(a\delta)(\beta\gamma)\cdot(a\rho)(\beta\gamma)=(a\delta\rho).$$

It follows as before that H is either $G_{n!}$ or $G_{\frac{1}{2}n!}$.

Suppose finally that $s=(ab)$. Then the self-conjugate subgroup H contains every transposition, so that $H=G_{n!}$.

46. THEOREM. *The alternating group on $n>4$ letters is simple.*

Let $G_{\frac{1}{2}n!}$ have a self-conjugate subgroup H larger than the identity group G_1. Of the substitutions of H different from the identical substitution I, consider those which affect the least number of letters. All the cycles of any one of them must contain the same number of letters; otherwise a suitable power would affect fewer letters without reducing to the identity I. Again, none of these substitutions contains more than 3 letters in any cycle. For, if H contains

$$s=(1234\lambda\ldots\rho)(\ldots)\ldots,$$

then H contains its transform by the *even* substitution $\sigma=(234)$:

$$s_1=\sigma^{-1}s\sigma=(1342\lambda\ldots\rho)(\ldots)\ldots,$$

where the dots indicate the same letters as in s. Hence H would contain

$$ss_1^{-1}=(142),$$

affecting fewer letters than does s. Finally, none of the substitutions in question contain more than a single cycle. For, if H contains either t or s, where

$$t=(12)(34)\ldots,\quad s=(123)(456)\ldots,$$

it would contain the transform of one of them by the *even* substitution $\kappa=(125)$ and consequently either $t\cdot\kappa^{-1}t\kappa$ or $s^{-1}\cdot\kappa^{-1}s\kappa$. The latter leaves 4 unaltered and affects no letter not contained in s; the former leaves 3 and 4 unaltered and affects but a single letter 5 not contained in t. In either case, there would be a reduction in the number of letters affected.

The substitutions, different from I, which affect the least number of letters are therefore of one of the types (ab), (abc). The former is excluded as it is odd. Hence H contains a substitution

(abc). Let α, β, γ be any three of the n letters, $\delta, \varepsilon, \ldots, \nu$ the others. Then (abc) is transformed into $(\alpha\beta\gamma)$ by *either* of the substitutions

$$r=\begin{pmatrix} a & b & c & d & e & \ldots & n \\ \alpha & \beta & \gamma & \delta & \varepsilon & \ldots & \nu \end{pmatrix}, \quad s=\begin{pmatrix} a & b & c & d & e & \ldots & n \\ \alpha & \beta & \gamma & \varepsilon & \delta & \ldots & \nu \end{pmatrix},$$

where the dots in r indicate the same letters as in s. Since $r=s(\delta\varepsilon)$, one of the substitutions r, s is *even* and hence in $G_{\frac{1}{2}n!}$. Hence, for $n>4$, H contains all the circular substitutions on 3 of the n letters, so that $H=G_{\frac{1}{2}n!}$.

47. It follows from the two preceding theorems that, *for $n>4$, there is a single series of composition of the symmetric group on n letters: $G_{n!}$, $G_{\frac{1}{2}n!}$, G_1.* The theorem holds also for $n=3$, since the only subgroup of G_6 of order 3 is G_3, while the three subgroups of G_6 of order 2 are not self-conjugate (§ 39, Ex. 2). The case $n=4$ is exceptional, since G_{12} contains the self-conjugate subgroup G_4 (§ 41).

Except for $n=4$, the factors of composition of the symmetric group on n letters are 2 and $\frac{1}{2}n!$.

48. It was proposed in § 38 to solve the general equation of degree n by means of a chain of binomial resolvent equations of prime degrees such that a root of each is expressible as a rational function of the roots $x_1, x_2, \ldots, x_n$ of that general equation. As shown in §§ 38–39, a necessary condition is the existence of a series of groups

$$G_{n!},\ H,\ K, \ldots, M,\ G_1, \tag{46}$$

each a self-conjugate subgroup of prime index under the preceding group. In the language of § 43, this condition requires that $G_{n!}$ shall have a series of composition (46) with the factors of composition all prime. By § 47, this condition is not satisfied if $n \geqq 5$, since $\frac{1}{2}n!$ is then not prime. But the condition is satisfied if $n=3$ or if $n=4$ (§ 39, Ex. 1; § 41). Under the proposed plan of solution, the general equation of degree $n>4$ is therefore not solvable by radicals, whereas the general cubic and general quartic equations are solvable by radicals under this plan (§ 34, § 42).

To complete the proof of the impossibility of the solution by radicals of the general equation of degree $n>4$, it remains to show that the proposed plan is the only possible method. This* was done by Abel (*Œuvres*, vol. 1, page 66) in 1826 by means of the theorem:

Every equation which is solvable by radicals can be reduced to a chain of binomial equations of prime degrees whose roots are rational functions of the roots of the given equation.

As the direct proof of this proposition from our present standpoint is quite lengthy, it will be deferred to Part II (see § 94), where a proof is given in connection with the more general theory due to Galois.

EXERCISES.

1. If $H=\{I, h_2, \dots, h_P\}$ is a subgroup of G of index 2, H is self-conjugate under G.

Hint: The substitutions of G not in H may be written $g, gh_2, \dots, gh_P$; or also $g, h_2g, \dots, h_Pg$. Hence every $h_\beta g$ is some gh_a, so that for every h_β, $g^{-1}h_\beta g$ is some h_a.

2. The group G_8 of § 21 has the self-conjugate subgroups G_2, G_4, H_4, $C_4=\{I, (1324), (12)(34), (1423)\}$. The only remaining self-conjugate subgroups are G_1 and G_8.

3. If a group contains all the circular substitutions on $m+2$ letters, it contains all the circular substitutions on m letters. Hint:

$(1\,2\,3 \dots m\; m+1\; m+2)^2(m\; m-1 \dots 3\; 2\; m+2\; 1\; m+1)=(1\,2\,3 \dots m-1\; m)$.

4. Compute directly the function $\psi_1{}^3$ of § 34 as follows:

$$\psi_1{}^3=x_1{}^3+x_2{}^3+x_3{}^3+6x_1x_2x_3+3\omega(x_1{}^2x_2+x_1x_3{}^2+x_2{}^2x_3)+3\omega^2(x_1x_2{}^2+x_1{}^2x_3+x_2x_3{}^2)$$
$$=x_1{}^3+x_2{}^3+x_3{}^3+6x_1x_2x_3-\tfrac{3}{2}(x_1{}^2x_2+x_1x_2{}^2+x_1{}^2x_3+x_1x_3{}^2+x_2{}^2x_3+x_2x_3{}^2)-\tfrac{3}{2}\sqrt{-3}\Delta,$$

since

$$x_1{}^2x_2-x_1x_2{}^2+x_1x_3{}^2-x_1{}^2x_3+x_2{}^2x_3-x_2x_3{}^2=-(x_1-x_2)(x_2-x_3)(x_3-x_1)=-\Delta.$$

Twice the remaining part of $\psi_1{}^3$ equals $2c_1{}^3-9c_1c_2+27c_3$ by § 3.

5. Compute directly the coefficients in § 36 as follows:

$$t_1{}^2+t_2{}^2+t_3{}^2=3\Sigma x_i{}^2-2\Sigma x_ix_j=3a^2-8b,$$
$$t_1t_2t_3=\Sigma x_1{}^3+2\Sigma x_1x_2x_3-\Sigma x_1(x_2{}^2+x_3{}^2+x_4{}^2)$$
$$=2\Sigma x_1{}^3+2\Sigma x_1x_2x_3-\Sigma x_i\Sigma x_j{}^2=4ab-8c-a^3$$

---

* For the simpler demonstration by Wantzel, see Serret, *Algèbre*, II, 4th or 5th Edition, p. 512.

SECOND PART.

GALOIS' THEORY OF ALGEBRAIC EQUATIONS.

CHAPTER V.

ALGEBRAIC INTRODUCTION TO GALOIS' THEORY.

49. Differences between Lagrange's and Galois' Theories. Heretofore we have been considering with Lagrange the **general equation** of degree n, that is, an equation with independent variables as coefficients and hence (see page 101) with independent quantities $x_1, x_2, \ldots, x_n$ as roots. Hence we have called two rational functions of the roots equal only when they are identical for all sets of values of $x_1, \ldots, x_n$.

But for an equation whose roots are definite constants, we must consider two rational functions of the roots to be equal when their numerical values are equal, and it may happen that two functions of different form have the same numerical value.

Thus the roots of $x^3+x^2+x+1=0$ are

$$x_1=-1,\ x_2=+i,\ x_3=-i \qquad (i\equiv\sqrt{-1}).$$

Hence the functions x_2^2, x_3^2, and x_1 are numerically equal although of different form. We may not apply to the equation $x_2^2=x_3^2$ the substitution $(x_1x_2x_3)$, since $x_3^2\neq x_1^2$. Again, the totality of the substitutions on the roots which leave the function x_2^2 numerically unaltered do not form a group, since the substitutions are I, (x_1x_3), (x_2x_3), $(x_1x_2x_3)$.

Again, the roots of $x^4+1=0$ are

$$x_1=\varepsilon,\quad x_2=i\varepsilon,\quad x_3=-\varepsilon,\quad x_4=-i\varepsilon \qquad \left(\varepsilon\equiv\frac{1+i}{\sqrt{2}}\right).$$

Hence $x_1^2=\varepsilon^2=i$, $x_2x_4=\varepsilon^2=i$. The functions x_1^2 and x_2x_4 differ in form, but are equal numerically. Also, x_1^2 equals x_3^2, but differs from x_2^2 and x_4^2. The 12 substitutions which leave x_1^2 numerically unaltered are I,(23),(24),(34),(234),(243),(13),(13)(24),(213),(413), (4213), (4132), the first six leaving x_1^2 formally unaltered and the last six replacing x_1^2 by x_3^2. They do not form a group, since the product (13)(23) is not one of the set.

There are consequently essential difficulties in passing from the theory of the general equation to that of special equations. This important step was made by Galois.*

In rebuilding our theory, special attention must be given to the nature of the coefficients of the equation under discussion,

$$(1) \qquad x^n-c_1x^{n-1}+c_2x^{n-2}-\ \dots\ +(-1)^nc_n=0.$$

Here $c_1, \dots, c_n$ may be definite constants, or independent variables, or rational functions of other variables. Whereas, in the Lagrange theory, roots of unity and other constants were employed without special notice being taken, in the Galois theory, particular attention is paid to the nature of all new constants introduced.

50. Domain of Rationality. To specify accurately what shall be understood to be a solution to a given problem, we must state the nature of the quantities to be allowed to appear in the solution. For example, we may demand as a solution a real num-

* Évariste Galois was killed in a duel in 1832 at the age of 21. His chief memoir was rejected by the French Academy as lacking rigorous proofs. The night before the duel, he sent to his friend Auguste Chevalier an account of his work including numerous important theorems without proof. The sixty pages constituting the collected works of Galois appeared, fifteen years after they were written, in the *Journal de mathématiques* (1846), and in *Œuvres mathématiques D'ÉVARISTE GALOIS, avec une introduction par M. Émile Picard,* Paris 1897.

ber or we may demand a positive number; for constructions by elementary geometry, we may admit square roots, but not higher roots of arbitrary positive numbers. In the study of a given equation, we naturally admit into the investigation all the irrationalities appearing in its coefficients; for example, $\sqrt{3}$ in considering $x^2+(2-5\sqrt{3})x+2=0$. We may agree beforehand to admit other irrationalities than those appearing in the coefficients.

In a given problem, we are concerned with certain constants or variables

$$(2) \qquad R', R'', \ldots, R^{(\mu)}$$

together with all quantities derived from them by a finite number of additions, subtractions, multiplications, and divisions (the divisor not being zero). The resulting system of quantities is called the *domain of rationality* * $(R', R'', \ldots, R^{(\mu)})$.

Example 1. The totality of rational numbers forms a domain. It is contained in every domain R. For if ω be any element $\neq 0$ of R, then $\omega \div \omega = 1$ belongs to R; but from 1 may be derived all integers by addition and subtraction, and from these all fractions by division.

Example 2. The numbers $a+bi$, where $i=\sqrt{-1}$, while a and b take all rational values, form a domain (i). But the numbers $a+bi$, where a and b take only integral values do not form a domain.

Definition. An equation whose coefficients are expressible as rational functions with integral coefficients of the quantities $R', R'', \ldots, R^{(\mu)}$ will be said to be algebraically solvable (or solvable by radicals) with respect to their domain, if its roots can be derived from $R', R'', \ldots$ by addition, subtraction, multiplication, division, and extraction of a † root of any index, the operations being applied a finite number of times.

51. The term **rational function** is used in Galois' theory only

---

* *Rationalitätsbereich* (Kronecker), *Körper* (Weber), *Field* (Moore).

† If we admitted the extraction of all the pth roots, we would admit the knowledge of all the pth roots of unity. This need not be admitted in Galois' theory (see § 89, Corollary).

in connection with a domain of rationality R. An **integral rational function for** R of certain quantities $u, v, w, \ldots$ is an expression

$$(3) \qquad \sum_{i, j, k, \ldots} C_{ijk\ldots} \, u^i v^j w^k \ldots,$$

where $i, j, k, \ldots$ are positive integers, and each coefficient $C_{ijk\ldots}$ is a quantity belonging to R. The quotient of two such functions (3) is a **rational function for** R.

Thus, $3u+\sqrt{2}$ is a rational function of u in $(\sqrt{2})$, but not in (1).

52. Equality. As remarked in § 49, two expressions involving only constants are regarded as equal when their *numerical* values are the same. Consider two rational functions

$$\phi(u, v, w, \ldots), \quad \psi(u, v, w, \ldots)$$

with coefficients in a domain $R=(R', R'', \ldots, R^{(\mu)})$. In case R', $R'', \ldots$ are all constants, we say that ϕ and ψ are **equal** if, for every set of numerical values $u_1, v_1, w_1, \ldots$ which $u, v, w, \ldots$ can assume, the resulting numerical values of ϕ and ψ are equal. In case $R', R'', \ldots, R^{(\mu)}$ depend upon certain independent variables $r', r'', \ldots, r^{(m)}$, we say that ϕ and ψ are equal if, for every set of numerical values which $u, v, w, \ldots, r', r'', \ldots, r^{(m)}$ may assume, the resulting numerical values of ϕ and ψ are equal. When not equal in this sense, ϕ and ψ are said to be **distinct** or **different.**

For example, if u and v are the roots of $x^2+2\rho x+1=0$, the functions $u+v$ and $-2\rho uv$ are rational functions in the domain (ρ), and these rational functions are equal.

DEFINITION. A rational function $\phi(x_1, \ldots, x_n)$ is said to be **unaltered** by a substitution s on $x_1, \ldots, x_n$ if the function $\phi_s(x_1, \ldots, x_n)$ is equal to ϕ in the sense just explained. For brevity, we shall often say that ϕ then remains *numerically* unaltered by s. If $x_1, x_2, \ldots, x_n$ are independent variables, as in Lagrange's theory, and if ϕ_s is identically equal to ϕ, i.e., for all values of $x_1, \ldots, x_n$, we say that ϕ remains *formally* unaltered by s. For examples, see § 49.

53. The preceding definitions are generalizations of those employed in the Lagrange theory. The so-called general equation of degree n may be viewed as an extreme case of the equations (1) whose coefficients $c_1, \ldots, c_n$ are rational functions in the domain $(R', R'', \ldots, R^{(\mu)})$. In fact, since its coefficients are independent variables belonging to the domain, they may be taken to replace an equal number of the quantities $R', R'', \ldots$ defining the domain, so that the general equation appears in the form

$$x^n+R'x^{n-1}+R''x^{n-2}+\ldots+R^{(n)}=0.$$

Its roots are likewise independent variables (p. 101), so that two rational functions of the roots are equal only when identically equal.

54. Reducibility and irreducibility. An integral rational function $F(x)$ whose coefficients belong to a domain R is said to be **reducible in** R if it can be decomposed into integral rational factors of lower degree whose coefficients likewise belong to R; **irreducible in** R if no such decomposition is possible.*

EXAMPLE 1. The function x^2+1 is reducible in the domain (i) since it has the factors $x+i$ and $x+i$, rational in (i). But x^2+1, which is a rational function of x in the domain of rational numbers, is irreducible in that domain.

EXAMPLE 2. x^4+1 is reducible in any domain to which either $\sqrt{2}$, or $\sqrt{-2}$, or i, or $\epsilon\equiv\dfrac{1+i}{\sqrt{2}}$, belongs, but is irreducible in all other domains. In fact, its linear factors are $x\pm\epsilon$, $x\pm i\epsilon=x\pm\epsilon^3$; while every quadratic factor is of the form $x^2\pm i$, or $x^2+ax\pm1$, $a^2=\pm2$.

If $F(x)$ is reducible in R, $F(x)=0$ is said to be a **reducible equation in** R; if $F(x)$ is irreducible in R, $F(x)=0$ is said to be an **irreducible equation** in R.

55. THEOREM. *Let the equations $F(x)=0$ and $G(x)=0$ have their coefficients in a domain R and let $F(x)=0$ be irreducible in R. If one root of $F(x)=0$ satisfies $G(x)=0$, then every root of $F(x)=0$ satisfies $G(x)=0$ and $F(x)$ is a divisor of $G(x)$ in R.*

After dividing out the coefficients of the highest power of x, let

$$F(x)=(x-\xi_1)(x-\xi_2)\ldots(x-\xi_n),\quad G(x)=(x-\eta_1)\ldots(x-\eta_m).$$

---

* A method to decompose a given integral function by a finite number of rational operations has been given by Kronecker, *Werke*, vol. 2, p. 256.

At least one ξ equals an η. Let $\xi_1 = \eta_1, \ldots, \xi_r = \eta_r$, while the remaining ξ's differ from each η. Then the function

$$H(x) \equiv (x-\xi_1) \ldots (x-\xi_r) \equiv (x-\eta_1) \ldots (x-\eta_r)$$

is the highest common factor of $F(x)$ and $G(x)$. But Euclid's process for finding this highest common factor involves only the operation division, so that the coefficients of $H(x)$ are rational functions of those of $F(x)$ and $G(x)$ and consequently belong to the domain R. Hence $F(x) = H(x) \cdot Q(x)$, where $H(x)$ and $Q(x)$ are integral functions with coefficients in R. Since $F(x)$ is irreducible in R, $Q(x)$ must be a constant, evidently 1. Hence $F(x) = H(x)$, so that $F(x)$ is a divisor of $G(x)$ in R.

COROLLARY I. If $G(x)$ is of degree $\overline{\gtrless} n-1$, then $G(x) \equiv 0$. A root of an irreducible equation in R does not satisfy an equation of lower degree in R.

COROLLARY II. If also $G(x) = 0$ is irreducible, then $G(x)$ is a divisor of $F(x)$, as well as $F(x)$ a divisor of $G(x)$. *If two irreducible equations in R have one root in common, they are identical.*

CHAPTER VI.

THE GROUP OF AN EQUATION.

EXISTENCE OF AN $n!$-VALUED FUNCTION; GALOIS' RESOLVENT.

56. Let there be given a domain R and an equation

$$(1) \qquad f(x) \equiv x^n - c_1 x^{n-1} + c_2 x^{n-2} - \ldots + (-1)^n c_n = 0,$$

whose coefficients belong to R. We assume that its roots $x_1, x_2, \ldots, x_n$ are all distinct.* It is then possible to construct a rational function V_1 of the roots with coefficients in R such that V_1 takes $n!$ distinct values under the $n!$ substitutions on $x_1, \ldots, x_n$. Such a function is

$$V_1 \equiv m_1 x_1 + m_2 x_2 + \ldots + m_n x_n,$$

if $m_1, \ldots, m_n$ are properly chosen in the domain R. Indeed, the two values V_a and V_b, derived from V_1 by two distinct substitutions a and b respectively, are not equal for all values of $m_1, \ldots, m_n$, since $x_1, \ldots, x_n$ are all distinct. It is therefore possible to choose values of $m_1, \ldots, m_n$ in R which satisfy none of the $\frac{1}{2}n!(n!-1)$ relations of the form $V_a = V_b$.

Then from an equation $V_{a'} = V_a$ will follow $a' = a$.

As an example, consider the equation $x^3 + x^2 + x + 1 = 0$, with the roots

$$x_1 = -1, \quad x_2 = +i \equiv \sqrt{-1}, \quad x_3 = -i,$$

and let R be the domain of all rational numbers. The six functions

$$-m_1 + im_2 - im_3, \quad -m_1 - im_2 + im_3, \quad im_1 - m_2 - im_3,$$
$$-im_1 + im_2 - m_3, \quad -im_1 - m_2 + im_3, \quad im_1 - im_2 - m_3,$$

---

* Equal roots of $F(x) = 0$ satisfy also $F'(x) = 0$, whose coefficients likewise belong to R, and consequently also $H(x) = 0$, where $H(x)$ is the highest common factor of $F(x)$ and $F'(x)$. If $F(x) \div H(x) = Q(x)$, the equation $Q(x) = 0$ has its coefficients in R and has distinct roots. After solving $Q(x) = 0$, the roots of $F(x) = 0$ are all known.

arising from the 3! permutations of x_1, x_2, x_3, will all be distinct if no one of the following relations holds:

$$m_2-m_3=0, \quad m_1-m_2=0, \quad m_1-m_3=0,$$
$$(i+1)m_1-2im_2+(i-1)m_3 \ =0, \qquad (i-1)m_1+(i+1)m_2-2im_3 \ =0,$$
$$(i-1)m_1-2im_2+(i+1)m_3 \ =0, \qquad (i+1)m_1+(i-1)m_2-2im_3 \ =0,$$
$$-2im_1+(i-1)m_2+(i+1)m_3=0, \qquad -2im_1+(i+1)m_2+(i-1)m_3=0,$$

of which the last six differ only by permutations of m_1, m_2, m_3. We may, for example, take $m_3=0$ and any rational values $\neq 0$ for m_1 and m_2 such that $m_1 \neq cm_2$, where c is 1, $\pm i$, $1\pm i$, $\frac{1}{2}(1\pm i)$. Thus $m_1x_1+x_2$ is a six-valued function in R if m_1 is any rational number different from 0 and 1.

[In the domain (i), we may take $m_1x_1+x_2$, where $m_1\neq 0$, 1, $\pm i$, $1\pm i$, $\frac{1}{2}(1\pm i)$.]

57. The $n!$ values of the function V_1 are the roots of an equation

$$F(V) \equiv (V-V_1)(V-V_2)\ldots(V-V_{n!})=0, \tag{4}$$

whose coefficients are integral rational functions of $m_1, \ldots, m_n$, $c_1, \ldots, c_n$ with integral coefficients and hence belong to the domain R (§ 50). If $F(V)$ is reducible in R, let $F_0(V)$ be that irreducible factor for which $F_0(V_1)=0$; if $F(V)$ is irreducible in R, let $F_0(V)$ be $F(V)$ itself. Then

$$F_0(V)=0 \tag{5}$$

is an irreducible equation called the **Galois resolvent** *of equation* (1).

Recurring to the example of the preceding section, take

$$V_1=x_2-x_1, \quad V_2=x_2-x_3, \quad V_3=x_3-x_1.$$

Then the six values of V_1 are $\pm V_1$, $\pm V_2$, $\pm V_3$, where

$$V_1=i+1, \quad V_2=2i, \quad V_3=-i+1.$$

The equation (4) now becomes

$$(V^2-V_1^2)(V^2-V_2^2)(V^2-V_3^2)=(V^2-2i)(V^2+4)(V^2+2i)$$
$$=V^6+4V^4+4V^2+16=0.$$

The irreducible factors of $F(V)$ in the domain of rational numbers are

$$V^2+4=(V-V_2)(V+V_2), \quad V^2-2V+2=(V-V_1)(V-V_3),$$
$$V^2+2V+2=(V+V_1)(V+V_3).$$

The Galois resolvent (5) is therefore

$$F_0(V)\equiv V^2-2V+2=0.$$

[For the domain (i), the Galois resolvent is $V-V_1 \equiv V-i-1=0$.]

58. THEOREM. *Any rational function, with coefficients in a domain R, of the roots of the given equation* (1) *is a rational function, with coefficients in R, of an $n!$-valued function V_1:*

$$\phi(x_1, x_2, \ldots, x_n) = \Phi(V_1). \tag{6}$$

Let first the coefficients $c_1, \ldots, c_n$ in equation (1) be arbitrary quantities so that the roots $x_1, \ldots, x_n$ are independent variables. We may then apply the proof in § 31 of Lagrange's Theorem, taking for ψ the function V_1 which is unaltered by the identical substitution alone, and obtain a relation

$$\phi = \lambda(V_1) \div F'(V_1), \tag{6'}$$

where $F'(V)$ is the derivative of $F(V)$ defined by (4). We next give to $c_1, \ldots, c_n$ their special values in R, so that $x_1, \ldots, x_n$ become the roots of the given equation. Since $F'(V_1) \neq 0$, relation (6′) becomes the desired relation (6), expressing ϕ as a rational function of V_1 with coefficients in R.

COROLLARY. *If s be any substitution on the letters $x_1, \ldots, x_n$, then*

$$\phi_s(x_1, x_2, \ldots, x_n) = \Phi(V_s), \tag{7}$$

provided no reduction in the form of $\Phi(V_1)$ has been made by means of the equation $F_0(V_1) = 0$ of § 57.*

As an example, we recur to the equation $x^3 + x^2 + x + 1 = 0$, and seek an expression for the function $\phi \equiv x_2$ in terms of $V_1 \equiv x_2 - x_1$. Then

$$F(V) = V^6 + 4V^4 + 4V^2 + 16, \quad F'(V) = 6V^5 + 16V^3 + 8V,$$

$$\lambda(V) = F(V) \left\{ \frac{x_2}{V - V_1} + \frac{x_1}{V + V_1} + \frac{x_2}{V - V_2} + \frac{x_3}{V - V_3} + \frac{x_3}{V + V_2} + \frac{x_1}{V + V_3} \right\}$$
$$= -2V^5 - 4V^4 - 12V^3 - 8V^2 - 16V - 48,$$

upon setting $x_1 = -1$, $x_2 = i$, $x_3 = -i$, $V_1 = i + 1$, $V_2 = 2i$, $V_3 = -i + 1$. Hence

$$x_2 = \frac{\lambda(V_1)}{F'(V_1)} = \frac{-2V_1^5 - 4V_1^4 - 12V_1^3 - 8V_1^2 - 16V_1 - 48}{6V_1^5 + 16V_1^3 + 8V_1} \equiv \Phi(V_1).$$

In verification, we find that

$$\lambda(V_1) = \lambda(i + 1) = -48i - 16, \quad F'(V_1) = 16i - 48, \quad \Phi(V_1) = i = x_2.$$

---

* That such a reduction invalidates the result is illustrated in the example of § 59.

In view of the corollary, we should have

$$x_1 = \Phi(-V_1), \quad x_2 = \Phi(V_2), \quad x_3 = \Phi(V_3), \quad x_3 = \Phi(-V_2), \quad x_1 = \Phi(-V_3).$$

To verify these results, we note that

$$\Phi(-V_1) = \frac{16i-48}{-16i+48} = -1, \quad \Phi(V_2) = \frac{-80}{80i} = i, \quad \Phi(-V_2) = \frac{-80}{-80i} = -i,$$

while $\Phi(V_3)$ and $\Phi(V_1)$, $\Phi(-V_3)$, and $\Phi(-V_1)$, x_3 and x_2, are conjugate imaginaries, and x_1 is real.

59. As a special case of the preceding theorem, *the roots of the given equation are rational functions of V_1 with coefficients in R:*

$$(8) \qquad x_1 = \psi_1(V_1), \; x_2 = \psi_2(V_1), \; \ldots, \; x_n = \psi_n(V_1).$$

Hence the determination of V_1 is equivalent to the solution of the given equation.

Since each V_s is a rational function of $x_1, \ldots, x_n$ with coefficients in R, it follows that *all the roots of the Galois resolvent are rational functions with coefficients in R of any one root V_1.*

EXAMPLE. For the equation $x^3+x^2+x+1=0$, and $V_1 = x_2 - x_1$, we have

$$x_1 = -1, \quad x_2 = V_1 - 1, \quad x_3 = -V_1 + 1, \quad V_2 = 2V_1 - 2, \quad V_3 = -V_1 + 2.$$

Although x_2 and $V_1 - 1$ are numerically equal, the functions x_1 and $-V_1 - 1$, obtained by applying the substitution (x_1x_2), are not equal. The relation $x_2 = V_1 - 1$ is a *reduced* form of $x_2 = \Phi(V_1)$, obtained in virtue of the identity $V_1^2 - 2V_1 + 2 = 0$ (§ 57). Thus

$$-2V_1^5 - 4V_1^4 - 12V_1^3 - 8V_1^2 - 16V_1 - 48 = -48V_1 + 32,$$
$$6V_1^5 + 16V_1^3 + 8V_1 = 16V_1 - 64,$$

$$\frac{-48V_1+32}{16V_1-64} = \frac{(-3V_1+2)(V_1+2)}{(V_1-4)(V_1+2)} = \frac{-3V_1^2-4V_1+4}{V_1^2-2V_1-8} = \frac{-10V_1+10}{-10} = V_1 - 1.$$

It happens, however, that the equality $x_2 = V_1 - 1$ leads to an equality $x_3 = V_3 - 1 = -V_1 + 1$ upon applying the substitution (x_2x_3). The fact that the identical substitution and (x_2x_3), but no other substitutions on x_1, x_2, x_3, lead to an equality when applied to $x_2 = V_1 - 1$ finds its explanation in the general theorems next established.

THE GROUP OF AN EQUATION.

60. Let the roots of Galois' resolvent (5) be designated

$$(9) \qquad V_1,\ V_a,\ V_b, \ldots, V_l,$$

the substitutions by which they are derived from V_1 being

$$(10) \qquad I,\ a,\ b, \ldots, l.$$

These substitutions form a group G, called the **group of the given equation** (1) *with respect to the domain of rationality R.*

The proof consists in showing that, if r and s are any two of the substitutions (10), the product rs occurs among those substitutions. Let therefore V_r and V_s be roots of (5). Then

$$F_0(V_r)=0.$$

Now V_r is a rational function of V_1 with coefficients in R:

$$(11) \qquad V_r=\theta(V_1),$$

the function θ being left in its unreduced form as determined in § 58. Hence $F_0[\theta(V_1)]=0$, so that one root V_1 of the equation (5) irreducible in R satisfies the equation

$$(12) \qquad F_0[\theta(V)]=0,$$

with coefficients in R. Hence (§ 55) the root V_s of (5) satisfies (12).

$$\therefore F_0[\theta(V_s)]=0.$$

In view of the corollary of § 58, it follows from (11) that

$$(V_r)_s \equiv V_{rs}=\theta(V_s).$$

Hence $F_0(V_{rs})=0$, so that V_{rs} occurs among the roots (9).

EXAMPLE. For the equation $x^3+x^2+x+1=0$ and the domain R of rational numbers, the Galois resolvent was shown in § 57 to be $V^2-2V+2=0$, having the roots V_1 and V_3. Since V_3 was derived from V_1 by the substitution (x_2x_3), the group of the equation $x^3+x^2+x+1=0$ with respect to R is $\{I, (x_2x_3)\}$.

For the domain (i), the Galois resolvent was shown to be $V-V_1=0$. Hence the group of the equation with respect to (i) is the identity.

61. The group G of order N of the equation (1) with the roots $x_1, x_2, \ldots, x_n$ possesses the following two fundamental properties:

A. *Every rational function $\phi(x_1, x_2, \ldots, x_n)$ of the roots which remains unaltered by all the substitutions of G lies in the domain R.*

B. *Every rational function $\phi(x_1, x_2, \ldots, x_n)$ of the roots which equals a quantity in R remains unaltered by all the substitutions of G.*

By a rational function $\phi = \phi(x_1, \ldots, x_n)$ of the roots is meant a rational function with coefficients in R. Then by § 58

$$(13) \qquad \phi = \Phi(V_1), \quad \phi_a = \Phi(V_a), \; \phi_b = \Phi(V_b), \ldots, \; \phi_l = \Phi(V_l),$$

where Φ is a rational function with coefficients in R.

Proof of A. If $\phi = \phi_a = \phi_b = \ldots = \phi_l$, it follows from (13) that

$$\phi = \frac{1}{N}\{\Phi(V_1) + \Phi(V_a) + \Phi(V_b) + \ldots + \Phi(V_l)\}.$$

The second member is a symmetric function of the N roots (9) of Galois' resolvent (5) and hence is a rational function of its coefficients which belong to R. Hence ϕ lies in R.

Proof of B. If ϕ equals a quantity r lying in R, we have, in view of (13), the equality

$$\Phi(V_1) - r = 0.$$

Hence V_1 is a root of the equation, with coefficients in R,

$$(14) \qquad \Phi(V) - r = 0.$$

Since one root V_1 of the irreducible Galois resolvent equation (5) satisfies (14), all the roots $V_1, V_a, \ldots, V_l$ of (5) satisfy (14), in view of § 55. Hence

$$\Phi(V_1) - r = 0, \quad \Phi(V_a) - r = 0, \quad \ldots, \quad \Phi(V_l) - r = 0.$$

It therefore follows from (13) that $\phi = \phi_a = \phi_b = \ldots = \phi_l$. Hence ϕ remains unaltered by all the substitutions of G.

62. By a **rational relation** between the roots $x_1, \ldots, x_n$ is meant an equality $\phi(x_1, \ldots, x_n) = \psi(x_1, \ldots, x_n)$ between two rational functions, *with coefficients in R.* Then $\phi - \psi$ is a rational function, equal to the quantity zero belonging to R, and therefore (by B) is unaltered by every substitution s of G. Hence $\phi_s - \psi_s = \phi - \psi = 0$, so that $\phi_s = \psi_s$. Hence the result:

Any rational relation between the roots remains true if both members be operated upon by any substitution of the group G.

Example. For the domain of rational numbers, it was shown in § 60 that the equation $x^3+x^2+x+1=0$ has the group $\{I, (x_2x_3)\}$. The rational relation (§ 59, Example)

$$x_2 = V_1 - 1 \equiv x_2 - x_1 - 1$$

leads to a true relation $x_3 = x_3 - x_1 - 1 \equiv V_3 - 1$ under the substitution (x_2x_3). If we apply (x_1x_2), we obtain a false relation $x_1 = x_1 - x_2 - 1$.

63. Theorem. *Properties* A *and* B *completely define the group G of the equation: any group having these properties is identical with G.*

Suppose first that we know of a group

$$G' = \{I,\ a',\ b',\ \ldots,\ m'\}$$

that every rational function of the roots $x_1, \ldots, x_n$, which remains unaltered by all the substitutions of G', lies in R. The equation

$$F'(V) \equiv (V-V_1)(V-V_{a'})(V-V_{b'}) \ldots (V-V_{m'}) = 0$$

has its coefficients in R since they are symmetric functions of $V_1, V_{a'}, \ldots, V_{m'}$ and therefore unaltered by the substitutions of G'. Since $F'(V)=0$ admits the root V_1 of the irreducible Galois resolvent (5), it admits all the roots $V_1, V_a, \ldots, V_l$ of (5). Hence $I, a, \ldots, l$ occur among the substitutions of G', so that G is a subgroup of G'.

Suppose next that we know of a group

$$G'' = \{I,\ a'',\ b'',\ \ldots,\ r''\}$$

that every rational function of $x_1, \ldots, x_n$ which lies in R remains unaltered by all the substitutions of G''. Then the rational function $F_0(V_1)$, being equal to the quantity zero lying in R, remains unaltered by $a'', b'', \ldots, r''$, so that

$$0 = F_0(V_1) = F_0(V_{a''}) = F_0(V_{b''}) = \ldots = F_0(V_{r''}).$$

Hence $V_1, V_{a''}, \ldots, V_{r''}$ occur among the roots $V_1, V_a, \ldots, V_l$ of $F_0(V)=0$. Hence G'' is a subgroup of G.

If both properties hold for a group, $G' \equiv G''$; then G' contains G as a subgroup and G' is a subgroup of G. Hence $G' \equiv G'' \equiv G$.

It follows that *the group of a given equation for a given domain is unique.* In particular, the group of an equation is independent of the special $n!$-valued function V_1 chosen.

EXAMPLE. For the equation $x^3+x^2+x+1=0$ and the domain R of all rational numbers, the functions $\pm V_1$, $\pm V_2$, $\pm V_3$ of § 57 are each 6-valued. Employing V_1, we obtain the Galois resolvent

$$(V-V_1)(V-V_3)=V^2-2V+2=0$$

and the group $\{I, x_2x_3)\}$. Evidently no change results from the employment of V_3. If we employ either $-V_1$ or $-V_3$, we obtain the Galois resolvent

$$(V+V_1)(V+V_3)=V^2+2V+2=0$$

and the group $\{I, (x_2x_3)\}$. If we employ either V_2 or $-V_2$, we get

$$(V-V_2)(V+V_2)=V^2+4=0.$$

Since $V_2=x_2-x_3$, the substitution replacing V_2 by $-V_2$ is (x_2x_3), so that the group is again $\{I, (x_2x_3)\}$.

ACTUAL DETERMINATION OF THE GROUP G OF A GIVEN EQUATION.

64. Group of the general equation of degree n. Its coefficients $c_1, \ldots, c_n$ are independent variables, and likewise its roots (p. 101). We proceed to show that, *for a domain R containing the coefficients and any assigned constants, the group of the general equation of degree n is the symmetric group $G_{n!}$.* It is only necessary to show that the Galois resolvent $F_0(V)=0$ is of degree $n!$. In the relation $F_0(V_1)=0$, we replace V_1 and the coefficients $c_1, \ldots, c_n$ by their expressions in terms of $x_1, \ldots, x_n$. Since the latter are independent. the resulting relation must be an identity (see p. 101) and hence remain true after any permutation of $x_1, \ldots, x_n$. By suitable permutations, V_1 is changed into $V_2, \ldots V_{n!}$ in turn, while $c_1, \ldots, c_n$, being symmetric functions, remain unaltered. Hence $F_0(V_2)=0$, $\ldots$, $F_0(V_{n!})=0$. Hence $F_0(V)=0$ has $n!$ distinct roots.

Another proof follows from § 63 by noting that properties A and B hold for the symmetric group $G_{n!}$ when $x_1, \ldots, x_n$ are independent variables. Thus A states that every symmetric function of the roots is rationally expressible in terms of the coefficients.

65. To determine the group of a special equation, we usually resort to some device. It is generally impracticable to construct an $n!$-valued function and then determine the Galois resolvent (5); or to apply properties A and B directly, since they relate to an infinite number of rational functions of the roots. Practical use may, however, be made of the following lemma, involving a knowledge of a single rational function:

LEMMA. *If a rational function $\psi(x_1, \ldots, x_n)$ remains formally unaltered by the substitutions of a group G' and by no other substitutions, and if ψ equals a quantity lying in the domain R, and if the conjugates of ψ under $G_{n!}$ are all distinct, then the group of the given equation for the domain R is a subgroup of G'.*

In view of the first part of § 63, it is only necessary to show that every rational function $\phi(x_1, \ldots, x_n)$, which remains *numerically* unaltered by all the substitutions of G', lies in R. If G' is of order P, we can set

$$\phi = \frac{1}{P}(\phi_1 + \phi_2 + \ldots + \phi_P),$$

so that ϕ can be given a form such that it is *formally* unaltered by all the substitutions of G'. Then, by Lagrange's Theorem (§ 31), ϕ is a rational function of ψ and hence equals a quantity lying in R.

EXAMPLE 1. To find the group of $x^3 - 1 = 0$ for the domain R of all rational numbers. The roots are

$$x_1 = 1, \quad x_2 = \tfrac{1}{2}(-1 + \sqrt{-3}), \quad x_3 = \tfrac{1}{2}(-1 - \sqrt{-3}).$$

Taking $\psi = x_1$, it follows from the lemma that G is a subgroup of $G' = \{I, (x_2x_3)\}$. Since x_2 does not lie in R, G is not the identity (property A). Hence $G = G'$.

EXAMPLE 2. To find the group G of $y^3 - 7y + 7 = 0$ for the domain R of all rational numbers.

For the cubic $y^3 + py + q = 0$, we have (§ 2)

$$D \equiv (y_1 - y_2)^2 (y_2 - y_3)^2 (y_3 - y_1)^2 = -27q^2 - 4p^3.$$

For $p = -7$, $q = 7$, we get $D = 7^2$. Hence the function

$$\psi \equiv (y_1 - y_2)(y_2 - y_3)(y_3 - y_1)$$

has a value ± 7 lying in R and its conjugates ψ and $-\psi$ under G_6 are distinct. By the lemma, G is therefore a subgroup of the alternating group G_3, and hence either G_3 itself or the identity G_1. Now, if the group of the equation were G_1, its roots would lie in R. But * a rational root of an equation of the form $y^3-7y+7=0$, having integral coefficients and unity as the coefficient of the highest power, is necessarily an integer. By trial, ± 1, ± 7 are not roots. Hence the roots are all irrational. Hence the group G is G_3.

EXAMPLE 3. Find the group of $x^4+1=0$ for the domain of rational numbers.

We seek a rational function of the roots x_1, x_2, x_3, x_4 which equals a rational number. Let us try the function $y_1=x_1x_2+x_3x_4$. Specializing the result holding for the general quartic equation (§ 4), we find that, for the quartic $x^4+1=0$, the resolvent equation (16) for y_1 is

$$y^3-4y=0.$$

By a suitable choice of notation to distinguish the roots x_i, we may set

$$y_1=-2, \quad y_2=0, \quad y_3=+2.$$

Hence y_1 equals a rational number and its conjugates under G_{24} are all distinct. Hence G is a subgroup of G_8, the group to which $x_1x_2+x_3x_4$ belongs *formally* (§ 21). Similarly, by considering the conjugate functions $y_2=x_1x_3+x_2x_4$, and $y_3=x_1x_4+x_2x_3$, we find that G is a subgroup of G_8' and G_8''. Hence G is a subgroup of G_4 (§ 21). Hence G is G_4, G_1,

$$G_2=\{I, (x_1x_2)(x_3x_4)\}, \quad G_2'=\{I, (x_1x_3)(x_2x_4)\}, \quad \text{or } G_2''=\{I, (x_1x_4)(x_2x_3)\}.$$

Now $G\neq G_1$, since no root of $x^4+1=0$ is rational.

If G_2, consider $t_1\equiv x_1+x_2-x_3-x_4$. For the general quartic equation $x^4+ax^3+bx^2+cx+d=0$, we have $t_1^2=a^2-4b+4y_1$ by § 5. Hence, for $x^4+1=0$, $t_1^2=-8$. Since t_1 is not rational, $G\neq G_2$.

If G_2'', consider $t_3\equiv x_1+x_4-x_2-x_3$. In general, $t_3^2=a^2-4b+4y_3$. Here $t_3^2=+8$. Since t_3 is not rational, $G\neq G_2''$.

If G_2', consider $t_2\equiv x_1+x_3-x_2-x_4$. In general, $t_2^2=a^2-4b+4y_2$. Here $t_2^2=0$. Since a conjugate $-t_2$ of t_2 equals t_2, no conclusion may be drawn from the use of t_2. But $\psi\equiv x_1x_3-x_2x_4$ is unaltered by G_2'. Now

$$\psi^2=(x_1x_3+x_2x_4)^2-4x_1x_2x_3x_4=y_2^2-4=-4.$$

Hence ψ is not rational, so that $G\neq G_2'$.

The group of $x^4+1=0$ for the domain of rational numbers is therefore G_4.

EXERCISES.

Find for the domain of rational numbers the group of

1. $x^3+x^2+x+1=0$ (using the lemma, § 65).
2. $(x-1)(x+1)(x-2)=0$.

---

* Dickson, *College Algebra* (John Wiley & Sons), p. 198.

3. $x^3-2=0$. [x_1, x_2, x_3 and $(x_1-x_2)(x_2-x_3)(x_3-x_1)$ are irrational.]

4. $x^4+x^3+x^2+x+1=0$ with roots $x_1=\varepsilon$, $x_2=\varepsilon^2$, $x_3=\varepsilon^4$, $x_4=\varepsilon^3$, where ε is an imaginary fifth root of unity. Since the resolvent for $x_1x_2+x_3x_4$ is $y^3-y^2-3y+2=0$ with the roots 2, $\frac{1}{2}(-1\pm\sqrt{5})$, G is a subgroup of G'_8. The latter has the subgroup $C_4=\{I, (1234), (13)(24), (1432)\}$, to which belongs $\psi_1=x_1^2x_2+x_2^2x_3+x_3^2x_4+x_4^2x_1$. Here $\psi_1=\varepsilon^4+\varepsilon^3+\varepsilon+\varepsilon^2=-1$ is rational. The six conjugates to ψ_1 under G_{24} are distinct; they are obtained from ψ_1 by applying I, (12)(34), (12), (14), (23), (34); their values are -1, 4, $1+2\varepsilon+\varepsilon^3$, $1+2\varepsilon^3+\varepsilon^4$, $1+2\varepsilon^2+\varepsilon$, $1+2\varepsilon^4+\varepsilon^2$, respectively. Hence G is a subgroup of C_4. To $G'_2=\{I, (13)(24)\}$ belongs

$$(x_1-x_3+ix_2-ix_4)^2=(1+2i)(\varepsilon^2+\varepsilon^3-\varepsilon^4-\varepsilon)=\pm\sqrt{5}(1+2i).$$

Hence $G\neq G'_2$. Evidently $G\neq G_1$. Hence $G=C_4$.

5. Show that, for the domain $(1, i)$, the group of $x^4+1=0$ is G'_2.

6. Show that, for the domain $(1, \omega)$, ω=imaginary cube root of unity, the group of $x^3-2=0$ is $C_3=\{I, (x_1x_2x_3), (x_1x_3x_2)\}$.

Hint: $(x_1+\omega x_2+\omega^2x_3)^3$ and $(x_1+\omega^2x_2+\omega x_3)^3$ have distinct rational values.

TRANSITIVITY OF GROUP; IRREDUCIBILITY OF EQUATION.

66. A group of substitutions on n letters is **transitive** if it contains a substitution which replaces an arbitrarily given letter by another arbitrarily given letter; otherwise the group is **intransitive**.

Thus the group $G_4=\{I, (x_1x_2)(x_3x_4), (x_1x_3)(x_2x_4), (x_1x_4)(x_2x_3)\}$ is transitive; I replaces x_1 by x_1, $(x_1x_2)(x_3x_4)$ replaces x_1 by x_2, $(x_1x_3)(x_2x_4)$ replaces x_1 by x_3, $(x_1x_4)(x_2x_3)$ replaces x_1 by x_4. Having a substitution s which replaces x_1 by any given letter x_i and a substitution t which replaces x_1 by any given letter x_j, the group necessarily contains a substitution which replaces x_i by x_j, namely, the product $s^{-1}t$.

The group $H_4=\{I, (x_1x_2), (x_3x_4), (x_1x_2)(x_3x_4)\}$ is intransitive.

67. THEOREM. *The order of a transitive group on n letters is divisible by n.*

Of the substitutions of the given group G, those leaving x_1 unaltered form a subgroup $H=\{I, h_2, \ldots, h_r\}$. Consider a rectangular array (§ 28) of the substitutions of G with those of H in the first row, choosing as g_2 any substitution replacing x_1 by x_2, as g_3 any substitution replacing x_1 by x_3, etc. Then all the substitutions of the second row and no others will replace x_1 by x_2, all of the third row and no others will replace x_1 by x_3, etc. Since G is transitive, there are $\nu=n$ rows. But the order of G is divisible by ν (§ 26).

Examples of transitive groups: $G_3^{(3)}$, $G_6^{(3)}$, $G_{24}^{(4)}$, $G_{12}^{(4)}$, $G_8^{(4)}$, $G_4^{(4)}$.

The least order of a transitive group on n letters is therefore n. A transitive group on n letters of order n is called a **regular group.** Thus $G_3^{(3)}$ and $G_4^{(4)}$ are regular.

68. THEOREM. *If an equation is irreducible for the domain R, its group for R is transitive; if reducible, the group is intransitive.*

First, if $f(x)=0$ is irreducible in R, its group for R is transitive. For, if intransitive, G contains substitutions replacing x_1 by x_1, $x_2, \ldots, x_m$, but not by $x_{m+1}, \ldots, x_n$, the notation for the roots being properly chosen. Hence every substitution of G permutes $x_1, \ldots, x_m$ amongst themselves and therefore leaves unaltered any symmetric function of them. Hence the function $g(x) \equiv (x-x_1)(x-x_2)\ldots(x-x_m)$ has its coefficients in R, so that $g(x)$ is a rational factor of $f(x)$, contrary to the irreducibility of $f(x)$.

Let next $f(x)$ be reducible in R and let $g(x) \equiv (x-x_1)\ldots(x-x_m)$ be a rational factor of $f(x)$, m being $<n$. The rational relation $g(x_1)=0$ remains true if operated upon by any substitution of G (§ 62). Hence no substitution of G can replace x_1 by one of the roots $x_{m+1}, \ldots, x_n$; for, if so, $g(x)=0$ would have as root one of the quantities $x_{m+1}, \ldots, x_n$, contrary to assumption. Hence G is intransitive.

EXAMPLE 1. The equation $x^3-1=0$ is reducible in the domain R of rational numbers; its group for R is $\{I, (x_2x_3)\}$ by § 65, Ex. 1, and is intransitive. A like result holds for $x^3+x^2+x+1=0$ (§ 60).

EXAMPLE 2. The equation $y^3-7y+7=0$ is irreducible in the domain R of rational numbers, since its left member has no linear factor in R (§ 65, Ex. 2). Hence its group for R is transitive. By § 65, the group is $G_3^{(3)}$.

EXAMPLE 3. The equation $x^4+1=0$ is irreducible in the domain R of rational numbers (§ 54, Ex. 2). Hence its group for R is transitive, and so is of order at least 4. We may therefore greatly simplify the work in § 65, Ex. 3, for the determination of the group G.

EXAMPLE 4. The equation $x^4+1=0$ is reducible in the domain $(1, i)$. Its group G_2' is intransitive (see Ex. 5, page 58).

RATIONAL FUNCTIONS BELONGING TO A GROUP.

69. THEOREM. *Those substitutions* **of the group** *G of an equation which leave unaltered a rational function ϕ of its roots form a group.*

Let I, a, b, . . . , k be all the substitutions of G which leave ϕ unaltered (in the numerical sense, § 52). Apply to the rational relation $\phi = \phi_a$ the substitution b of the group G. Then (§ 62) $\phi_b = \phi_{ab}$. Hence $\phi_{ab} = \phi$, so that the product ab is one of the substitutions leaving ϕ unaltered. Hence the substitutions I, a, b, . . . , k form a group H.

No matter what group ϕ belongs to *formally* (§ 21), we shall henceforth say that ϕ **belongs to the group** H, a subgroup of G.

EXAMPLE. For the domain R of rational numbers the group of $x^4+1=0$ is

$$G_4 = \{I, (x_1x_2)(x_3x_4), (x_1x_3)(x_2x_4), (x_1x_4)(x_2x_3)\},$$

by § 65, Ex. 3. Of the 12 substitutions which leave x_1^2 numerically unaltered (§ 49), only I and $(x_1x_3)(x_2x_4)$ occur in G_4. Hence the function x_1^2 of the roots of $x^4+1=0$ belongs to the group $\{I, (x_1x_3)(x_2x_4)\}$.

70. THEOREM. *If H is any subgroup of the group G of a given equation for a domain R, there exists a rational function of its roots with coefficients in R which belongs to H.*

Let V_1 be any $n!$-valued function of the roots with coefficients in R (§ 56). Let V_1, V_a, . . . , V_k be the functions derived from V_1 by applying the substitutions of H. Then the product

$$\phi \equiv (\rho - V_1)(\rho - V_a) \ldots (\rho - V_k)$$

in which ρ is a suitably chosen quantity in R, is a rational function of the roots with coefficients in R which belongs to H (compare § 25).

71. THEOREM. *If a rational function ψ of the roots of an equation belongs to a subgroup H of index ν under the group G of the equation for a domain R, then ψ takes ν distinct values when operated upon by all the substitutions of G; they are the roots of a resolvent equation with coefficients in R,*

$$g(y) \equiv (y-\psi_1)(y-\psi_2) \ldots (y-\psi_\nu) = 0. \qquad (15)$$

The proof that there are exactly ν distinct values of ψ under the substitutions of G is the same as in § 29, the term *distinct* now having the meaning given in § 52.

Any substitution *of the group* G merely permutes the functions $\psi_1, \psi_2, \ldots, \psi_\nu$ (compare § 30), so that any symmetric function of them is unaltered by all the substitutions of G and hence equals a quantity in R (Theorem A, § 61). Hence the coefficients of (15) lie in R.

REMARK. *The resolvent equation* (15) *is irreducible in* R.

Let $\gamma(y)$ be a rational factor of $g(y)$. Applying to the rational relation $\gamma(\psi_1)=0$ the substitutions of G, we get $\gamma(\psi_2)=0, \ldots, \gamma(\psi_\nu)=0$. Hence $\gamma(y)=0$ admits all the roots of $g(y)=0$, so that $\gamma(y)\equiv g(y)$.

EXAMPLE 1. For the domain R of rational numbers, the group G of $x^3+x^2+x+1=0$ is $\{I, (x_2x_3)\}$, by § 60. The conjugates to x_2-x_1 under G are $\psi_1=x_2-x_1$, $\psi_2=x_3-x_1$. They are the roots of

$$y^2-(\psi_1+\psi_2)y+\psi_1\psi_2=y^2-2y+2=0.$$

EXAMPLE 2. For the domain $(1, i)$, the group G of $x^4+1=0$ is $\{I, (x_1x_3)(x_2x_4)\}$, by Ex. 5, page 58, employing the notation of § 49 for the roots. The conjugates to x_1 under G are $\psi_1=x_1$, $\psi_2=x_3$. They are the roots of

$$y^2-(\varepsilon-\varepsilon)y+\varepsilon(-\varepsilon)=y^2-i=0.$$

It is irreducible in $(1, i)$, since $\sqrt{i}=(1+i)\div\sqrt{2}$.

72. LAGRANGE'S THEOREM GENERALIZED BY GALOIS. *If a rational function* $\phi(x_1, x_2, \ldots, x_n)$ *of the roots of an equation* $f(x)=0$ *with coefficients in a domain* R *remains unaltered by all those substitutions of the group* G *of* $f(x)=0$ *which leave another rational function* $\psi(x_1, x_2, \ldots, x_n)$ *unaltered, then* ϕ *is a rational function of* ψ *with coefficients in* R.

The function ψ belongs to a certain subgroup H of G, say of index ν. By means of a rectangular array of the substitutions of G with those of H in the first row, we obtain the ν distinct conjugate functions $\psi_1, \psi_2, \ldots, \psi_\nu$ and a set of functions $\phi_1, \phi_2, \ldots, \phi_\nu$, not necessarily distinct, but such that a substitution of G which replaces ψ_i by ψ_j will replace ϕ_i by ϕ_j (compare § 31). If $g(t)$ be defined by (15), then

$$\lambda(t) \equiv g(t)\left(\frac{\phi_1}{t-\psi_1}+\frac{\phi_2}{t-\psi_2}+\ldots+\frac{\phi_\nu}{t-\psi_\nu}\right)$$

is an integral function of t which remains unaltered by all the substitutions of G, so that its coefficients lie in R (§ 71). Taking $\psi_1 \equiv \psi$ for t, we get $\phi = \lambda(\psi) \div g'(\psi)$.

For examples, see § 58. The function V_1 is unaltered by the **identical** substitution only, which leaves unaltered any rational function.

REDUCTION OF THE GROUP BY ADJUNCTION.

73. For the domain $R=(1)$ of all rational numbers, the group of the equation $x^3+x^2+x+1=0$ is $G_2=\{I, (x_2x_3)\}$; while its group for the domain $R'=(1, i)$ is the identity G_1 (see § 60). In the language of Galois and Kronecker, we derive the domain $R'=(1, i)$ from the included domain $R=(1)$ by **adjoining** the quantity i to the domain R. By this adjunction the group G_2 of x^3+x^2+x+1 is **reduced** to the subgroup G_1. The adjoined quantity i is here a rational function of the roots, $i=x_2=-x_3$, in the notation of § 49 for the roots. The Galois resolvent $V^2-2V+2=0$ for R becomes reducible in R', viz., $(V-i-1)(V+i-1)=0$.

For the domain $R=(1)$, the group of $x^4+1=0$ is G_4; for the domain $(1, i)$, its group is the subgroup $G_2'=\{I, (x_1x_3)(x_2x_4)\}$, by § 65. By the adjunction of i to the domain R, the group is reduced to a subgroup G_2'. Here $i=x_1^2=x_3^2=-x_2^2=-x_4^2=x_2x_4$, in the notation of § 49. The subgroup of G_4 to which x_1^2 belongs is G_2'. If we afterwards adjoin $\sqrt{2}$, the roots will all belong to the enlarged domain $(1, i, \sqrt{2})$, so that the group reduees to the identity. For example, $x_1=(1+i)\div\sqrt{2}$.

For the domain $R=(1)$, the group of $x^3-2=0$ is G_6; for the domain $(1, \omega)$, ω being an imaginary cube root of unity, the group is the cyclic group C_3 (Exercises 3 and 6, page 58). Call the roots

$$x_1=\sqrt[3]{2}, \quad x_2=\omega\sqrt[3]{2}\equiv\omega x_1, \quad x_3=\omega^2\sqrt[3]{2}\equiv\omega^2 x_1.$$

Then $\omega=x_2/x_1$, a rational function belonging to C_3. In fact, $(x_1x_2x_3)$ replaces x_2/x_1 by $x_3/x_2=\omega=x_2/x_1$, $(x_1x_3x_2)$ replaces x_2/x_1 by $x_1/x_3=\omega^{-2}=\omega$; while these two substitutions and the identity are the only substitutions leaving x_2/x_1 unaltered. If we subsequently adjoin $\sqrt[3]{2}$, the roots all belong to the enlarged domain $(1, \omega, \sqrt[3]{2})$, so that the group reduces to the identity.

74. In general, we are given a domain $R=(R', R'', \ldots)$ and an equation $f(x)=0$ with coefficients in that domain. Let G be its group for R. Adjoin a quantity ξ. The irreducible Galois resolvent $F_0(V)=0$ for the initial domain R may become reducible in the enlarged domain $R_1=(\xi; R', R'', \ldots)$. Let $\lambda(V, \xi)$ be that factor of $F_0(V)$ which is rational and irreducible in R_1 and vanishes for $V=V_1$. If $V_1, V_a, \ldots, V_k$ are the roots of $\lambda(V, \xi)=0$, then $G'=\{I, a, \ldots, k\}$ is the group of $f(x)=0$ in R_1 (§ 57). Hence G' is a subgroup of G, including the possibility $G'=G$, which occurs if $F_0(V)$ remains irreducible after the adjunction of ξ, so that $\lambda(V, \xi)=F_0(V)$.

THEOREM. *By an adjunction, the group G is reduced to a subgroup G'.*

75. Suppose that, as in the examples in § 73, the quantity adjoined to the given domain R is a rational function $\psi(x_1, x_2, \ldots, x_n)$ of the roots with coefficients in R.

THEOREM. *By the adjunction of a rational function $\psi(x_1, \ldots, x_n)$ belonging to a subgroup H of G, the group G of the equation is reduced precisely to the subgroup H.*

It is to be shown that the group H has the two characteristic properties (§ 61) of the group of the equation for the new domain $R_1=(\psi; R', R'', \ldots)$. First, any rational function $\phi(x_1, \ldots, x_n)$ which remains unaltered by all the substitutions of H is a rational function of ψ with coefficients in R (§ 72) and hence lies in R_1. Second, any rational function $\phi(x_1, \ldots, x_n)$ which equals a quantity ρ in R_1 remains unaltered by all the substitutions of H. For the relation $\phi=\rho$ may be expressed as a rational relation in R and hence leads to a true relation when operated upon by any substitution of G (§ 62) and, in particular, by the substitutions of the subgroup H. The latter leave ψ, and hence also ρ, unaltered. Hence the left member ϕ of the relation remains unaltered by all the substitutions of H.

CHAPTER VII.

SOLUTION BY MEANS OF RESOLVENT EQUATIONS.

76. Before developing the theory further, it is desirable to obtain a preview of the applications to be made to the solution of any given equation $f(x)=0$. Suppose that we are able to solve the resolvent equation (15), one of whose roots is the rational function ψ belonging to the subgroup H of the group G of $f(x)=0$. Since ψ is then known, it may be adjoined to the given domain of rationality $(R', R'', \ldots)$. For the enlarged domain $R_1 = (\psi; R', R'', \ldots)$, the group of $f(x)=0$ is H. Let $\chi(x_1, \ldots, x_n)$ be a rational function with coefficients in R_1 which belongs to a subgroup K of H. Suppose that we are able to solve the resolvent equation one of whose roots is χ. Then χ may be adjoined to the domain R_1. For the enlarged domain $R_2 = (\chi, \psi; R', R'', \ldots)$, the group of $f(x)=0$ is K. Proceeding in this way, we reach a final domain R_k for which the group of $f(x)=0$ is the identity G_1. Then the roots $x_1, \ldots, x_n$, being unaltered by the identity, lie in this domain R_k (property A, § 61). The solution of $f(x)=0$ may therefore be accomplished if all the resolvent equations can be solved. To apply Galois' methods to the solution of each resolvent, the first step is to find its group for the corresponding domain of rationality.

77. Isomorphism. Let G be the group of a given equation $f(x)=0$ for a given domain R. Let $\psi(x_1, \ldots, x_n)$ be a rational function of its roots with coefficients in R and let ψ belong to a subgroup H of index ν under G. Consider a rectangular array of the substitutions of G with those of H in the first row, and the resulting functions conjugate to ψ:

$$\begin{array}{llll|l} h_1=I & h_2 & \ldots & h_P & \psi_1=\psi \\ g_2 & h_2g_2 & \ldots & h_Pg_2 & \psi_2=\psi_{g_2} \\ \cdot & \cdot & \cdot & \cdot & \cdot\;\cdot\;\cdot \\ g_\nu & h_2g_\nu & \ldots & h_Pg_\nu & \psi_\nu=\psi_{g_\nu} \end{array}$$

Apply any substitution g of the group G to the ν conjugates

(16) $$\psi,\ \psi_{g_2},\ \psi_{g_3},\ \ldots,\ \psi_{g_\nu}.$$

The resulting functions

(17) $$\psi_g,\ \psi_{g_2g},\ \psi_{g_3g},\ \ldots,\ \psi_{g_\nu g}$$

are merely a permutation of the functions (16), as shown in § 29. Hence to any substitution g of the group G on the letters $x_1, \ldots, x_n$, there corresponds one definite substitution

$$\gamma=\begin{pmatrix}\psi & \psi_{g_2} & \ldots & \psi_{g_\nu} \\ \psi_g & \psi_{g_2g} & \ldots & \psi_{g_\nu g}\end{pmatrix}\equiv\begin{pmatrix}\psi_{g_i} \\ \psi_{g_ig}\end{pmatrix}$$

on the letters (16). We therefore obtain* a set Γ of substitutions γ, not all of which are distinct in certain cases (Exs. 2 and 3 below).

THEOREM. *The set Γ of substitutions γ forms a group.*

For to g, g', and gg' correspond respectively

$$\gamma=\begin{pmatrix}\psi_{g_i} \\ \psi_{g_ig}\end{pmatrix},\quad \gamma'=\begin{pmatrix}\psi_{g_i} \\ \psi_{g_ig'}\end{pmatrix},\quad \gamma''=\begin{pmatrix}\psi_{g_i} \\ \psi_{g_igg'}\end{pmatrix}.$$

To compute the product $\gamma\gamma'$, we vary the order of the letters in the first line of γ' and have

$$\gamma'=\begin{pmatrix}\psi_{g_ig} \\ \psi_{g_ig\cdot g'}\end{pmatrix},\quad \gamma\gamma'=\begin{pmatrix}\psi_{g_i} \\ \psi_{g_igg'}\end{pmatrix}=\gamma''.$$

Hence if Γ contains γ and γ', it contains the product $\gamma\gamma'$.

Since Γ contains a substitution replacing ψ by ψ_{g_i} for any $i=1, \ldots, \nu$, *the group Γ is transitive* (§ 66).

* For a definition of Γ without using the function ψ, see § 104.

Definitions. The group Γ is said to be **isomorphic** to G, since to every substitution g of G corresponds *one* substitution γ of Γ, and to the product gg' of any two substitutions of G corresponds the product $\gamma\gamma'$ of the two corresponding substitutions of Γ. If, inversely, to every substitution of Γ corresponds but one substitution of G, the groups are said to be **simply isomorphic**;* otherwise, **multiply isomorphic**.*

Example 1. Let $G=G_6^{(3)}$, $H=G_1$, $\psi=x_1+\omega x_2+\omega^2 x_3$. Set (compare § 9)

$$\psi_1=\psi, \quad \psi_2=\psi_a, \quad \psi_3=\psi_b, \quad \psi_4=\psi_c, \quad \psi_5=\psi_d, \quad \psi_6=\psi_e.$$

Then $a=(x_1x_2x_3)$ replaces ψ_1 by $\psi_2=\omega^2\psi_1$, and ψ_4 by $\psi_6=\omega\psi_4$. Hence a replaces ψ_2 by $\omega^4\psi_1=\psi_3$, ψ_3 by $\omega^6\psi_1=\psi_1$, ψ_6 by $\omega^2\psi_4=\psi_5$, ψ_5 by $\omega^3\psi_4=\psi_4$. Hence to a corresponds $\alpha=(\psi_1\psi_2\psi_3)(\psi_4\psi_6\psi_5)$. Similarly, we find that to $c=(x_2x_3)$ corresponds $\gamma=(\psi_1\psi_4)(\psi_2\psi_5)(\psi_3\psi_6)$. Hence to $b=a^2$ corresponds $\beta=\alpha^2$, to $d=a^{-1}ca$ corresponds $\delta=\alpha^{-1}\gamma\alpha$, to $e=b^{-1}cb$ corresponds $\epsilon=\beta^{-1}\gamma\beta$. We have therefore the following holoedric isomorphism between G and Γ:

I	I
$a=(x_1x_2x_3)$	$\alpha=(\psi_1\psi_2\psi_3)(\psi_4\psi_6\psi_5)$
$b=(x_1x_3x_2)$	$\beta=(\psi_1\psi_3\psi_2)(\psi_4\psi_5\psi_6)$
$c=(x_2x_3)$	$\gamma=(\psi_1\psi_4)(\psi_2\psi_5)(\psi_3\psi_6)$
$d=(x_1x_3)$	$\delta=(\psi_2\psi_6)(\psi_3\psi_4)(\psi_1\psi_5)$
$e=(x_1x_2)$	$\epsilon=(\psi_3\psi_5)(\psi_1\psi_6)(\psi_2\psi_4)$

It may be verified directly that to b, d, e correspond β, δ, ϵ, respectively.

Since I, α, β, γ, δ, ϵ replace ψ_1 by ψ_1, ψ_2, ψ_3, ψ_4, ψ_5, ψ_6, respectively, Γ is transitive.

Example 2. Let $G=G_{12}^{(4)}$, $H=G_4$, $\psi=(x_1-x_2)(x_3-x_4)$. Set

$$\psi_1=\psi, \quad \psi_2=(x_1-x_3)(x_4-x_2), \quad \psi_3=(x_1-x_4)(x_2-x_3).$$

We obtain the following meriedric isomorphism between G and Γ:

I,	$(x_1x_2)(x_3x_4)$,	$(x_1x_3)(x_2x_4)$,	$(x_1x_4)(x_2x_3)$	I
$(x_2x_3x_4)$,	$(x_1x_3x_2)$,	$(x_1x_4x_3)$,	$(x_1x_2x_4)$	$(\psi_1\psi_2\psi_3)$
$(x_2x_4x_3)$,	$(x_1x_4x_2)$,	$(x_1x_2x_3)$,	$(x_1x_3x_4)$	$(\psi_1\psi_3\psi_2)$

The group Γ is transitive since it contains substitutions replacing ψ_1 by ψ_1, ψ_2, or ψ_3.

---

* Other terms are **holoedric** and **meriedric** for simple and multiple isomorphism.

78. Order of the group Γ. To find the number of distinct substitutions in Γ, we seek the conditions under which two substitutions γ and γ' of Γ are identical. Using the notation of § 77, the conditions are

$$\psi_{g_i g} = \psi_{g_i g'} \qquad (i=1, 2, \ldots, \nu),$$

if we set $g_1 = I$. Applying to this identity the substitution $g^{-1}g_i^{-1}$, we get

$$\psi = \psi_{g_i g' g^{-1} g_i^{-1}}.$$

Hence $g_i g' g^{-1} g_i^{-1} = h$, where h is some substitution leaving ψ unaltered and hence in the group H. Then

$$g' g^{-1} = g_i^{-1} h g_i \qquad (i=1, 2, \ldots, \nu).$$

But $g_i^{-1} h g_i$ belongs to the group $H_i \equiv g_i^{-1} H g_i$ of the function ψ_{gi} (§ 39). Hence $g' g^{-1}$ belongs simultaneously to $H_1, H_2, \ldots, H_\nu$, and therefore to their greatest common subgroup J.

Inversely, any substitution σ of J leaves $\psi_1, \psi_2, \ldots, \psi_\nu$ unaltered and hence corresponds to the identity in Γ. Then g and $g' = \sigma g$ correspond to substitutions γ and γ' which are identical.

If G is of order k and if the greatest common subgroup J of H_1, $H_2, \ldots, H_\nu$ is of order j, then Γ is of order k/j.

EXAMPLE 1. For $G = G_6$, $H = G_1$, the order of Γ is 6 (§ 77, Ex. 1).

EXAMPLE 2. For $G = G_{12}^{(4)}$, $H = G_4$ (§ 77, Ex. 2), we have $H_1 = H_2 = H_3$, since G_4 is self-conjugate under G_{12} (§ 41). Hence $k = 12$, $j = 4$, so that the order of Γ is 3.

EXAMPLE 3. For $G = G_{24}^{(4)}$, $H_1 = G_8$, $\psi = x_1x_2 + x_3x_4$, we set (§ 29, Ex. 2)

$$\psi_1 = x_1x_2 + x_3x_4, \quad \psi_2 = x_1x_3 + x_2x_4, \quad \psi_3 = x_1x_4 + x_2x_3.$$

Then $H_1 = G_8$, $H_2 = G_8'$, $H_3 = G_8''$, $J = G_4$ (§ 21). Hence Γ is of order $\frac{24}{4} = 6$. This result may be verified directly. There are only 6 possible substitutions on 3 letters ψ_1, ψ_2, ψ_3. But the substitutions of G which lead to the identical substitution of Γ must leave ψ_1, ψ_2, ψ_3 all unaltered and hence belong to the greatest common subgroups G_4 of H_1, H_2, H_3. Hence exactly four substitutions of G correspond to each substitution of Γ, so that the order of Γ is $\frac{24}{4} = 6$. The four substitutions of any set form one row of the rectangular array for

G_{24} with the substitutions I, $(x_1x_2)(x_3x_4)$, $(x_1x_3)(x_2x_4)$, $(x_1x_4)(x_2x_3)$ of G_4 in the first row. As right-hand multipliers we may take

$$g_1=I,\quad g_2=(x_2x_3x_4),\quad g_3=(x_2x_4x_3),\quad g_4=(x_3x_4),\quad g_5=(x_2x_4),\quad g_6=(x_2x_3).$$

To the four substitutions of the first row, the four of the second row, . . . , correspond

$$I,\quad (\psi_1\psi_2\psi_3),\quad (\psi_1\psi_3\psi_2),\quad (\psi_2\psi_3),\quad (\psi_1\psi_3),\quad (\psi_1\psi_2).$$

79. Of special importance is the case in which $H_1, H_2, \ldots, H_\nu$ are identical, so that *H is self-conjugate under G*. Then $J=H$, so that the order k/j of Γ equals the index ν of H under G. Hence the number of distinct substitutions of Γ equals the number of letters $\psi_1, \ldots, \psi_\nu$ upon which its substitutions operate, or *the order and the degree of the group Γ are equal.* Moreover, Γ was seen to be transitive. Hence Γ is a *regular group* (§ 67).

DEFINITION.* When H is self-conjugate under G, the group Γ is called the **quotient-group** of G by H and designated G/H. In particular, the order of G/H is the quotient of the order of G by that of H.

EXAMPLE 1. By Examples 1 and 2 of § 77, the quotient-group G_6/G_1 is a regular group on six letters; the quotient-group G_{12}/G_4 is the cycle group $\{I, (\psi_1\psi_2\psi_3), (\psi_1\psi_3\psi_2)\}$, which is a regular group.

EXAMPLE 2. We may not employ the symbol G_{24}/G_8, since G_8 is not self-conjugate under G_{24} (§ 78, Ex. 3).

EXAMPLE 3. Consider the groups G_6 and G_3 on three letters. To G_3 belongs $\psi_1=(x_1-x_2)(x_2-x_3)(x_3-x_1)$; under G_6 it takes a second value $\psi_2=-\psi_1$ (§ 9). We obtain the following isomorphism between G_6 and Γ:

$$\left.\begin{matrix} I, & (x_1x_2x_3), & (x_1x_3x_2) \\ (x_2x_3), & (x_1x_3), & (x_1x_2), \end{matrix}\right| \begin{matrix} I \\ (\psi_1\psi_2) \end{matrix}$$

Since G_3 is self-conjugate under G_6, we have $\Gamma=G_6/G_3=\{I, (\psi_1\psi_2)\}$.

COROLLARY. *If H is a self-conjugate subgroup of G of prime index ν, then Γ is a cyclic group of order ν* (§ 27).

Illustrations are afforded by the groups G_{12}/G_4 and G_6/G_3 of Exs. 1 and 2.

REMARK. Any substitution group G is simply isomorphic with a regular group. In proof, we have merely to take as ψ any $n!$-valued function V_1, whence Γ will be of order equal to the order of G.

---

* Hölder, *Math. Ann.*, vol. 24, page 31.

80. Let H be a *maximal* self-conjugate subgroup of G (§ 43). The quotient-group $\Gamma = G/H$ is then *simple* (§ 43). For if Γ has a self-conjugate subgroup Δ distinct from both Γ and the identity G_1, there would exist, in view of the correspondence between G and Γ, a self-conjugate subgroup D of G, such that D contains H but is distinct from both G and H. This would contradict the hypothesis that H was maximal.

For example, if H is a self-conjugate subgroup of G of prime index ν, it is necessarily maximal. Then Γ is a cyclic group of prime order ν (Cor., § 79) and consequently a simple group.

81. The importance of the preceding investigation of the group Γ of substitutions on the letters $\psi_1, \psi_2, \ldots, \psi_\nu$ lies in the significance of Γ in the study of the resolvent equation

$$(15) \qquad g(y) \equiv (y-\psi_1)(y-\psi_2) \ldots (y-\psi_\nu) = 0,$$

whose coefficients belong to the given domain R. We proceed to prove the

THEOREM. *For the domain R, the group of the equation* (15) *is Γ.*

We show that Γ has the characteristic properties A and B of § 61. Any rational function $\rho(\psi_1, \psi_2, \ldots, \psi_\nu)$ with coefficients in R may be expressed as a rational function $r(x_1, x_2, \ldots, x_n)$ with coefficients in R:

$$(18) \qquad \rho(\psi_1, \psi_2, \ldots, \psi_\nu) = r(x_1, x_2, \ldots, x_n).$$

From this rational relation we obtain a true relation (§ 62) upon applying any substitution g of the group G on $x_1, \ldots, x_n$. But g gives rise to a substitution γ of the group Γ on $\psi_1, \ldots, \psi_\nu$. Hence the resulting relation is

$$(19) \qquad \rho_\gamma(\psi_1, \psi_2, \ldots, \psi_\nu) = r_g(x_1, x_2, \ldots, x_n).$$

To prove A, let $\rho(\psi_1, \ldots, \psi_\nu)$ remain unaltered by all the substitutions of Γ, so that $\rho_\gamma = \rho$, for any γ in Γ. Then, by (18) and (19), $r_g = r$, for any g in G. Hence r lies in the domain R (property A for the group G). Hence ρ lies in R.

To prove B, let ρ lie in the domain R. Then, by (18), r lies in R. Hence $r_g = r$, for any g in G (property B for the group G). Hence, by (18) and (19), $\rho_\gamma = \rho$, so that ρ remains unaltered by all the substitutions γ of Γ.

COR. 1. Since Γ is transitive (§ 77), equation (15) is irreducible in R (§ 68). This was shown otherwise in § 71.

COR. 2. If the group H to which ψ belongs is self-conjugate under G, the group of the resolvent (15) is regular (§ 79). The resolvent is then said to be a **regular equation.**

COR. 3. If H is a self-conjugate subgroup of G of prime index ν, the group of (15) is cyclic (§ 79, Corollary). The resolvent is then said to be a **cyclic equation** of prime degree ν.

COR. 4. If H is a maximal self-conjugate subgroup of G, the group of (15) is simple (§ 80). The resolvent is then said to be a **regular and simple equation.**

82. THEOREM. *The solution of any given equation can be reduced to the solution of a chain of simple regular equations.*

Let G be the group of the given equation for a given domain R, and let a series of composition (§ 43) of G be

$$G, H, K, \ldots, M, G_1,$$

the factors of composition being λ (index of H under G), μ (index of K under H), $\ldots, \rho$ (index of G_1 under M). Let $\phi, \psi, \ldots, \chi, V$ be rational functions of the roots belonging to $H, K, \ldots, M, G_1$, respectively (§ 70). Then ϕ is a root of a resolvent equation of degree λ with coefficients in R, which is a simple regular equation (§ 81, Cor. 4). By the adjunction of ϕ to the domain R, the group G of the equation is reduced to H (§ 75). Then ψ is a root of a simple regular equation of degree μ with coefficients in the enlarged domain (ϕ, R). By the adjunction of ψ, the group is reduced to K. When, in this way, the group has reduced to the identity G_1, the roots $x_1, \ldots, x_n$ lie in the final domain reached (compare § 76).

In particular, *if the factors of composition $\lambda, \mu, \ldots, \rho$ are all prime numbers, the resolvent equations are all regular cyclic equations of prime degrees* (§ 81, Cor. 3).

83. THEOREM. *A cyclic equation of prime degree p is solvable by radicals.*

Let R be a given domain to which belong the coefficients of the given equation $f(x)=0$ with the roots $x_0, x_1, \ldots, x_{p-1}$, and for which the group of $f(x)=0$ is the cyclic group $G=\{I, s, s^2, \ldots, s^{p-1}\}$, where $s=(x_0x_1x_2\ldots x_{p-1})$. Adjoin to the domain R an imaginary pth root of unity * ω and let the group of $f(x)=0$ for the enlarged domain R' be G'. Consider the rational functions, with coefficients in R',

$$\theta_i \equiv x_0+\omega^i x_1+\omega^{2i}x_2+\ldots+\omega^{(p-1)i}x_{p-1}. \tag{20}$$

Under the substitution s, θ_i is changed into $\omega^{-i}\theta_i$. Hence $\theta_i^p \equiv \Theta_i$ is unaltered by s and therefore by every substitution of G and of the *subgroup* G' (§ 74). Hence Θ_i lies in the domain R' (§ 61). Extracting the pth root, we have $\theta_i=\sqrt[p]{\Theta_i}$. Since the function (20) belongs to the identity group, it must be possible, by Lagrange's Theorem (§ 72), to express the roots $x_0, x_1, \ldots, x_{p-1}$ rationally in terms of θ_i. The actual expressions for the roots were found in the following elegant way by Lagrange. We have, by (20),

$$\begin{array}{llll}
x_0+x_1 & +x_2 & +\ldots+x_{p-1} & =c \\
x_0+\omega x_1 & +\omega^2 x_2 & +\ldots+\omega^{p-1}x_{p-1} & =\sqrt[p]{\Theta_1} \\
x_0+\omega^2 x_1 & +\omega^4 x_2 & +\ldots+\omega^{2(p-1)}x_{p-1} & =\sqrt[p]{\Theta_2} \\
\cdots & \cdots & \cdots & \cdots \\
x_0+\omega^{p-1}x_1 & +\omega^{2(p-1)}x_2 & +\ldots+\omega^{(p-1)^2}x_{p-1} & =\sqrt[p]{\Theta_{p-1}}
\end{array}$$

where $c\equiv\sqrt[p]{\Theta_0}$ is the negative of the coefficient of x^{p-1} in $f(x)=0$. Multiplying these equations by $1, \omega^{-i}, \omega^{-2i}, \ldots, \omega^{-(p-1)i}$, respectively, and adding the resulting equations, and then dividing by p, we get †

$$x_i=\frac{1}{p}\left\{c+\omega^{-i}\sqrt[p]{\Theta_1}+\omega^{-2i}\sqrt[p]{\Theta_2}+\ldots+\omega^{-(p-1)i}\sqrt[p]{\Theta_{p-1}}\right\},$$

* As shown in § 89, ω can be determined by a finite number of applications of the operation *extraction of a single root of a known quantity.*

† Since $1+\omega^t+\omega^{2t}+\ldots+\omega^{(p-1)t}=0$ for $t=1, 2, \ldots, p-1$.

for $i=0, 1, \ldots, p-1$. The value of one of these $p-1$ radicals, say $\sqrt[p]{\theta_1}$, may be chosen arbitrarily; but the others are then fully determined, being rationally expressible in terms of that one. Indeed,

$$\sqrt[p]{\theta_i} \div (\sqrt[p]{\theta_1})^i \equiv \theta_i \div \theta_1^i$$

becomes $\omega^{-i}\theta_i \div (\omega^{-1}\theta_1)^i$ upon applying the substitution s and hence is unaltered by s, and is therefore in the domain R'.

84. From the results of §§ 82–83, we have the following

THEOREM. *If the group of an equation has a series of composition for which the factors of composition are all prime numbers, the equation is solvable by radicals, that is, by the extraction of roots of known quantities.*

The group property thus obtained as a sufficient condition for the algebraic solvability of a given equation will be shown (§ 92) to be also a necessary condition.

CHAPTER VIII.

REGULAR CYCLIC EQUATIONS; ABELIAN EQUATIONS.

85. Let $f(x)=0$ be an equation whose group G for a domain R consists of the powers of a circular substitution $s=(x_1x_2\ldots x_n)$:

$$G=\{I, s, s^2, \ldots, s^{n-1}\},$$

n being any integer. Since the cyclic group G is transitive and of order equal to its degree, it is *regular* (§ 67). Inversely, the generator s of a transitive cyclic group is necessarily a circular substitution on the n letters.*

The equation $f(x)=0$ then has the properties:

(a) It is irreducible, since its group is transitive (§ 68).

(b) All the roots are rational functions, with coefficients in R, of any one root x_1. Indeed, there are only n substitutions in the transitive group on n letters, and consequently a single substitution (the identity) leaving x_1 unaltered. Since x_1 belongs to the identity group, the result follows by Lagrange's Theorem (§ 72). Let $x_2=\theta(x_1)$. To this rational relation we may apply all the substitutions of G (§ 62). Hence

$$(21)\qquad x_2=\theta(x_1),\ x_3=\theta(x_2),\ \ldots,\ x_n=\theta(x_{n-1}),\ x_1=\theta(x_n).$$

Definition. An irreducible equation for a domain R between whose n roots exist relations of the form (21), θ being a rational function with coefficients in R, is called an **Abelian equation**.†

---

* A non-circular substitution, as $t=(x_1x_2x_3)(x_4x_5)$, generates an intransitive group. Thus the powers of t replace x_1 by x_1, x_2, or x_3 only.

† More explicitly, uniserial Abelian (einfache Abel'sche, Kronecker). A more general type of "Abelian equations" was studied by Abel, *Œuvres*, I, No. XI, pp. 114–140.

86. THEOREM. *The group G of an Abelian equation is a regular cyclic group.*

Denote any substitution of the group G by

$$g=\begin{pmatrix} x_1 & x_2 & x_3 & \dots & x_n \\ x_\alpha & x_\beta & x_\gamma & \dots & x_\nu \end{pmatrix}.$$

Applying to the rational relations (21) the substitutions g (§ 62),

$$x_\beta=\theta(x_\alpha),\ x_\gamma=\theta(x_\beta),\dots,\ x_\alpha=\theta(x_\nu).$$

But, by (21), $\theta(x_\alpha)=x_{\alpha+1}$, holding also for $\alpha=n$ if we agree to set $x_i=x_{i+n}=x_{i+2n}=\dots$ It follows that

$$x_\beta=x_{\alpha+1},\ x_\gamma=x_{\beta+1},\dots,\ x_\alpha=x_{\nu+1}.$$

Since the equation is irreducible, its roots are all distinct. Hence, aside from multiples of n,

$$\beta=\alpha+1,\quad \gamma=\beta+1=\alpha+2,\quad \delta=\gamma+1=\alpha+3,\dots$$

$$\therefore\ g=\begin{pmatrix} x_1 & x_2 & x_3 & \dots & x_n \\ x_\alpha & x_{\alpha+1} & x_{\alpha+2} & \dots & x_{\alpha+n-1} \end{pmatrix}.$$

Since g replaces x_i by $x_{i+\alpha-1}$, it is the power $\alpha-1$ of the circular substitution $s=(x_1x_2x_3\dots x_n)$ which replaces x_i by x_{i+1}. Hence G is a subgroup of $G'=\{I,\ s,\ s^2,\dots,\ s^{n-1}\}$. But G is transitive, since the equation is irreducible. Hence $G=G'$.

EXAMPLE. The equation $x^4+x^3+x^2+x+1\equiv\dfrac{x^5-1}{x-1}=0$ has the roots

$$x_1=\epsilon,\quad x_2=\epsilon^2,\quad x_3=\epsilon^4,\quad x_4=\epsilon^3,$$

where ϵ is an imaginary fifth root of unity. Hence

$$x_2=x_1^2,\ x_3=x_2^2,\ x_4=x_3^2,\ x_1=x_4^2.$$

Moreover, the equation is irreducible in the domain R of all rational numbers (§ 88). This may be verified directly by observing that the linear factors are $x-\epsilon^i$ and hence irrational, while

$$x^4+x^3+x^2+x+1\equiv(x^2+ax+r)(x^2+bx+r^{-1})$$

gives $a+b=1$, $ab+r+r^{-1}=1$, $ar^{-1}+br=1$, so that either

$$a=\tfrac{1}{2}(1\pm\sqrt{5}),\quad b=\tfrac{1}{2}(1\mp\sqrt{5}),\quad r=1,$$

or,
$$a=\frac{r}{r+1},\quad b=\frac{1}{r+1},\quad r^4+r^3+r^2+r+1=0.$$

Hence the group for R is a cyclic group. Compare Ex. 4, page 58.

87. Cyclotomic equation for the pth roots of unity, p being prime,

$$x^{p-1}+x^{p-2}+\dots+x+1=0. \tag{22}$$

Let ε be one root of (22), so that $\varepsilon^p=1$, $\varepsilon\neq 1$. Then

$$\varepsilon,\ \varepsilon^2,\ \varepsilon^3,\ \dots,\ \varepsilon^{p-1} \tag{23}$$

are all roots of (22) and are all distinct. Hence they furnish all the roots of (22). As shown in the Theory of Numbers, there exists,* for every prime number p, an integer g such that g^m-1 is divisible by p for $m=p-1$ but not for a smaller positive integer m. Such an integer g is called a **primitive root of** p. It follows that the series of integers

$$1,\ g,\ g^2,\ \dots,\ g^{p-2},$$

when divided by p, yield in some order the remainders

$$1,\ 2,\ 3,\ \dots,\ p-1.$$

Hence the roots (23) may be written

$$x_1=\varepsilon,\ x_2=\varepsilon^g,\ x_3=\varepsilon^{g^2},\ \dots,\ x_{p-1}=\varepsilon^{g^{2-p}}.$$

$$\therefore\ x_2=x_1^g,\ x_3=x_2^g,\ \dots,\ x_{p-1}=x_{p-2}^g,\ x_1=x_{p-1}^g,$$

the last relation following from the definition of g, thus:

$$(\varepsilon^{g^{p-2}})^g=\varepsilon^{g^{p-1}}=\varepsilon^{1+qp}=\varepsilon.$$

Hence the roots have the property indicated by formulæ (21). In view of the next section, we may therefore state the

THEOREM. *The cyclotomic equation for the imaginary pth roots of unity, p being prime, is an Abelian equation with respect to the domain of all rational numbers.*

---

* For example, if $p=5$, we may take $g=2$, since

$$2^1-1=1,\quad 2^2-1=3,\quad 2^3-1=7,\quad 2^4-1=15.$$

For $p=5$ the results of this section were found in the example of § 86.

88. Irreducibility of the cyclotomic equation (22) in the domain R of all rational numbers.* Suppose that

$$x^{p-1}+x^{p-2}+\ldots+x+1=\phi(x)\cdot\psi(x),$$

where ϕ and ψ are integral functions of degree $<p-1$ with integral † coefficients. Taking $x=1$, we get

$$p=\phi(1)\cdot\psi(1).$$

Since p is prime, one of the integral factors, say $\phi(1)$, must be ± 1. Since $\phi(x)=0$ has at least one root in common with (22), whose roots are (23), at least one of the expressions $\phi(\epsilon^t)$ is zero. Hence

$$\phi(\epsilon)\cdot\phi(\epsilon^2)\cdot\phi(\epsilon^3)\ldots\phi(\epsilon^{p-1})=0. \tag{24}$$

For any positive integer s less than p, the series

$$\epsilon^s,\ \epsilon^{2s},\ \epsilon^{3s},\ldots,\ \epsilon^{(p-1)s} \tag{25}$$

is identical, apart from the order of the terms, with the series (23). For, every number (25) equals a number (23), and the numbers (25) are all distinct. In fact, if

$$\epsilon^{rs}=\epsilon^{ts},\ \text{whence}\ \epsilon^{(r-t)s}=1,\qquad (0\overline{\overline{<}}r<p,\ 0\overline{\overline{<}}t<p)$$

then $(r-t)s$, and consequently also $r-t$, is divisible by p, so that $r=t$. Hence (24) holds true when ϵ is replaced by ϵ^s. Hence

$$\phi(x)\cdot\phi(x^2)\ldots\phi(x^{p-1})=0$$

is an equation having all the numbers (23) as roots. Its left member is therefore divisible by $x^{p-1}+\ldots+x+1$, so that

$$\phi(x)\cdot\phi(x^2)\ldots\phi(x^{p-1})=Q(x)\cdot(x^{p-1}+x^{p-2}+\ldots+x+1),$$

where $Q(x)$ is an integral function with integral coefficients. Setting $x=1$, we get

$$[\phi(1)]^{p-1}=[\pm 1]^{p-1}=p\cdot Q(1).$$

Since ± 1 is not divisible by p, the assumption that $x^{p-1}+\ldots+x+1$ is reducible in R leads to a contradiction.

---

* The proof is that by Kronecker, *Crelle*, vol. 29; other proofs have been given by Gauss, Eisenstein (*Crelle*, vol. 39, p. 167), Dedekind (Jordan, *Traité des substitutions*, Nos. 413–414).

† If rational, then integral (Weber, *Algebra*, I, 1895, p. 27).

89. THEOREM. *Any Abelian equation is solvable by radicals.*

Let n be the degree of the Abelian equation. By § 86, its group G is a regular cyclic group $\{I, s, s^2, \ldots, s^{n-1}\}$ of order n. Set $n = p \cdot n'$, where p is prime. Set $s^p = s'$. Then the group

$$H = \{I, s', s'^2, \ldots, s'^{n'-1}\}$$

is a subgroup of G of prime index p. It is self-conjugate, since

$$s^{-\beta} s'^{a} s^{\beta} = s^{-\beta} s^{ap} s^{\beta} = s^{ap} = s'^{a}$$

by § 13. Hence H may be taken as the second group of a series of composition of G. Proceeding with H as we did with G, we finally reach the conclusion:

The factors of composition of a cyclic group of order n are the prime factors of n each repeated as often as it occurs in n.

In view of the remark at the end of § 82, it now follows that *any Abelian equation of degree n can be reduced to a chain of Abelian equations whose degrees are the prime factors of n.*

We may now show by induction that every Abelian equation of prime degree p is solvable by radicals. We suppose solvable all Abelian equations of prime degrees less than a certain prime p. Among them are the Abelian equations of prime degrees to which can be reduced the Abelian equation of degree $p-1$, giving an imaginary pth root of unity (§ 87). The latter being therefore known, every Abelian equation of degree p is solvable by radicals (§ 83). Now an Abelian equation of degree 2 is solvable by radicals. Hence the induction is complete.

It follows now that an Abelian equation of any degree is solvable.

COROLLARY. If p is a prime number, all the pth roots of unity can be found by a finite number of applications of the operation *extraction of a single root of a known quantity*, the index of each radical being a prime divisor of $p-1$.

90. LEMMA. *If p be prime, and if A be a quantity lying in a domain R but not the pth power of a quantity in R, then $x^p - A$ is irreducible in R.*

For, if reducible in R, so that

$$x^p - A = \phi_1(x) \cdot \phi_2(x) \ldots,$$

the several factors are of the same degree only when each is of degree 1, the only divisor of p. In the latter case, the roots would all lie in R, contrary to assumption. Let then ϕ_1 be of higher degree than ϕ_2 and set

$$\phi_1(x)=(x-x_1')\ldots(x-x'_{n_1}),\quad \phi_2(x)=(x-x_1'')\ldots(x-x''_{n_2}),$$

so that $n_1-n_2>0$. The last coefficients in the products are

$$\pm x_1'x_2'\ldots x'_{n_1}=\pm\omega^{\sigma_1}x_1^{n_1},\quad \pm x_1''x_2''\ldots x''_{n_2}=\pm\omega^{\sigma_2}x_1^{n_2},$$

respectively, since the roots of $x^p-A=0$ are

$$(26)\qquad x_1,\quad \omega x_1,\quad \omega^2x_1,\quad \ldots,\quad \omega^{p-1}x_1,$$

ω being an imaginary pth root of unity. But the last coefficients, and their quotient $\pm\omega^\sigma x_1{}^m$, where $m=n_1-n_2>0$, lie in R. Since p and m are relatively prime, integers μ and ν exist for which

$$m\mu-p\nu=1.$$

$$\therefore\quad (\omega^\sigma x_1{}^m)^\mu=\omega^{\sigma\mu}x_1{}^{p\nu+1}=\omega^{\sigma\mu}A^\nu x_1=A^\nu x',$$

where x' is one of the roots (26). Hence $A_\nu x'$, and consequently x', lies in R. Then A equals the pth power of a quantity x' in R, contrary to assumption. Hence x^p-A must be irreducible.

91. THEOREM. *A binomial equation of prime degree p,*

$$x^p-A=0,$$

can be solved by means of a chain of Abelian equations of prime degree.

Let R be the given domain to which A belongs. Adjoin ω and denote by R' the enlarged domain. Then the roots (26) satisfy the relations

$$x_2=\omega x_1,\quad x_3=\omega x_2,\quad \ldots,\quad x_p=\omega x_{p-1},\quad x_1=\omega x_p,$$

of the type (21) of § 85, $\theta(x)$ being here the rational function ωx. The discussion in § 90 shows that x^p-A is either irreducible in the enlarged domain R' or else has *all* its roots in R'. In the former case, the group of $x^p-A=0$ for R' is a regular cyclic group (§ 86); in the latter case, the group for R' is the identity. But ω itself is determined by an Abelian equation (§ 87). Hence, in either case, $x^p-A=0$ is made to depend upon a chain of Abelian equations, whose degrees may be supposed to be prime (§ 89).

CHAPTER IX.

CRITERION FOR ALGEBRAIC SOLVABILITY.

92. We are now in a position to complete the theory of the algebraic solution of an arbitrarily given equation of degree n,

$$(1) \qquad f(x)=0.$$

A group property expressing a sufficient condition for the algebraic solvability of (1) was established in § 84. To show that this property expresses a necessary condition, we begin with a discussion of equation (1) under the hypothesis that it is solvable by radicals, namely (§ 50), that its roots $x_1, \ldots, x_n$ can be derived from the initially given quantities $R', R'', \ldots$ by addition, subtraction, multiplication, division, and extraction of a root of any index. These indices may evidently be assumed to be prime numbers. If $\xi, \eta, \ldots, \psi$ denote all the radicals which enter the expressions for all the roots $x_1, x_2, \ldots, x_n$, the solution may be exhibited by a chain of binomial equations of prime degree:

$$\xi^\lambda=L(R', R'', \ldots), \quad \eta^\mu=M(\xi, R', R'', \ldots), \quad \ldots,$$
$$\psi^\rho=P(\ldots, \eta, \xi, R', R'', \ldots),$$
$$x_i=R_i(\psi, \ldots, \eta, \xi, R', R'', \ldots) \qquad (i=1, \ldots, n),$$

$L, M, \ldots, P, R_i$ being rational functions with integral coefficients, in which some of the arguments $\xi, \eta, \ldots$ written may be wanting. By § 91, each of these binomial equations, and therefore also the complete chain, can be replaced by a chain of Abelian equations of prime degrees;

$\Phi(y;\ R', R'', \ldots)=0,$	Abelian for domain R;
$\Psi(z;\ y, R', R'', \ldots)=0,$	Abelian for (y, R);
. . . .	. . . .
$\theta(w;\ \ldots, z, y, R', R'', \ldots)=0,$	Abelian for $(\ldots, z, y, R)$;
$x_i=\Omega_i(w, \ldots, z, y, R', R'', \ldots)$	$(i=1, \ldots, n)$.

We begin by solving the first Abelian equation $\Phi(y)=0$ and adjoining one of its roots, say y, to the original domain R; the group G of (1) then reduces to a certain subgroup, say H, including the possibility $H=G$ (§ 74). Then we solve the second Abelian equation $\Psi(z)=0$ and adjoin one of its roots, say z, to the enlarged domain (y, R); the group H reduces to a certain subgroup, say J, including the possibility $J=H$. Proceeding in this way, until the last equation $\theta(w)=0$ has been solved and one of its roots, say w, has been adjoined, we finally reach the domain $(w, \ldots, z, y, R)$, with respect to which the group of (1) is the identity G_1, since all the roots x_i lie in that domain.

By every one of these successive adjunctions, either the group of equation (1) is not reduced at all or else the group is reduced to a self-conjugate subgroup of prime index. This theorem, due to Galois, is established as a corollary in the next section; its importance is better appreciated if we remark that each adjoined quantity is not supposed to be a rational function of the roots, in contrast with § 75, so that we shall be able to draw an important conclusion, due to Abel, concerning the nature of the irrationalities occurring in the expressions for the roots of a solvable equation (§ 94).

From this theorem of Galois, it follows that the different groups through which we pass in the process of successive adjunction of a root of each Abelian equation in the chain to which the given solvable equation was reduced must form a series of composition of the group G of the given equation having only prime numbers as factors of composition. Indeed, the series of groups beginning with G and ending with the identity G_1 are such that each is a self-conjugate subgroup of prime index under the preceding. Hence the sufficient condition (§ 84) for the algebraic solvability of a given equation is also a necessary condition, so that we obtain Galois' criterion for algebraic solvability:

In order that an equation be solvable by radicals, it is necessary and sufficient that its group have a series of composition in which the factors of composition are all prime numbers.

93. Theorem of Jordan,* as amplified and proved by Hölder: †

For a given domain R let the group G_1 of an equation $F_1(x)=0$ be reduced to G_1' by the adjunction of all the roots of a second equation $F_2(x)=0$, and let the group G_2 of the second equation be reduced to G_2' by the adjunction of all the roots of the first equation $F_1(x)=0$. Then G_1' and G_2' are self-conjugate subgroups of G_1 and G_2 respectively, and the quotient-groups G_1/G_1' and G_2/G_2' are simply isomorphic.

Let $\psi_1(\xi_1, \xi_2, \ldots, \xi_n)$ be a rational function, with coefficients in R, of the roots of the first equation which belongs to the subgroup G_1' of the group G_1 of the first equation (§ 70). By hypothesis, the adjunction of the roots $\eta_1, \eta_2, \ldots, \eta_m$ of the equation $F_2(x)=0$ reduces the group G_1 to G_1'. Hence ψ_1 lies in the enlarged domain, so that

$$(27) \qquad \psi_1(\xi_1, \xi_2, \ldots, \xi_n)=\phi_1(\eta_1, \eta_2, \ldots, \eta_m),$$

the coefficients of the rational function ϕ_1 being in R.

Let $\psi_1, \psi_2, \ldots, \psi_k$ denote all the numerically distinct values which ψ_1 can take under the substitutions (on $\xi_1, \ldots, \xi_n$) of G_1. Then G_1' is of index k under G_1 (§ 71). Let $\phi_1, \phi_2, \ldots, \phi_l$ denote all the numerically distinct values which ϕ_1 can take under the substitutions (on $\eta_1, \ldots, \eta_m$) of G_2. The k quantities ψ are the roots of an irreducible equation in R (§ 71); likewise for the l quantities ϕ. Since these two irreducible equations have a common root $\psi_1=\phi_1$, they are identical (§ 55, Cor. II). Hence $\psi_1, \ldots, \psi_k$ coincide in some order with $\phi_1, \ldots, \phi_l$; in particular, $k=l$.

If s_i is a substitution of G_1 which replaces ψ_1 by its conjugate ψ_i, then s_i transforms G_1', the group of ψ_1 by definition, into the group of ψ_i of the same order as G_1'. But ψ_i, being equal to a ϕ, lies in

---

* *Traité des substitutions*, pp. 269, 270.

† *Math. Annalen*, vol. 34.

the domain $R' \equiv (R;\ \eta_1,\ \ldots,\ \eta_m)$, and hence is unaltered by the substitutions of the group G_1' of the equation $F_1(x)=0$ for that domain R' (§ 61, property B). Hence the group of ψ_i contains all the substitutions of G_1'; being of the same order, the group of ψ_i is identical with G_1'. *Hence G_1' is self-conjugate under G_1.* The group of the irreducible equation satisfied by ψ_1 is therefore the quotient-group G_1/G_1' (§ 79).

Let H_2 be the subgroup of G_2 to which belongs $\phi_1(\eta_1, \eta_2, \ldots, \eta_m)$. Since ϕ_1 is a root of an irreducible equation in R of degree $l=k$, the group H_2 is of index k under G_2 (§ 71). By the adjunction of ϕ_1 (or, what amounts to the same thing in view of (27), by the adjunction of ψ_1), the group G_2 of equation $F_2(x)=0$ for R is reduced to H_2 (§ 75). If not merely $\psi_1(\xi_1, \ldots, \xi_n)$, but all the ξ's themselves be adjoined, the group G_2 reduces perhaps further to a subgroup of H_2. Hence G_2' is contained in H_2. We thus have the preliminary result: If the group of $F_1(x)=0$ reduces to a subgroup of index k on adjoining all the roots of $F_2(x)=0$, then the group of $F_2(x)=0$ reduces to a subgroup of index k_1, $k_1 \overline{\gtrless} k$, on adjoining all the roots of $F_1(x)=0$.

Interchanging F_1 and F_2 in the preceding statement we obtain the result: If the group of $F_2(x)=0$ reduces to a subgroup of index k_1 on adjoining all the roots of $F_1(x)=0$, then the group of $F_1(x)=0$ reduces to a subgroup of index k_2, $k_2 \overline{\gtrless} k_1$, on adjoining all the roots of $F_2(x)=0$. Since the hypothesis for the second statement is identical with the conclusion for the first statement, it follows that

$$k_2 = k, \quad k_1 \overline{\gtrless} k, \quad k_2 \overline{\gtrless} k_1,$$

so that $k_1=k$. Hence the group G_2' of the theorem is identical with the group H_2 of all the substitutions in G_2 which leave ϕ_1 unaltered. It follows that *G_2' is self-conjugate under G_2* (for the same reason that G_1' is self-conjugate under G_1). The irreducible equation in R satisfied by ϕ_1 has for its group the quotient-group G_2/G_2'.

But the two irreducible equations for R satisfied by ϕ_1 and ψ_1, respectively, were shown to be identical. Hence the groups

G_1/G_1' and G_2/G_2' differ only in the notations employed for the letters on which they operate, and hence are simply isomorphic.

COROLLARY. For the particular case in which the second equation is an Abelian equation of prime degree p, all of its roots are rational functions in R of any one root, so that by adjoining one we adjoin all its roots. *By the adjunction of any one root of an Abelian equation of prime degree p, the group of the given equation $F_1(x)=0$ either is not reduced at all or else is reduced to a self-conjugate subgroup of index p.*

94. If G_2 is simple and if the adjunction causes a reduction, then G_2 is reduced to the identity. Hence the group $G_2'=H_2$, to which belongs ϕ_1, is the identity. Hence the roots $\eta_1, \eta_2, \ldots, \eta_m$ of $F_2(x)=0$ are rational functions in R of ϕ_1 (§ 72) and therefore, in view of (27), of the roots $\xi_1, \ldots, \xi_n$ of $F_1(x)=0$.

If the group of an equation $F_1(x)=0$ for a domain R is reduced by the adjunction of all the roots of an equation $F_2(x)=0$ whose group for R is simple, then all the roots of $F_2(x)=0$ are rational functions in R of the roots of $F_1(x)=0$.

Since the group of a solvable equation $f(x)=0$ has a series of composition in which the factors of composition are all prime numbers, the equation can be replaced by a chain of resolvent equations each an Abelian equation of prime degree (end of § 82, § 85). The adjunction of a root of each resolvent reduces the group of the equation and the group of the resolvent is simple, being cyclic of prime order. Hence the roots of each Abelian resolvent equation are all rational functions of the roots of $f(x)=0$. But the radicals entering the solution of an Abelian equation of prime degree are rationally expressible in terms of its roots and an imaginary pth root of unity (§ 83),

$$\sqrt[p]{\theta_1}=x_0+\omega x_1+\omega^2 x_2+\ldots+\omega^{p-1}x_{p-1}, \ldots$$

and hence are rationally expressible in terms of the roots of $f(x)=0$ and pth roots of unity. We therefore state Abel's Theorem:

The solution of an algebraically solvable equation can always be performed by a chain of binomial equations of prime degrees whose *roots are rationally expressible in terms of the roots of the given equation and of certain roots of unity.*

The roots of an algebraically solvable equation can therefore be given a form such that all the radicals entering them are rationally expressible in terms of the roots of the equation and of certain roots of unity. This result was first shown empirically by Lagrange for the general quadratic, cubic, and quartic equations (see Chapter I).

The Theorem of Abel supplies the step needed to complete the proof of the impossibility of the algebraic solution of the general equation of degree $n>4$ (§ 48).

95. By way of illustrating Galois' theory, we proceed to give algebraic solutions of the general equations of the third and fourth degrees by chains of Abelian equations.

For the cubic $x^3-c_1x^2+c_2x-c_3=0$, let the domain of rationality be $R=(c_1, c_2, c_3)$. The group of the cubic for R is the symmetric group G_6 (§ 64). To the subgroup G_3 belongs

$$\Delta=(x_1-x_2)(x_2-x_3)(x_3-x_1).$$

In view of Ex. 3, page 4, Δ is a root of the equation

$$\Delta^2=c_1^2c_2^2+18c_1c_2c_3-4c_2^3-4c_1^3c_3-27c_3^2. \tag{28}$$

Its second root $-\Delta$ is rationally expressible in terms of the first root Δ, and (28) is irreducible since Δ is not in R for general c_1, c_2, c_3. Hence (28) is Abelian (§ 85). By adjoining Δ to R, the group reduces to G_3 (§ 75). Solve the Abelian equation $\omega^2+\omega+1=0$ (§ 87) and adjoin ω to the domain (Δ, R). To the enlarged domain $R'=(\omega, \Delta, c_1, c_2, c_3)$ belong the coefficients of the function

$$\psi_1=x_1+\omega x_2+\omega^2x_3.$$

By § 34, ψ_1^3 has a value lying in R', namely,

$$\psi_1^3=\tfrac{1}{2}[2c_1^3-9c_1c_2+27c_3-3(\omega-\omega^2)\Delta].$$

This binomial is an Abelian equation for the domain R' (§ 91). By the adjunction of ψ_1, the group of the cubic reduces to the identity. Hence x_1, x_2, x_3 lie in the domain $(\psi_1, \omega, \Delta, c_1, c_2, c_3)$. Thus, by § 34,

$$x_1=\tfrac{1}{3}\left(c_1+\psi_1+\frac{c_1^2-3c_2}{\psi_1}\right), \quad x_2=\tfrac{1}{3}\left(c_1+\omega^2\psi_1+\omega\frac{(c_1^2-3c_2)}{\psi_1}\right).$$

We may, however, solve the cubic without adjoining ω. In the domain (Δ, c_1, c_2, c_3), the cubic itself is an Abelian equation, since its group G_3 is cyclic (§ 85). By the adjunction of a root x_1 of this Abelian equation, the group reduces to the identity, so that x_2 and x_3 must lie in the domain $(x_1, \Delta, c_1, c_2, c_3)$. The explicit expressions for x_2 and x_3 are given by Serret, *Algèbre supérieure*, vol. 2, No. 511:

$$x_2=\frac{1}{2\Delta}\{(6c_2-2c_1^2)x_1^2+(9c_3-7c_1c_2+2c_1^3-\Delta)x_1+4c_2^2-c_1^2c_2-3c_1c_3+c_1\Delta\},$$

the value of x_3 being obtained by changing the sign of Δ throughout.

96. For the general quartic $x^4+ax^3+bx^2+cx+d=0$, the group for the domain $R=(a, b, c, d)$ is G_{24}. To the subgroup G_{12} belongs

$$\Delta=(x_1-x_2)(x_1-x_3)(x_1-x_4)(x_2-x_3)(x_2-x_4)(x_3-x_4).$$

Since Δ^2 is an integral function of a, b, c, d with rational coefficients (§ 42), we obtain Δ by solving an equation which is Abelian for R. After the adjunction of Δ, the group is G_{12}. To the *subgroup* G_4 *of* G_{12} belongs the function $y_1=x_1x_2+x_3x_4$. It satisfies the cubic resolvent equation (§ 4)

$$(16) \qquad y^3-by^2+(ac-4d)y-a^2d+4bd-c^2=0.$$

The group of this resolvent for the domain (Δ, a, b, c, d) is a cyclic group of order 3 (§ 79, Cor.), so that the resolvent is Abelian. By the adjunction of y_1, the group of the quartic reduces to G_4. To the subgroup G_2 of G_4 belongs the function $t=x_1+x_2-x_3-x_4$. It is determined by the Abelian equation (§ 5)

$$(29) \qquad t^2=a^2-4b+4y_1.$$

By the adjunction of t, the group reduces to G_2. To the identity subgroup G_1 of G_2 belongs x_1; it is a root of (17), § 4:

$$x^2+\tfrac{1}{2}(a-t)x+\tfrac{1}{2}y_1-(\tfrac{1}{2}ay_1-c)/t=0.$$

After the adjunction of a root x_1 of this Abelian equation, the group is the identity G_1. Hence (§ 72) all the roots lie in the domain $(x_1, t, y_1, \Delta, a, b, c, d)$. This is evident for x_2, since $x_1+x_2=-\frac{1}{2}(a-t)$. For x_3 and x_4, we have

$$x_3+x_4=x_1+x_2-t, \quad x_3-x_4=(y_2-y_3)\div(x_1-x_2),$$

while y_2 and y_3 are rationally expressible in terms of y_1, Δ, and the coefficients of (16), as shown at the end of § 95. In fact, $(y_1-y_2)(y_2-y_3)(y_1-y_3)$ has the value Δ by § 7.

97. Another method of solving the general quartic was given in § 42. For the domain $R=(\omega, a, b, c, d)$, where ω is an imaginary cube root of unity, the group is G_{24} (§ 64). After the adjunction of Δ, the group is G_{12}. To the self-conjugate subgroup G_4 belongs $\phi_1=y_1+\omega y_2+\omega^2 y_3$, where $y_1=x_1x_2+x_3x_4$, etc., so that ϕ_1 is a rational function of x_1, x_2, x_3, x_4, with coefficients in R. By § 42,

$$\phi_1{}^3=\tfrac{3}{2}(\omega-\omega^2)\Delta-216J,$$

so that ϕ_1 is determined by an equation which is Abelian for the domain $(\Delta, \omega, a, b, c, d)$. Then, by § 42, y_1, y_2, y_3 belong to the enlarged domain $(\phi_1, \Delta, \omega, a, b, c, d)$.

By the adjunction of t, a root of the binomial Abelian equation (29), the group reduces to G_2. By the adjunction* of both $i=\sqrt{-1}$ and $V=x_1-x_2+ix_3-ix_4$, which is a root of a binomial quadratic equation (§ 42), the group reduces to the identity G_1. The expressions for x_1, x_2, x_3, x_4 in terms of t, V, i, and a, are given by formula (41), in connection with (40), of § 37.

---

* Without adjoining i and V, we may determine $t_2=x_1+x_3-x_2-x_4$ from $t_2{}^2=a^2-4b+4y_2$. Then $t_3=x_1+x_4-x_2-x_3$ is known, since $t_1t_2t_3=4ab-8c-a^3$ by formula (39) of § 36, where $t_1=t$. Then

$$x_1=\tfrac{1}{4}(-a+t_1+t_2+t_3), \quad x_2=\tfrac{1}{4}(-a+t_1-t_2-t_3), \text{ etc.}$$

CHAPTER X.

METACYCLIC EQUATIONS; GALOISIAN EQUATIONS.

98. Analytic representation of substitutions. Given any substitution

$$s = \begin{pmatrix} x_0 & x_1 & x_2 & \dots & x_{n-1} \\ x_a & x_b & x_c & \dots & x_k \end{pmatrix},$$

so that $a, b, \dots, k$ form a permutation of $0, 1, \dots, n-1$, it is possible to construct a function $\phi(z)$ of one variable z such that

$$\phi(0) = a, \quad \phi(1) = b, \quad \phi(2) = c, \quad \dots, \quad \phi(n-1) = k.$$

Indeed, such a function is given by Lagrange's Interpolation-Formula,

$$\phi(z) = \frac{aF(z)}{zF'(0)} + \frac{bF(z)}{(z-1)F'(1)} + \dots + \frac{kF(z)}{(z-n+1)F'(n-1)},$$

where $F(z) \equiv z(z-1)(z-2)\dots(z-n+1)$ and $F'(z)$ is the derivative of $F(z)$. Then the substitution s is represented analytically as follows:

$$s = \begin{pmatrix} x_z \\ x_{\phi(z)} \end{pmatrix}.$$

We confine our attention to the case in which n is a prime number p, and agree to take $x_z = x_{z+p} = x_{z+2p} = \dots.$ Then (as in § 86) the circular substitution $t = (x_0\, x_1\, x_2 \dots x_{p-1})$ may be represented in the form

$$t = \begin{pmatrix} x_z \\ x_{z+1} \end{pmatrix}.$$

Let G be the largest group of substitutions on $x_0, x_1, \dots, x_{p-1}$

under which the cyclic group $H=\{I, t, t^2, \ldots, t^{p-1}\}$ is self-conjugate. The general substitutions g of G and h of H may be written

$$g=\begin{pmatrix} x_z \\ x_{\phi(z)} \end{pmatrix}, \quad h=\begin{pmatrix} x_z \\ x_{z+a} \end{pmatrix}=t^a.$$

By hypothesis, $g^{-1}tg$ belongs to H and hence is of the form t^a.

$$g^{-1}=\begin{pmatrix} x_{\phi(z)} \\ x_z \end{pmatrix}, \quad g^{-1}t=\begin{pmatrix} x_{\phi(z)} \\ x_{z+1} \end{pmatrix}, \quad g^{-1}tg=\begin{pmatrix} x_{\phi(z)} \\ x_{\phi(z+1)} \end{pmatrix}.$$

But t^a replaces $x_{\phi(z)}$ by $x_{\phi(z)+a}$. Hence must

$$x_{\phi(z+1)}=x_{\phi(z)+a}.$$

Taking in turn $z=0, 1, 2, \ldots$, and writing $\phi(0)=b$, we get

$$x_{\phi(1)}=x_{b+a}, \quad x_{\phi(2)}=x_{\phi(1)+a}=x_{b+2a}, \quad x_{\phi(3)}=x_{\phi(2)+a}=x_{b+2a}, \quad \ldots$$

By simple induction, we get $x_{\phi(z)}=x_{b+za}$ for any integer z. Hence

(30) $$g=\begin{pmatrix} x_z \\ x_{az+b} \end{pmatrix}.$$

Here a and $b\equiv\phi(0)$ are integers. Also a is not divisible by p, since $g^{-1}tg$ is not the identity. The distinct substitutions * g are obtained by taking the values

$$a=1, 2, \ldots, p-1; \quad b=0, 1, 2, \ldots, p-1.$$

The resulting $p(p-1)$ substitutions form a group called the **metacyclic group** of degree p. This follows from its origin or from

$$\begin{pmatrix} x_z \\ x_{az+b} \end{pmatrix}\begin{pmatrix} x_z \\ x_{\alpha z+\beta} \end{pmatrix}=\begin{pmatrix} x_z \\ x_{\alpha(az+b)+\beta} \end{pmatrix}\equiv\begin{pmatrix} x_z \\ x_{\alpha az+(\alpha b+\beta)} \end{pmatrix}.$$

REMARK. The only circular substitutions of period p in the metacyclic group are the powers of t. For $a=1$, (30) becomes t^b; for $a\neq 1$, (30) leaves one root unaltered, namely, that one whose index z makes $az+b$ and z differ by a multiple of p.

---

* Formula (30) does, indeed, define a substitution on $x_0, x_1, \ldots, x_{n-1}$,

$$\begin{pmatrix} x_0 & x_1 & x_2 & \ldots \\ x_b & x_{a+b} & x_{2a+b} & \ldots \end{pmatrix},$$

since $b, a+b, 2a+b, \ldots, (p-1)a+b$ give the remainders $0, 1, 2, \ldots, p-1$, in some order, when divided by p. In proof, the remainders are all different.

99. A metacyclic equation of degree p is one whose group G for a domain R is the metacyclic group of degree p. It is irreducible since G is transitive, its cyclic subgroup H being transitive. Again, all its roots are rational functions of two of the roots with coefficients in R. For, by the adjunction of two roots, say x_u and x_v, the group reduces to the identity. Indeed, if g leaves x_u and x_v unaltered, then

$$(au+b)-u, \quad (av+b)-v$$

are multiples of p, so that their difference $(a-1)(u-v)$ is a multiple of p, whence $a=1$, and therefore $b=0$. Hence the identity alone leaves x_u and x_v unaltered.

DEFINITION. For a domain R, an irreducible equation of prime degree whose roots are all rational functions of two of the roots is called a **Galoisian equation.**

Hence *a metacyclic equation is a Galoisian equation.*

100. Given, inversely, a Galoisian equation of prime degree p, we can readily determine its group G for a domain R. The equation being irreducible, its group is transitive, so that the order of G is divisible by p (§ 67). Hence G contains a cyclic subgroup H of order p (see foot-note to § 27). Let x_0 and x_1 denote the two roots in terms of which all the roots are supposed to be rationally expressible. Among the powers of any circular substitution of period p, there is one which replaces x_0 by x_1. Hence, by a suitable choice of notation for the remaining roots, we may assume that H contains the substitution

$$t=(x_0\, x_1\, x_2 \dots x_{p-1}).$$

To show that H is self-conjugate under G, it suffices to prove that any circular substitution, contained in G,

$$r=(x_{i_0}\, x_{i_1}\, x_{i_2} \dots x_{i_{p-1}})$$

is a power of t; for, the transform of t by any substitution of G will then belong to H (§ 40). Since every two adjacent letters in r are different, $i_{z+1}-i_z$ is never a multiple of p and hence, for at least two values μ and ν of z chosen from the series $0, 1, \ldots, p-1$, gives the same remainder when divided by p. Hence

$$x_{i_{\mu+1}-i_{\mu}}=x_{i_{\nu+1}-i_{\nu}}, \text{ say } =x_k.$$

Since r is a power of a circular substitution replacing x_0 by x_1, we may assume that $i_0=0$, $i_1=1$. The hypothesis then gives

$$x_{i_a}=\theta_a(x_{i_0},\ x_{i_1}) \qquad (a=0,\ 1,\ldots,\ p-1),$$

where θ_a is a rational function with coefficients in R. Applying to these rational relations the substitutions $r^{\mu}t^{-i_{\mu}}$ and $r^{\nu}t^{-i_{\nu}}$ of the group G, we obtain, by § 62,

$$x_{i_{a+\mu}-i_{\mu}}=\theta_a(x_0, x_k),\quad x_{i_{a+\nu}-i_{\nu}}=\theta_a(x_0,\ x_k).$$

Hence the subscripts in the left members are equal, so that

$$i_{a+\mu}-i_{a+\nu}=i_{\mu}-i_{\nu}=c \qquad (a=0,\ 1,\ldots,\ p-1),$$

omitting multiples of p. Hence every subscript in r exceeds by c the $(\mu-\nu)$th subscript preceding it. Hence r is a power of t.

Since G has a self-conjugate cyclic subgroup H, it is contained in the metacyclic group of degree p (§ 98).

The group of a Galoisian equation of prime degree p is a subgroup of the metacyclic group of degree p.

101. A metacyclic equation is readily solved by means of a chain of two Abelian equations. Let $\psi=R(x_0,\ x_1,\ldots,\ x_{p-1})$ belong to the subgroup H of G. Then

$$\psi_1=\psi,\ \psi_2=R(x_0, x_2, x_4, \ldots, x_{2p-2}), \ldots, \psi_{p-1}=R(x_0, x_{p-1}, x_{2p-2}, \ldots, x_{(p-1)^2})$$

are the $p-1$ values of ψ under G. But ψ_i is changed into ψ_{ki} by the substitution which replaces x_z by x_{kz}. It follows that the $p-1$ values of ψ are permuted cyclically under the $p(p-1)$ substitutions of G. The group of the resolvent equation

$$(w-\psi_1)(w-\psi_2)\ldots(w-\psi_{p-1})=0$$

is therefore a cyclic group of order $p-1$, so that the resolvent is an Abelian equation (§ 85). By the adjunction of ψ, the group of the original equation reduces to the cyclic group H, so that it is Abelian in the enlarged domain.

The method applies also to any Galoisian equation. Its group G is a subgroup of the metacyclic group and yet contains H as a subgroup. The order of G is therefore pd, where d is a divisor of $p-1$. The two auxiliary Abelian equations are then of degrees d and p respectively. Applying § 89, we have the results:

A Galoisian equation can be solved by a chain of Abelian equations of prime degree and hence is solvable by radicals.

EXAMPLE 1. Let A be a quantity lying in a given domain R but not the pth power of a quantity in R. Then the equation

$$x^p - A = 0$$

is irreducible in R (§ 90). Its roots are

$$x_0, \quad x_1 = \omega x_0, \quad x_2 = \omega^2 x_0, \quad \dots, \quad x_{p-1} = \omega^{p-1} x_0.$$

All the roots are rationally expressible in terms of x_0 and x_1:

$$x_i = \left(\frac{x_1}{x_0}\right)^i x_0 \qquad (i = 0, 1, \dots, p-1).$$

The equation is therefore a Galoisian equation. For the function ψ belonging to the cyclic subgroup H we may take

$$\frac{x_1}{x_0} = \frac{x_2}{x_1} = \dots = \frac{x_0}{x_{p-1}} = \omega.$$

The resolvent equation $\omega^{p-1} + \dots + \omega + 1 = 0$ is indeed Abelian (§ 87). After the adjunction of ω, $x^p - A = 0$ becomes an Abelian equation (§ 91).

EXAMPLE 2. To solve the quintic equation *

$$(e) \qquad y^5 + py^3 + \tfrac{1}{5}p^2 y + r = 0,$$

set $y = z - \frac{p}{5z}$. Then (compare the solution of the cubic, § 2)

$$z^5 - \frac{p^5}{5^5 z^5} + r = 0.$$

$$\therefore\ z^5 = -\frac{r}{2} + \sqrt{Q}, \quad Q \equiv \frac{r^2}{4} + \left(\frac{p}{5}\right)^5.$$

If ε is an imaginary fifth root of unity, the roots of (e) are

$$y_1 = A + B, \quad y_2 = \varepsilon A + \varepsilon^4 B, \quad y_3 = \varepsilon^2 A + \varepsilon^3 B, \quad y_4 = \varepsilon^3 A + \varepsilon^2 B, \quad y_5 = \varepsilon^4 A + \varepsilon B,$$

where

$$A = \sqrt[5]{-\frac{r}{2} + \sqrt{Q}}, \quad B = \sqrt[5]{-\frac{r}{2} - \sqrt{Q}}.$$

* Compare Dickson's *College Algebra*, pages 189 and 193.

Evidently A and B may be expressed as linear functions of y_1 and y_2. Hence y_3, y_4, y_5 are rational functions of y_1 and y_2 with coefficients in the domain $R=(\varepsilon, p, r)$. For general p and r, equation (e) is irreducible in R, since no one of its roots lies in R and since it has no quadratic factor in R (as may be shown from the form of the roots). Hence (e) is a Galoisian equation.

102. LEMMA. *If L is a self-conjugate subgroup of K of prime index ν and if k is any substitution of K not contained in L, then k^ν, and no lower power of k, belongs to L, and the period of k is divisible by ν.*

By the Corollary of § 79, the quotient-group K/L is a cyclic group

$$\{I, \gamma, \gamma^2, \ldots, \gamma^{\nu-1}\}.$$

Hence to k corresponds a power of γ, say γ^κ, where κ is not divisible by ν. Then to k^ν corresponds $(\gamma^\kappa)^\nu=I$, so that k^ν belongs to L. If $0<m<\nu$, k^m does not belong to L, since $(\gamma^\kappa)^m=I$ requires that κm be divisible by the prime number ν.

Let the period μ of k be written in the form

$$\mu=q\nu+\tau \qquad (0\leqq\tau<\nu).$$

Since $k^\nu=h$, a substitution of L, we get $I=k^\mu=h^q k^\tau$. Hence $k^\tau=h^{-q}$, so that $\tau=0$, in view of the earlier result concerning powers of k. Hence μ is divisible by ν.

103. THEOREM (Galois). *Every irreducible equation of prime degree p which is solvable by radicals is a Galoisian equation.*

Let G be the group of the equation for a domain R and let

$$(31) \qquad G, H, \ldots, J, K, L, \ldots, G_1$$

be a series of composition of G. Since the equation is solvable by radicals, the factors of composition are all prime numbers (§ 92). Since the equation is irreducible in R, G is transitive (§ 68), so that its order is divisible by p (§ 67). Hence (foot-note to § 27), G contains a circular substitution of period p, say $t=(x_0\, x_1 \ldots x_{p-1})$. Let K denote the last group in the series (31) which contains t. Then the group L, immediately following K, and of prime index ν under K, does not contain t. Since $t^p=I$ belongs to L, while no lower power of t belongs to L, it follows from § 102 that $\nu=p$.

To show that L is the identity G_1, suppose that L contains a substitution s replacing x_α by a different letter x_β. Then $u=st^{\alpha-\beta}$ leaves x_α unaltered and belongs to K. Since $\alpha-\beta$ is not divisible by p and since t does not belong to L, it follows that u does not belong to L. By the Lemma of § 102, the period of u is divisible by $\nu=p$. This is impossible since u is a substitution on p letters, one of which remains unaltered.

Since $L=G_1$ and the index of L under K is p, the group K is the cyclic group of order p formed by the powers of t. Since the group J immediately preceding K in the series (31) contains the cyclic group K as a self-conjugate subgroup, J is contained in the metacyclic group of degree p (§ 98). By the remark at the end of § 98, J contains no circular substitutions of period p other than the powers of t. If J' be the group immediately preceding J in the series (31), so that J is self-conjugate under J', the transform of t by any substitution of J' belongs to J and is a circular substitution of period p, and therefore is a power of t. Hence the cyclic group K is self-conjugate under J', as well as under J. Hence J' is contained in the metacyclic group (§ 98). Proceeding in this way until we reach the group G, we find that G is contained in the metacyclic group. The theorem therefore follows from § 101.

CHAPTER XI.

AN ACCOUNT OF MORE TECHNICAL RESULTS.

104. Second definition of the group Γ of § 77. To show that Γ is completely defined by the given groups G and H and is entirely independent of the function ψ used in defining it, we define a group Γ_1 independently of functions belonging to H and prove that $\Gamma_1 = \Gamma$.

Consider a rectangular array of the substitutions of G with those of the subgroup H in the first row:

$$(32) \qquad \begin{array}{r|llll} r_1 & g_1 = I & h_2 & \dots & h_t \\ r_2 & g_2 & h_2 g_2 & \dots & h_t g_2 \\ \dots & \cdot & \cdot & \cdot & \cdot \\ r_\nu & g_\nu & h_2 g_\nu & \dots & h_t g_\nu \end{array}$$

where r_j denotes the jth row of the array. Let g be any substitution of G. Since $g_1 g, \dots, g_\nu g$ lie in the array (32), we may write

$$(33) \qquad g_1 g = h_{\alpha'} g_\alpha, \quad g_2 g = h_{\beta'} g_\beta, \quad \dots, \quad g_\nu g = h_{\kappa'} g_\kappa.$$

Hence the products of the substitutions in the array (32) by g on the right-hand may be written (retaining the same order):

$$(34) \qquad \begin{array}{r|llll} r_\alpha & h_{\alpha'} g_\alpha & (h_2 h_{\alpha'}) g_\alpha & \dots & (h_t h_{\alpha'}) g_\alpha \\ r_\beta & h_{\beta'} g_\beta & (h_2 h_{\beta'}) g_\beta & \dots & (h_t h_{\beta'}) g_\beta \\ \dots & \cdot & \cdot & \cdot & \cdot \\ r_\kappa & h_{\kappa'} g_\kappa & (h_2 h_{\kappa'}) g_\kappa & \dots & (h_t h_{\kappa'}) g_\kappa \end{array}$$

Now $h_{\alpha'}, h_2 h_{\alpha'}, \dots, h_t h_{\alpha'}$ form a permutation of $h_1 = I, h_2, \dots, h_t$. Hence the substitutions in the first row of (34) are identical, apart from their order, with those of the αth row of (32). Similarly for the other rows. Hence the multiplication of (32) on the right by g gives rise to the following permutation of the *rows:*

$$\gamma=\begin{pmatrix} r_1 & r_2 & \ldots & r_\nu \\ r_\alpha & r_\beta & \ldots & r_\kappa \end{pmatrix}.$$

To identify the group Γ_1 of these substitutions γ with the group Γ given by the earlier definition, we note that to g corresponds, under the earlier definition,

$$\begin{pmatrix} \psi_{g_1} & \psi_{g_2} & \ldots & \psi_{g_\nu} \\ \psi_{g_1 g} & \psi_{g_2 g} & \ldots & \psi_{g_\nu g} \end{pmatrix}=\begin{pmatrix} \psi_{g_1} & \psi_{g_2} & \ldots & \psi_{g_\nu} \\ \psi_{g_\alpha} & \psi_{g_\beta} & \ldots & \psi_{g_\kappa} \end{pmatrix},$$

since, by (33), $\psi_{g_1 g}=\psi_{h_\alpha, g_\alpha}=\psi_{g_\alpha}$, etc. But this substitution differs from γ only in notation. Hence $\Gamma_1=\Gamma$.

EXAMPLE 1. Let G be the cyclic group $\{I, c, c^2, c^3, c^4, c^5\}$, where $c^6=I$, and let H be the subgroup $\{I, c^3\}$. The array is

$$\begin{array}{c|cc} r_1 & I & c^3 \\ r_2 & c & c^4 \\ r_3 & c^2 & c^5 \end{array}$$

To c corresponds $(r_1r_2r_3)$. Hence $\Gamma=\{I, (r_1r_2r_3), (r_1r_3r_2)\}$.

EXAMPLE 2. Let G be the alternating group $G_{12}^{(4)}$ and let H be the commutative subgroup G_4 (§ 21, Ex. *f*). The rectangular array for G is given in § 77, Ex. 2. Multiplying its substitutions on the right by $(x_1x_2)(x_3x_4)$, we obtain the array

$$\begin{array}{llll} (x_1x_2)(x_3x_4), & I, & (x_1x_4)(x_2x_3), & (x_1x_3)(x_2x_4) \\ (x_1x_2x_4), & (x_1x_4x_3), & (x_1x_3x_2), & (x_2x_3x_4) \\ (x_1x_2x_3), & (x_1x_3x_4), & (x_2x_4x_3), & (x_1x_4x_2) \end{array}$$

Hence each row as a whole remains unaltered, so that to $(x_1x_2)(x_3x_4)$ corresponds the identity. A like result follows for $(x_1x_3)(x_2x_4)$ and for the product $(x_1x_4)(x_2x_3)$ of the two. But $(x_2x_3x_4)$ applied as a right-hand multiplier gives rise to the permutation $(r_1r_2r_3)$ of the rows, as follows immediately from the formation of the rectangular array by means of the right-hand multipliers $(x_2x_3x_4)$ and $(x_2x_3x_4)^2$. Hence $\Gamma=\{I, (r_1r_2r_3), (r_1r_3r_2)\}$.

105. Constancy of the factors of composition. By the criterion of § 92, an equation is solvable by radicals if, and only if, the group G of the equation has a series of composition in which the factors of composition are all prime numbers. In applying the criterion, it might be necessary to investigate all the series of compositions of G to decide whether or not there is one series with the factors of composition all prime. The practical value of the criterion is greatly enhanced by the theorem of C. Jordan:*

If a group has two different series of composition, the factors of composition for one series are the same, apart from their order, as the factors of composition for the other series.

EXAMPLE 1. Let G_8, G_4, H_4 be defined as in § 21; G_2, G'_2, G''_2 as in Example 3 of § 65; and let
$C_4=\{I,\ (x_1x_3x_2x_4),\ (x_1x_2)(x_3x_4),\ (x_1x_4x_2x_3)\}$, $H_2=\{I,\ (x_1x_2)\}$, $H'_2=\{I,\ (x_3x_4)\}$.
Then G_8 has the following series of compositions:

$$G_8, G_4, G_2, G_1;\quad G_8, G_4, G'_2, G_1;\quad G_8, G_4, G''_2, G_1;$$
$$G_8, C_4, G_2, G_1;\quad G_8, H_4, G_2, G_1;\quad G_8, H_4, H_2, G_1;\quad G_8, H_4, H'_2, G_1.$$

In each case the factors of composition are 2, 2, 2.

EXAMPLE 2. Let C_{12} be the cyclic group formed by the powers of the circular substitution $a=(x_1x_2x_3\ldots x_{12})$. Its subgroups are

$$C_6=\{I, a^2, a^4, a^6, a^8, a^{10}\},\qquad C_4=\{I, a^3, a^6, a^9\},$$
$$C_3=\{I, a^4, a^8\},\qquad C_2=\{I, a^6\},\quad C_1=\{I\}.$$

The only series of composition of C_{12} are the following: †

$$C_{12}, C_6, C_3, C_1;\quad C_{12}, C_6, C_2, C_1;\quad C_{12}, C_4, C_2, C_1.$$

The factors of composition are respectively 2, 2, 3; 2, 3, 2; 3, 2, 2.

106. Constancy of the factor-groups. In a series of composition of G,

$$G,\ G',\ G'',\ldots,\ G_1,$$

each group is a maximal self-conjugate subgroup of the preceding group (§ 43). The succession of quotient-groups

$$G/G',\ G'/G'',\ G''/G''',\ \ldots$$

forms a series of **factor-groups** of G. Each factor-group is simple (§ 80). The theorem of Jordan on the constancy of the numerical

---

* *Traité des substitutions*, pp. 42–48. For a shorter proof, see Netto-Cole, *Theory of Substitutions*, pp. 97–100.

† Every subgroup is self-conjugate since $a^{-i}a^ja^i=a^j$ (§ 13).

factors of composition is included in the following theorem of Hölder:*

For two series of composition of a group, the factor-groups of one series are identical, apart from their order, with the factor-groups of the other series.

Thus, in Example 1 of § 105, the factor-groups are all cyclic groups of order 2. In Example 2, the factor-groups for the respective series are

$$K_2, K_2, K_3; \quad K_2, K_3, K_2; \quad K_3, K_2, K_2,$$

where K_2 and K_3 are cyclic groups of orders 2 and 3 respectively. That C_6/C_2 is the cyclic group K_3 follows from § 104, Ex. 1, by setting $a^2=c$. That C_{12}/C_4 is K_3 follows readily from § 104.

107. Hölder's investigation† on the reduction of an arbitrary equation to a chain of auxiliary equations is one of the most important of the recent contributions to Galois' theory. The earlier restriction to *algebraically* solvable equations is now removed. As shown in § 82, the solution of a given equation can be reduced to the solution of a chain of simple regular equations by employing rational functions of the roots of the given equation. The groups of the auxiliary equations are the simple factor-groups G of the given equation. Can any one of these simple groups be avoided by employing *accessory irrationalities*, namely, quantities not rational functions of the roots of the given equation? That this question is to be answered in the negative is shown by Hölder's result that the factor-groups of G must occur among the groups of the auxiliary simple equations however the latter be chosen. Any auxiliary compound may first be replaced by a chain of equivalent simple equations. The number of factor-groups of G therefore gives the minimum number of necessary auxiliary simple equations. If this minimum number is not exceeded, then Hölder's theorem states that all the roots of all the auxiliary equations are

* Hölder, *Math. Ann.*, vol. 34, p. 37; Burnside, *The Theory of Groups*, p. 118; Pierpont, *Galois' Theory of Algebraic Equations*, *Annals of Math.*, 1900, p. 51.

† *Mathematische Annalen*, vol. 34, p. 26; Pierpont, *l. c.*, p. 52.

rational functions of the roots of the given equation and the quantities in the given domain of rationality.

Hölder's proof of these results, depending of course upon the constancy of the factor-groups of *G*, is based upon the fundamental theorem of § 93.

The special importance thus attached to simple groups has led to numerous investigations of them. Several infinite systems of simple groups have been found and a table of the known simple groups of composite orders less than one million has been prepared.*

For full references and for further developments of Galois' theory, the reader may consult *Encyklopädie der Mathematischen Wissenschaften*, I, pp. 480–520.

---

* Dickson, *Linear Groups*, pp. 307–310, Leipzig, 1901.

APPENDIX.

RELATIONS BETWEEN THE ROOTS AND COEFFICIENTS OF AN EQUATION.

Let $x_1, x_2, \ldots, x_n$ denote the roots of an equation $f(x)=0$ in which the coefficient of x^n has been made unity by division. Then

$$f(x) \equiv (x-x_1)(x-x_2)\ldots(x-x_n),$$

as shown in elementary algebra by means of the factor theorem. Writing $f(x)$ in full, and expanding the second member, we get

$$x^n - c_1x^{n-1} + c_2x^{n-2} - \ldots + (-1)^n c_n \equiv x^n - (x_1+x_2+\ldots+x_n)x^{n-1} + (x_1x_2+x_1x_3+x_2x_3+\ldots+x_{n-1}x_n)x^{n-2} - \ldots + (-1)^n x_1x_2\ldots x_n.$$

Equating coefficients of like powers of x, we get

(*i*) $x_1+x_2+\ldots+x_n=c_1,\ x_1x_2+\ldots+x_{n-1}x_n=c_2, \ldots,\ x_1\ldots x_n=c_n.$

These combinations of $x_1, \ldots, x_n$ are called the **elementary symmetric functions** of the roots. Compare Exs. 5 and 6 of page 4.

FUNDAMENTAL THEOREM ON SYMMETRIC FUNCTIONS.*

Any integral symmetric function of $x_1, x_2, \ldots, x_n$ can be expressed in one and only one way as an integral function of the elementary symmetric functions $c_1, c_2, \ldots, c_n$.

A term $x_1^{m_1}x_2^{m_2}x_3^{m_3}\ldots$ is called **higher** than $x_1^{n_1}x_2^{n_2}x_3^{n_3}\ldots$ if the first one of the differences $m_1-n_1, m_2-n_2, m_3-n_3, \ldots$, which

* The proof is that by Gauss, *Gesammelte Werke*, III, pp. 37, 38.

does not vanish, is *positive*. Then $c_1, c_2, c_3, \ldots, c_i$ have for their highest terms $x_1, x_1x_2, x_1x_2x_3, \ldots, x_1x_2\ldots x_i$, respectively. In general, the function $c_1^{\alpha}c_2^{\beta}c_3^{\gamma}\ldots$ has for its highest term

$$x_1^{\alpha+\beta+\gamma+\cdots}\, x_2^{\beta+\gamma+\cdots}\, x_3^{\gamma+\cdots}\ldots$$

Hence it has the same highest term as $c_1^{\alpha'}c_2^{\beta'}c_3^{\gamma'}\ldots$ if, and only if,

$$\alpha+\beta+\gamma+\ldots=\alpha'+\beta'+\gamma'+\ldots,\ \beta+\gamma+\ldots=\beta'+\gamma'+\ldots,\ \gamma+\ldots=\gamma'+\ldots,$$

which require that $\alpha=\alpha'$, $\beta=\beta'$, $\gamma=\gamma'$, ...

Let S be a given symmetric function. Let its highest term be

$$h\equiv a\, x_1^{\alpha}\, x_2^{\beta}\, x_3^{\gamma}\, x_4^{\delta}\ldots x_n^{\nu}\quad\ldots(\alpha\geqq\beta\geqq\gamma\geqq\delta\ldots\geqq\nu).$$

We build the symmetric function

$$\sigma\equiv a\, c_1^{\alpha-\beta}\, c_2^{\beta-\gamma}\, c_3^{\gamma-\delta}\ldots c_n^{\nu}.$$

In its expansion in terms of $x_1, \ldots, x_n$ by means of formulæ (i), its terms are all of the same degree and the highest term is evidently h. The difference

$$S_1\equiv S-\sigma$$

is a symmetric function simpler than S, since the highest term h has been cancelled. Let the highest term of S_1 be

$$h_1\equiv a_1\, x_1^{\alpha_1}\, x_2^{\beta_1}\, x_3^{\gamma_1}\, x_4^{\delta_1}\ldots$$

A symmetric function with a still lower highest term is given by

$$S_2\equiv S_1-a_1\, c_1^{\alpha_1-\beta_1}\, c_2^{\beta_1-\gamma_1}\, c_3^{\gamma_1-\delta_1}\ldots$$

Since the degrees of S_1 and S_2 are not greater than the degree of S, and since there is only a finite number of terms $x_1^{m_1}x_2^{m_2}x_3^{m_3}\ldots$ of a given degree which are lower than the term h, we must ultimately obtain, by a repetition of the process, the symmetric function 0:

$$0\equiv S_k-a_k\, c_1^{\alpha_k-\beta_k}\, c_2^{\beta_k-\gamma_k}\, c_3^{\gamma_k-\delta_k}\ldots$$

We therefore reach the desired result

$$S=a_1\, c_1^{\alpha-\beta}\, c_2^{\beta-\gamma}\ldots+a_2\, c_1^{\alpha_1-\beta_1}c_2^{\beta_1-\gamma_1}\ldots+\ldots+a_kc_1^{\alpha_k-\beta_k}c_2^{\beta_k-\gamma_k}\ldots$$

To show that the expression of a symmetric function S in terms of $c_1, \ldots, c_n$ is unique, suppose that S can be reduced to both $\phi(c_1, c_2, \ldots, c_n)$ and $\psi(c_1, c_2, \ldots, c_n)$, where ϕ and ψ are different integral functions of $c_1, \ldots, c_n$. Then $\phi-\psi$, considered as a function of $c_1, \ldots, c_n$, is not identically zero. After collecting like terms in $\phi-\psi$, let $bc_1^{\alpha}c_2^{\beta}c_3^{\gamma}\ldots$ be a term with $b\neq 0$. When expressed in $x_1, \ldots, x_n$, it has for its highest term

$$b\, x_1^{\alpha+\beta+\gamma+\cdots} x_2^{\beta+\gamma+\cdots} x_3^{\gamma+\cdots}\ldots$$

As shown above, a different term $b'c_1^{\alpha'}c_2^{\beta'}c_3^{\gamma'}\ldots$ has a different highest term. Hence of these highest terms one must be higher than the others. Since the coefficient of this term is not zero, the function $\phi-\psi$ cannot be identically zero in $x_1, \ldots, x_n$. This contradicts the assumption that $S\equiv\phi$, $S\equiv\psi$, for all values of $x_1, \ldots, x_n$.

COROLLARY. *Any integral symmetric function of $x_1, \ldots, x_n$ with integral coefficients can be expressed as an integral function of $c_1, \ldots, c_n$ with integral coefficients.*

Examples showing the practical value of the process for the computation of symmetric functions are given in Serret, *Algèbre supérieure,* fourth or fifth edition, vol. 1, pp. 389–395.

ON THE GENERAL EQUATION.

Let the coefficients $c_1, c_2, \ldots, c_n$ be indeterminate quantities. The roots $x_1, x_2, \ldots, x_n$ are functions of $c_1, \ldots, c_n$; the notation $x_1, \ldots, x_n$ is definite for each set of values of $c_1, \ldots, c_n$. We proceed to prove the theorem:*

If a rational, integral function of $x_1, \ldots, x_n$ with constant coefficients equals zero, it is identically zero.

Let $\psi[x_1, \ldots, x_n]=0$. Let $\xi_1, \ldots, \xi_n$ denote indeterminates and $\sigma_1, \ldots, \sigma_n$ their elementary symmetric functions $\xi_1+\ldots+\xi_n$, $\ldots, \xi_1\cdot\xi_2\ldots\xi_n$. Then

* This proof by Moore is more explicit than that by Weber, *Algebra,* II (1900), § 566.

$$\Pi\psi[\xi_{s_1}, \ldots, \xi_{s_n}] = \Psi[\sigma_1, \ldots, \sigma_n],$$

the product extending over the $n!$ permutations $s_1, \ldots, s_n$ of $1, \ldots, n$, and Ψ denoting a rational, integral function. Hence

$$\Pi\psi[x_{s_1}, \ldots, x_{s_n}] = \Psi[c_1, \ldots, c_n] = 0,$$

since one factor $\psi[x_1, \ldots, x_n]$ is zero. Since $c_1, \ldots, c_n$ are indeterminates, $\Psi[c_1, \ldots, c_n]$ must be identically zero, i.e., formally in $c_1, \ldots, c_n$. Consider $c_1, \ldots, c_n$ to be functions of new indeterminates $y_1, \ldots, y_n$. Then

$$\Psi[c_1(y_1, \ldots, y_n), \ldots, c_n(y_1, \ldots, y_n)] \equiv 0$$

formally in $y_1, \ldots, y_n$. Hence, by a change of notation,

$$\Psi[\sigma_1(\xi_1, \ldots, \xi_n), \ldots, \sigma_n(\xi_1, \ldots, \xi_n)] \equiv 0$$

formally in $\xi_1, \ldots, \xi_n$. Hence, for some factor,

$$\psi[\xi_{s_1}, \ldots, \xi_{s_n}] \equiv 0$$

formally in $\xi_1, \ldots, \xi_n$. As a mere change of notation,

$$\psi[\xi_1, \ldots, \xi_n] \equiv 0.$$

As an application, we may make a determination of the group of the general equation more in the spirit of the theory of Galois than that of § 64. If, in the domain $R = (c_1, \ldots, c_n)$, a rational function $\phi(x_1, \ldots, x_n)$ with coefficients in R has a value lying in R, there results a relation

$$\psi[x_1, \ldots, x_n] = 0,$$

upon replacing $c_1, \ldots, c_n$ by the elementary symmetric functions of $x_1, \ldots, x_n$. By the theorem above, $\psi[x_{s_1}, \ldots, x_{s_n}] = 0$, so that

$$\phi(x_{s_1}, \ldots, x_{s_n}) = \phi(x_1, \ldots, x_n).$$

INDEX.

(The numbers refer to pages.)