SOME NEW ASPECTS OF THE GALOIS THEORY

25

by

Anna Christine McBride, A.B., B.S.

SUBMITTED IN PARTIAL FULFILLMENT OF THE
REQUIREMENTS FOR THE DEGREE OF
MASTER OF ARTS
in the

GRADUATE SCHOOL

of the

UNIVERSITY OF MISSOURI

1913

Contents.

Chapter I.

An Elementary Consideration of Quadratic and Cubic Equations from the Group Standpoint.

Chapter II.

A More Detailed Study of the Processes Involved in the Solution of the Cubic Equation.

Chapter III.

The Plan of Solution for Quadratic and Cubic Equations Extended to Equations of Higher Degree.

Chapter IV.

The Group of an Equation.

Chapter V.

Reducibility and Irreducibility.

Chapter VI.

The Solution of Equations from the Standpoint of the Galois Theory.

Bibliography.

Dickson, L. E; *Introduction to the Theory of Algebraic Equations.*
John Wiley and Sons, London, 1903.

Bolza, Oskar: *On the Theory of Substitution - Groups and its Applications to Algebraic Equations.*
American Journal of Mathematics, Vol. 13, p. 59. 1891.

Pierpont, James: *Galois' Theory of Algebraic Equations*
Annals of Mathematics. Ser. 2.
Vol. 1. p. 113. 1899-1900
Vol. 2. p. 22. 1900-1901

Cajori, Florian: *An Introduction to the Modern Theory of Equations.*
Macmillan Company, London, 1904.

Netto, Eugen: *The Theory of Substitutions* (Translated by F. N. Cole).
The Inland Press, Ann Arbor, Michigan. 1892.

Bôcher, Maxime: *Introduction to Higher Algebra.*
Macmillan Company, New York, 1907.

Netto, Eugen: *Vorlesungen über Algebra.* Erster Band
Druck und Verlag von B. G. Teubner, Leipzig, 1896.

Burnside, W.: *Theory of Groups of Finite Order.*
C. F. Clay and Sons at the Cambridge University Press, 1897.

Introduction.

Realizing that the Galois theory of algebraic equations as commonly presented seems artificial, abstract, and intricate, we have been led in the following paper to attempt to present in a clear, tangible fashion the general, fundamental principles involved in the algebraic solution of equations. In carrying out this aim we have found it necessary to generalize certain methods of procedure still more than is done in the extant treatments of this subject, to formulate some of the theorems differently, and most of all to define the Galois group of an equation from an entirely new point of view.

In Chapter I we consider in a very elementary manner the solution of quadratic and cubic equations from the group standpoint. From this elementary discussion it is hoped that the student will see that even the very simple and familiar processses which he perhaps thought mechanical or trick processes are but parts of a general scheme. In Chapter II we study more in detail the processes involved in the solution of the cubic equation, introducing the general theory as needed. Having found the conditions under which the various processes can actually be performed, we attempt in Chapter III to extend the plan of solution for quadratic and cubic equations to equations of higher degree.

After the student has a general picture of the solution of an equation from the group standpoint, we

introduce in Chapter IV the idea of "the" group of an equation. As mentioned above, we discard the ordinary definition of the Galois group of an equation, and formulate a definition which we believe to be more convenient and tangible. It is to be observed that the finding of the group of an equation according to our definition does not involve knowledge of the roots of the equation. We are able to prove that the group of an equation according to our definition is identical with the group according to the customary definition; and, furthermore, from our definition we are able to prove all the fundamental theorems of the general theory together with other new theorems which become fundamental under our definition. After considering in Chapter V the question of the reducibility of an equation, a question of prime importance for our method, we present in Chapter VI the solution of equations from the standpoint of the Galois theory.

CHAPTER I.

An Elementary Consideration of Quadratic and Cubic Equations from the Group Standpoint.

1. **The Quadratic Equation.** The general quadratic equation can be written in the form

$$x^2 - c_1 x + c_2 = 0. \qquad \text{I.}$$

since the coefficient of x^2 can always be reduced to unity by the proper division.

Let us designate the roots of equation I by x_1 and x_2. Knowing that the coefficients of equation I can be expressed as rational, symmetric* functions of the roots (namely $c_1 = x_1 + x_2$ and $c_2 = x_1 x_2$),** we are able to solve for x_1 and x_2 as follows:

Take the rational, non-symmetric functions

$$v_1 = x_1 - x_2 \quad \text{and} \quad v_2 = x_2 - x_1.$$

These functions are the roots of the equation

$$(v - v_1)(v - v_2) = 0. \qquad \text{II.}$$

Expanding, $v^2 - (v_1 + v_2)\, v + v_1 v_2 = 0.$

Since $v_2 = - v_1$, equation II becomes

$$v^2 - v_1^2 = 0.$$

* If a function of two or more quantities remains unaltered when any two of the quantities are interchanged, it is called a symmetric function.

** For the relation between the roots and coefficients of an equation see L. E. Dickson's "Introduction to the Theory of Algebraic Equations" p. 99. (This book will henceforth be referred to as "Dickson").

Expressing v_1^2 in terms of x_1 and x_2,

$$v^2 - (x_1 - x_2)^2 = 0.$$

$$v^2 = x_1^2 - 2x_1x_2 + x_2^2.$$

Now $x_1^2 - 2x_1x_2 + x_2^2 = x_1^2 + 2x_1x_2 + x_2^2 - 4x_1x_2 = c_1^2 - 4c_2.$

Hence, $v^2 = c_1^2 - 4c_2,$

and $v = \pm\sqrt{c_1^2 - 4c_2}.$

We may choose arbitrarily one of the square roots of $c_1^2 - 4c_2$ for v_1. Having done so, the value of v_2 is then determined.

Let us take $v_1 = +\sqrt{c_1^2 - 4c_2},$

then $v_2 = -\sqrt{c_1^2 - 4c_2}.$

Knowing the roots of equation II we can now determine the roots of equation I in the following manner:

$$\begin{aligned} x_1 - x_2 &= \sqrt{c_1^2 - 4c_2} \\ x_1 + x_2 &= c_1 \\ \hline x_1 &= \frac{c_1 + \sqrt{c_1^2 - 4c_2}}{2}. \\ x_2 &= \frac{c_1 - \sqrt{c_1^2 - 4c_2}}{2}. \end{aligned}$$

We have thus solved equation I by means of the auxiliary equation II. Such an auxiliary equation used in the solution of a given equation is called a "resolvent" equation.

2. <u>The Cubic Equation</u>. Our solution of the quadratic equation depends upon the fact that certain auxiliary functions chosen are symmetric and others are not. We wish to see if this method of solution can be extended to the cubic equation.

The general cubic equation

$$ay^3 + by^2 + cy + d = 0 \qquad \text{(A)}$$

can be reduced to the form

$$x^3 + c_2 x - c_3 = 0 \qquad \text{(B)} \quad \text{where} \begin{cases} c_2 = \frac{c}{a} \frac{-b^2}{3a^2} \\ c_3 = \frac{-d}{a} + \frac{bc}{3a^2} - \frac{2b^3}{27a^3} \end{cases}$$

by dividing by a and substituting

$$y = x - \frac{b}{3a} .$$

Let us consider the reduced cubic (B) and call its root x_1, x_2, x_3.

The coefficients can be expressed as rational, symmetric functions of the roots, namely

$$c_1 = x_1 + x_2 + x_3 = 0.$$

$$c_2 = x_1 x_2 + x_2 x_3 + x_1 x_3$$

$$c_3 = x_1 x_2 x_3 .$$

Following the procedure used in solving the quadratic equation, we desire now to set up functions non-symmetric in x_1, x_2, and x_3. We will be greatly aided in doing this if we understand substitution-groups.

3. Substitutions. The operation of permuting a number of objects is called a substitution. The substitution which replaces x_1 by x_α, x_2 by x_β, --- x_n by x_γ, where $\alpha, \beta, \cdots \gamma$ constitute a permutation of 1, 2, - - -, n is usually denoted by

$$\begin{pmatrix} x_1 & x_2 & - - - & x_n \\ x_\alpha & x_\beta & - - - & x_\gamma \end{pmatrix},$$

the order of the columns being immaterial.

The identical substitution

$$\begin{pmatrix} x_1 & x_2 & - - - & x_n \\ x_1 & x_2 & - - - & x_n \end{pmatrix}$$

leaves every letter unaltered and is denoted by 1.

With three letters $x_1, x_2,$ and x_3 we have $3! = 6$ substitutions

(1). The identical substitution 1.

(2). Substitutions which leave one letter unaltered and interchange the other two.

$$\begin{pmatrix} X_1 & X_2 & X_3 \\ X_1 & X_3 & X_2 \end{pmatrix} \quad \begin{pmatrix} X_1 & X_2 & X_3 \\ X_2 & X_1 & X_3 \end{pmatrix} \quad \begin{pmatrix} X_1 & X_2 & X_3 \\ X_3 & X_2 & X_1 \end{pmatrix}$$

The abbreviated notation for such substitutions is (23) (12) (13).

(3). Substitutions which interchange the letters cyclically.

$$\begin{pmatrix} X_1 & X_2 & X_3 \\ X_2 & X_3 & X_1 \end{pmatrix} \quad \begin{pmatrix} X_1 & X_2 & X_3 \\ X_3 & X_1 & X_2 \end{pmatrix}$$

or in abbreviated notation

(1 2 3) (1 3 2).

Such substitutions are called cycles, or circular substitutions, and when they involve only two letters are called transpositions. Thus (23), (12), and (13) are transpositions.

The substitution $\begin{pmatrix} x_1 & x_2 & x_3 & x_4 & x_5 \\ x_3 & x_1 & x_2 & x_5 & x_4 \end{pmatrix}$ would be denoted in abbreviated form by (132) (45). In fact, any substitution can be expressed as a product of cycles affecting different letters.*

* Dickson: Art. 18.

Any substitution can also be expressed as a product of transpositions,** e.g.

$$(13254) = (13)\ (12)\ (15)\ (14)$$

When a substitution contains an even number of transpositions it is called an "even" substitution.***

4. Substitution - Groups. A set of distinct substitutions such that the product of any two of them (equal or different) belongs itself to the set is called a group of substitutions, or a "substitution-group ".**** When using the word group we shall always mean a substitution-group.

A convenient way to determine whether or not a set of substitutions constitutes a group is to construct the multiplication table. The table gives the product a x b in the intersection of the row headed by a and column headed by b.

For the six substitutions on three letters the multiplication table is as follows:

** Dickson: Art. 22.

*** For a more detailed treatment of substitutions see Dickson: Chap. II or Cajori's': "Theory of Equations" Chapter X (Henceforth referred to as "Cajori").

**** For the general definition of a group see Bôcker: "Introduction to Higher Algebra" Art. 26.

	1	(123)	(132)	(23)	(13)	(12)
1	1	(123)	(132)	(23)	(13)	(12)
(123)	(123)	(132)	1	(13)	(12)	(23)
(132)	(132)	1	(123)	(12)	(23)	(13)
(23)	(23)	(12)	(13)	1	(132)	(123)
(13)	(13)	(23)	(12)	(123)	1	(132)
(12)	(12)	(13)	(23)	(132)	(123)	1

The multiplication table contains no substitution which is not a substitution of the set, and thus the set constitutes a group. In the general case, all the n! substitutions on n letters from a group.*

The number m of distinct substitutions of a group is called its order; the number n of letters operated upon, its degree. A group is designated $G^{(n)}_{m}$, or simply G_m.

5. Subgroups. Upon further investigation we find that there are groups within the group G_6. We find one group of order three,

$$G_3\left[1,\ (123),\ (132)\right]$$

three groups of order two,

$$G'_2\ \left[1,\ (23)\right],\quad G''_2\left[1,\ (13)\right],\quad G'''_2\ \left[1,\ (12)\right]$$

and one group of order one,

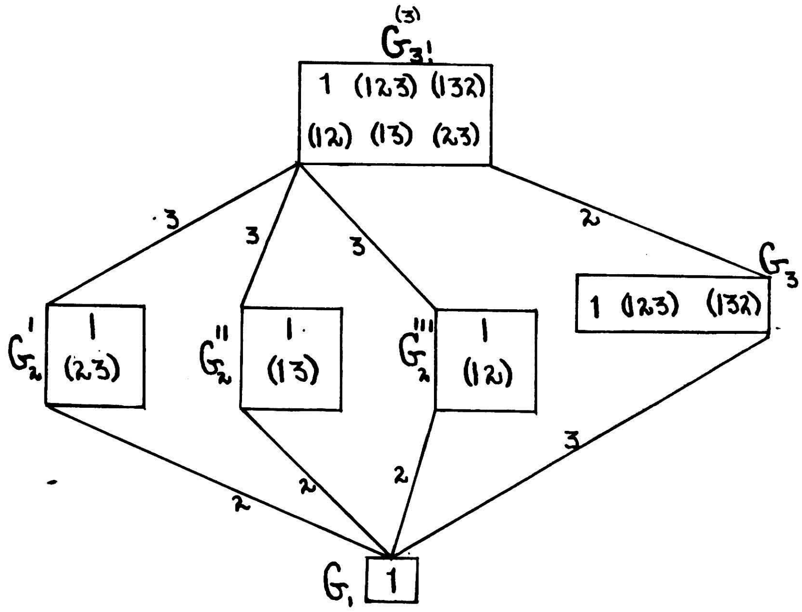
$$G_1\ [1].$$

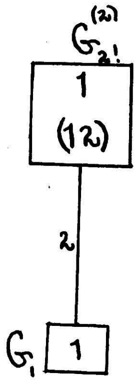
[*] See Cajori: Art. 97.

These groups are called "subgroups" of the group G_6,— *if all the substitutions of any group H are contained in a group G, H is called a subgroup of G.* Notice that by this definition any group is a subgroup of itself.

If n is the order of a group G and m the order of a subgroup H of G, the quotient $\frac{n}{m}$ is called the "index" of H under G and is represented diagramatically $\frac{n}{m}\Big|_{H}^{G}$. The index is always an integer since the order of a subgroup is a divisor of the order of the group to which it belongs.*

We may display $G_{3!}^{(3)}$ and $G_{2!}^{(2)}$ together with their subgroups as follows:





6. *Rational Functions Belonging Formally to a Group.* Upon subjecting the rational functions x_1+x_2 and x_1x_2 to the substitutions of $G_{2!}$ we find that they remain formally** un-

* Dickson: Art. 26.

** Two functions in $x_1 x_2 \ldots x_n$ are formally equal if they are numerically equal for all sets of values of the x's. Two functions may be formally unequal and still be equal for particular sets of values of the x's. Later this dis-

altered since x_1 and x_2 are merely interchanged by the substitutions of $G_{2!}$. On the other hand, the rational functions $x_1 - x_2$ and $x_2 - x_1$ change sign under the substitutions of $G_{2!}$, remaining formally unaltered only by $G_1(1)$. We say that the rational functions $x_1 + x_2$ and $x_1 x_2$ "belong formally" to $G_{2!}$, while the rational functions $x_1 - x_2$ and $x_2 - x_1$ "belong formally" to $G_1(1)$. *By saying that a rational function "belongs formally" to a group we mean that it is formally unaltered by all the substitutions of the group and formally altered by every substitution not in the group.**

Similarly, let us find rational functions belonging formally to the group $G_{3!}$ and to its subgroups.

Any symmetric function of x_1, x_2, and x_3, being formally unaltered when any two of the letters are permuted, is formally unaltered by any substitution of G_6 and thus belongs formally to G_6. Then $x_1 + x_2 + x_3$, $x_1x_2 + x_2x_3 + x_3x_1$, and $x_1x_2x_3$ are functions belonging formally to G_6. Since this property with regard to symmetric functions is characteristic of $G_{n!}$, it is designated as the symmetric group.

The group G_3 consists of all the even substitutions on three letters (which includes the identical element). A function belonging formally to G_3 is

$$\Delta = (x_1 - x_2)(x_2 - x_3)(x_3 - x_1)$$

tinction becomes important, and it will often be necessary to know that two functions are numerically distinct for specific values of the x's.

* For proof that all the substitutions which leave a rational function $(x_1, x_2, \ldots x_n)$ formally unaltered form a group, see Dickson: Art. 21.

since any even substitution leaves it formally unaltered, while any odd substitution changes its sign. A function of n distinct magnitudes, as Δ, such that a single transposition changes its sign is called an alternating function and it belongs formally to the group which consists of all the even substitutions on n letters.* This group is called the alternating group and its order is $\frac{n!}{2}$**.

The function x_1 is unchanged formally by every substitution in G_2' and is changed formally by every substitution not in G_2'. Hence, x_1 belongs formally to G_2'. Similarly, x_2 belongs formally to G_2'', and x_3 belongs formally to G_2'''.

A function which belongs formally to G_1 is changed by every substitution of G_6 other than the identical substitution, Such a function is $k_1x_1+k_2x_2+k_3x_3$ where k_1, k_2, and k_3 are distinct constants. An especially useful function belonging formally to G_1 is the function $v_1=x_1+\omega x_2$***$+\omega^2x_3$.

7. Conjugate Values of a Function under a Group. We observe that the function v_1 is six-valued under G_6 (that is, it takes on six formally distinct values when operated on by all the substitutions of G_6) and is two-valued under G_2', G_2'', and G_2'''. Similarly, the function Δ_1 is two-valued under G_6, and the functions X_1, X_2, and x_3 are three-valued under G_6. For the general case, we

* For proof that all the even substitutions on n letters form a group, see Dickson: Art. 23

** Dickson: Art. 24

*** $\omega=-\frac{1}{2}+\frac{1}{2}\sqrt{-3}$, an imaginary cube root of 1, obtained thus:

$\omega^2=-\frac{1}{2}-\frac{1}{2}\sqrt{-3}$

$$x^3-1=0.$$
$$(x-1)(x^2+x+1)=0.$$
$$x=1 \quad x=-\frac{1}{2}+\frac{1}{2}\sqrt{-3}$$

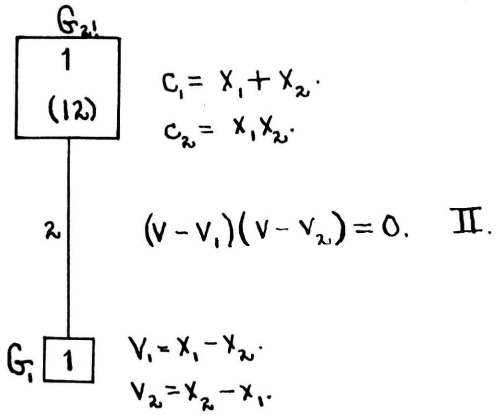
state that the number of formally distinct values which a function belonging formally to a subgroup H of G takes on under G is equal to the index of H under G.* These formally distinct values are called the "conjugate" values of the function under the group G.

8. <u>The Solution of the Cubic Equation</u>. Let us now return to the consideration of the reduced cubic equation

$$x^3 + c_2 x - c_3 = 0$$

and try to solve it by a scheme similar to that which we used in solving the quadratic equation (Art. 1).

$$x^2 - c_1 X + c_2 = 0. \qquad \text{I.}$$

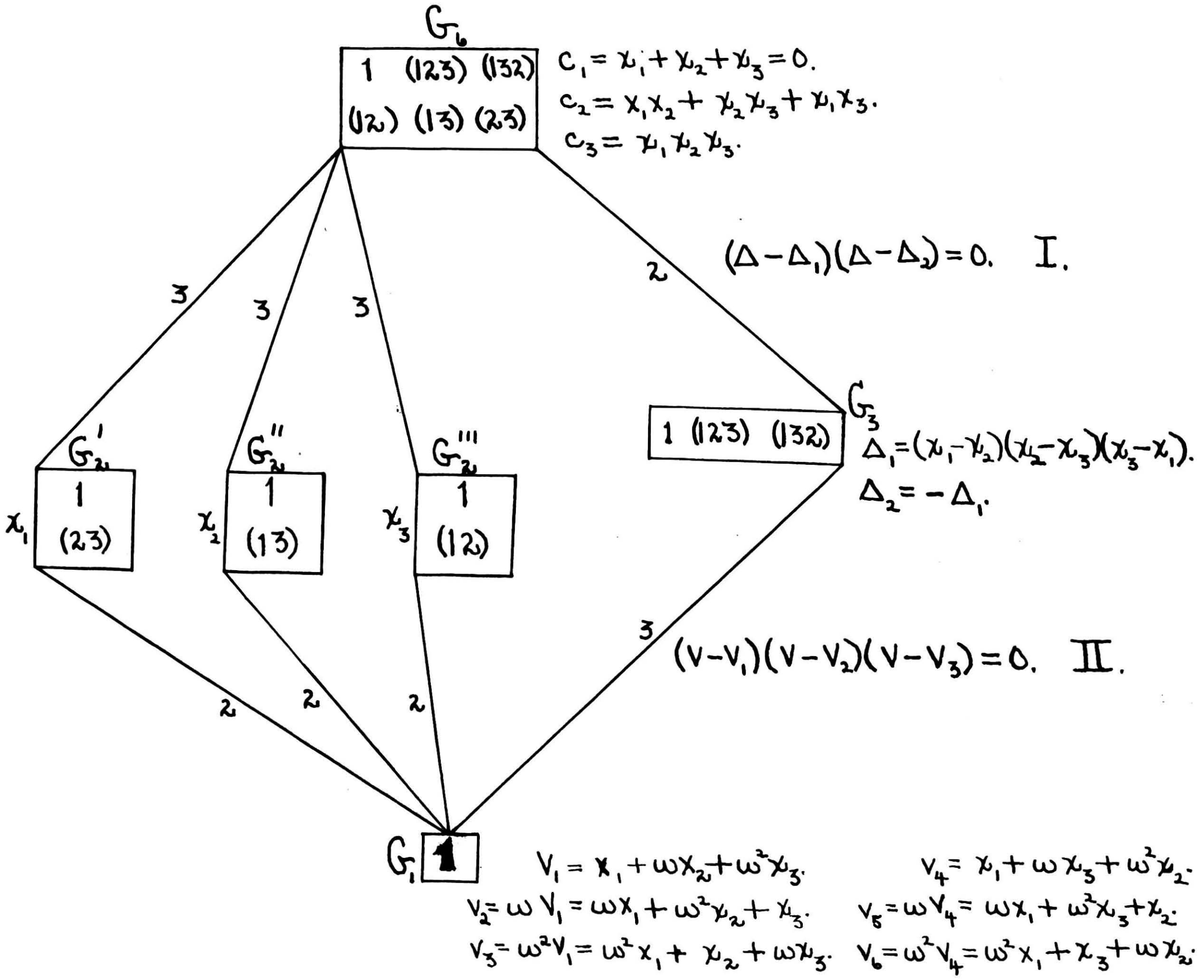


We observe that in solving the quadratic equation what we did was to pick out the rational, nonsymmetric functions v_1 and v_2 belonging formally to $G_1[1]$ and the rational, symmetric functions c_1 and c_2 belonging formally to $G_{2!}$ (See Att.1). We then constructed the resolvent equation II, expressed its coefficient in terms of the c's,

* Dickson: Art.29.

and obtained the value of the functions v_1 and v_2 in terms of the c's. This enabled us to combine and solve for x_1 and x_2.

We have already found certain rational functions belonging formally to G_6 and its subgroups. Using these same functions, we may proceed with our scheme. The following group-display shows these functions together with the resolvent equations which we intend to use.



$$c_1 = x_1 + x_2 + x_3 = 0.$$
$$c_2 = x_1x_2 + x_2x_3 + x_1x_3.$$
$$c_3 = x_1x_2x_3.$$

$$(\Delta-\Delta_1)(\Delta-\Delta_2)=0. \quad \text{I.}$$

$$\Delta_1 = (x_1-x_2)(x_2-x_3)(x_3-x_1).$$
$$\Delta_2 = -\Delta_1.$$

$$(v-v_1)(v-v_2)(v-v_3)=0. \quad \text{II.}$$

$$V_1 = x_1 + \omega x_2 + \omega^2 x_3. \qquad V_4 = x_1 + \omega x_3 + \omega^2 x_2.$$
$$V_2 = \omega V_1 = \omega x_1 + \omega^2 x_2 + x_3. \qquad V_5 = \omega V_4 = \omega x_1 + \omega^2 x_3 + x_2.$$
$$V_3 = \omega^2 V_1 = \omega^2 x_1 + x_2 + \omega x_3. \qquad V_6 = \omega^2 V_4 = \omega^2 x_1 + x_3 + \omega x_2.$$

Our scheme is to write out the resolvent equation I, express its coefficients in terms of the c's, and and solve, thus getting the value of Δ in terms of c's.

We will then write out the resolvent equation II, express its coefficient in terms of Δ and the c's, and solve, thus getting the value of v in terms of Δ and the c's. Having done this, we will combine and solve for x_1, x_2, and x_3, which roots we assume are distinct.*

Let us now consider in detail each step in our scheme.

Constructing a resolvent equation which has Δ_1 and Δ_2 for its roots, we have

$$(\Delta-\Delta_1)(\Delta-\Delta_2)=0. \qquad \text{I.}$$

$$\Delta^2-(\Delta_1+\Delta_2)\Delta+\Delta_1\Delta_2=0.$$

Since $\Delta_1=-\Delta_2$, equation I becomes

$$\Delta^2-\Delta_1^2=0. \qquad \text{I}'.$$

We now desire to express $\Delta_1^2=(x_1-x_2)^2(x_2-x_3)^2(x_3-x_1)^2$ in terms of the c's. We will show later** that $\Delta_1^2=c_2^2c_1^2-4c_1^3c_3-4c_2^3+18c_3c_2c_1-27c_3^2$; and since $c_1=0$ in the reduced cubic equation, equation I$'$ becomes,

$$\Delta^2+4c_2^3+27c_3^2=0.$$

Solving, $\Delta=\pm\sqrt{-27c_3^2-4c_2^3}$.

We may choose arbitrarily one of the square roots of $-27c_3^2-4c_2^3$ for Δ_1. Having done so, the value of Δ_2 is then determined.

* In this and the following discussion we will always exclude the case where $f(x)=0$ has equal roots. Equal roots of $f(x)=0$ also satisfy $f'(x)=0$. If $H(x)$ is the highest common factor of $f(x)$ and $f'(x)$ and if $\varphi(x)=f(x)\div H(x)$ the equation $\varphi(x)=0$ has distinct roots and every root of $f(x)=0$ is a root of $\varphi(x)=0$.

** See Chap. II Art. 10.

Let us take $\Delta_1 = +\sqrt{-27c_3^2 - 4c_2^3}$.

then $\Delta_2 = -\sqrt{-27c_3^2 - 4c_2^3}$.

Constructing a resolvent equation which has v_1, v_2, and v_3 for roots, we have

$$(v - v_1)(v - v_2)(v - v_3) = 0. \qquad \text{II.}$$

Since $v_2 = \omega v_1$ and $v_3 = \omega^2 v_1$, equation II becomes a binominal equation,

$$v^3 - v_1^3 = 0. \qquad \text{II}'.$$

We desire now to express $v_1^3 = (x_1 + \omega x_2 + \omega^2 x_3)^3$ in terms of Δ_1 and the c's. It can be shown that

$$v_1^3 = \tfrac{1}{2}(2c_1^3 - 9c_1 c_2 + 27c_3 - 3\Delta_1\sqrt{-3}).$$

Since $c_1 = 0$ in the reduced cubic equation, equation II$'$ becomes

$$v^3 - \tfrac{1}{2}(27c_3 - 3\Delta_1\sqrt{-3}) = 0. \qquad \text{II}''.$$

Solving, $v = \sqrt[3]{\tfrac{1}{2}(27c_3 - 3\Delta_1\sqrt{-3})}$.

Choosing arbitrarily any one of the cubic roots of $\tfrac{1}{2}(27c_3 - 3\Delta_1\sqrt{-3})$ for the root v_1, then the other two roots are $v_2 = \omega v_1$ and $v_3 = \omega^2 v_1$.

Similarly, we can construct a resolvent equation which has v_4, v_5, and v_6 for its roots:

$$(v - v_4)(v - v_5)(v - v_6) = 0. \qquad \text{III.}$$

Since $v_5 = \omega v_4$ and $v_6 = \omega^2 v_4$, equation III becomes a binomial equation

$$v^3 - v_4^3 = 0. \qquad \text{III}'.$$

Expressing $v_4^3 = (x_1 + \omega x_3 + \omega^2 x_2)^3$ in terms of Δ_2 and the c's,

$$v^3 - \tfrac{1}{2}(27c_3 - 3\Delta_2\sqrt{-3}) = 0. \qquad \text{III}''.$$

Solving, $v = \sqrt[3]{\tfrac{1}{2}(27c_3 - 3\Delta_2\sqrt{-3})}$.

We observe that equation III″ differs from equation II″ only in that it contains Δ_2 in place of Δ_1.

We must now determine which of the three cube roots of $\frac{1}{2}(27c_3 \quad -3\Delta_2\sqrt{-3})$ we should choose. We cannot choose this value (call it v_4) arbitrarily as we did v_1.

If we choose $v_1 = x_1+\omega x_2+\omega^2 x_3$,

then we must choose $v_4 = x_1+\omega^2 x_2+\omega x_3$.

Multiplying v_1 by v_4,

$$v_1 v_4 = (x_1+\omega x_2+\omega^2 x_3)(x_1+\omega^2 x_2+\omega x_3) = -3c_2.$$

This is a relation which must be satisfied by the values chosen for v_1 and v_4.*

Combining with v_1 and v_4 the equation

$$x_1+x_2+x_3 = c_1 = 0,$$

we are able to find the roots x_1, x_2, and x_3 as follows:

$$\begin{array}{ll} x_1+\omega x_2+\omega^2 x_3 = v_1 & \text{(A)} \\ x_1+\omega^2 x_2+\omega x_3 = v_4 & \text{(B)} \\ x_1+x_2+x_3 = 0 & \text{(C)} \\ \hline x_1 \qquad\qquad = 1/3\ (v_1+v_4). & \end{array}$$

Multiplying (A) by ω^2, (B) by ω , and (C) by 1, and adding, we get

$$x_2 = 1/3\ (\omega^2 v_1 + \omega v_4).$$

Multiplying (A) by ω, (B) by ω^2, and (C) by 1, and adding, we get

$$x_3 = 1/3\ (\omega v_1 + \omega^2 v_4).$$

* A general explanation of the reason for this will be given later. (See footnote page 35.)

CHAPTER II.

A More Detailed Study of the Processes Involved in the Solution of the Cubic Equation.

9. The solution of the cubic equation given in Chapter I suggests a general plan for the solution of equations of higher degrees. Before giving a general plan, however, we must first study the solution of the cubic equation still more in detail and learn under what conditions we can actually perform the various operations.

10. We observe that the coefficients of the resolvent equation

$$(\Delta-\Delta_1)(\Delta-\Delta_2)=0. \qquad \text{I.}$$

are symmetric functions of x_1, x_2, and x_3, (Art. 8 page 14). It follows from the fundamental theorem on symmetric functions* that the coefficient can be expressed as rational, integral functions of the c's. In his "Introduction to the Theory of Algebraic Equations" Dickson has given a plan by Gauss for expressing any symmetric function of the x's as a rational, integral function of the c's.* To illustrate this plan in a special case, we will proceed to express the symmetric function $\Delta_1\Delta_2$(which occurs as a coefficient in equation I) in terms of thé c's.

* Dickson: Appendix p. 99.

Following the plan given by Dickson:

Designate the given symmetric function $\Delta_1\Delta_2$ by S.

$$S \equiv \Delta_1\Delta_2 = -(x_1 - x_2)^2 (x_2 - x_3)^2 (x_3 - x_1)^2 = 6x_1^2 x_2^2 x_3^2 - 2x_1 x_2^3 x_3^2 - x_2^4 x_3^2 - 2x_1^2 x_2 x_3^3 - 2x_1 x_2^2 x_3^3 + 2x_2^3 x_3^3 - x_1^2 x_3^4 + 2x_1 x_2 x_3^4 - x_2^2 x_3^4 - 2x_1^3 x_2^2 x_3 - 2x_1^2 x_2^3 x_3 + 2x_1 x_2^4 x_3 - 2x_1^3 x_2 x_3^2 + 2x_1^3 x_3^3 \underline{- x_1^4 x_2^2} + 2x_1^3 x_2^3 - x_1^2 x_2^4 + 2x_1^4 x_2 x_3 - x_1^4 x_3^2 .$$

The highest* term of S is

$$h \equiv - x_1^4 x_2^2 .$$

Build the symmetric function

$$\sigma \equiv - c_1^{4-2} c_2^2 = - c_1^2 c_2^2 .$$

Expanding σ in terms of x_1, x_2, and x_3, we have

$$\sigma \equiv -(x_1 + x_2 + x_3)^2 (x_1 x_2 + x_2 x_3 + x_1 x_3) = -15 x_1^2 x_2^2 x_3^2 - 8x_1 x_2^3 x_3^2 - x_2^4 x_3^2 - 8x_1^2 x_2 x_3^3 - 8x_1 x_2^2 x_3^3 - 2x_2^2 x_3^3 - x_1^2 x_3^4 - 2x_1 x_2 x_3^4 - x_2^2 x_3^4 - 8 x_1^3 x_2^2 x_3 - 8x_1^2 x_2^3 x_3 - 2x_1 x_2^4 x_3 - 8x_1^3 x_2 x_3^2 - 2x_1^3 x_3^3 \underline{- x_1^4 x_2^2} - 2x_1^3 x_2^3 - x_1^2 x_2^4 - 2x_1^4 x_2 x_3 - x_1^4 x_3^2 .$$

We observe that the highest term of σ is h.

Then the difference

$$S_1 \equiv S - \sigma$$

is a symmetric function which has its highest term lower then h.

$$S_1 \equiv S - \sigma = 21x_1^2 x_2^2 x_3^2 + 6x_1 x_2^3 x_3^2 + 6x_1^2 x_2 x_3^3 + 6x_1 x_2^2 x_3^3 + 4x_2^3 x_3^3 + 4x_1 x_2 x_3^4 + 6x_1^3 x_2^2 x_3 + 6x_1^2 x_2^3 x_3 + 4x_1 x_2^4 x_3 + 6x_1^3 x_2 x_3^2 + 4x_1^3 x_3^3 + 4x_1^3 x_2^3 \underline{+ 4x_1^4 x_2 x_3 .}$$

The highest term of S_1 is

$$h_1 \equiv 4 x_1^4 x_2 x_3 .$$

*$x_1^{m_1} x_2^{m_2} x_3^{m_3}$... is called higher than $x_1^{n_1} x_2^{n_2} x_3^{n_3}$ ... if the first one of the differences $m_1 - n_1$, $m_2 - n_2$, ... which does not vanish is positive.

Build the symmetric function

$$\sigma_1 \equiv 4c_1^{4-1}\ c_2^{1-1}\ c_3 = 4c_1^3\ c_3.$$

Expanding σ_1 in terms of x_1, x_2, and x_3, we have

$$\sigma_1 \equiv 4(x_1+x_2+x_3)^3\ x_1x_2x_3 = 24x_1^2\ x_2^2\ x_3^2 + 12x_1x_2^3\ x_3^2 + 12x_1^2\ x_2x_3^3 + 12x_1x_2^2\ x_3^3 + 4x_1x_2x_3^4 + 12x_1^3\ x_2^2\ x_3 + 12x_1^2\ x_2^3\ x_3 + 4x_1x_2^4\ x_3 + 12x_1^3\ x_2\ x_3^2 \underline{+ 4x_1^4\ x_2x_3.}$$

Since the highest term of σ_1 is h_1, the difference

$$S_2 \equiv S_1 - \sigma_1$$

is a symmetric function which has its highest term lower than h_1.

$$S_2 \equiv S_1 - \sigma_1 = -3x_1^2\ x_2^2\ x_3^2 - 6x_1x_2^3\ x_3^2 - 6x_1^2\ x_2\ x_3^3 - 6x_1x_2^2\ x_3^3 + 4x_2^3\ x_3^3 - 6x_1^3\ x_2^2\ x_3 - 6x_1^2\ x_2^3\ x_3 - 6x_1^3\ x_2\ x_3^2 + 4x_1^3\ x_3^3 \underline{+ 4x_1^3\ x_2^3\ .}$$

The highest term of S_2 is

$$h_2 \equiv 4x_1^3\ x_2^3\ .$$

Build the symmetric function

$$\sigma_2 \equiv 4c_1^{3-3}\ c_2^3 = 4c_2^3\ .$$

Expanding σ_2 in terms of x_1, x_2, and x_3, we have

$$\sigma_2 \equiv 4(x_1x_2+x_2x_3+x_1x_3)^3 = 24x_1^2\ x_2^2\ x_3^2 + 12x_1\ x_2^3\ x_3^2 + 12x_1^2\ x_2\ x_3^3 + 12x_1x_2^2\ x_3^3 + 4x_2^3\ x_3^3 + 12x_1^3\ x_2^2\ x_3 + 12x_1^2\ x_2^3\ x_3 + 12x_1^3\ x_2x_3^2 + 4x_1^3\ x_3^3 + \underline{4x_1^3\ x_2^3\ .}$$

Since the highest term of σ_2 is h_2, the difference

$$S_3 \equiv S_2 - \sigma_2$$

is a symmetric function which has its highest term lower than h_2.

$$S_3 \equiv S_2 - \sigma_2 = - 27\, x_1^2 x_2^2 x_3^2 - 18\, x_1 x_2^3 x_3^2$$
$$- 18x_1^2 x_2 x_3^3 - 18x_1 x_2^2 x_3^3 \underline{- 18x_1^3 x_2^2 x_3} - 18x_1^2 x_2^3 x_3 -$$
$$18x_1^3 x_2 x_3^2 .$$

The highest term of S_3 is

$$h_3 \equiv - 18x_1^3 x_2^2 x_3.$$

Build the symmetric function

$$\sigma_3 \equiv - 18c_1^{3-2} c_2^{2-1} c_3 = - 18c_1 c_2 c_3.$$

Expanding σ_3 in terms of x_1, x_2, and x_3, we have

$$\sigma_3 = -54x_1^2 x_2^2 x_3^2 - 18x_1 x_2^3 x_3^2 - 18x_1^2 x_2 x_3^3 - 18x_1 x_2^2 x_3^3 -$$
$$\underline{- 18x_1^3 x_2^2 x_3} - 18x_1^2 x_2^3 x_3 - 18x_1^3 x_2 x_3^2 .$$

Since the highest term of σ_3 is h_3, the difference

$$S_4 \equiv S_3 - \sigma_3$$

is a symmetric function which has its highest term lower than h_3.

$$S_4 \equiv S_3 - \sigma_3 = 27x_1^2 x_2^2 x_3^2 .$$

The highest term of S_4 is S_4 itself,

$$h_4 \equiv 27x_1^2 x_2^2 x_3^2 .$$

Build the symmetric function

$$\sigma_4 \equiv 27\, c_1^{2-2} c_2^{2-2} c_3^2 = 27c_3^2 .$$

Expanding σ_4 in terms of x_1, x_2, ahd x_3, we have

$$\sigma_4 = 27x_1^2 x_2^2 x_3^2 .$$

and the difference

$$S_5 \equiv S_4 - \sigma_4 = 0.$$

Now let us express S in terms of the σ's.

$$
\begin{aligned}
0 &= S_5 \\
&= S_4 - \sigma_4 \\
&= S_3 - \sigma_3 - \sigma_4 \\
&= S_2 - \sigma_2 - \sigma_3 - \sigma_4 \\
&= S_1 - \sigma_1 - \sigma_2 - \sigma_3 - \sigma_4 \\
&= S \;\; - \sigma_1 - \sigma_2 - \sigma_3 - \sigma_4 - \sigma \;.
\end{aligned}
$$

$$
\therefore \; S = \sigma + \sigma_1 + \sigma_2 + \sigma_3 + \sigma_4.
$$

$$
= - c_1^2 c_2^2 + 4c_1^3 c_3 + 4c_2^3 - 18c_1 c_2 c_3 + 27c_3^2 .^*
$$

11. After expressing the coefficient of equation I in terms of the c's, we proceed to solve for Δ. This is easily done, since equation I is a binomial equation.

The coefficients of the second resolvent equation

$$(v - v_1)(v - v_2)(v - v_3) = 0 \qquad \text{II}$$

were found to be expressible in terms of Δ and the c's. The discussion of this point will be delayed until the next chapter.** Like equation I, equation II is binomial and thus can be easily solved.

We have been concerning ourselves with resolvent equations over the path $G_6 - G_3 - G_1$. But why not choose the alternative path $G_6 - G_2'$, select x_1 belonging formally to G_2', and write the resolvent equation for finding x_1 directly? Upon doing this, we obtain the following resolvent equation:

$$(x - x_1)(x - x_2)(x - x_3) = 0.$$

$$\text{or} \quad x^3 - c_1 x^2 + c_2 x - c_3 = 0.$$

$$\text{or since } c_1 = 0, \; x^3 + c_2 x - c_3 = 0. \qquad \text{III}$$

* Such a computation is long, and for a special case the values of the c's should merely be substituted in the general formula.

**Chap. III Art. 18.

We observe, however, that equation III is the original equation, and therefore nothing is gained.

Why are we able to solve equation I and equation II when we cannot solve equation III directly? We can easily solve equation I and equation II because they are binomial. We are here then concerned with learning the conditions for a binomial resolvent. Whether or not the resolvent equation for a certain function will turn out to be binomial depends upon the function itself and upon a certain characteristic of the group to which the function formally belongs. Before appreciating a more specific statement of the conditions for a binomial resolvent we must understand what is meant by a "self-conjugate" subgroup.

12. *Self Conjugate Subgroups*. We know that the function x_1 belonging formally to G_2' takes on under G_6 the three conjugate values x_1, x_2, and x_3, belonging formally to the subgroups G_2', G_2'', and G_2''' respectively. The subgroups G_2', G_2'', and G_2''' are called "conjugate" subgroups of G .

Similarly, the function $\Delta_1 = (x_1 - x_2)(x_2 - x_3)(x_3 - x_1)$ belonging formally to G_3 takes on under G_6 the conjugate values Δ_1 and $\Delta_2 = -\Delta_1$, but we observe that both of these conjugate values belong to the same group G_3. The group G_3 is called a "self conjugate" subgroup of G_6. For the general case, *if a rational function ψ belongs formally to a subgroup H of G and if the conjugates of ψ under G all belong formally to H, then H is called a*

self-conjugate subgroup of G.

The idea of conjugate and self-conjugate subgroups may also be approached without reference to the functions belonging to the groups. Given a subgroup H of index k under a group G, we can get the k conjugate subgroups of index k under G by applying within the cycles constituting H the substitutions of G not contained in H.* For instance, applying the substitution (12) of G_6 within the cycles of $G_2' [1\ (23)]$

we get $(12)\ G_2' [1\ (23)] = [1\ (13)] = G_2''$.

Similarly,

$$(13)\ G_2' [1\ (23)] = [1\ (12)] = G_2''' .$$

$$(123)\ G_2' [1\ (23)] = [1\ ,(13)] = G_2'' .$$

$$(132)\ G_2' [1\ (23)] = [1\ ,(12)] = G_2''' .$$

Thus the three conjugate groups of index 3 under G are $G_2' [1\ (23)]$, $G_2'' [1,(13)]$, and $G_2''' [1,(12)]$.

If, however, a subgroup H of G remains invariant under all the substitutions of G, H is called a self-conjugate subgroup of G.

For instance, consider the subgroup G_3 of G_6. The substitutions of G_6 not contained in G_3 are (12),(13), and (23). Applying these substitutions within the cycles of G_3 we have

$$(12)\ G_3 [1,(123),(132)] = [1,(132),(123)] = G_3$$

$$(13)\ G_3 [1,(123),(132)] = [1,(132),(123)] = G_3$$

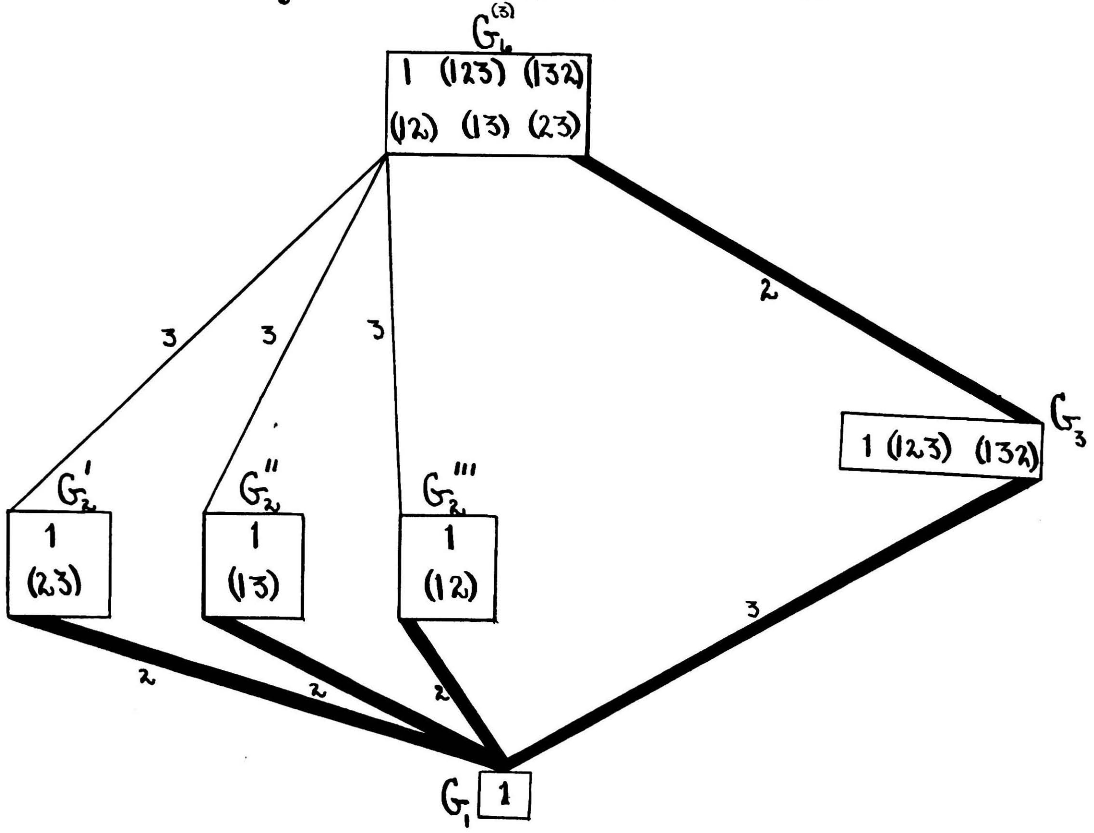
$$(23)\ G\ [1,(123),(132)] = [1,(132),(123)] = G_3$$

Hence G_3 is a self-conjugate subgroup of G_6.

* Dickson: Art. 40.

It is evident that $G_1(1)$ is always a self-conjugate subgroup since it remains invariant under any substitution.

In our diagrams we will indicate that a subgroup is self-conjugate by the use of a heavy line. The diagram of $G_6^{(3)}$ and its subgroups would appear as follows:



13. *Conditions for a Binomial Resolvent.* In order for the resolvent equation for a rational function $\psi(x_1 x_2 x_3 \dots x_n)$, belonging formally to a subgroup H of G, to be binomial the conjugate values of ψ under G, from which the resolvent equation is formed, must differ only by a constant factor and must therefore all belong formally to H.* We have seen that if all the conjugates of ψ under G belong formally to H, H is a self-conjugate subgroup of G. Thus we have a *necessary* condition for a

binomial resolvent.

Is this condition for a binomial resolvent also sufficient? Suppose we choose the rational function $v_1 = 2x_1 - x_2$which belongs formally to the self-conjugate subgroup $G_1^{(2)}$ of $G_{2!}^{(1)}$. The resolvent equation for v_1 is

$$(v - v_1)(v - v_2) = 0. \quad \text{II.}$$

$$v^2 - (v_1 + v_2)\, v + v_1 v_2 = 0.$$

Substituting $v_1 = 2x_1 - x_2$ and $v_2 = 2x_2 - x_1$,

$$v^2 - (x_1 + x_2)\, v + 5x_1x_2 - 2x_2^2 - 2x_1^2 = 0.$$

Here we have an example of a rational function belonging formally to a self-conjugate subgroup and for which the resolvent equation is not binomial. Therefore, in order that the resolvent equation for a rational function be binomial, it is <u>necessary</u> but <u>not</u> <u>sufficient</u> that the group of the function be a self-conjugate subgroup.

However, upon choosing $v_1 = x_1 - x_2$we have found that the resolvent equation II becomes binomial (Art. 1). Similarly, we have found that the resolvent equation for the function $v_1 = x_1 + \omega x_2 + \omega^2 x_3$ belonging formally to the self-conjugate subgroups $G_1^{(3)}$ of $G_{3!}^{(1)}$ becomes binomial (Art.8). It can be shown that if ψ is any rational function belonging formally to a self-conjugate subgroup H of prime index γ under G and if $\psi_1, \psi_2, \cdots \psi_\gamma$ are the conjugate values of ψ under G, then the function

$$\psi_1 + \omega^{**}\psi_2 + \omega^2\psi_3 + \cdots + \omega^{\gamma-1}\psi_\gamma$$

[*] Dickson: Art. 38.

[**] ω is obtained by solving $x^\gamma - 1 = 0$. $(x - 1)(x^{\gamma-1} + x^{\gamma-2} + \ldots + x + 1) = 0$. ω is a root of $x^{\gamma-1} + x^{\gamma-2} + \ldots + x + 1 = 0$.

is a function which belongs formally to H and whose resolvent equation becomes binomial.*

Thus the necessary and sufficient conditions that a resolvent equation of prime degree should turn out to be binomial are that the rational function φ for which the resolvent equation is formed under G should belong formally to a self-conjugate subgroup H of prime index under G and that φ should be a properly chosen function. Moreover, these conditions are also general, since any binomial equation of degree which is not prime may be replaced by a chain of binomial equations of prime degrees. For example, suppose that $x^6 = c$ is the resolvent equation formed under a group G for a function φ belonging formally to a self-conjugate group H of index 6 under G. The binomial equation $x^6 = c$ may be replaced by the binomial equations $x^3 = y$ and $y^2 = c$. This means that between G and H there is an intermediate self-conjugate group of prime index three under G. That is to say, the resolvent equation formed for a rational function φ under G becomes binomial no matter if the group H to which φ formally belongs is not of prime index under G, providing that there is a chain** of self-conjugate subgroups of prime index beginning with G and terminating with H and providing that φ is a properly chosen function. We may then without loss of generality limit our discussions to binomial equations of prime degrees.

* See Bolza's article "On the Theory of Substitution Groups and its applications to Algebraic Equations" in Mathematical Journal Vol. 13, 1891 p. 96, Art. 42.

** Groups constitute a chain when each group is a subgroup of the preceding group.

14. After solving the binomial equations I and II, we are able to combine and solve for the roots (Art. 8 page 16). This solution can be extended to the case of an equation of degree n.

Suppose we have the equations

$$x_1+x_2+x_3+\dots+x_n=c$$
$$x_1+\omega x_2+\omega^2x_3+\dots+\omega^{n-1}x_n=v_1$$
$$x_1+\omega^2x_2+\omega^4x_3+\cdots+\omega^{2(n-1)}x_n=v_2$$
$$\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot$$
$$x_1+\omega^{n-1}x_2+\omega^{2(n-1)}x_3+\dots+\omega^{(n-1)^2}x_n=v_{n-1}\ .$$

To find x_{k+1} we multiply these equations by $1, \omega^{-k}, \omega^{-2k}, \cdots \omega^{-(n-1)k}$ respectively and add the resulting equations.

Remembering that $1+\omega^m+\omega^{2m}+\cdots+\omega^{(n-1)m}=0$ for $m=1, 2, \dots n-1$, we get

$$x_{k+1}=\frac{1}{n}\left\{c_1+\omega^{-k}v_1+\omega^{-2k}v_2+\cdots+\omega^{-(n-1)k}v_{n-1}\right\}.$$

The form of the equations which we combine is easily recognizable. The first is of the form

$$x_1+x_2+x_3+\dots+x_n=c_1\ .$$

The second is of the form

$$x_1+\omega x_2+\omega^2x_3+\dots+\omega^{n-1}x_n=v_1\ .$$

The third is obtained from the second by replacing ω by ω^2, ω^2 by ω^4, ... ω^{n-1} by $\omega^{2(n-1)}$. Similarly, the forth is obtained from the third by replacing ω^2 by ω^3, ω^4 by ω^6, ...$\omega^{2(n-1)}$ by $\omega^{3(n-1)}$, etc.

It now remains to see if we can find the values of the v's which occur in these equations. This will be done later.*

* See footnote: Chapter III, p. 35.

CHAPTER III.

The Plan of Solution for Quadratic and Cubic Equations Extended to Equations of Higher Degree.

15. **The Display of $G_{n!}$ and its Subgroups.** As the degree of an equation increases, the display of $G_{n!}$ and its subgroups becomes correspondingly more complex.

To determine all the substitution-groups which can be formed with n letters we may proceed by writing down all the n! substitutions and by selecting any r of them. If the multiplication table for these r substitutions contains no additional substitutions, the r substitutions constitute a group; if it contains additional substitutions, add them to the system and form the enlarged table. Continuing this process we will finally arrive at a group, since there are only a finite number (n!) of different substitutions. It is also advantageous to keep the following theorems in mind when determining subgroups:

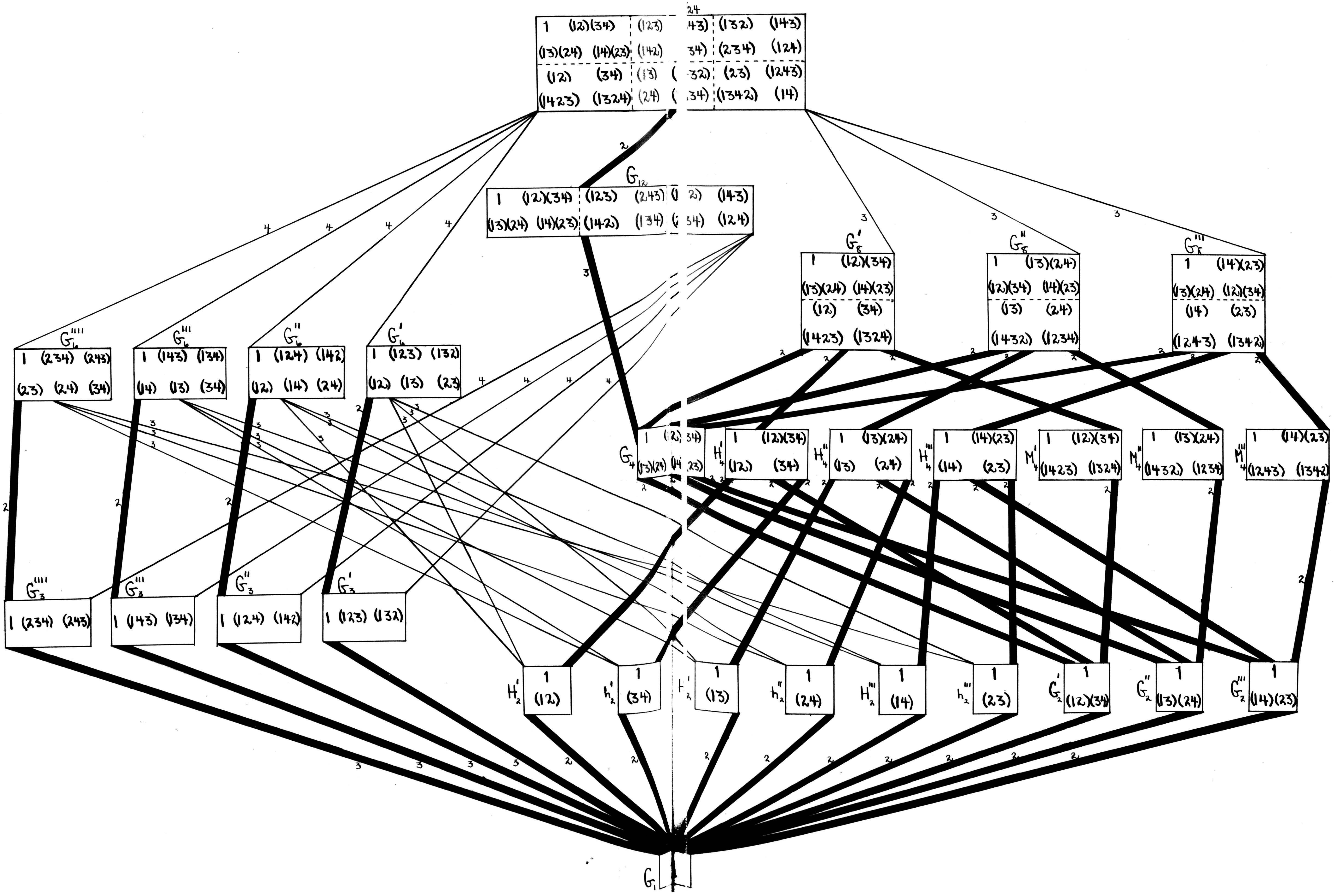
1. The order of any subgroup of a group G is a factor of the order of G.*

2. If p^{α} is the highest power of a prime number p which divides the order of a group G, G contains a single conjugate set of $kp+1$ subgroups of order p^{α} (where k is an integer)**

3. If p^{r} is any power of a prime number p which divides the order of a group G, G contains $lp+1$ sub-

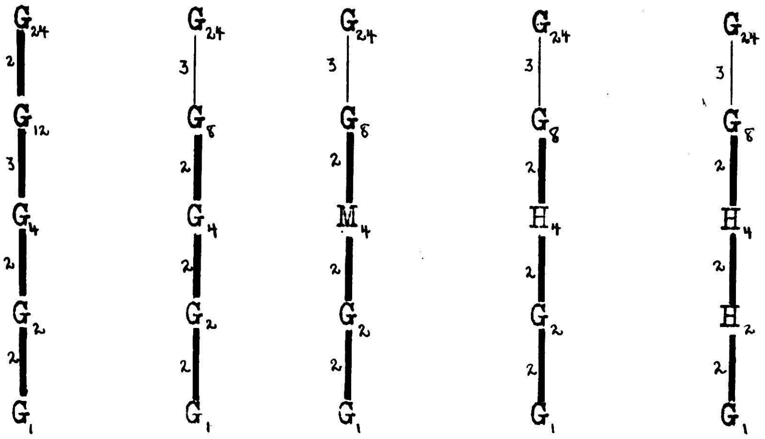
* Burnside: Theory of Groups of Finite Order. Art.22 p 25
Dickson Art 26. p. 20.

** Burnside: Theory of Groups " " " Art.86 p. 108.


24
1 (12)(34) (123) 43) (132) (143)
(13)(24) (14)(23) (142) 34) (234) (124)
(12) (34) (13) 32) (23) (1243)
(1423) (1324) (24) 34) (1342) (14)
2
G_12
1 (12)(34) (123) (243) 2) (143)
(13)(24) (14)(23) (142) (134) 34) (124)
4
4
4
4
3
3
3
3
G'_8
1 (12)(34)
(13)(24) (14)(23)
(12) (34)
(1423) (1324)
G''_8
1 (13)(24)
(12)(34) (14)(23)
(13) (24)
(1432) (1234)
G'''_8
1 (14)(23)
(13)(24) (12)(34)
(14) (23)
(1243) (1342)
G''''_6
1 (234) (243)
(23) (24) (34)
G'''_6
1 (143) (134)
(14) (13) (34)
G''_6
1 (124) (142)
(12) (14) (24)
G'_6
1 (123) (132)
(12) (13) (23)
4
4
4
4
G_4
1 (12) 34)
(13)(24) (14 23)
H'_4
1 (12)(34)
(12) (34)
H''_4
1 (13)(24)
(13) (24)
H'''_4
1 (14)(23)
(14) (23)
M'_4
1 (12)(34)
(1423) (1324)
M''_4
1 (13)(24)
(1432) (1234)
M'''_4
1 (14)(23)
(1243) (1342)
2
3
G''''_3
1 (234) (243)
G'''_3
1 (143) (134)
G''_3
1 (124) (142)
G'_3
1 (123) (132)
H'_2
1 (12)
h'_2
1 (34)
H'_2
1 (13)
h''_2
1 (24)
H'''_2
1 (14)
h'''_2
1 (23)
G'_2
1 (12)(34)
G''_2
1 (13)(24)
G'''_2
1 (14)(23)
3
3
3
3
2
2
G_1

groups of order p^{l} (where l is an integer.) [These groups do not necessarily form a single conjugate set.] *

16. Upon displaying G_{24} and its subgroups (See opposite page) the following five direct paths seem open for the solution of the biquadratic equation (all other direct paths involving non-binomial resolvents of fourth degree):



In accordance with the plan used in the solution of the quadratic and cubic equations we should now like to know if we can obtain rational functions of the roots belonging formally to each group involved.

We can always do this, for consider the formally n! - valued function

$$v_1 = m_1x_1 + m_2x_2 + \dots . + m_nx_n$$

where the m's are all distinct constants.

Applying to v_1 the k substitutions of G, we get

$$v_1 , \quad v_2 , \dots v_k ,$$

which are all formally distinct,

The function

$$\psi = (v - v_1)(v - v_2) \dots (v - v_k)$$

* Burnside: Theory of Groups of Finite Order Art. 77. p. 91.

where v is an independent variable remains formally unaltered by any substitution of G and formally altered by any substitution not in G. Hence ψ is a function belonging formally to G.

Taking $v_1 = x_1 - x_2 + i(x_3 - x_4)$ let us find a function belonging formally to $G_2^{(4)\prime}$ $[1:(12)(34)]$ by this method.

Applying to v_1 the substitutions of G_2' we get

$$v_1 = x_1 - x_2 + i(x_3 - x_4)$$

$$v_2 = -[x_1 - x_2 + i\ (x_3 - x_4)] .$$

$$\psi = (v - v_1)(v - v_2) = v^2 - (v_1 + v_2)\ v + v_1 v_2$$

$$= v^2 - 0 - [(x_1 - x_2) + i(x_3 - x_4)]^2 .$$

The value $v = 0$ keeps ψ formally distinct from any value obtained for it upon applying any substitution not in G_2'. Hence $[(x_1 - x_2) + i(x_3 - x_4)]^2$ belongs formally to G_2' .

17. The use of the above method of finding functions belonging formally to a group does not always furnish simple results so directly. It may, however, be that ψ itself is composed of parts which are functions of the desired kind. In many cases the calculation of ψ is rendered difficult by long multiplication. This can be avoided by choosing as a basis for construction the n! valued function

$$\theta = x_1^{a_1}\ x_2^{a_2}\ \dots\ x_n^{a_n} ,$$

the a's being distinct, but otherwise arbitrarily chosen.

Applying to θ the k substitutions of G, we get

$$\theta_1 , \theta_2 , \cdot \cdot \cdot \cdot \theta_k .$$

which are all formally distinct.

Then the function

$$\Phi = \theta_1 + \theta_2 + \cdot \cdot \cdot + \theta_k$$

is formally unchanged by every substitution in G and formally changed by every substitution not in G.

Let us apply this method to find a function belonging formally to the group $G_8^{(4)'}$ [1, (12), (34), (12)(34), (13)(24), (14)(23), (1423], (1324)] taking $\theta_1 = x_1^0 x_2^1 x_3^2 x_4^3$.

Applying to θ the eight substitutions of G_8', we get $\theta_1 = x_2 x_3^2 x_4^3$, $\theta_2 = x_1 x_3^2 x_4^3$, $\theta_3 = x_2 x_3^3 x_4^2$, $\theta_4 = x_1 x_3^3 x_4^2$, $\theta_5 = x_1^2 x_2^3 x_4$, $\theta_6 = x_1^3 x_2^2 x_3$, $\theta_7 = x_1^2 x_2^3 x_3$, $\theta_8 = x_1^3 x_2^2 x_4$.

$$\Phi = x_2 x_3^2 x_4^3 + x_1 x_3^2 x_4^3 + x_2 x_3^3 x_4^2 + x_1 x_3^3 x_4^2 + x_1^2 x_2^3 x_4 + x_1^3 x_2^2 x_3 + x_1^2 x_2^3 x_3 + x_1^3 x_2^2 x_4 .$$

$$= (x_1 + x_2)(x_3^2 x_4^3 + x_3^3 x_4^2) + (x_3 + x_4)(x_1^2 x_2^3 + x_1^3 x_2^2)$$

$$= (x_1 + x_2)(x_3 + x_4)(x_3^2 x_4^2 + x_1^2 x_2^2).$$

The function Φ belongs formally to G_8', but by the inspection of Φ we arrive at the two simpler functions

$(x_1 + x_2)(x_3 + x_4)$ and $x_1 x_2 + x_3 x_4$ which also themselves belong formally to G_8'.

18. <u>Lagrange's</u> <u>Theorem</u>. In the solution of the cubic equation we have occasion to express the coefficients

of equation I (Chap. I Art. 8. p. 14), which belong formally to G_6, rationally in terms of the c's, which are functions which also belong to G_6. Furthermore we express the coefficients of equation II (Chap. I. Art. 8. p. 15), which belong formally to G_3, rationally in terms of Δ_1, which belongs formally to G_3, and the c's, which belong formally to G_6. Can we always express two rational functions belonging formally to the same group as rational functions of each other? Can we always express a rational function belonging formally to a certain group rationally in terms of another rational function belonging formally to that group and rational functions belonging formally to the symmetric group?

The above questions are answered in a theorem due to Lagrange which states that "if a rational function $\varphi(x_1, x_2, \dots x_n)$ remains unaltered by all the substitutions which leave another rational function $\psi(x_1, x_2, \dots x_n)$ unaltered, then φ is rationally expressible in terms of ψ and $c_1 c_2 \dots c_n$ *

Following the plan of Lagrange* let us express $\varphi = v_4 = x_1 + \omega^2 x_2 + \omega\ x_3$ in terms of $\psi = v_1 = x_1 + \omega x_2 + \omega^2 x_3$, φ being unaltered formally by all the substitutions which leave ψ unaltered, namely the identical substitution. In this case we are dealing with two functions belonging formally to the same group G_1 (1). We observe that the theorem also includes the case where ψ belongs

* Dickson: Art. 31.

formally to a subgroup of the group to which φ formally belongs.

Consider an array of the substitutions of G_6 with the substitution of $G_1(1)$ in the first place :

$$\begin{array}{l|l|l}
1 & x_1+\omega x_2+\omega^2 x_3 = v_1 = \psi_1 & x_1+\omega^2 x_2+\omega x_3 = v_4 = \varphi_1 . \\
(132) & \omega x_1+\omega^2 x_2 + x_3 = \omega v_1 = \psi_2 & \omega^2 x + \omega x_2 + x_3 = \omega^2 v_4 = \varphi_2 . \\
(123) & \omega^2 x_1 + x_2 + \omega x_3 = \omega^2 v_1 = \psi_3 & \omega x_1 + x_2 + \omega^2 x_3 = \omega v_4 = \varphi_3 . \\
(23) & x_1+\omega^2 x_2+\omega x_3 = v_4 = \psi_4 & x_1+\omega x_2+\omega^2 x_3 = v_1 = \varphi_4 . \\
(12) & \omega x_1 + x_2+\omega^2 x_3 = \omega v_4 = \psi_5 & \omega^2 x_1 + x_2 + \omega x_3 = \omega^2 v_1 = \varphi_5 . \\
(13) & \omega^2 x_1 + \omega x_2 + x_3 = \omega^2 v_4 = \psi_6 & \omega x_1+\omega^2 x_2 + x_3 = \omega v_1 = \varphi_6 .
\end{array}$$

Set

$$\begin{aligned}
g(t) &= (t - \psi_1)(t - \psi_2)(t - \psi_3)(t - \psi_4)(t - \psi_5)(t - \psi_6) \\
&= (t - v_1)(t - \omega v_1)(t - \omega^2 v)(t - v_4)(t - \omega v_4)(t - \omega^2 v_4) \\
&= (t^3 - v_1^3)(t^3 - v_4^3) \\
& \quad t^6 - (v_1^3 + v_4^3)t^3 + v_1^3 v_4^3 .
\end{aligned}$$

Since $g(t)$ remains formally unaltered by every substitution of G_6, its coefficients belong formally to G_6, and thus are rationally expressible in terms of c_1, c_2, and c_3.

$$\begin{aligned}
v_1^3 + v_4^3 &= 2(x_1^3+x_2^3+x_3^3) - 3(x_1^2 x_2 + x_1 x_2^2 + x_1^2 x_3 + \\
&\qquad x_1 x_3^2 + x_2^2 x_3 + x_2 x_3^2) + 12 x_1 x_2 x_3 \\
&= 3(x_1^3+x_2^3+x_3^3) - (x_1+x_2+x_3)^3 + 18 x_1 x_2 x_3 . \\
&\quad 2c_1^3 - 9c_1 c_2 + 27 c_3 .
\end{aligned}$$

$$\begin{aligned}
v_1^3 v_4^3 &= [x_1^2+x_2^2+x_3^2+(\omega+\omega^2)(x_1x_2+x_1x_3+x_2x_3)]^3 \\
&= [(x_1+x_2+x_3)^2 - 3(x_1x_2+x_1x_3+x_2x_3)]^3 \\
&= [c_1^2 - 3c_2]^3 .
\end{aligned}$$

For the reduced cubic $c_1 = 0$ and

$$v_1^3 + v_4^3 = 27c_3$$

$$v_1^3 v_4^3 = - 3c_2^3 \text{ .*}$$

$$\therefore \; g(t) = t^6 - 27c_3 t^3 + 3c_2^3$$

$$g'(t) = 6t - 81c_3 t.$$

Set

$$\lambda(t) = g(t)\left[\frac{q_1}{t-\psi_1} + \frac{q_2}{t-\psi_2} + \frac{q_3}{t-\psi_3} + \frac{q_4}{t-\psi_4} + \frac{q_5}{t-\psi_5} + \frac{q_6}{t-\psi_6}\right]$$

Taking $\psi_1 \equiv \psi$ for t,

$$\lambda(\psi_1) = (\psi_1-\psi_2)(\psi_1-\psi_3)(\psi_1-\psi_4)(\psi_1-\psi_5)(\psi_1-\psi_6)q_1$$

$$= g'(\psi_1)q_1$$

$$q_1 = \frac{\lambda(\psi_1)}{g'(\psi_1)}$$

or $v_4 = \dfrac{\lambda(v_1)}{g'(v_1)}$.

We now desire to express the coefficients of $\lambda(t)$ rationally in terms of the c's, as we did the coefficients of $g'(t)$.

We know that this is possible because since $\lambda(t)$ remains unaltered formally by every substitution of G_6, its coefficients belong formally to G_6 and hence are rationally expressible in terms of the c's.

$$\lambda(t) = v_4(t - \omega v_1)(t - \omega^2 v_1)(t - v_4)(t - \omega v_4)(t - \omega^2 v_4)$$

$$+\omega^2 v_4(t - v_1)(t - \omega^2 v_1)(t - v_4)(t - \omega v_4)(t - \omega^2 v_4)$$

$$+\omega v_4(t - v_1)(t - \omega v_1)(t - v_4)\; t - \omega v_4)(t - \omega^2 v\;)$$

$$+ v_1(t - v_1)(t - \omega v_1)(t - \omega^2 v_1)(t - \omega v_4)(t - \omega^2 v_4).$$

$$+\omega^2 v_1(t - v_1)(t - \omega v_1)(t - \omega^2 v_1)(t - v_4)(t - \omega^2 v_4).$$

$$+\omega v_1(t - V_1)(t - \omega V_1)(t - \omega^2 v_1)(t - v_4)(t - \omega v_4).$$

* In this case the result is complete at this point. This is merely accidental and is not the case in general.

Simplifying,

$$\begin{aligned}\lambda(t) = {} & v_4(t^2+v_1 t+v_1^2)(t^3-v_4^3)\\ & +\omega^2 v_4(t^2+\omega v_1 t+\omega^2 v_1^2)(t^3-v_4^3)\\ & +\omega v_4(t^2+\omega^2 v_1 t+\omega v_1^2)(t^3-v_4^3)\\ & +v_1(t^3-v_1^3)(t^2+v_4 t+v_4^2)\\ & +\omega^2 v_1(t^3-v_1^3)(t^2+\omega v_4 t+\omega^2 v_4^2)\\ & +\omega v_1(t^3-v_1^3)(t^2+\omega^2 v_4 t+\omega v_4^2).\\ = {} & 6v_1 v_4 t^4 - 3v_1 v_4(v_1^3+v_4^3)t\\ = {} & 6(-3c_2)t^4 - 3(-3c_2)27c_3 t\\ = {} & -18c_2 t^4 + 243c_2 c_3 t.\end{aligned}$$

$$\lambda(v_1) = -18c_2 v_1^4 + 243c_2 c_3 v_1.$$

$$g'(v_1) = 6v_1^5 - 81c_3 v_1^2.$$

and we have,

$$v_4 = -\frac{18c_2 v_1^4 + 243c_2 c_3 v_1}{6v_1^5 - 81c_3 v_1^2} = -\frac{3c_2}{v_1} \quad *$$

19. Lagrange's theorem is apt to be misinterpreted if special attention is not given to the above process. Evidently the theorem must fail when $g'(\psi_1)=(\psi_1-\psi_2)\cdots(\psi-\psi_n)$ is identically equal to zero. As long as $x_1, x_2, \ldots x_n$ are independent variables, $\psi_1, \psi_2, \cdots \psi_n$ are all formally distinct and the theorem holds . But if we are

* In Chap. I. Art.8 p. 16 we stated that having chosen v_1 arbitrarily we must choose v_4 so that $v_1 v_4 = -3c_2$. We see now that having chosen v_1 arbitrarily, v_4 is completely determined since it is rationally expressible in terms of v_1. Thus also in Chap. II Art.14 p. 27 having chosen arbitrarily one of the v's, the others are completely determined since they are rationally expressible in terms of that one.

dealing with a special equation, two or more of the functions $\psi_1, \psi_2, \cdots \psi_n$ may be *numerically* equal, in which case $g'(\psi)$ would vanish and Lagrange's theorem could no longer be applied to the function ψ. Thus in order for the theorem to hold true without any exception it should be stated more exactly:

If a rational function $\phi(x_1, x_2, \dots x_n)$ remains formally unaltered by all those substitutions which leave another rational function $\psi(x_1, x_2, \dots x_n)$ formally unaltered and if the conjugates of ψ under $G_{n!}$ are numerically distinct, then ϕ is rationally expressible in terms of ψ and $c_1, c_2, \dots c_n$.

If in the above theorem ψ belongs formally to $G_1(1)$ we have the following corollary: Every rational function of $x_1, x_2, \dots x_n$ is rationally expressible in terms of any numerically $n!$-valued function.

20. When $x_1, x_2, \dots x_n$ are specific numbers it is always possible to construct a rational function of them which takes on $n!$ numerically distinct values under $G_{n!}$ Such a function is

$$v_1 = m_1 x_1 + m_2 x_2 + \dots + m_n x_n$$

where $x_1, x_2, \dots x_n$ are distinct as usual and where the m's are properly chosen.* For let us apply to v_1 any two substitutions of $G_{n!}$, say a and b, getting v_a and v_b respectively. We do not want to choose the m's so that $v_a = v_b$. The substitutions of $G_{n!}$ would

* Dickson: Art. 56.

furnish $n! \frac{(n! -1)}{2}$ relations of the form $v_s = v_t$. We may solve these relations to find the m's which would satisfy them and upon forming the function v_1 we avoid these values for the m's, which are finite in number.

Furthermore, given H a subgroup of G we can always construct a rational function belonging formally to H and whose conjugates under G are numerically distinct. Such a function is

$$\varphi = (r - v_1)(r - v_2) --- (r - v_k)$$

where r is a properly chosen quantity and $v_1, v_2, \cdot\cdot v_k$ are the functions derived from v_1 by applying the substitutions of H.* For applying to φ all the substitutions of G we would get a finite number of formally distinct φ's,—namely μ formally distinct φ's, where μ is the index of H under G. We do not want to choose r so that any two of these formally distinct φ's are equal. Thus we have $\frac{\mu(\mu- 1)}{2}$ relations to avoid. We may solve these relations to find the values of r which would satisfy them and upon forming the function φ we avoid these values for r, which are finite in number.

21. Rational Functions Belonging to a Group. Such a function as φ, which belongs formally to a subgroup H of G and whose conjugate values under G are numerically distinct, we shall henceforth say "belongs to the group H under G." We shall say a rational function "belongs to a group H" when the function belongs formally to H

* Dickson : Art. 70. Art. 25.

and it conjugates under the next higher* group are numerically distinct.**

It is to be observed that the expression "belongs to a group H" applies to all those functions which "belong to a group H under G" and others which do not belong to H under G (providing G is not the next higher group of H). Thus if a function "belongs to H under G" it "belongs to H", but the converse is not necessarily true.

Unless otherwise specified we shall exclude from our discussion all functions belonging formally to a group but whose conjugates under the next higher group are not numerically distinct.

22. Generalization of Lagrange's Theorem. Given a rational function $\psi(x_1, x_2, \dots x_n)$ which belongs to a subgroup H of G under G and a rational function $\chi(x_1, x_2, \dots x_n)$ which belong to G under $G_{n!}$. Then if $\varphi(x_1, x_2 \dots x_n)$ is a rational function which is unchanged formally by all the substitutions of H, φ can be expressed rationally in terms of ψ, χ, c_1, c_2, ... c_n.

$$\begin{tikzcd} G \arrow[d, dash, "\mu"'] \\ H \end{tikzcd}$$

χ belongs to G under $G_{n!}$.

ψ belongs to H under G.

φ is formally unchanged by H.

Let the index of H under G be μ.

Writing the substitutions of G with those of H in the first row:

* G is the next higher group of $H(H \not\equiv G)$ if H is a subgroup of no group of lower order than G(excluding the case where H is a subgroup of itself).

** This idea is different from that usually expressed by "belongs to a group". Dickson Art. 69.

$$\begin{array}{l|l|l}
1\ ,\ h_2,\ \ldots\ h_p & \psi = \psi_1 & \varphi = \varphi_1 \\
g_2,\ h_2 g_2,\ \ldots\ h_p g_2 & \psi_{g_2} = \psi_2 & \varphi_{g_2} = \varphi_2 \\
\cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot & \cdot\ \cdot\ \cdot & \cdot\ \cdot\ \cdot \\
g_\mu,\ h_2 g_\mu,\ \ldots\ h_p g_\mu & \psi_{g_\mu} = \psi_\mu & \varphi_{g_\mu} = \varphi_\mu
\end{array}$$

Under the substitutions of G,the function ψ will take on μ numerically distinct values, $\psi_1, \psi_2, \cdot\cdot \psi_\mu$; the function φ need not take on μ numerically distinct values since φ belongs to a group of which H is a subgroup.

Set

$$g(t) = (t - \psi_1)(t - \psi_2) \ --- \ (t - \psi_\mu).$$

$$\lambda(t) = g(t)\left[\frac{\varphi_1}{t-\psi_1} + \frac{\varphi_2}{t-\psi_2} + \cdots + \frac{\varphi_\mu}{t-\psi_\mu}\right].$$

The coefficients of $\lambda(t)$ belong formally to G and by Lagrange's theorem (Art. 19) are rationally expressible in terms of c_1, c_2, -- c_n and any rational function χ belonging to G under $G_{n!}$.

$$\lambda(t) = R\left[c_1,\ c_2,\ \ldots\ c_n,\ \chi,\ t\right].$$

Putting $\psi_1 = \psi$ for t,

$$\begin{aligned}
\lambda(\psi_1) &= R\left[c_1,\ c_2,\ \ldots\ c_n,\ \chi,\ \psi_1\right] \\
&= (\psi_1 - \psi_2)(\psi_1 - \psi_3)\cdots(\psi - \psi_\mu)\varphi_1 \\
&= g'(\psi_1)\varphi_1
\end{aligned}$$

Therefore, $\varphi = \dfrac{R\left[c_1,\ c_2,\ \ldots\ c_n, \psi, \chi\right]}{g'(\psi)} = \text{Rat. Func.}\left[c_1 c_2 .. c_n, \chi, \psi\right]$

23. From the above generalization it easily follows that if a rational function φ is formally unchanged by the substitutions of a group H, then φ is rationally expressible in terms of c_1, c_2, ... c_n and rational functions belonging

to successive subgroups of $G_{n!}$ each under the preceding subgroup, H being the last subgroup taken. For example, suppose φ is formally unaltered by G'''' and that conditions are as indicated in the diagram.

$G_{n!}$ $c_1 c_2 \cdots c_n$

G' ω belongs to G' under $G_{n!}$

G'' χ belongs to G'' under G'

Δ " " " " $G_{n!}$

G''' ψ belongs to G''' under G''

Φ " " " " $G_{n!}$

G'''' η belongs to G'''' under G'''

By the generalized theorem we have

$$\varphi = R_1(\eta, \Phi, c_1, c_2, ---, c_n).$$

But also by this theorem,

$$\Phi = R_2(\psi, \Delta, c_1, c_2, ---, c_n).$$

and $\Delta = R_3(\chi, \omega, c_1, c_2, ---, c_n)$.

Therefore $\varphi = R_4(\eta, \psi, \chi, \omega, c_1, c_2, ---, c_n)$.

(Notice that Φ and Δ are used only for the purpose of the proof and need not be computed in the application of the theorem).

24. In order to understand clearly that our generalized theorem says more than the ordinary theorem, suppose we have such a case as the following:

G_6 $\qquad$ $x_1 = -x_2$

$\qquad$ $x_2 \neq x_3$

G_2 $[1\ (23)]$

x_1

G_1 $x_1^2 + 2x_2^2 + 3x_3^2.$

Under the conditions of the problem, x_1 belongs to G_2 under G_6, and $x_1^2 + 2x_2^2 + 3x_3^2$ belongs to G_1 under

G_2 but not under G_6.

If $\varphi(x_1,x_2,x_3)$ is any rational function formally unaltered by G_1, by our generalized Lagrange theorem we may say

$$\varphi = \text{Rat. Func. } (x_1^2 + 2x_2^2 + 3x_3^2\ ,\ x_1,\ c_1, c_2, c_3).$$

We observe that the ordinary Lagrange theorem cannot be applied here since the conjugates of $x_1^2+2x_2^2+3x_3^2$ under G_6 are not numerically distinct, i.e.

$$\varphi \neq \text{Rat. Func. } (x_1^2 + 2x_2^2 + 3x_3^2\ ,\ c_1, c_2, c_3).$$

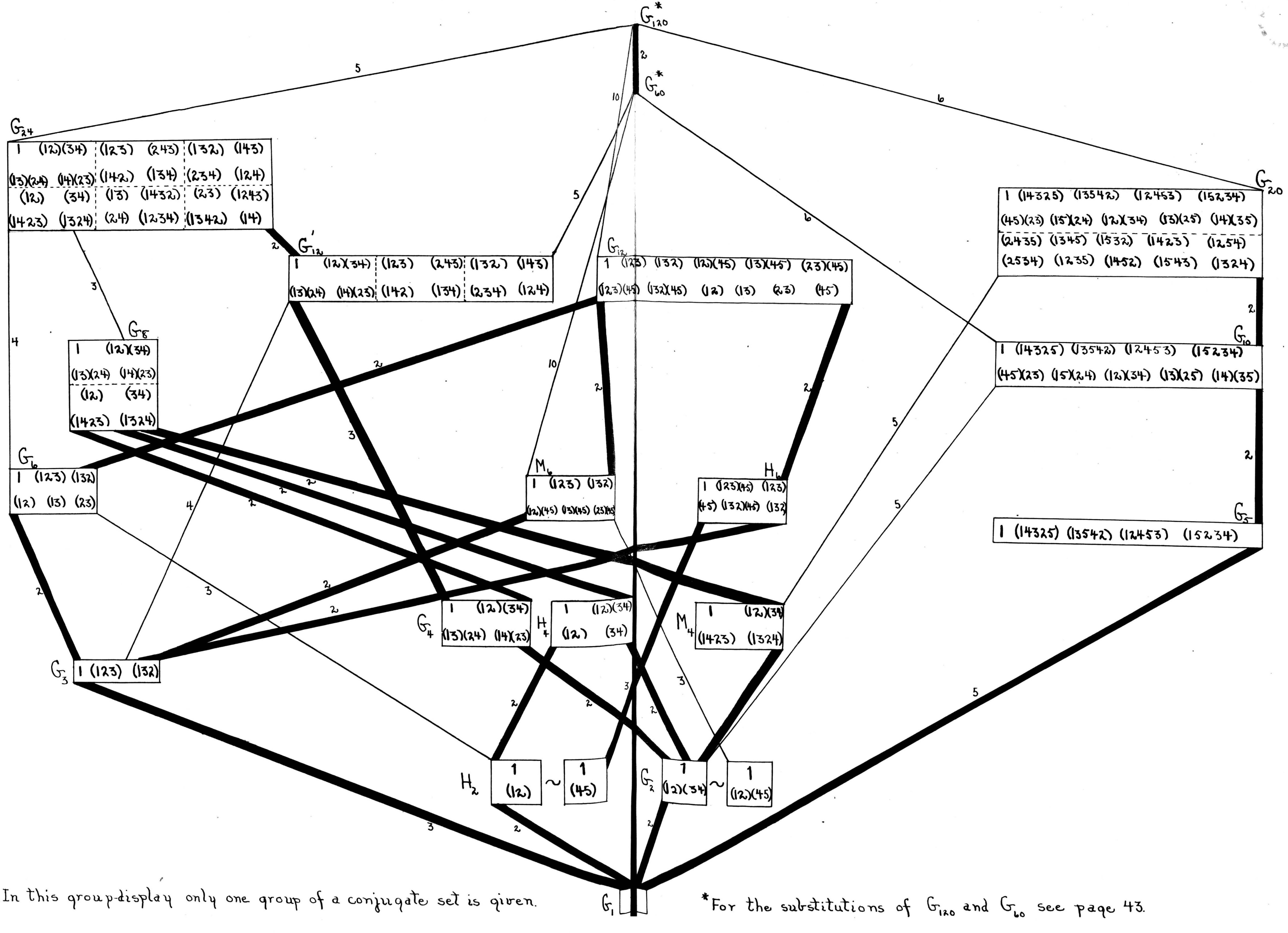
25. <u>The Biquadratic Equation</u>. From the display of G_{24} we observe that we can pick out five direct series of groups leading from G_{24} to G_1 in which all the indices in the series are less than four. (Art. 16). The path $G_{24}\overset{2}{\overline{\hspace{3em}}}G_{12}\overset{3}{\overline{\hspace{3em}}}G_{4}\overset{2}{\overline{\hspace{3em}}}G_{2}\overset{2}{\overline{\hspace{3em}}}G_{1}$ affords a chain of binomial equations of prime degree, since each group is a self-conjugate group of prime index inder the preceding group. Or we may pass from G_{24} to G_8 by the solution of a non-binomial cubic and from G_8 to G_1 in four direct ways by the solution of binomial equations of prime degree.

26. <u>Summary of Method for Equations of any Degree</u>. By calling forth general theorems, the consideration of the biquadratic equation has enabled us to state a plan to be tried for equations of any degree. First display $G_{n!}$ and its subgroups and learn what groups are self-conjugate.

Then seek to find the value of a function belonging to each group involved, beginning with functions belonging to the higher groups and going down by any path. We generally go to $G_{[1]}$ and from there to the group to which the roots belong, for as soon as a numerically n! - valued function is known the roots are known, since by Lagrange's theorem they are rationally expressible in terms of that function. We observe that our scheme merely reduces the solution of the given equation to the solution of a chain of resolvent equations. It is evident that this reduction will be a real simplification if the degrees of the resolvent equations are less than n, or if the chain of resolvent equations should turn out to be binomial . If a resolvent equation does not turn out to be binomial but has a rational linear factor, we can find at least one of its roots* and thus proceed along the path.

27. The Quintic Equation. Upon displaying G_{120} and its subgroups (See following page), we observe that the alternating group and the identical group are the only self-conjugate subgroups of G_{120}. In case of the general equation the symmetric functions are the only rational functions of the roots which are rationally expressible in terms of the coefficients, and thus we must start from the symmetric group. Over any path from G_{120} to G_1 we must solve a non-binomial equation of degree

* The question of the reducibility of an equation will be treated in Chap. V.



Note: In this group-display only one group of a conjugate set is given.

*For the substitutions of G_{120} and G_{60} see page 43.

five or higher. Our method then would seem to fail. However, in case of a special equation, we may know the value of a function belonging to some group besides G_{120} or G_{60}. If so, we see from the group display that we could proceed through a chain of binomial resolvents of prime degrees to $G_1[1]$ and thus solve the equation by our method.

G_{120}

1*	(12345)*	(5234)	(134)*	(15)(23)*
	(12354)*	(5243)	(143)*	(15)(24)*
	(12435)*	(5324)	(523)*	(15)(34)*
	(12453)*	(5342)	(532)*	(23)(45)*
	(12543)*	(5423)	(524)*	(24)(35)*
	(12534)*	(5432)	(542)*	(25)(34)*
	(13245)*	(1534)	(534)*	(123)(45)
	(13254)*	(1543)	(543)*	(132)(45)
	(13425)*	(1354)	(153)*	(124)(35)
	(13452)*	(1345)	(135)*	(142)(35)
	(13524)*	(1453)	(154)*	(134)(25)
	(13542)*	(1435)	(145)*	(143)(25)
	(14235)*	(1254)	(125)*	(135)(24)
	(14253)*	(1245)	(152)*	(153)(24)
	(14325)*	(1524)	(12)	(145)(23)
	(14352)*	(1542)	(13)	(154)(23)
	(14523)*	(1425)	(14)	(125)(34)
	(14532)*	(1452)	(15)	(152)(34)

(15234)*
(15243)*
(15324)*
(15342)*
(15423)*
(15432)*
(1234)
(1243)
(1324)
(1342)
(1423)
(1432)

(1235)
(1253)
(1325)
(1352)
(1523)
(1532)
(123)*
(132)*
(124)*
(142)*
(234)*
(243)*

(23)
(24)
(25)
(34)
(35)
(45)
(12)(34)*
(12)(35)*
(12)(45)*
(13)(24)*
(13)(25)*
(13)(45)*
(14)(23)*
(14)(25)*
(14)(35)*

(234)(15)
(243)(15)
(235)(14)
(253)(14)
(245)(13)
(254)(13)
(345)(12)
(354)(12)

Note: Those substitutions marked * constitute G_{60}.

CHAPTER IV.

The Group of an Equation.

28. Domain of Rationality. In the foregoing chapters we have said nothing concerning the nature of the quantities to be allowed to appear in the solution of an equation. It is evident that this question is of prime importance when the solvability of an equation is under consideration. For instance, the equation $x^2 - 2 = 0$ is not solvable if we allow only rational numbers to appear in the solution, while it is solvable if we allow $\sqrt{2}$ to appear in the solution.

In the study of an equation we naturally admit into consideration the coefficients and may admit other quantities. The quantities $R', R'', --- R^k$ which we admit together with all quantities derived from them by a finite number of additions, subtractions, multiplications, and divisions (not including division by zero) constitute the domain of rationality $R\ (R', R'', --- R^k)$. The simplest domain of rationality is the domain of rational numbers and is designated by $R(1)$.

29. In Chapters I, II, and III we have discussed the solution of equations, aided by the group-display. For any given equation and any given domain R, however, there is one group whose properties are of such importance in the study of the equation that this group is called "the" group of the equation for domain R. This chapter will be devoted to the development of this notion, but

the method of development will not be that of extant works on the subject.

30. Let $f(x) = 0$ be an equation of degree n with coefficients in a domain R and let us designate its roots by x_1, x_2, --- x_n. *If one rational function** *$\psi(x_1, x_2, --- x_n)$ which belongs to a group G under $G_{n!}$*** *lies in a domain R we will say that "G lies in R".*

31. *Theorem: If a group G lies in R, all rational functions belonging formally to G** lie in R.*

Since G lies in R there is a rational function $\psi(x_1 x_2 --- x_n)$ which belongs to G under $G_{n!}$ and which lies in R (Art. 30). It now easily follows from Lagrange's theorem that all rational functions belonging formally to G lie in R, since they are rationally expressible in terms of ψ and c_1, c_2, --- c_n.

32. *Theorem: If one rational function $\Phi(x_1, x_2, --- x_n)$ which belongs formally to a group G does not lie in R, no rational function belonging to G under $G_{n!}$ lies in R.*

Let $\varphi(x_1, x_2, --- x_n)$ be any rational function ($\varphi \neq \Phi$) which belongs to G under $G_{n!}$. By

* In the Galois Theory when we say a function is a rational function of x_1, x_2, --- x_n, we always mean a rational function with coefficients in the domain of rationality.

** For the definition of "belongs to a group G under $G_{n!}$" and for the distinction between this and "belongs to G" see Chap. III Art. 21. The expression "belonging formally to G" applies both to functions "belonging to G" and functions belonging formally to G, but whose conjugates under the next higher group are not numerically distinct.

Lagrange's theorem Φ=Rat. Func. (φ, c_1, c_2, ... c_n) . If φ lies in R, Φ lies in R since it is rationally expressible in terms of φ and the c's, which is a contradiction. Therefore φ does not lie in R, and our theorem is proved.

The above theorem may also be stated as follows: *If one rational function which belongs formally to a group G does not lie in R, G does not lie in R.*

33. *Theorem*: *If a group G lies in R, all supergroups* of G lie in R.*

Let φ (x_1, x_2, ... x_n) be any rational function belonging to any supergroup of G under $G_{n!}$. By Lagrange's theorem φ can be expressed rationally in terms of c_1, c_2, ... c_n and any rational function ψ (x_1, x_2, ... x_n) which belongs to G under $G_{n!}$. Since ψ and the c's lie in R, φ lies in R and hence the supergroup lies in R.

34. *Theorem*: *If a group G does not lie in R, no subgroup of G lies in R.*

For suppose any subgroup H of G lies in R. Then by Art. 33 all supergroups of H lie in R ,and hence G lies in R, which contradicts hypothesis. Therefore H does not lie in R.

* By a "supergroup of G" we mean a group of which G is a subgroup. Notice that by this definition G is a supergroup of itself.

35. Theorem: If two groups lie in R their greatest common subgroup lies in R.

Suppose G and M are two groups which lie in R. Either (1). G is a subgroup or supergroup of M or (2). G is not a subgroup or supergroup of M.

Case (1). If G(orM) is a subgroup of M (or G) G(or M) itself is the greatest common subgroup of G and M and by hypothesis lies in R.

Case (2). If G is not a subgroup or supergroup of M, G and M have a greatest common subgroup H which consists of all the substitutions common to G and M*.

Let $\varphi_1(x_1 x_2, --- x_n)$ and $\varphi_2(x_1, x_2, --- x_n)$ be rational functions belonging respectively to G and M under $G_{n!}$.

Form the function

$\psi = \varphi_1 + K\varphi_2$ (Where K is a quantity to be chosen later).

The function ψ is formally unchanged by any substitution of H. Any substitution which belongs to G or M and not to both changes ψ formally, since it changes one of the φ's formally and not the other. Let us find for what values of K the function ψ would be left numerially unchanged by any substitution which belongs to G or M and not to both.

Upon applying to ψ a substitution which belongs

* For proof that all the substitutions common to two groups form a group see Netto: Theory of Substitutions (Trans. by F. N. Cole) Art. 44 p. 47.

to G but not to M, φ_1 remains formally unaltered but φ_2 becomes formally altered, and call this new function φ_2'. If ψ remains numerically unaltered, we have

$$\varphi_1 + K\varphi_2 = \varphi_1 + K\varphi_2'$$

$$K = \frac{\varphi_1 - \varphi_1}{\varphi_2 - \varphi_2'} = 0.$$

Similarly, if ψ remains numerically unaltered upon applying a substitution which belongs to M but not to G, we have

$$\varphi_1 + K\varphi_2 = \varphi_1' + K\varphi_2$$

$$K = \frac{\varphi_1' - \varphi_1}{\varphi_2 - \varphi_2} = \infty.$$

Thus if we choose K any definite quantity not zero, ψ will be numerically altered by any substitution which belongs to G or M and not to both.

We now desire to find for what value of K the function ψ is left numerically unaltered by any substitution which belongs to neither G nor M. Upon applying to ψ any such substitution, both φ_1 and φ_2 are formally altered and let us call the new functions φ_1' and φ_2' respectively. If ψ remains numerically unaltered, we have

$$\varphi_1 + K\varphi_2 = \varphi_1' + K\varphi_2'$$

and $$K = \frac{\varphi_1 - \varphi_1'}{\varphi_2' - \varphi_2}.$$

Thus we can apply to ψ all the substitutions which are in neither G nor M and upon each substitution we can ascertain the value of K which would leave ψ numerically unaltered by the substitution. Since there is one and only one value of K for each substitution,

these values are finite in number. Thus we can choose K some rational number not zero which is equal to none of these values. Then $\varphi_1+K\varphi_2$ is a rational function which belongs to H under $G_{n!}$ and lies in R. Therefore H lies in R.

36. <u>Theorem: If a group G lies in R and has a subgroup H to which there belongs under G a rational function $\varphi(x_1, x_2, --- x_n)$ which lies in R, then H lies in R.</u>

G Φ belongs to G under $G_{n!}$ and lies in R.

H φ belongs to H under G and lies in R.

χ belongs to H under $G_{n!}$.

Let Φ and χ be rational functions which belong respectively to G and H under $G_{n!}$.

By our generalized Lagrange Theorem (Chap. III Art. 22.)

$$\chi = \text{Rat. Func. } (\varphi, \Phi, c_1, c_2, --- c_n)$$

Since φ, Φ, and the c's lie in R, χ lies in R, and hence H lies in R.

From this theorem we observe that although a group H may have a rational function belonging to it under a group G and lying in R, we cannot conclude that H lies in R unless we know that G lies in R.

37. *Definition of the Group of an Equation. If a group G lies in R and has no maximum* subgroup which lies in R, we define G to be the group of the equation for domain R.*

38. *Every Equation Has a Group.* It is evident that every equation has a group for any given domain R including its coefficients. For since c_1, c_2, --- c_n belong to $G_{n!}$, $G_{n!}$ lies in R. Proceeding from group to subgroup and testing each successively we will surely find a group which lies in R and has no maximum subgroup which lies in R. If all the groups lie in R, the identity group meets this requirement and is the group of the equation.

39. Making use of the theorems of Arts. 33, 34, 35 we are able to deduce the following important theorem concerning the relation of groups which lie in R to a group which satisfies the above definition of the group of an equation.

Theorem: If G satisfies the definition of the group of an equation for a given domain R, all supergroups of G and no other groups lie in R.

We have shown (Art. 33) that if a group lies in

* A subgroup H of G ($H \not\equiv G$) is a maximum subgroup of G if it is not contained in a larger subgroup of G. (excluding the case where G is a subgroup of itself).

R, all its supergroups lie in R. By hypothesis G lies in R. Therefore all supergroups of G lie in R.

It now remains for us to show that no group which is not a supergroup of G lies in R. Suppose M is a group which is not a supergroup of G and which lies in R. Then G and M have a greatest common subgroup H, which is not G and which consists of all the substitutions common to G and M. Now if two groups lie in R, their greatest common subgroup lies in R(Art.35). It follows that H lies in R. But this is absurd, for by hypothesis no maximum subgroup G' of G lies in R and by Art. 34 no subgroup of G' lies in R, and hence no subgroup of G(except itself) lies in R. Thus our hypothesis concerning M cannot hold, and our theorem is proved.

40. The Group of an Equation is Unique. In Art. 38 we saw that any equation has at least one group for a given domain R including its coefficients. It now easily follows that any equation has only one group for a domain R.

For let G and L be any two groups which satisfy the definition of the group of an equation. Then G and L both lie in R. Since G lies in R, it is a supergroup of L (Art.39). Similarly, since L lies in R, it is a supergroup of G. It follows that

G and L must be identical.

41. The Ordinary Galoisian Definition of the Group of an Equation. We have defined the group of an equation for domain R as that group which lies in R and has no maximum subgroup which lies in R. Our definition of the group of an equation differs from the ordinary Galoisian definition which is arrived at as follows:*

Let there be given an equation of degree n with coefficients belonging to domain R.

Form the equation

$$F(v) \equiv (v - v_1)(v - v_2) ---(v - v_{n!}) = 0$$

where $v_1 \equiv m_1 x_1 + m_2 x_2 + ---+ m_n x_n$, the m's being chosen in R and such that v_1 takes on n! numerically distinct values under the n! substitutions on x_1, x_2, --- x_n.

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 $F_0(v) = 0$ is an irreducible equation called the "Galois resolvent" of the given equation.

Let the roots of the Galois resolvent be denoted by v_1, v_a, --- v_l. The substitutions by which they are derived from v_1, namely 1,a, --- l

* Dickson: Arts. 56, 57, 60.

** If F(v) can be decomposed into factors of lower degree such that the coefficients of the factors are numbers belonging to domain R, then F(v) is called reducible in R.

form a group, called the group of *the given equation for domain R*.

42. Let us call G the group of a given equation of degree n for domain R according to our definition and M the group for domain R according to the Galoisian definition. We will proceed to show that G and M are identical.

In the first place, we know that the coefficients of the Galois resolvent $F_0(v)=0$ belong to M under $G_{n!}$ and also lie in R, since they are integral, rational functions of the m's and c's. It follows that M lies in R.

Now we have shown that all supergroups of G and no other groups lie in R. (Art.39). Therefore M is either a supergroup of higher order than G or is identical with G.

Let us suppose that M is a supergroup of higher order than G. Form the equation $F_G(v)=0$, taking for its roots those roots of the Galois resolvent $F_0(v)=0$ which can be derived from v_1 by the substitutions of G. The coefficients of $F_G(v)=0$ belong to G under $G_{n!}$ and therefore lie in R. Then $F_G(v)$ is a rational factor of $F_0(v)$, i. e. the Galois resolvent is reducible for domain R, which is absurd. It follows therefore that G and M must be identical.

43. *The Group of the General Equation of Degree n.* By a general equation we mean an equation whose roots

and likewise whose coefficients are independent variables. Let us find the group of the general equation of degree n for a domain R, containing the coefficients of the equation (and no other functions of the roots) and any assigned constants.

The symmetric group $G_{n!}$ lies in R since to it belong the coefficients of the equation. Now consider any subgroup H of $G_{n!}$ ($H \not\equiv G_{n!}$) and any rational function $\varphi(x_1 x_2 --- x_n)$ belonging to H under $G_{n!}$. If φ lies in R ,it is rational in the coefficients* and hence belongs to G , which is a contradiction. Since φ was any rational function belonging under $G_{n!}$ to any subgroup of $G_{n!}$(except itself), it follows that no rational function belonging under $G_{n!}$ to any subgroup of $G_{n!}$ (except itself) lies in R and hence that no subgroup of $G_{n!}$(except itself) lies in R. The group $G_{n!}$ is thus the group of the equation for domain R, since it lies in R and has no subgroup (except itself) which lies in R.

44. <u>Finding the Group of an Equation.</u> Let us consider the chain** of groups $G_{n!}$, I , H, G. Suppose we have found that I lies in R by testing a rational

* If, however the coefficients are not independent variables, there are some relations between them. In this case it is possible that a function which is formally irrational in the coefficients may by elimination by means of these relations become a rational function in the elements of the domain. The group of the equation would then be different from $G_{n!}$.

** Groups constitute a chain when each group is a subgroup of the preceding group.

function α belonging to I under $G_{n!}$. We now desire to know if H lies in R. By definition H lies in R if a rational function β belongs to H under $G_{n!}$ and lies in R. However, as a result of applying our generalized Lagrange theorem we know that β need merely belong to H under I and lie in R, in order to conclude that H lies in R. (Art. 36). Having found that H lies in R, similarly G lies in R if one rational function belonging to G under H lies in R. On the other hand, if one rational function belonging formally to H does not lie in R, H does not lie in R (Art. 32). Thus to conclude that any group G lies in R, it is necessary to know that one rational function lies in R which belongs to G under a supergroup of G which lies in R; while to conclude that G does not lie in R, it is necessary to know that one rational function which belongs formally to G does not lie in R.

As long as we find successive subgroups lying in R, we may proceed along a single chain. But when we find a group not lying in R, we must continue to test the maximum subgroups of the last group found in R until we find one lying in R or find that none lie in R. If we find one lying in R, we may proceed again along a single chain until we come to a group not lying in R. Hereupon, we test as before the maximum subgroups of the last group found in R. Continuing this process we

will arrive at a group which lies in R and has no maximum subgroup which lies in R. This group of lowest order found in R is the group of the equation for R.

Instead of considering groups which belong to the same chain, it may oftentimes be simpler to consider two groups which belong to different chains, remembering that if two groups are found to lie in R their greatest common subgroup lies in R (Art.35).

In the above method we observe that it is immaterial whether or not we begin with the investigation of the nearest subgroups of $G_{n!}$. If desired, groups to be tested may be selected at random, though any information gained from a random selection would naturally influence the student in choosing groups for subsequent tests.

If we do not know the value of a function belonging formally to a group G, we consider the resolvent equation for the function between G and a supergroup M which lies in R. If the equation is binomial, we can easily solve it and find the value of the function. If the equation is not binomial, we test it for a rational linear factor*. If the equation does not have a rational linear factor, the function does not lie in R, and thus by Art. 32 the group G does not lie in R. If the equation does have a rational

* The method of doing this will be explained in Chap. V.

linear factor, it remains for us to see if the equation has distinct roots in order to find whether or not the function has distinct conjugates under M.

To find if an equation $f(x) = 0$ has distinct roots we may form the discriminant by means of a determinant of $(2n - 1)$ order.

$$f(x) = a_0x^n + a_1x^{n-1} + \dots + a_n$$

$$f'(x) = na_0x^{n-1} + (n-1)a_1x^{n-2} + (n-2)a_2x^{n-3} + \dots + a_{n-1}.$$

$$D = \left|\begin{array}{cccccc} a_0 & a_1 & a_2 \cdots & a_{n-1} & a_n & 0 \cdots \\ 0 & a_0 & a_1 \cdots & a_{n-2} & a_{n-1} & a_n \cdots \\ \cdot & \cdot & \cdot\cdots & \cdot & \cdot & \cdot\cdots \\ na_0 & (n-1)a_1 & (n-2)a_2 \cdots & a_{n-1} & 0 & 0 \cdots \\ 0 & na_0 & (n-1)a_1 \cdots & 2a_{n-2} & a_{n-1} & 0 \cdots \\ \cdot & \cdot & \cdot\cdots & \cdot & \cdot & \cdot\cdots \\ \cdot & \cdot & \cdot\cdots & \cdot & \cdot & \cdot\cdots \end{array}\right| \begin{array}{l} \left.\begin{array}{l} \\ \\ \\ \end{array}\right\} n-1 \text{ rows.} \\ \left.\begin{array}{l} \\ \\ \\ \\ \end{array}\right\} n \text{ rows.} \end{array}$$

D will vanish if $f(x) = 0$ has equal roots.*

If the roots are distinct, the function belongs to G under M and will serve our purpose. If the roots are not distinct, the function does not belong to G under M and under such conditions we must choose another function if we are to pass directlyfrom M to G. If M is not the next higher group of G it may be that the function belongs to G under a group of lower order than M

* See Cajori: Art. 76.

The method for determining whether or not the roots of an equation are distinct by finding the greatest common divisor of f(x) and f'(x) has been explained in a footnote (p. 14.)

and in that case it together with other functions belonging to subgroups of M would enable us to pass by steps from M to G.

45. The problem of finding the group of an equation is most simple if the nature of the roots is known. Let us consider the quadratic and cubic equations in this connection.

I. Quadratic Equation.

Case A. Given: x_1 and x_2 lie in R.

Then G_2 lies in R

G_1 lies in R

and G_1 is the group for R.

Case B. Given: x_1 and x_2 do not lie in R.

Then G_2 lies in R.

G_1 does not lie in R

and G_2 is the group for R.

II. Cubic Equation.

Case A. Given: x_1, x_2, and x_3 lie in R.

Then G_6 lies in R.

G_3 lies in R.

G_2 lies in R.

G_1 lies in R.

and G_1 is the group for R.

Case B. Given: x_1 and x_2 lie in R, but x_3 does not lie in R.

This is impossible for we have the relation,

$$c_1 = x_1 + x_2 + x_3$$

$$x_3 = c_1 - (x_1 + x_2)$$

which shows that x_3 is the difference of two quantities which lie in R and hence must lie in R.

Case C. Given: x_1 lies in R, but x_2 and x_3 do not lie in R.

Then G_6 lies in R.

G_2' lies in R.

G_1 does not lie in R.

and G_2' is the group for R.

Case D. Given: x_1, x_2, and x_3 do not lie in R.

Then G_6 lies in R.

G_3 <u>may</u> lie in R.

G_2 does not lie in R

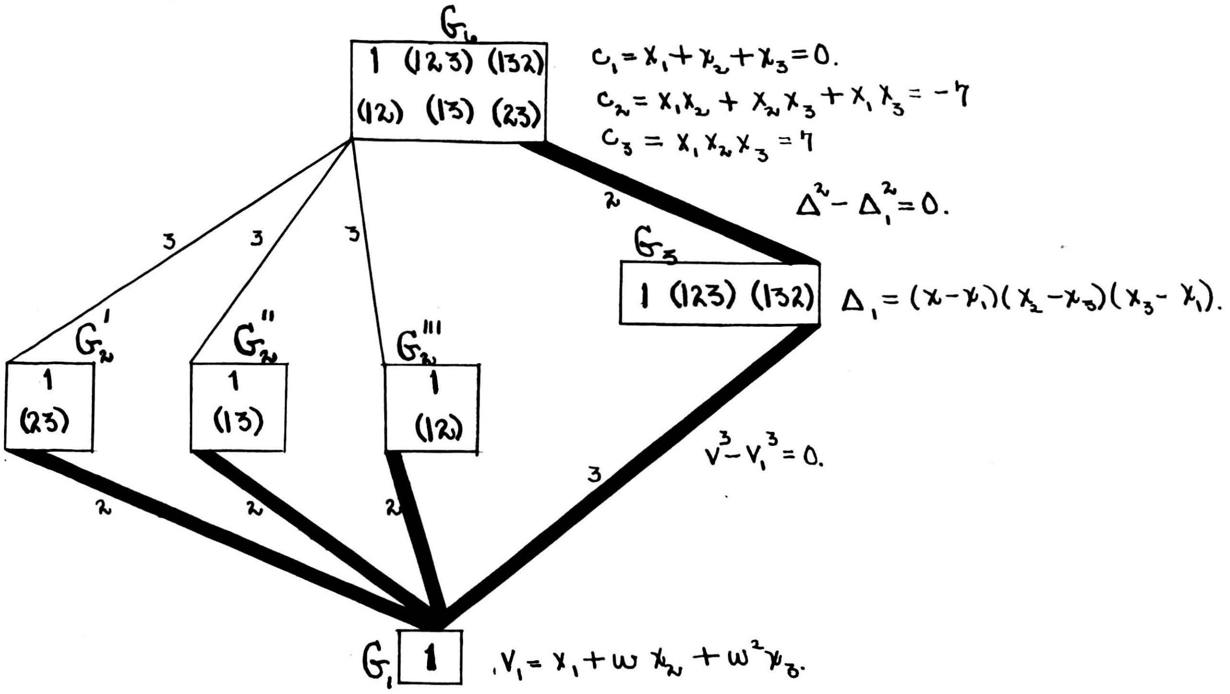
G_1 does not lie in R.

and the group for R is G_6 or G_3.

To test whether or not G_3 lies in R, solve the resolvent equation for the function $\Delta_1 = (x_1 - x_2)(x_2 - x_3)(x_3 - x_1)$. If Δ_1 lies in R, the group for R is G_3, otherwise the group is G_6.

46. The problem of finding the group of an equation becomes more complex when the roots of the equation are unknown. As an illustration let us find the group of the cubic equation

$x^3 - 7x+7 = 0$ for domain R(1).



The symmetric group lies in R, since to it belong the coefficients.

Let us now see if G_3 lies in R. To do this we must solve the resolvent equation

$$\Delta^2 - \Delta_1^2 = 0$$

Substituting $\Delta_1^2 = c_1^2 c_2^2 - 4c_1^3 c_3 - 4c_2^3 + 18c_1c_2c_3 - 27c_3^2$ *

$= 0 - 0 + 1372 + 0 - 1323$

$= 49.$

we have

$$\Delta^2 - 49 = 0$$

$$\Delta = \pm 7.$$

* For the derivation of this expression see Chap. II. Art. 10.

Since Δ lies in R and belongs to G_3 under G_6, G_3 lies in R.

It now remains to investigate G_1. If G_1 lies in R., all the roots of the given equation must lie in R. Now a rational root of an equation of the form $x^3 - 7x + 7 = 0$ must be an integer.* By trial we find that ±1 and ±7 are not roots, and thus G_1 does not lie in R. The group of the equation, therefore, is G_3.

47. Reduction of the Group of an Equation by Adjunction. For a given domain R, the group of an equation is completely determined. It is evident, however, that if we change the domain of rationality the group of the equation may undergo a corresponding shift.

Suppose we have found that G is the group of a given equation for domain $R = (R', R'', \dots R^k)$ where $R', R'', \dots R^k$ are certain constants or variables including the coefficients of the equation. Take H any subgroup of G ($H \neq G$) and ψ any rational function of the roots belonging to H under G. By hypothesis ψ does not lie in R. Now adjoin ψ to domain R. The group H lies in the extended domain $(\psi, R', R'', \dots R^k)$ since ψ belongs to H and lies in the domain (Art. 36).

Furthermore, no subgroup of H (except itself) lies in domain $(\psi, R', \dots R^k)$. For suppose H' is

[*] Hawkes: Advanced Algebra Art. 178.

a subgroup of $H(H' \neq H)$ which lies in $(\psi, R', \dots R^k)$. Then any rational function Φ belonging to H' under H lies in $(\psi, R', \dots R^k)$ and can be expressed rationally in terms of ψ, R', ... R^k.

$$\Phi = \text{Rat. Func. } (\psi, R', R'', \dots R^k).$$

By hypothesis Φ cannot be expressed in terms of R', R'', ... R^k alone; for if it could, H' would lie in domain $(R', R'', \dots R^k)$ [See Art. 36].

From the above relation we see that Φ is formally unaltered by any substitution which leaves ψ formally unaltered; so that the group to which Φ belongs must contain that to which ψ belongs, i. e. H' must contain H. This is absurd, for by hypothesis H' is a subgroup of H $(H' \neq H)$. Therefore H' cannot lie in domain $(\psi, R' \dots R^k)$; and H satisfies the definition of the group of the equation for domain $(\psi, R' \dots R^k)$, since it lies in the domain and has no subgroup (except itself) which lies in the domain.

We have thus shown that

By the adjunction of a rational function $\psi(x_1, x_2, \dots x_n)$ which belongs under the group G of the equation to a subgroup H of G, the group of the equation is reduced precisely to the subgroup H.

48. Solution of an Equation by Resolvent Equations. Suppose the group of a given equation is G $(G \neq G_1[1])$ for a given domain of rationality $(R', R'', \dots R^k)$. Let H be a subgroup of $G(H \neq G)$

and let ψ be a rational function belonging to H under G. Suppose we are able to solve the resolvent equation for ψ and let us adjoin ψ to the domain of rationality. The group of the equation for the enlarged domain (ψ, R', R'', ... R^{k}) is precisely H (Art. 47). Suppose we are able to solve the resolvent equation for a rational function λ which belongs to a subgroup M of H under H. Upon adjoining λ to the domain of rationality the group of the equation becomes M. Proceeding in this way we would finally reach a domain for which the group of the equation would be G, [1] , providing all the resolvent equations could be solved; * and the roots of the equation could then be expressed in terms of the quantities of this domain.

* This question is discussed in Chap. VI.

CHAPTER V.

Reducibility and Irreducibility.

49. In Chapter III Art. 26 we made the statement that if a non-binomial resolvent equation has a rational linear factor we can find at least one of its roots and thus proceed along the path. The question of the reducibility of an equation is then of prime importance in our method. Also, if the given equation is reducible we may substitute for its solution the solution of equations of lower degrees, in which case its solution would generally be much simplified.

It is evident that the terms "reducible" and "irreducible" are meaningless except when referred to some domain of rationality.* Taking the simplest case first, let us consider the ways in which we may learn whether or not an equation with rational coefficients is reducible in the domain of rational numbers R(1).

50. Reducibility for R(1). Linear Factors.

Suppose we have given the equation

$$f(x) = a_0x^n + a_1x^{n-1} + \dots + a_n = 0. \qquad \text{I.}$$

where the a's are integers.

Let us test this equation for rational linear factors. The most satisfactory method of doing this is as follows:

* See footnote page 53.

If $a_0 \neq 1$, divide equation I by a and multiply the roots by a constant so chosen as to give an equation of the form

$$x^n + c_1 x^{n-1} + \dots + c_n = 0. \qquad \text{II}$$

where the c's are integers*.

By Gauss's Lemma**, if a function has integral coefficients and can be resolved into rational factors, it can be resolved into rational factors with integral coefficients. Therefore, if equation II has a rational root, this root must be an integer and ,furthermore, from the relation which exists between the roots and coefficients of an equation, it must be a factor of c_n. Test each integral factor c of c_n by dividing equation II by x - c. If there is no remainder upon at least one of the trial divisions, then equation II has a rational root and is thus reducible for R(1).

If equation II has a rational root, equation I is reducible for R(1), since it has a rational root which can be obtained by dividing the integral root found for equation II by the constant by which the roots of equation I were multiplied.

50. Kronecker's Method of Testing Reducibility for R(1). It may be that f(x) (Art. 50) has no linear rational factors, but has factors of higher degree. When the degree of f(x) does not exceed five,

*Cajori: Arts. 29, 55.
** Cajori: Art. 127.

we can ascertain by the aid of ordinary algebra whether or not the function has factors of higher degree than unity.* However, a method which can be applied to f(x), no matter how high its degree, is that due to Kronecker, and is as follows:

Suppose we wish to see if f(x) has a rational factor of degree α ($\alpha < n$).

Assuming that f(x) has such a factor $\varphi(x)$, we write

$$f(x) = \varphi(x)\ \psi(x).$$

Select any $\alpha + 1$ integers, z_1, z_2, z_3, ... $z_{\alpha+1}$ preferably numbers such that $f(z_1)$, $f(z_2)$, $f(z_3)$ ... $f(z_{\alpha+1})$ have the least number of integral factors.

Now construct the functions

$$M_{z_1}(x) = \frac{(x - z_2)(x - z_3)\ \ldots\ (x - z_n)}{(z_1 - z_2)(z_1 - z_3)\ \ldots\ (z_1 - z_n)}$$

$$M_{z_2}(x) = \frac{(x - z_1)(x - z_3)\ \ldots\ (x - z_n)}{(z_2 - z_1)(z_2 - z_3)\ \ldots\ (z_2 - z_n)}$$

$$\cdot\ \cdot\ \ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot$$

$$M_{z_{\alpha+1}}(x) = \frac{(x - z_1)(x - z_2)\ \ldots\ (x - z_\alpha)(x - z_{\alpha+2})\ldots(x - z_n)}{(z_{\alpha+1} - z_1)(z_{\alpha+1} - z_2)\ \ldots(z_{\alpha+1} - z_\alpha)(z_{\alpha+1} - z_{\alpha+2})\ldots(z_{\alpha+1} - z_n)}$$

Observing that the function

$\varphi(z_1)\, M_{z_1}(x) + \varphi(z_2)\, M_{z_2}(x) + \ldots + \varphi(z_{z_{\alpha+1}})\, M_{z_{\alpha+1}}(x)$ is equal to $\varphi(z_1)$ for $x = z_1$, to $\varphi(z_2)$ for $x = z_2$, ... to $\varphi(z_{\alpha+1})$ for

* Cajori Art. 128.

$x = z_{\alpha+1}$, we may write

$$\varphi(z_1)M_{z_1}(x) + \varphi(z_2)M_{z_2}(x) + \ldots + \varphi(z_{\alpha+1})M_{z_{\alpha+1}}(x) \equiv \varphi(x).^*$$

We now desire to find $\varphi(z_1)$, $\varphi(z_2)$, ... $\varphi(z_{\alpha+1})$. Denote the integral factors of

$$\begin{array}{lllll}
f(z_1) & \text{by} & d_1', \; d_1'', \; d_1''', & \ldots\ldots \\
f(z_2) & '' & d_2', \; d_2'', \; d_2''', & \ldots\ldots \\
\cdot & \cdot & \cdot \quad \cdot \quad \cdot & \cdot \; \cdot \; \cdot \\
\cdot & \cdot & \cdot \quad \cdot \quad \cdot & \cdot \; \cdot \; \cdot \\
f(z_{\alpha+1}) & '' & d_{\alpha+1}', \; d_{\alpha+1}'', \; d_{\alpha+1}''', & \ldots\ldots
\end{array}$$

$\varphi(z_1)$ is one of the d_1's; $\varphi(z_2)$ is one of the d_2's ; ... $\varphi(z_{\alpha+1})$ is one of the $d_{\alpha+1}$'s.

Try some d_1 for $\varphi(z_1)$, some d_2 for $\varphi(z_2)$ ... some $d_{\alpha+1}$ for $\varphi(z_{\alpha+1})$, and ascertain by division whether or not

$$d_1 M_{z_1}(x) + d_2 M_{z_2}(x) + \ldots + d_{\alpha+1} M_{z_{\alpha+1}}(x)$$

is a factor of $f(x)$. If not, try another combination of the d's. Trying all possible combinations of the d's, we will ascertain in a finite number of trials whether or not $f(x)$ has a rational factor $\varphi(x)$ of degree α.**

52. As an illustration of the above method let us see if the equation

$$f(x) = x^5 + 5x^3 + 3x^2 + 6x + 6 = 0$$

has a rational factor of second degree.

* Bôcher: "Introduction to Higher Algebra", page 3, Theorems 3 and 4.

** Netto: Vorlesungen über Algebra Art. 50. Erster Band.

Assuming that f(x) has such a factor $\varphi(x)$ we write

$$f(x)=\varphi(x)\,\psi(x).$$

Select any 3 integers, say $z_1=1$, $z_2=0$, $z_3=-1$.

Then
$$M_{z_1}(x)=\frac{(x-0)(x+1)}{(1-0)(1+1)}=\frac{x^2+x}{2}.$$

$$M_{z_2}(x)=\frac{(x-1)(x+1)}{(0-1)(0+1)}=\frac{x^2-1}{-1}.$$

$$M_{z_3}(x)=\frac{(x-1)(x-0)}{(-1-1)(-1-0)}=\frac{x^2-x}{2}.$$

$$\varphi(1)\,\frac{x^2+x}{2}+\varphi(0)\,\frac{x^2-1}{-1}+\varphi(-1)\,\frac{x^2-x}{2}\equiv\varphi(x).$$

The integral factors of

$f(1)=21$ are 21, -21, 1, -1, 3, -3, 7, -7.

$f(0)=6$ " 6, -6, 1, -1, 3, -3, 2, -2.

$f(-1)=-3$ " 3, -3, 1, -1,

$\varphi(1)$ is one of the integral factors of f(1); $\varphi(0)$ is one of the integral factors of f(0); $\varphi(-1)$ is one of the integral factors of f(-1).

Let us try 3 for $\varphi(1)$, 2 for $\varphi(0)$, and 3 for $\varphi(-1)$. As our trial $\varphi(x)$ we have

$$\frac{3(x^2+x)}{2}+\frac{2(x^2-1)}{-1}+\frac{3(x^2-x)}{2}=x^2+2.$$

Testing x^2+2 as a divisor of f(x), we find that

$$\frac{f(x)}{x^2+2}=x^2+3x+3.$$

which shows that f(x) has a rational factor of second degree, namely x^2+2.

53. Eisenstein's Test for Irreducibility for R(1). Eisenstein has given a test for irreducibility which, when it can be applied, is much simpler than Kronecker's method. The conditions are the following:

If an equation with integral coefficients

$$f(x) = a_0 x^n + a_1 x^{n-1} + \dots + a_n = 0$$

is such that all its coefficients except a_0 are divisible by a prime number p, but a_n is not divisible by p^2, then $f(x) = 0$ is irreducible for R(1).*

Applying the above test we know immediately that such an equation as $3x^5 + 5x^4 + 15x^3 + 40x^2 + 35 = 0$ is irreducible for R(1), since all its coefficients except the first are divisible by the prime number 5 and 35 is not divisible by $(5)^2$.

54. Reducibility for an Arbitrary Domain. In the study of an equation we may admit into the investigation various irrationalities and desire to know whether or not the equation is reducible for this domain. Thus it becomes necessary to consider the reduction of an integral rational function f(x) into irreducible factors for an arbitrary domain. Following the method given by Pierpont** for the general case, we will work with a special case with the hope of making the general procedure more intelligible. For the general case, the student

* Cajori: Art. 129.

** Annals of Mathematics. Ser. 2, 1900-1901, page 31, Art. 44.

is referred to Pierpont's article.*

Let us take the function

$$f(x) = x^2 - 2\pi x + \pi^2 - 2$$

and attempt to factor it for domain R $(\pi, \sqrt{2})$.

The coefficients of f(x) are in the domain. The $\sqrt{2}$ does not appear explicitly in f(x) but may be contained implicitly since certain rational functions of $\sqrt{2}$ are rational numbers. The quantity π appears explicitly in f(x) and whenever it is contained in f(x) it must appear explicitly, since it is transcendental. Because of this property of π, we may deal with π as a variable without altering the character of our problem.

Now f(x) does not contain $\sqrt{2}$ explicitly; so we replace x successively by $t+\sqrt{2}$ and $t - \sqrt{2}$.

$$f(t+\sqrt{2}) = t^2+2(\sqrt{2}-\pi)t + \pi(\pi-2\sqrt{2}). \quad \text{(A)}$$

$$f(t-\sqrt{2}) = t^2+2(-\sqrt{2}-\pi)t + \pi(\pi+2\sqrt{2}). \quad \text{(B.)}$$

The necessity that $\sqrt{2}$ shall appear explicitly will appear later. If f already contains $\sqrt{2}$ explicitly this substitution is unnecessary.

Multiplying (A) by (B),

$$f(t+\sqrt{2})\, f(t-\sqrt{2}) = t^4 - 4\pi t^3 + (6\pi^2-8)t^2 \; (16\pi - 4\pi^3)t$$
$$+\pi^4 - 8\pi^2.$$

Notice that $\sqrt{2}$ no longer appears explicitly.

The product $f(t+\sqrt{2})\, f(t-\sqrt{2})$ is called the "norm" of f and is designated Nf.

* Annals of Mathematics. Ser. 2. Vol. 2, 1900-1901, page 31, Art. 44.

Supposing $f(t \pm\sqrt{2})$ is reducible for $R(\pi, \sqrt{2})$, we may write

$$\begin{aligned} f(t+\sqrt{2}) &= G(t+\sqrt{2}) \quad H(t+\sqrt{2}) \\ \underline{f(t-\sqrt{2})} &\underline{= G(t-\sqrt{2}) \quad H(t-\sqrt{2})} \end{aligned}$$

$$f(t+\sqrt{2})\ f(t-\sqrt{2}) = \left[G(t+\sqrt{2})\ G(t-\sqrt{2})\right]\left[H(t+\sqrt{2})\ H(t-\sqrt{2})\right].$$

or $Nf = NG \cdot NH.$ (1)

The functions Nf, NG, and NH are integral functions of t and π. Grom relation (1) we see that if Nf is irreducible for $R(1)$, $f(t+\sqrt{2})$ is irreducible for $R(\pi, \sqrt{2})$; and every divisor of $f(t+\sqrt{2})$ is a common divisor of $f(t+\sqrt{2})$ and a factor of Nf. Thus our procedure is to find all the factors of Nf for $R(1)$ and find the greatest common factor of $f(t+\sqrt{2})$ and one of these factors, which takes but a finite number of operations.

Since we are dealing with π as a variable we propose to attempt to factor the function Nf of the two variables t and π for domain $R(1)$.

Since Nf is of fourth degree in t, we need not test it for factors of higher degree than two in t.

Let us test Nf for a factor of degree two in t.

To do this we select arbitrarily three values for t, say $t_1 = 0$, $t_2 = 1$, $t_3 = -1$.

Now form the functions

$$M_{t_1}(t) = \frac{(t - t_2)(t - t_3)}{(t_1 - t_2)(t_1 - t_3)} = \frac{(t - 1)(t + 1)}{(0 - 1)(0 + 1)} = 1 - t^2.$$

$$M_{t_2}(t) = \frac{(t - t_1)(t - t_3)}{(t_2 - t_1)(t_2 - t_3)} = \frac{(t - 0)(t + 1)}{(1 - 0)(1 + 1)} = \frac{t^2 + t}{2}.$$

$$M_{t_3}(t) = \frac{(t - t_1)(t - t_2)}{(t_3 - t_1)(t_3 - t_2)} = \frac{(t - 0)(t - 1)}{(- 1 - 0)(- 1 - 1)} \quad \frac{t^2 - t}{2}.$$

Since the function $NG(t_1)\, M_{t_1}(t) + NG(t_2) M_{t_2}(t) + NG(t_3) M_{t_3}(t)$ is equal to $NG(t_1)$ for $t = t_1$, to $NG(t_2)$ for $t = t_2$, and to $NG(t_3)$ for $t = t_3$, we may write

$$NG(t_1)(1 - t^2) + NG(t_2)\frac{t^2 + t}{2} + NG(t_3)\frac{t^2 - t}{2} \equiv NG(t).$$

We now desire to find $NG(t_1)$, $NG(t_2)$, and $NG(t_3)$.

$Nf(t_1) = \pi^4 - 8\pi^2$ and its factors are

$$\pi, \pi^2, \pi^2 - 8, \quad \pi(\pi^2 - 8).$$

$Nf(t_2) = -7 + 12\pi - 2\pi^2 - 4\pi^3 + \pi^4$ and its factors are $(\pi - 1)$, $(\pi - 1)^2$, $(\pi^2 - 2\pi - 7)$, $(\pi - 1)(\pi^2 - 2\pi - 7)$ [by Kronecker's method for factoring an integral function of one variable in $R(1)$] .

$Nf(t_3) = - 7 - 12\pi - 2\pi^2 + 4\pi^3 + \pi^4$ and its factors are $(\pi + 1)$, $(\pi + 1)^2$, $(\pi^2 + 2\pi - 7)$, $(\pi + 1)(\pi^2 + 2\pi - 7)$.

$NG(t_1)$ must be one of the factors of $Nf(t_1)$; $NG(t_2)$, one of the factors of $Nf(t_2)$; $NG(t_3)$, one of the factors of $Nf(t_3)$.

Let us try $\pi^2 - 8$ for $NG(t_1)$, $\pi^2 - 2\pi - 7$ for $NG(t_2)$, and $\pi^2 + 2\pi - 7$ for $NG(t_3)$.

Then as a trial value for NG we have

$$(\pi^2 - 8)(1 - t^2) + (\pi^2 - 2\pi - 7)\frac{t^2 + t}{2} + (\pi^2 + 2\pi - 7)\frac{t^2 - t}{2} =$$

$$\pi^2 - 8 - \pi^2 t^2 + 8t^2 + \tfrac{1}{2}\left[\pi^2 t^2 - 2\pi t^2 - 7t^2 + \pi^2 t - 2\pi t - 7t\right] +$$

$$\tfrac{1}{2}\left[\pi^2 t^2 + 2\pi t^2 - 7t^2 - \pi^2 t - 2\pi t + 7t\right] = t^2 - 2\pi t + \pi^2 - 8.$$

Testing $t^2 - 2\pi t + \pi^2 - 8$ as a factor of Nf, we find

$$\frac{Nf}{t^2 - 2\pi t + \pi^2 - 8} = \frac{t^4 - 4\pi t^3 + (6\pi^2 - 8)t^2 + (16\pi - 4\pi^3 t + \pi^4 - 8\pi^2}{t^2 - 2\pi t + \pi^2 - 8} =$$

$$(t - \pi)^2.$$

Thus $t^2 - 2\pi t + \pi^2 - 8 = NG$, i.e. is a factor of Nf.

It now remains to find the highest common factor of $f(t + \sqrt{2})$ and $t^2 - 2\pi t + \pi^2 - 8$ by the ordinary method.

$$\begin{array}{lll}
 & t^2 + 2(\sqrt{2} - \pi)t + \pi^2 - 2\pi\sqrt{2}\,) & t^2 - 2\pi t + \pi^2 - 8 \\
 & &)\ 1 \\
 & \underline{t \quad - 2\pi t \qquad + \pi^2 - 8} & \\
2\sqrt{2} & \underline{\big|\ 2\sqrt{2}t \quad - \quad 2\pi\sqrt{2} + 8} & \\
 & \underline{t \quad - \quad \pi + 2\sqrt{2}\,\big|} & t^2 - 2\pi t + \pi^2 - 8 \ \big|\ \underline{t - (\pi + 2\sqrt{2})} \\
 & & \underline{t^2 - \quad \pi t + 2\sqrt{2}t} \\
 & & -\pi t - 2\sqrt{2}t + \pi^2 - 8 \\
 & & \underline{-\pi t - 2\sqrt{2}t + \pi^2 - 8}
\end{array}$$

We thus find that $t - \pi + 2\sqrt{2}$ is the highest common factor of $f(t + \sqrt{2})$ and $t^2 - 2\pi t + \pi^2 - 8$.

Applying now the reverse substitution $x = t + \sqrt{2}$, we have

$$t - \pi + 2\sqrt{2} = x - \pi + \sqrt{2}.$$

Therefore, $x - \pi + \sqrt{2}$ is a factor of f(x) for $R(\pi, \sqrt{2})$. By division we find that $x - \pi - \sqrt{2}$ is also a factor of f(x), i.e. $f(x) = (x - \pi + \sqrt{2})(x - \pi - \sqrt{2})$.

55. Reducibility and Transitivity. With the property of the reducibility or irreducibility of a given equation for a domain R is correlated a corresponding property of its group for that domain. That is, knowing whether or not an equation is reducible, we are able to state a certain characteristic of its group; and on the other hand, knowing its group, we are able to state whether or not the equation is reducible. The property of the group to which we refer is its "transitivity" or "intransitivity". By a transitive group is meant one which carries any arbitrarily given letter into any other arbitrarily given letter.

We will now proceed to show (A) if the group of an equation is intransitive, the equation is reducible; and conversely, (B) if the equation is reducible its group is intransitive.

(A). Let there be given the equation

$$f(x) = (x - x_1)(x - x_2) \ldots (x - x_n) = 0$$

whose group G for domain R is intransitive and connects x_1 with only the elements

$x_2, x_3, \ldots x_p.$ $(p < n)$.

Then the function

$$\varphi(x) = (x - x_1)(x - x_2) \ldots (x - x_p)$$

has its coefficients formally unchanged by all the substitutions of G, since they are symmetric in $x_1, x_2, \ldots x_p$ and every substitution of G merely permutes $x_1, x_2, \ldots x_p$ among themselves.

By Lagrange's theorem the coefficients of $\varphi(x)$ can be expressed rationally in terms of $c_1, c_2, \ldots c_n$ and any function belonging to G under $G_{n!}$ and thus lie in R. It follows that $\varphi(x)$ is a rational factor of f(x), and therefore that the given equation $f(x) = 0$ is reducible for domain R.

(B). Let there be given the equation

$$f(x) = (x - x_1)(x - x_2) \ldots (x - x_n) = 0$$

reducible for domain R, namely such that

$$f(x) = \varphi(x) \ \psi(x)$$

where the coefficients of $\varphi(x) = (x - x_1)(x - x_2) \ldots (x - x_p)$ and $\psi(x) = (x - x_{p+1})(x - x_{p+2}) \ldots (x - x_n)$ lie in R. Since any summetric function of $x_1, x_2, \ldots x_p$ and any symmetric function of $x_{p+1}, x_{p+2}, \ldots x_n)$ lies in R, the function $\psi =$ Sym. Funct. $(x_1, x_2, \ldots x_p) +$ K Sym. Funct. $(x_{p+1}, \ldots x_n)$ (where K is a quantity in R) lies in R.

The function ψ is formally unchanged by any substitution of the group H, which consists of all the substitutions on $x_1, x_2, \ldots x_p$ among themselves, all the substitutions on $x_{p+1}, x_{p+2}, \ldots x_n$ among themselves, and all the products of the above-mentioned substitutions. On the other hand, ψ is formally changed by any substitution not in H, i.e. by any substitution which carries any of the elements $x_1, x_2, \ldots x_p$ into any of the elements $x_{p+1}, x_{p+2}, \ldots x_n$.

Therefore ψ belongs formally to the intransitive group H.

Having properly chosen K, the conjugates of ψ under $G_{n!}$ are numerically distinct and ψ belongs to H under $G_{n!}$. Since ψ belongs to H under $G_{n!}$ and lies in R, H lies in R ; and since H lies in R , the group G of $f(x)=0$ for domain R is a subgroup of H. But H is intransitive, and since any subgroup of an intransitive group is intransitive, G must be intransitive.

56. It is evident that in the determination of the group of an equation the fact that the reducibility (or irreducibility) of the equation is correlated with the intransitivity (or transitivity) of its group directs us in the choice of groups for investigation. This fact is especially useful when we reach the biquadratic equation, where the determination of the group begins to show complexities.

CHAPTER VI.

The Solution of Equations from the Standpoint of the Galois Theory.

57. In Chapter IV we found that for any given equation and any given domain R there is one group whose properties are of such importance in the study of an equation that this group is called "the" group of the equation for domain R. By making use of this idea of the group of an equation we are enabled to view the solution of equations in a manner somewhat different from that used in earlier chapters.

58. Quadratic Equation. The Galois group of the general quadratic equation

$$x^2 - c_1 x + c_2 = 0$$

for domain $R(c_1, c_2)$ is the symmetric group $G_{2!}^{(2)}$ (Chap.IV, Art. 43.)

$$\begin{array}{l|l} G_{2!}^{(2)} & c_1 = x_1 + x_2 \\ & c_2 = x_1 x_2 \\ 2 & (v - v_1)(v - v_2) = 0. \\ G_1^{(2)} & v_1 = x_1 - x_2 \end{array}$$

The only subgroup of $G_{2!}$ is G_1. We are able to solve the resolvent equation $(v - v_1)(v - v_2) = 0$ for the function v_1 belonging to G_1 (Chap.I, Art.1).

Upon adjoining v_1 to the domain of

rationality the group of the equation becomes G_1. (Chap. IV, Art. 47).

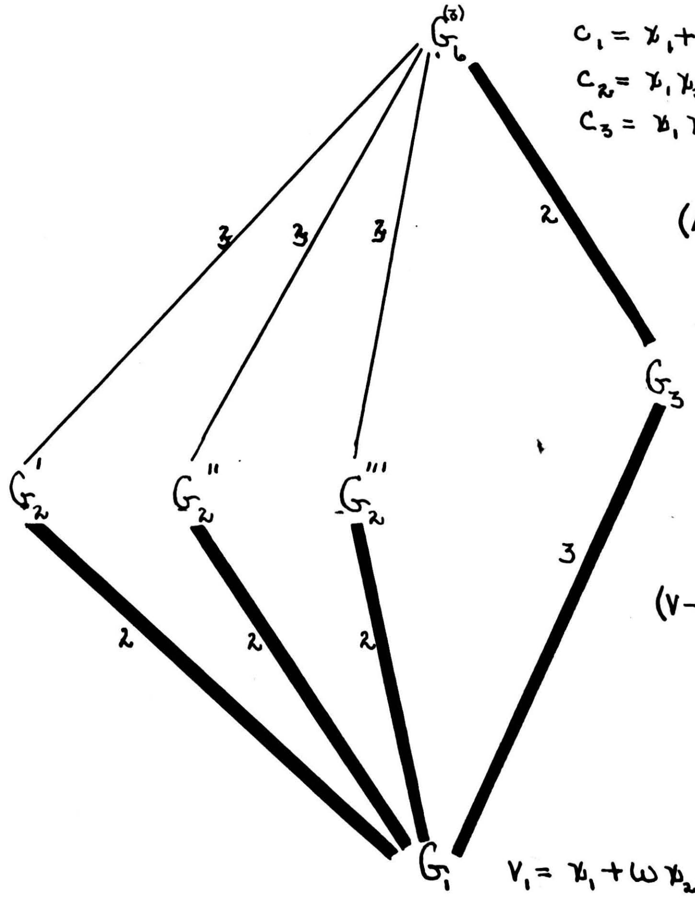
Knowing that $c_1 = x_1 + x_2$ and $v_1 = x_1 - x_2$ we are able to express x_1 and x_2 in terms of elements of the domain: $x_1 = \dfrac{c_1 + v_1}{2}$,

$x_2 = \dfrac{c_1 - v_1}{2}$. (See Chap. I. Art. 1).

59. The Cubic Equation. The Galois group of the general reduced cubic equation

$$x^3 + c_2 x - c_3 = 0$$

for domain $R(c_1, c_2, c_3)$ is $G_6^{(3)}$.



$c_1 = x_1 + x_2 + x_3 = 0.$
$c_2 = x_1 x_2 + x_2 x_3 + x_1 x_3.$
$c_3 = x_1 x_2 x_3.$

$(\Delta - \Delta_1)(\Delta - \Delta_2) = 0.$ I.

$\Delta_1 = (x_1 - x_2)(x_2 - x_3)(x_3 - x_1).$
$\Delta_2 = -\Delta_1.$

$(v - v_1)(v - v_2)(v - v_3) = 0.$ II.

$v_1 = x_1 + \omega x_2 + \omega^2 x_3.$

In Chap. I, Art. 8 we solved the resolvent equation I for the function Δ_1, which belongs to G_3 under G_6. Upon adjoining Δ_1 to the domain the group of the equation becomes G_3. Similarly, in Chapter I, Art. 8 we solved the resolvent equation II for the function v_1, which belongs to G_1 under G_3. Upon adjoining v_1 to the domain the group of the equation becomes G_1, and we are able to express its roots in terms of elements of the domain $R(c_1, c_2, c_3, \Delta_1, v_1)$.

$$x_1 = 1/3 \left[v_1 - \frac{3c_2}{v_1} \right]$$

$$x_2 = 1/3 \left[\omega^2 v_1 - \frac{\omega 3c_2}{v_1} \right]$$

$$x_3 = 1/3 \left[\omega v_1 - \frac{\omega^2 3c_2}{v_1} \right]$$

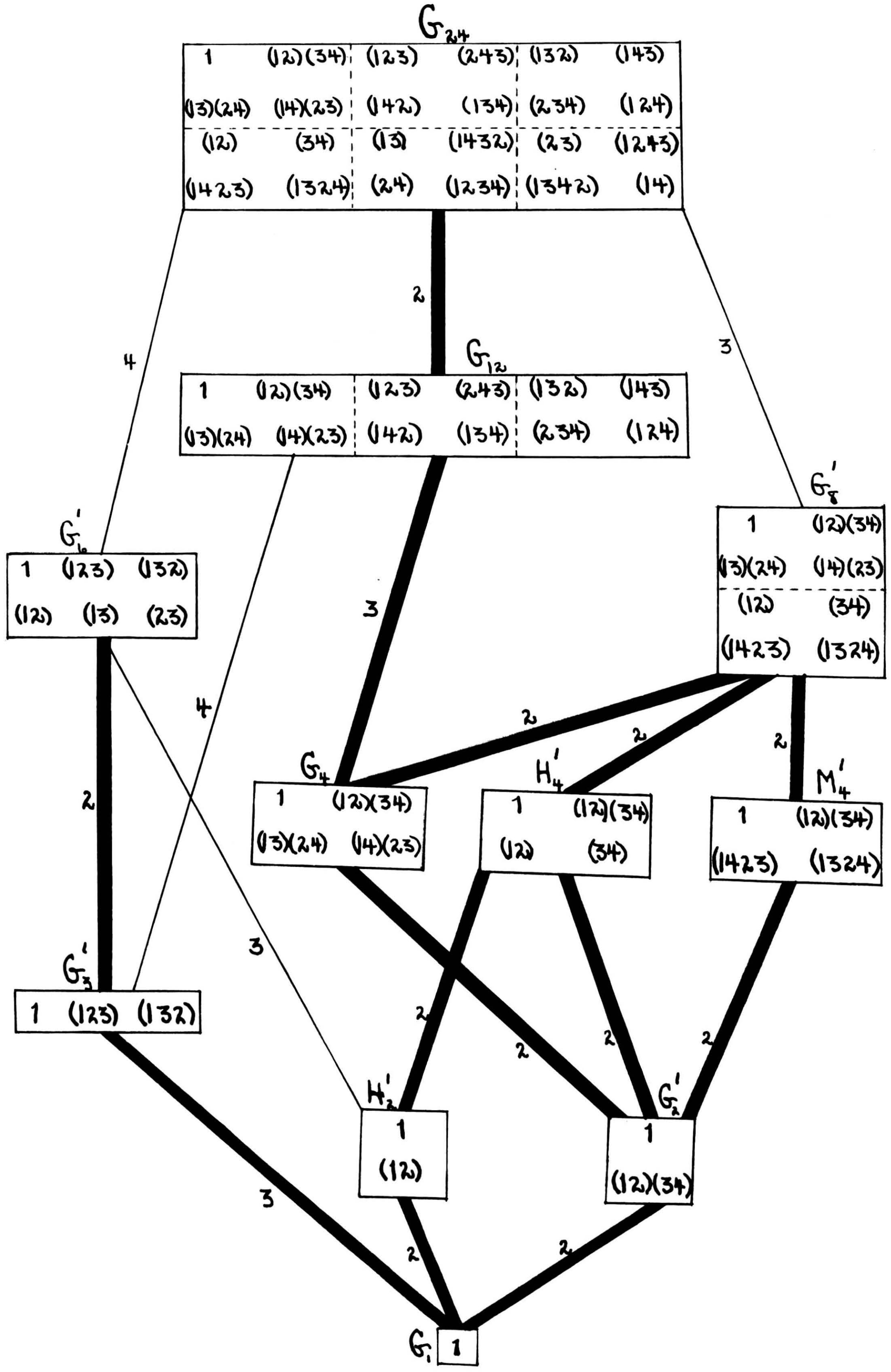
(See Chap.I Art.8 page 16).

60. The Biquadratic Equation. The Galois Group of the general biquadratic equation

$$x^4 - c_1 x^3 + c_2 x^2 - c_3 x + c_4 = 0$$

for domain $R(c_1, c_2, c_3, c_4)$ is $G_{24}^{(4)}$. We have seen that five direct paths are open for the solution of the biquadratic equation (See Chapter III. Art. 16 and group-displays opposite pages 29 and 81). Since we may select not only a great variety of functions at each adjunction but also different groups, we can account for the fact that the number of different solutions that has been given for the biquadratic equation is enormous.*

* For details of solution see Dickson Arts. 4 - 7, 35 - 42. For information on different solutions see Matthiesen: **Grundzüge der Antiken u. Modernern Algebra.**



Note: In this group-display only one group of a conjugate set is given.

Let us consider the following path:

$$G_{24} \quad c_1, c_2, c_3, c_4$$

$$2 \quad (\Delta - \Delta_1)(\Delta - \Delta_2) = 0. \qquad \text{I.}$$

$$G_{12} \quad \Delta_1 = (x_1 - x_2)(x_1 - x_3)(x_1 - x_4)(x_2 - x_3)(x_2 - x_4)(x_3 - x_4).$$

$$3 \quad (\varphi - \varphi_1)(\varphi - \varphi_2)(\varphi - \varphi_3) = 0. \qquad \text{II.}$$

$$G_4 \quad \varphi_1 = (x_1 x_2 + x_3 x_4) + \omega(x_1 x_3 + x_2 x_4) + \omega^2(x_1 x_4 + x_2 x_3).$$

$$2 \quad (\lambda - \lambda_1)(\lambda - \lambda_2)(\lambda - \lambda_3) = 0. \qquad \text{III.}$$

$$G_2' \quad \lambda_1 = \varphi_1 \div (x_1 + x_2 - x_3 - x_4)$$

$$2 \quad (v - v_1)(v - v_2) = 0. \qquad \text{IV.}$$

$$G_1 \quad v_1 = x_1 - x_2 + i x_3 - i x_4.$$

The resolvent equations I, II, III, and IV can be solved since they are quadratic and cubic equations. Upon adjoining Δ_1, φ_1, λ_1, and v_1 to the domain, the group of the equation becomes G_1, and the roots may be expressed in terms of elements of the domain.

If we choose a path in which we pass from G_{24} to G_8 (See Chapter III, Art. 16), we must solve a non-binomial equation in order to find a function belonging to G_8 under G_{24}, since G_8 is not self-conjugate under G_{24}. But since this non-binomial equation is only of third degree, there is no difficulty due to this situation. Thus along any of the paths indicated in

Chapter III, Art. 16, the resolvent equations can be solved, since they are not of higher degree than three, and the solution of the given equation can be accomplished.

61. The Quintic Equation. The Galois group of the general quintic equation

$$x^5 - c_1 x^4 + c_2 x^3 - c_3 x^2 + c_4 x - c_5 = 0$$

for domain $R(c_1, c_2, c_3, c_4, c_5)$ is $G_{120}^{(5)}$.

Apparently the method of procedure used in solving the general equations of second, third, and fourth degrees should lead to the solution of the general quintic, but a difficulty arises in that in each possible path from G_{120} there occur non-binomial equations of degree five or higher (See group-display opposite page 43).

The maximum subgroups of G_{120} are G_{24}, G_{12}, G_{60}, and G_{20}. Passing to G_{24} would involve the solution of a non-binomial equation of fifth degree; passing to G_{12}, a non-binomial equation of tenth degree; passing to G_{20}, a non-binomial equation of sixth degree. Since G_{120} is the group of the equation for R, the groups G_{24}, G_{12}, and G_{20} do not lie in R, and it is thus impossible to solve any of the above resolvents by inspection (i.e. by finding a rational linear factor in R). Our procedure then is blocked. On the other hand, we may pass to G_{60}

by a binomial resolvent of second degree, but to pass from G_{60} to a maximum subgroup of G_{60} we would have to solve non-binomial resolvents of fifth, sixth, or tenth degrees. Since no maximum subgroup of G_{60} lies in R, none of these resolvents can be solved by inspection, and our procedure is here also blocked.

We thus arrive at the conclusion that the general quintic equation cannot be solved by our method. Furthermore, it is evident that the same is true for any special quintic equation which has for its group for $R(c_1, c_2, c_3, c_4)$ the symmetric or alternating group.

Let us now consider the case of a special quintic equation whose group is neither G_{120} nor G_{60}. The group may or may not be a subgroup of G_{60} ($\neq G_{60}$).

Case (1). Suppose the group is not a subgroup of G_{60}. Since by hypothesis G_{120} is not the group of lowest order in R, at least one of the non-binomial resolvent equations to be tried in passing from G_{120} to a maximum subgroup of G_{120} has a rational linear factor in R and can thus be solved by inspection. We observe from the group display of G_{120} that starting from any maximum subgroup of G_{120}, other than G_{60}, we can select a series of groups terminating with $G_1(1)$ in which each group is a self-conjugate subgroup of prime index under the preceding

group, and can therefore pass to $G_1(1)$ by a chain of binomial equations of prime degrees.

Case (2). Suppose that the group is a subgroup of G_{60} ($\neq G_{60}$). We can pass to G_{60} by the solution of a binomial equation. Since by hypothesis a subgroup of G_{60} of lower order than G_{60} lies in R, at least one of the non-binomial resolvent equations to be tried in passing from G_{60} to a maximum subgroup of G_{60} has a rational linear factor in R and can thus be solved by inspection. We observe from the group display of G_{120} that starting from any maximum subgroup of G_{60} we can select a series of groups terminating with $G_1(1)$ in which each group is a self-conjugate subgroup of prime index under the preceding group. Therefore, as in case (1), we can pass to $G_1(1)$ by solving a chain of binomial equations of prime degrees; and the solution of any quintic equation whose group is neither the symmetric nor alternating group can thus be accomplished by our method.

62. Algebraic Solvability of Equations of Higher than Fourth Degree. We observe that we can always solve any equation by our method if starting from the group of the equation we can select a series of groups terminating with $G_1(1)$ in which each group is a self-conjugate subgroup of prime index under the preceding group.

Furthermore, it is shown in treatments of this subject that this condition is not only sufficient but also necessary for the algebraic solution of any equation.*

Since it has been proved that the symmetric group $G_{n!}$ on $n > 4$ letters contains no self-conjugate subgroups besides itself, $G_{\frac{n!}{2}}$, and $G_1(1)$,** it follows immediately that the general equation of higher than fourth degree is not solvable algebraically. For although the index of $G_{\frac{n!}{2}}$ under $G_{n!}$ is the prime number 2, the index of G_1 under $G_{\frac{n!}{2}}$ is the number $\frac{n!}{2}$, which is not prime for $n > 4$. However, it is clear that a special equation of higher than fourth degree may have a group which meets the above conditions and thus may be solvable algebraically.

* Dickson: Arts. 84, 92.

** Dickson: Art. 45.