INTRODUCTION TO THE

THEORY OF ALGEBRAIC EQUATIONS.

BY

LEONARD EUGENE DICKSON, PH.D.,

ASSISTANT PROFESSOR OF MATHEMATICS IN
THE UNIVERSITY OF CHICAGO.

FIRST EDITION.

SECOND THOUSAND.

NEW YORK:

JOHN WILEY & SONS.

LONDON: CHAPMAN & HALL, LIMITED.

1903.

ROBERT DRUMMOND, PRINTER, NEW YORK.

PREFACE.

THE solution of the general quadratic equation was known as early as the ninth century; that of the general cubic and quartic equations was discovered in the sixteenth century. During the succeeding two centuries many unsuccessful attempts were made to solve the general equations of the fifth and higher degrees. In 1770 Lagrange analyzed the methods of his predecessors and traced all their results to one principle, that of rational resolvents, and proved that the general quintic equation cannot be solved by rational resolvents. The impossibility of the algebraic solution of the general equation of degree n ($n>4$), whether by rational or irrational resolvents, was then proved by Abel, Wantzel, and Galois. Out of these algebraic investigations grew the theory of substitutions and groups. The first systematic study of substitutions was made by Cauchy (*Journal de l'école polytechnique*, 1815).

The subject is here presented in the historical order of its development. The First Part (pp. 1–41) is devoted to the Lagrange-Cauchy-Abel theory of general algebraic equations. The Second Part (pp. 42–98) is devoted to Galois' theory of algebraic equations, whether with arbitrary or special coefficients. The aim has been to make the presentation strictly elementary, with practically no dependence upon any branch of mathematics beyond elementary algebra. There occur numerous illustrative examples, as well as sets of elementary exercises.

In the preparation of this book, the author has consulted, in addition to various articles in the journals, the following treatises:

Lagrange, *Réflexions sur la résolution algébrique des équations*; Jordan, *Traité des substitutions et des équations algébriques*; Serret, *Cours d'Algèbre supérieure*; Netto-Cole, *Theory of Substitutions and its Applications to Algebra*; Weber, *Lehrbuch der Algebra*; Burnside, *The Theory of Groups* Pierpont, *Galois' Theory of Algebraic Equations*, Annals of Math., 2d ser., vols. 1 and 2; Bolza, *On the Theory of Substitution-Groups and its Applications to Algebraic Equations*, Amer. Journ. Math., vol. XIII.

The author takes this opportunity to express his indebtedness to the following lecturers whose courses in group theory he has attended: Oscar Bolza in 1894, E. H. Moore in 1895, Sophus Lie in 1896, Camille Jordan in 1897.

But, of all the sources, the lectures and publications of Professor Bolza have been of the greatest aid to the author. In particular, the examples (§ 65) of the group of an equation have been borrowed with his permission from his lectures.

The present elementary presentation of the theory is the outcome of lectures delivered by the author in 1897 at the University of California, in 1899 at the University of Texas, and twice in 1902 at the University of Chicago.

CHICAGO, *August*, 1902

TABLE OF CONTENTS.

PREFACE.

THE solution of the general quadratic equation was known as early as the ninth century; that of the general cubic and quartic equations was discovered in the sixteenth century. During the succeeding two centuries many unsuccessful attempts were made to solve the general equations of the fifth and higher degrees. In 1770 Lagrange analyzed the methods of his predecessors and traced all their results to one principle, that of rational resolvents, and proved that the general quintic equation cannot be solved by rational resolvents. The impossibility of the algebraic solution of the general equation of degree n ($n>4$), whether by rational or irrational resolvents, was then proved by Abel, Wantzel, and Galois. Out of these algebraic investigations grew the theory of substitutions and groups. The first systematic study of substitutions was made by Cauchy (*Journal de l'école polytechnique*, 1815).

The subject is here presented in the historical order of its development. The First Part (pp. 1–41) is devoted to the Lagrange-Cauchy-Abel theory of general algebraic equations. The Second Part (pp. 42–98) is devoted to Galois' theory of algebraic equations, whether with arbitrary or special coefficients. The aim has been to make the presentation strictly elementary, with practically no dependence upon any branch of mathematics beyond elementary algebra. There occur numerous illustrative examples, as well as sets of elementary exercises.

In the preparation of this book, the author has consulted, in addition to various articles in the journals, the following treatises:

Lagrange, *Réflexions sur la résolution algébrique des équations*; Jordan, *Traité des substitutions et des équations algébriques*; Serret, *Cours d'Algèbre supérieure*; Netto-Cole, *Theory of Substitutions and its Applications to Algebra*; Weber, *Lehrbuch der Algebra*; Burnside, *The Theory of Groups* Pierpont, *Galois' Theory of Algebraic Equations*, Annals of Math., 2d ser., vols. 1 and 2; Bolza, *On the Theory of Substitution-Groups and its Applications to Algebraic Equations*, Amer. Journ. Math., vol. XIII.

The author takes this opportunity to express his indebtedness to the following lecturers whose courses in group theory he has attended: Oscar Bolza in 1894, E. H. Moore in 1895, Sophus Lie in 1896, Camille Jordan in 1897.

But, of all the sources, the lectures and publications of Professor Bolza have been of the greatest aid to the author. In particular, the examples (§ 65) of the group of an equation have been borrowed with his permission from his lectures.

The present elementary presentation of the theory is the outcome of lectures delivered by the author in 1897 at the University of California, in 1899 at the University of Texas, and twice in 1902 at the University of Chicago.

CHICAGO, *August*, 1902

TABLE OF CONTENTS.

THEORY OF ALGEBRAIC EQUATIONS.

FIRST PART.

THE LAGRANGE-ABEL-CAUCHY THEORY OF GENERAL ALGEBRAIC EQUATIONS.

CHAPTER I.

SOLUTION OF THE GENERAL QUADRATIC, CUBIC, AND QUARTIC EQUATIONS. LAGRANGE'S THEOREM* ON THE IRRATIONALITIES ENTERING THE ROOTS.

1. **Quadratic equation.** The roots of $x^2+px+q=0$ are

$$x_1=\tfrac{1}{2}(-p+\sqrt{p^2-4q}),\quad x_2=\tfrac{1}{2}(-p-\sqrt{p^2-4q}).$$

By addition, subtraction, and multiplication, we get

$$x_1+x_2=-p,\quad x_1-x_2=\sqrt{p^2-4q},\quad x_1x_2=q.$$

Hence the irrationality $\sqrt{p^2-4q}$, which occurs in the expressions for the roots, is rationally expressible in terms of the roots, being equal to x_1-x_2. Unlike the last function, the functions x_1+x_2 and x_1x_2 are *symmetric* in the roots and are rational functions of the coefficients.

2. **Cubic equation.** The general cubic equation may be written

$$x^3-c_1x^2+c_2x-c_3=0. \tag{1}$$

Setting $x=y+\frac{1}{3}c_1$, the equation (1) takes the simpler form

$$y^3+py+q=0, \tag{2}$$

* *Réflexions sur la résolution algébrique des équations*, Œuvres de Lagrange, Paris, 1869, vol. 3; first printed by the Berlin Academy, 1770–71.

if we make use of the abbreviations

$$p=c_2-\tfrac{1}{3}c_1^2, \quad q=-c_3+\tfrac{1}{3}c_1c_2-\tfrac{2}{27}c_1^3. \tag{3}$$

The cubic (2), lacking the square of the unknown quantity, is called the *reduced cubic equation*. When it is solved, the roots of (1) are found by the relation $x=y+\frac{1}{3}c_1$.

The cubic (2) was first solved by Scipio Ferreo before 1505. The solution was rediscovered by Tartaglia and imparted to Cardan under promises of secrecy. But Cardan broke his promises and published the rules in 1545 in his *Ars Magna*, so that the formulæ bear the name of Cardan. The following method of deriving them is essentially that given by Hudde in 1650. By the transformation

$$y=z-\frac{p}{3z}, \tag{4}$$

the cubic (2) becomes $z^3-\dfrac{p^3}{27z^3}+q=0$, whence

$$z^6+qz^3-\frac{p^3}{27}=0. \tag{5}$$

Solving the latter as a quadratic equation for z^3, we get

$$z^3=-\tfrac{1}{2}q\pm\sqrt{R}, \quad R\equiv\tfrac{1}{4}q^2+\tfrac{1}{27}p^3.$$

Denote a definite one of the cube roots of $-\frac{1}{2}q+\sqrt{R}$ by

$$\sqrt[3]{-\tfrac{1}{2}q+\sqrt{R}}.$$

The other two cube roots are then

$$\omega\sqrt[3]{-\tfrac{1}{2}q+\sqrt{R}}, \quad \omega^2\sqrt[3]{-\tfrac{1}{2}q+\sqrt{R}},$$

where ω is an imaginary cube root of unity found as follows. The three cube roots of unity are the roots of the equation

$$r^3-1=0, \quad \text{or} \quad (r-1)(r^2+r+1)=0.$$

The roots of $r^2+r+1=0$ are $-\frac{1}{2}+\frac{1}{2}\sqrt{-3}\equiv\omega$ and $-\frac{1}{2}-\frac{1}{2}\sqrt{-3}=\omega^2$. Then

$$\omega^2+\omega+1=0, \quad \omega^3=1. \tag{6}$$

In view of the relation

$$(-\tfrac{1}{2}q+\sqrt{R})(-\tfrac{1}{2}q-\sqrt{R})=\tfrac{1}{4}q^2-R=-\tfrac{1}{27}p^3,$$

a particular cube root $\sqrt[3]{-\frac{1}{2}q-\sqrt{R}}$ may be chosen so that

$$\sqrt[3]{-\tfrac{1}{2}q+\sqrt{R}}\cdot\sqrt[3]{-\tfrac{1}{2}q-\sqrt{R}}=-\tfrac{1}{3}p.$$

$$\therefore\quad \omega\sqrt[3]{-\tfrac{1}{2}q+\sqrt{R}}\cdot\omega^2\sqrt[3]{-\tfrac{1}{2}q-\sqrt{R}}=-\tfrac{1}{3}p,$$

$$\omega^2\sqrt[3]{-\tfrac{1}{2}q+\sqrt{R}}\cdot\omega\sqrt[3]{-\tfrac{1}{2}q-\sqrt{R}}=-\tfrac{1}{3}p.$$

Hence the six roots of equation (5) may be separated into pairs in such a way that the product of two in any pair is $-\frac{1}{3}p$. The root paired with z is therefore $-\dfrac{p}{3z}$, and their sum $z-\dfrac{p}{3z}$ is, in view of (4), a root y of the cubic (2). In particular, the two roots of a pair lead to the same value of y, so that the *six* roots of (5) lead to only *three* roots of the cubic, thereby explaining an apparent difficulty. Since the sum of the two roots of any pair of roots of (5) leads to a root of the cubic (2), we obtain Cardan's formulæ for the roots y_1, y_2, y_3 of (2):

$$(7)\qquad \begin{cases} y_1=\sqrt[3]{-\frac{1}{2}q+\sqrt{R}}+\sqrt[3]{-\frac{1}{2}q-\sqrt{R}}, \\ y_2=\omega\sqrt[3]{-\frac{1}{2}q+\sqrt{R}}+\omega^2\sqrt[3]{-\frac{1}{2}q-\sqrt{R}}, \\ y_3=\omega^2\sqrt[3]{-\frac{1}{2}q+\sqrt{R}}+\omega\sqrt[3]{-\frac{1}{2}q-\sqrt{R}}. \end{cases}$$

Multiplying these expressions by 1, ω^2, ω and adding, we get, by (6),

$$\sqrt[3]{-\tfrac{1}{2}q+\sqrt{R}}=\tfrac{1}{3}(y_1+\omega^2y_2+\omega y_3).$$

Using the multipliers 1, ω, ω^2, we get, similarly,

$$\sqrt[3]{-\tfrac{1}{2}q-\sqrt{R}}=\tfrac{1}{3}(y_1+\omega y_2+\omega^2y_3).$$

Cubing these two expressions and subtracting the results, we get

$$\sqrt{R}=\tfrac{1}{54}\{(y_1+\omega^2y_2+\omega y_3)^3-(y_1+\omega y_2+\omega^2y_3)^3\}$$

$$=\frac{\sqrt{-3}}{18}(y_1-y_2)(y_2-y_3)(y_3-y_1),$$

upon applying the Factor Theorem and the identity $\omega-\omega^2=\sqrt{-3}$. Hence all the irrationalities occurring in the roots (7) are rationally expressible in terms of the roots, a result first shown by **Lagrange.**

The function

$$(y_1-y_2)^2(y_2-y_3)^2(y_3-y_1)^2=-27q^2-4p^3$$

is called the *discriminant* of the cubic (2).

The roots of the general cubic (1) are

$$x_1=y_1+\tfrac{1}{3}c_1, \quad x_2=y_2+\tfrac{1}{3}c_1, \quad x_3=y_3+\tfrac{1}{3}c_1.$$

$$\therefore\ x_1-x_2=y_1-y_2, \quad x_2-x_3=y_2-y_3, \quad x_3-x_1=y_3-y_1,$$

$$(8)\qquad (x_1-x_2)(x_2-x_3)(x_3-x_1)=(y_1-y_2)(y_2-y_3)(y_3-y_1)$$

$$=\frac{18}{\sqrt{-3}}\sqrt{R}=-6\sqrt{-3}\sqrt{\tfrac{1}{4}q^2+\tfrac{1}{27}p^3}.$$

EXERCISES.

1. Show that $x_1+\omega^2x_2+\omega x_3=y_1+\omega^2y_2+\omega y_3$, $x_1+\omega x_2+\omega^2x_3=y_1+\omega y_2+\omega^2y_3$.

2. The cubic (2) has one real root and two imaginary roots if $R>0$; three real roots, two of which are equal, if $R=0$; three real and distinct roots if $R<0$ (the so-called irreducible case).

3. Show that the discriminant $(x_1-x_2)^2(x_2-x_3)^2(x_3-x_1)^2$ of the cubic (1) equals

$$c_1^2c_2^2+18c_1c_2c_3-4c_2^3-4c_1^3c_3-27c_3^2.$$

Hint: Use formula (8) in connection with (3).

4. Show that the nine expressions $\sqrt[3]{-\tfrac{1}{2}q+\sqrt{R}}+\sqrt[3]{-\tfrac{1}{2}q-\sqrt{R}}$, where all combinations of the cube roots are taken, are the roots of the cubics

$$y^3+py+q=0, \quad y^3+\omega py+q=0, \quad y^3+\omega^2py+q=0.$$

5. Show that $y_1+y_2+y_3=0$, $y_1y_2+y_1y_3+y_2y_3=p$, $y_1y_2y_3=-q$.

6 Show that $x_1+x_2+x_3=c_1$, $x_1x_4+x_1x_3+x_2x_3=c_2$, $x_1x_2x_3=c_3$, using Ex. 5. How may these results be derived directly from equation (1)?

3. Aside from the factor $\frac{1}{3}$, the roots of the sextic (5) are

$$\psi_1=x_1+\omega x_2+\omega^2x_3, \qquad \psi_4=x_1+\omega x_3+\omega^2x_2,$$
$$\psi_2=\omega^2\psi_1=x_2+\omega x_3+\omega^2x_1, \qquad \psi_5=\omega^2\psi_4=x_3+\omega x_2+\omega^2x_1,$$
$$\psi_3=\omega\psi_1=x_3+\omega x_1+\omega^2x_2, \qquad \psi_6=\omega\psi_4=x_2+\omega x_1+\omega^2x_3.$$

These functions differ only in the permutations of x_1, x_2, x_3. As there are just six permutations of three letters, these functions

give all that can be obtained from ψ_1 by permuting x_1, x_2, x_3. For this reason, ψ_1 is called a *six-valued* function.

Lagrange's *à priori* solution of the general cubic (1) consists in determining these six functions $\psi_1, \ldots, \psi_6$ directly. They are the roots of the sextic equation $(t-\psi_1)\ldots(t-\psi_6)=0$, whose coefficients are symmetric functions of $\psi_1, \ldots, \psi_6$ and consequently symmetric functions of x_1, x_2, x_3 and hence * are rationally expressible in terms of c_1, c_2, c_3. Since $\psi_2=\omega^2\psi_1$, $\psi_3=\omega\psi_1$, etc., we have by (6)

$$(t-\psi_1)(t-\psi_2)(t-\psi_3)=t^3-\psi_1{}^3,$$
$$(t-\psi_4)(t-\psi_5)(t-\psi_6)=t^3-\psi_4{}^3.$$

Hence the *resolvent* sextic becomes

$$t^6-(\psi_1{}^3+\psi_4{}^3)t^3+\psi_1{}^3\psi_4{}^3=0. \tag{9}$$

But
$$\psi_1\psi_4=x_1{}^2+x_2{}^2+x_3{}^2+(\omega+\omega^2)(x_1x_2+x_1x_3+x_2x_3)$$
$$=(x_1+x_2+x_3)^2-3(x_1x_2+x_1x_3+x_2x_3)=c_1{}^2-3c_2,$$

in view of Ex. 6, page 4. Also, $\psi_1{}^3+\psi_4{}^3$ equals

$$2(x_1{}^3+x_2{}^3+x_3{}^3)-3(x_1{}^2x_2+x_1x_2{}^2+x_1{}^2x_3+x_1x_3{}^2+x_2{}^2x_3+x_2x_3{}^2)+12x_1x_2x_3$$
$$=3(x_1{}^3+x_2{}^3+x_3{}^3)-(x_1+x_2+x_3)^3+18x_1x_2x_3$$
$$=2c_1{}^3-9c_1c_2+27c_3.$$

Hence equation (9) becomes

$$t^6-(2c_1{}^3-9c_1c_2+27c_3)t^3+(c_1{}^2-3c_2)^3=0.$$

Solving it as a quadratic equation for t^3, we obtain two roots θ and θ', and then obtain

$$\psi_1=\sqrt[3]{\theta}, \quad \psi_4=\sqrt[3]{\theta'}.$$

Here $\sqrt[3]{\theta}$ may be chosen to be an arbitrary one of the cube roots of θ, but $\sqrt[3]{\theta'}$ is then that definite cube root of θ' for which

$$\sqrt[3]{\theta}\cdot\sqrt[3]{\theta'}=c_1{}^2-3c_2. \tag{10}$$

We have therefore the following known expressions:

$$x_1+\omega x_2+\omega^2x_3=\sqrt[3]{\theta}, \quad x_1+\omega^2x_2+\omega x_3=\sqrt[3]{\theta'}, \quad x_1+x_2+x_3=c_1.$$

* The fundamental theorem on symmetric functions is proved in the Appendix.

Multiplying them by 1, 1, 1; then by $\omega^2, \omega, 1$; and finally by $\omega, \omega^2, 1$; and adding the resulting equations in each case, we get

$$(11)\qquad \begin{cases} x_1=\frac{1}{3}(c_1+\sqrt[3]{\theta}+\sqrt[3]{\theta'}), \\ x_2=\frac{1}{3}(c_1+\omega^2\sqrt[3]{\theta}+\omega\sqrt[3]{\theta'}), \\ x_3=\frac{1}{3}(c_1+\omega\sqrt[3]{\theta}+\omega^2\sqrt[3]{\theta'}). \end{cases}$$

4. Quartic equation. The general equation of degree four,

$$(12)\qquad x^4+ax^3+bx^2+cx+d=0,$$

may be written in the form

$$(x^2+\tfrac{1}{2}ax)^2=(\tfrac{1}{4}a^2-b)x^2-cx-d.$$

With Ferrari, we add $(x^2+\frac{1}{2}ax)y+\frac{1}{4}y^2$ to each member. Then

$$(13)\qquad (x^2+\tfrac{1}{2}ax+\tfrac{1}{2}y)^2=(\tfrac{1}{4}a^2-b+y)x^2+(\tfrac{1}{2}ay-c)x+\tfrac{1}{4}y^2-d.$$

We seek a value y_1 of y such that the second member of (13) shall be a perfect square. Set

$$(14)\qquad a^2-4b+4y_1=t^2.$$

The condition for a perfect square requires that

$$(15)\qquad \tfrac{1}{4}t^2x^2+(\tfrac{1}{2}ay_1-c)x+\tfrac{1}{4}y_1^2-d=\left(\tfrac{1}{2}tx+\frac{\frac{1}{2}ay_1-c}{t}\right)^2.$$

$$\therefore\ \tfrac{1}{4}y_1^2-d=\left(\frac{\frac{1}{2}ay_1-c}{t}\right)^2\equiv\frac{(\frac{1}{2}ay_1-c)^2}{a^2-4b+4y_1}.$$

Hence y_1 must be a root of the cubic, called the *resolvent*,

$$(16)\qquad y^3-by^2+(ac-4d)y-a^2d+4bd-c^2=0.$$

In view of (15), equation (13) leads to the two quadratic equations

$$(17)\qquad x^2+(\tfrac{1}{2}a-\tfrac{1}{2}t)x+\tfrac{1}{2}y_1-(\tfrac{1}{2}ay_1-c)/t=0,$$

$$(18)\qquad x^2+(\tfrac{1}{2}a+\tfrac{1}{2}t)x+\tfrac{1}{2}y_1+(\tfrac{1}{2}ay_1-c)/t=0.$$

Let x_1 and x_2 be the roots of (17), x_3 and x_4 the roots of (18). Then

$$x_1+x_2=-\tfrac{1}{2}a+\tfrac{1}{2}t,\quad x_1x_2=\tfrac{1}{2}y_1-(\tfrac{1}{2}ay_1-c)/t,$$

$$x_3+x_4=-\tfrac{1}{2}a-\tfrac{1}{2}t,\quad x_3x_4=\tfrac{1}{2}y_1+(\tfrac{1}{2}ay_1-c)/t.$$

By addition and subtraction, we get

$$x_1+x_2-x_3-x_4=t, \quad x_1x_2+x_3x_4=y_1. \tag{19}$$

In solving (17) and (18), two radicals are introduced, one equal to x_1-x_2 and the other equal to x_3-x_4 (see § 1). Hence all the irrationalities entering the expressions for the roots of the general quartic are rational functions of its roots.

If, instead of y_1, another root of the resolvent cubic (16) be employed, quadratic equations different from (17) and (18) are obtained, such, however, that their four roots are x_1, x_2, x_3, x_4, but paired differently. It is therefore natural to expect that the three roots of (16) are

$$y_1=x_1x_2+x_3x_4, \quad y_2=x_1x_3+x_2x_4, \quad y_3=x_1x_4+x_2x_3. \tag{20}$$

It is shown in the next section that this inference is correct.

5. Without having recourse to Ferrari's device, the two quadratic equations whose roots are the four roots of the general quartic equation (12) may be obtained by an *à priori* study of the rational functions $x_1x_2+x_3x_4$ and $x_1+x_2-x_3-x_4=t$. The three quantities (20) are the roots of $(y-y_1)(y-y_2)(y-y_3)=0$, or

$$y^3-(y_1+y_2+y_3)y^2+(y_1y_2+y_1y_3+y_2y_3)y-y_1y_2y_3=0. \tag{21}$$

Its coefficients may be expressed * as rational functions of a, b, c, d;

$$y_1+y_2+y_3=x_1x_2+x_3x_4+x_1x_3+x_2x_4+x_1x_4+x_3x_4=b,$$

$$\begin{aligned} y_1y_2+y_1y_3+y_2y_3 &= -4x_1x_2x_3x_4 \\ &\quad +(x_1+x_2+x_3+x_4)(x_1x_2x_3+x_1x_2x_4+x_1x_3x_4+x_2x_3x_4) \\ &= ac-4d, \end{aligned}$$

$$\begin{aligned} y_1y_2y_3 &= (x_1x_2x_3+x_1x_2x_4+x_1x_3x_4+x_2x_3x_4)^2 \\ &\quad +x_1x_2x_3x_4\{(x_1+x_2+x_3+x_4)^2-4(x_1x_2+x_1x_3+\ldots+x_3x_4)\} \\ &= c^2+d(a^2-4b). \end{aligned}$$

* This is due to the fact (shown in § 29, Ex. 2, and § 30) that any permutation of x_1, x_2, x_3, x_4 merely permutes y_1, y_2, y_3, so that any symmetric function of y_1, y_2, y_3 is a symmetric function of x_1, x_2, x_3, x_4 and hence rationally expressible in terms of a, b, c, d.

Hence equation (21) is identical with the resolvent (16). Next,

$$\begin{aligned} t^2 &= (x_1+x_2+x_3+x_4)^2-4(x_1+x_2)(x_3+x_4) \\ &= a^2-4(x_1x_2+x_1x_3+\ \ldots\ +x_3x_4)+4x_1x_2+4x_3x_4 \\ &= a^2-4b+4y_1. \end{aligned}$$

Again, $x_1+x_2+x_3+x_4=-a$. Hence

$$x_1+x_2=\tfrac{1}{2}(t-a), \quad x_3+x_4=\tfrac{1}{2}(-t-a).$$

To find x_1x_2 and x_3x_4, we note that their sum is y_1, while

$$-c=x_1x_2(x_3+x_4)+x_3x_4(x_1+x_2)=x_1x_2\left(\frac{-t-a}{2}\right)+x_3x_4\left(\frac{t-a}{2}\right).$$

$$\therefore\ x_1x_2=(c-\tfrac{1}{2}ay_1+\tfrac{1}{2}ty_1)/t, \quad x_3x_4=(-c+\tfrac{1}{2}ay_1+\tfrac{1}{2}ty_1)/t.$$

Hence x_1 and x_2 are the roots of (17), x_3 and x_4 are the roots of (18).

6. Lagrange's *à priori* solution of the quartic (12) is quite similar to the preceding. A root $y_1=x_1x_2+x_3x_4$ of the cubic (16) is first obtained. Then $x_1x_2\equiv z_1$ and $x_3x_4\equiv z_2$ are the roots of

$$z^2-y_1z+d=0.$$

Then x_1+x_2 and x_3+x_4 are found from the relations

$$(x_1+x_2)+(x_3+x_4)=-a,$$

$$z_2(x_1+x_2)+z_1(x_3+x_4)=x_3x_4x_1+x_3x_4x_2+x_1x_2x_3+x_1x_2x_4=-c.$$

$$\therefore\ x_1+x_2=\frac{-az_1+c}{z_1-z_2}, \quad x_3+x_4=\frac{az_2-c}{z_1-z_2}.$$

Hence x_1 and x_2 are given by a quadratic, as also x_3 and x_4.

7. In solving the auxiliary cubic (16), the first irrationality entering (see § 2) is

$$\Delta\equiv(y_1-y_2)(y_2-y_3)(y_1-y_3).$$

But

$$y_1-y_2=(x_1-x_4)(x_2-x_3),$$

$$y_2-y_3=(x_1-x_2)(x_3-x_4), \quad y_1-y_3=(x_1-x_3)(x_2-x_4),$$

in view of (20). Hence

$$\Delta=(x_1-x_2)(x_1-x_3)(x_1-x_4)(x_2-x_3)(x_2-x_4)(x_3-x_4). \tag{22}$$

By § 2, the reduced form of (16) is $\eta^3+P\eta+Q=0$, where

$$(23) \qquad \begin{cases} P=ac-4d-\frac{1}{3}b^2, \\ Q=-a^2d+\frac{1}{3}abc+\frac{8}{3}bd-c^2-\frac{2}{27}b^3. \end{cases}$$

Applying (8), with a change of sign, we get

$$(24) \qquad \Delta=6\sqrt{-3}\sqrt{\tfrac{1}{4}Q^2+\tfrac{1}{27}P^3}.$$

CHAPTER II.

SUBSTITUTIONS; RATIONAL FUNCTIONS.

8. The operation which replaces x_1 by x_α, x_2 by x_β, x_3 by x_γ, ..., x_n by x_ν, where $\alpha, \beta, \ldots, \nu$ form a permutation of $1, 2, \ldots, n$, is called a **substitution** on $x_1, x_2, x_3, \ldots, x_n$. It is usually designated

$$\begin{pmatrix} x_1 & x_2 & x_3 & \ldots & x_n \\ x_\alpha & x_\beta & x_\gamma & \ldots & x_\nu \end{pmatrix}.$$

But the order of the columns is immaterial; the substitution may also be written

$$\begin{pmatrix} x_2 & x_1 & x_3 & \ldots & x_n \\ x_\beta & x_\alpha & x_\gamma & \ldots & x_\nu \end{pmatrix}, \quad \text{or} \quad \begin{pmatrix} x_n & x_1 & x_2 & x_3 & \ldots \\ x_\nu & x_\alpha & x_\beta & x_\gamma & \ldots \end{pmatrix}, \ldots$$

The substitution which leaves every letter unaltered,

$$\begin{pmatrix} x_1 & x_2 & x_3 & \ldots & x_n \\ x_1 & x_2 & x_3 & \ldots & x_n \end{pmatrix},$$

is called the **identical substitution** and is designated I.

9. THEOREM. *The number of distinct substitutions on n letters is* $n! \equiv n(n-1) \ldots 3 \cdot 2 \cdot 1$.

For, to every permutation of the n letters there corresponds a substitution.

EXAMPLE. The $3!=6$ substitutions on $n=3$ letters are:

$$I = \begin{pmatrix} x_1 & x_2 & x_3 \\ x_1 & x_2 & x_3 \end{pmatrix}, \quad a = \begin{pmatrix} x_1 & x_2 & x_3 \\ x_2 & x_3 & x_1 \end{pmatrix}, \quad b = \begin{pmatrix} x_1 & x_2 & x_3 \\ x_3 & x_1 & x_2 \end{pmatrix},$$
$$c = \begin{pmatrix} x_1 & x_2 & x_3 \\ x_1 & x_3 & x_2 \end{pmatrix}, \quad d = \begin{pmatrix} x_1 & x_2 & x_3 \\ x_3 & x_2 & x_1 \end{pmatrix}, \quad e = \begin{pmatrix} x_1 & x_2 & x_3 \\ x_2 & x_1 & x_3 \end{pmatrix}.$$

Applying these substitutions to the function $\psi \equiv x_1 + \omega x_2 + \omega^2 x_3$, we obtain the following six distinct functions (cf. § 3):

$$\psi_I = x_1 + \omega x_2 + \omega^2 x_3 \equiv \psi, \quad \psi_a = x_2 + \omega x_3 + \omega^2 x_1 = \omega^2 \psi, \quad \psi_b = x_3 + \omega x_1 + \omega^2 x_2 = \omega \psi,$$
$$\psi_c = x_1 + \omega x_3 + \omega^2 x_2, \quad \psi_d = x_2 + \omega x_2 + \omega^2 x_1 = \omega^2 \psi_c, \quad \psi_e = x_2 + \omega x_1 + \omega^2 x_3 = \omega \psi_c.$$

Applying them to the function $\phi \equiv (x_1-x_2)(x_2-x_3)(x_3-x_1)$, we obtain

$$\phi_I = \phi_a = \phi_b = \phi, \qquad \phi_c = \phi_d = \phi_e = -\phi.$$

Hence ϕ remains unaltered by I, a, b, but is changed by c, d, e.

10. Product. Apply first a substitution s and afterwards a substitution t, where

$$s = \begin{pmatrix} x_1 & x_2 & \dots & x_n \\ x_\alpha & x_\beta & \dots & x_\nu \end{pmatrix}, \quad t = \begin{pmatrix} x_\alpha & x_\beta & \dots & x_\nu \\ x_{\alpha'} & x_{\beta'} & \dots & x_{\nu'} \end{pmatrix}.$$

The resulting permutation $x_{\alpha'}, x_{\beta'}, \dots, x_{\nu'}$ can be obtained directly from the original permutation $x_1, x_2, \dots, x_n$ by applying a *single* substitution, namely,

$$u = \begin{pmatrix} x_1 & x_2 & \dots & x_n \\ x_{\alpha'} & x_{\beta'} & \dots & x_{\nu'} \end{pmatrix}.$$

We say that u is the **product** of s by t and write $u = st$.

Similarly, stv denotes the substitution w which arises by applying first s, then t, and finally v, so that $stv = uv = w$. The order of applying the factors is from left to right.*

EXAMPLES. For the substitutions on three letters (§ 9),

$$ab = ba = I, \quad ac = d, \quad ca = e, \quad ad = e, \quad da = c,$$
$$aa = b, \quad bb = a, \quad abc = Ic = c, \quad aca = da = c.$$

Applying the substitution a to the function ϕ, we get ϕ_a; applying the substitution c to ϕ_a, we get ϕ_d. Hence $\phi_{ac} = \phi_d$. Likewise $\phi_{ab} = \phi_I = \phi$, $\phi_{ba} = \phi$.

11. Multiplication of substitutions is **not commutative** in general.

Thus, in the preceding example, $ac \neq ca$, $ad \neq da$. But $ab = ba$, so that a and b are said to be **commutative**.

12. Multiplication of substitutions is **associative**: $st \cdot v = s \cdot tv$.

Let s, t, and their product $st = u$ have the notations of § 10. If

$$v = \begin{pmatrix} x_{\alpha'} & x_{\beta'} & \dots & x_{\nu'} \\ x_{\alpha''} & x_{\beta''} & \dots & x_{\nu''} \end{pmatrix}, \quad \text{then } tv = \begin{pmatrix} x_\alpha & x_\beta & \dots & x_\nu \\ x_{\alpha''} & x_{\beta''} & \dots & x_{\nu''} \end{pmatrix}.$$

$$\therefore\ st \cdot v = uv = \begin{pmatrix} x_1 & x_2 & \dots & x_n \\ x_{\alpha''} & x_{\beta''} & \dots & x_{\nu''} \end{pmatrix} = \begin{pmatrix} x_1 & x_2 & \dots & x_n \\ x_\alpha & x_\beta & \dots & x_\nu \end{pmatrix} \begin{pmatrix} x_\alpha & \dots & x_\nu \\ x_{\alpha''} & \dots & x_{\nu''} \end{pmatrix} = s \cdot tv.$$

EXAMPLE. For 3 letters, $ac \cdot a = da = c$, $a \cdot ca = ae = c$.

* This is the modern use. The inverse order ts, vts was used by Cayley and Serret.

13. Powers. We write s^2 for ss, s^3 for sss, etc. Then

$$s^m s^n = s^{m+n} \qquad (m \text{ and } n \text{ positive integers}). \tag{25}$$

For, by the associative law, $s^m s^n = s^m \cdot ss^{n-1} = s^{m+1}s^{n-1} = \ldots$

14. Period. Since there is only a finite number $n!$ of distinct substitutions on n letters, some of the powers

$$s,\ s^2,\ s^3,\ \ldots \text{ ad infinitum}$$

must be equal, say $s^m = s^{m+n}$, where m and n are positive integers. Then $s^m = s^m s^n$, in view of (25). Hence s^n leaves unaltered each of the n letters, so that $s^n = I$.

The *least* positive integer σ such that $s^\sigma = I$ is called the **period** of s. It follows that

$$s,\ s^2,\ \ldots\ s^{\sigma-1},\ s^\sigma \equiv I \tag{26}$$

are all distinct; while $s^{\sigma+1}, s^{\sigma+2}, \ldots, s^{2\sigma-1}, s^{2\sigma}$ are repetitions of the substitutions (26). Hence the first σ powers are repeated periodically in the infinite series of powers.

EXAMPLES. From the example in § 10, we get

$a^2 = b$, $a^3 = a^2 a = ba = I$, whence a is of period 3;
$b^2 = a$, $b^3 = b^2 b = ab = I$, whence b is of period 3;
c, d, e are of period 2; I is of period 1.

15. Inverse substitution. To every substitution s there corresponds one and only one substitution s' such that $ss' = I$. If

$$s = \begin{pmatrix} x_1 & x_2 & \ldots & x_n \\ x_\alpha & x_\beta & \ldots & x_\nu \end{pmatrix}, \text{ then } s' = \begin{pmatrix} x_\alpha & x_\beta & \ldots & x_\nu \\ x_1 & x_2 & \ldots & x_n \end{pmatrix}.$$

Evidently $s's = I$. We call s' the **inverse** of s and denote it henceforth by s^{-1}. Hence

$$ss^{-1} = s^{-1}s = I, \quad (s^{-1})^{-1} = s.$$

If s is of period σ, then $s^{-1} = s^{\sigma-1}$. Since s replaces a rational function $f \equiv f(x_1, \ldots, x_n)$ by $f_s \equiv f(x_\alpha, \ldots, x_\nu)$, s^{-1} replaces f_s by f.

EXAMPLES. For the substitutions on 3 letters (§ 9),

$$a = \begin{pmatrix} x_1 & x_2 & x_3 \\ x_2 & x_3 & x_1 \end{pmatrix}, \quad a^{-1} = \begin{pmatrix} x_2 & x_3 & x_1 \\ x_1 & x_2 & x_3 \end{pmatrix} \equiv \begin{pmatrix} x_1 & x_3 & x_2 \\ x_3 & x_1 & x_2 \end{pmatrix} = b,$$

$$b^{-1} = a, \quad c^{-1} = c, \quad d^{-1} = d, \quad e^{-1} = e, \quad I^{-1} = I.$$

These results also follow from those of the examples in § 14. For the functions of § 9 the substitution a replaces ψ by ψ_a; $a^{-1}=b$ replaces ψ_a by ψ.

16. THEOREM. *If* $st=sr$, *then* $t=r$.

Multiplying st and sr on the left by s^{-1}, we get

$$s^{-1}st=t, \quad s^{-1}sr=r.$$

17. THEOREM. *If* $ts=rs$, *then* $t=r$.

18. Abbreviated notation for substitutions. Substitutions like

$$a=\begin{pmatrix} x_1 & x_2 & x_3 \\ x_2 & x_3 & x_1 \end{pmatrix}, \quad b=\begin{pmatrix} x_1 & x_3 & x_2 \\ x_3 & x_2 & x_1 \end{pmatrix}, \quad q=\begin{pmatrix} x_2 & x_3 & x_1 & x_4 \\ x_3 & x_1 & x_4 & x_2 \end{pmatrix},$$

which replace the first letter in the upper row by the second letter in the upper row, the second by the third letter in the upper row, and so on, finally, the last letter of the upper row by the first letter of the upper row, are called **circular substitutions** or **cycles.** Instead of the earlier double-row notation, we employ a single-row notation for cycles. Thus

$$a=(x_1x_2x_3), \quad b=(x_1x_3x_2), \quad q=(x_2x_3x_1x_4).$$

Evidently $(x_1x_2x_3)=(x_2x_3x_1)=(x_3x_1x_2)$, since each replaces x_1 by x_2, x_2 by x_3, and x_3 by x_1. *A cycle is not altered by a cyclic permutation of its letters.*

Any substitution can be expressed as a product of circular substitutions affecting different letters. Thus

$$\begin{pmatrix} x_1 & x_2 & x_3 \\ x_1 & x_3 & x_2 \end{pmatrix}=(x_1)(x_2x_3), \quad \begin{pmatrix} x_1 & x_2 & x_3 & x_4 & x_5 & x_6 \\ x_3 & x_6 & x_5 & x_4 & x_1 & x_2 \end{pmatrix}=(x_1x_3x_5)(x_2x_6)(x_4).$$

A cycle of a single letter is usually suppressed, with the understanding that a letter not expressed is unaltered by the substitution. Thus $(x_1)(x_2x_3)$ is written (x_2x_3).

A circular substitution of two letters is called a **transposition.**

19. Tables of all substitutions on n letters, for $n=3, 4, 5$.

For $n=3$, the $3!=6$ substitutions are (compare § 9):

I=identity, $a=(x_1x_2x_3)$, $b=(x_1x_3x_2)$,
$c=(x_2x_3)$, $d=(x_1x_3)$, $e=(x_1x_2)$.

For $n=4$, the 24 substitutions are (only the indices being written):

I=identity;

6 transpositions: (12), (13), (14), (23), (24), (34);

8 cycles of 3 letters: (123), (132), (124), (142), (134), (143), (234), (243);

6 cycles of 4 letters: (1234), (1243), (1324), (1342), (1423), (1432);

3 products of 2 transpositions: (12)(34), (13)(24), (14)(23).

For $n=5$ the $5!=120$ substitutions include

I=identity;

$\frac{5\cdot4}{2}=10$ transpositions of type (12);

$\frac{5\cdot4\cdot3}{3}=20$ cycles of type (123);

$\frac{5\cdot4\cdot3\cdot2}{4}=30$ cycles of type (1234);

$\frac{5\cdot4\cdot3\cdot2\cdot1}{5}=24$ cycles of type (12345);

$5\cdot3=15$ * products of type (12)(34);

20 † products of type (123)(45).

EXERCISES.

1. The period of $(1\,2\,3\ldots n)$ is n; its inverse is $(n\,n-1\ldots3\,2\,1)$.

2. The period of any substitution is the least common multiple of the periods of its cycles. Thus (123)(45) is of period 6.

3. Give the number of substitutions on 6 letters of each type.

4. Show that the function $x_1x_2+x_3x_4$ is unaltered by the substitutions I, (x_1x_2), (x_3x_4), $(x_1x_2)(x_3x_4)$, $(x_1x_3)(x_2x_4)$, $(x_1x_4)(x_2x_3)$, $(x_1x_3x_2x_4)$, $(x_1x_4x_2x_3)$.

5. Show that $x_1x_2+x_3x_4$ is changed into $x_1x_3+x_2x_4$ by (x_2x_3), (x_1x_4), $(x_1x_3x_2)$, $(x_1x_2x_4)$, $(x_1x_4x_3)$, $(x_2x_3x_4)$, $(x_1x_2x_4x_3)$, $(x_1x_3x_4x_2)$.

6. Write down the eight substitutions on four letters not given in Exs. 4 and 5, and show that each changes $x_1x_2+x_3x_4$ into $x_1x_4+x_2x_3$.

---

* Since the omitted letter may be any one of five, while one of the four chosen letters may be associated with any one of the other three letters.

† The same number as of type (123), since $(45)=(54)$.

CHAPTER III.

SUBSTITUTION GROUPS; RATIONAL FUNCTIONS.

20. A set of distinct substitutions $s_1, s_2, \ldots, s_m$ forms a **group** if the product of any two of them (whether equal or different) is a substitution of the set. The number m of distinct substitutions in a group is called its **order**, the number n of letters operated on by its substitutions is called its **degree**. The group is designated $G_m^{(n)}$.

All the $n!$ substitutions on n letters form a group, called the **symmetric group on n letters** $G_{n!}^{(n)}$. In fact, the product of any two substitutions on n letters is a substitution on n letters. The name of this group is derived from the fact that its substitutions leave unaltered any rational symmetric function of the letters.

EXAMPLE 1. For the six substitutions on $n=3$ letters, given in § 9, the *multiplication table* is as follows:*

$G_6^{(3)}$:

	I	a	b	c	d	e
I	I	a	b	c	d	e
a	a	b	I	d	e	c
b	b	I	a	e	c	d
c	c	e	d	I	b	a
d	d	c	e	a	I	b
e	e	d	c	b	a	I

Thus $ad=e$ is given in the intersection of row a and column d.

EXAMPLE 2. The substitutions I, a, b form a group with the multiplication table

	I	a	b
I	I	a	b
a	a	b	I
b	b	I	a

* It was partially established in the example of § 10.

If s is a substitution of period m, the substitutions

$$I, s, s^2, \ldots, s^{m-1}$$

form a group of order m called a **cyclic group.**

EXAMPLE 3. I, $a=(123)$, $b=a^2=(132)$ form a cyclic group (Ex. 2).

EXAMPLE 4. I, $s=(123)(45)$, $s^2=(132)$, $s^3=(45)$, $s^4=(123)$, $s^5=(132)(45)$ form a cyclic group of order 6 and degree 5.

21. FUNDAMENTAL THEOREM. *All the substitutions on $x_1, x_2, \ldots, x_n$ which leave unaltered a rational function $\phi(x_1, x_2, \ldots, x_n)$ form a group G.*

Let ϕ_s denote the function obtained by applying to ϕ the substitution s. If a and b are two substitutions which leave ϕ unaltered, then $\phi_a \equiv \phi$, $\phi_b \equiv \phi$. Hence

$$(\phi_a)_b = (\phi)_b = \phi_b = \phi, \quad \text{or} \quad \phi_{ab} = \phi.$$

Hence the product ab is one of the substitutions which leave ϕ unaltered. Hence the set has the group property.

The group G is called the **group of the function** ϕ, while ϕ **is said to belong to the group** G.

EXAMPLE 1. The only substitutions on 3 letters which leave unaltered the function $(x_1-x_2)(x_2-x_3)(x_3-x_1)$ are (by § 9) I, $a=(x_1x_2x_3)$, $b=(x_1x_3x_2)$. Hence they form a group (compare Ex. 2, § 20). Another function belonging to this group is

$$(x_1+\omega x_2+\omega^2 x_3)^3, \quad \omega \text{ an imaginary cube root of unity.}$$

EXAMPLE 2. The only substitution on 3 letters which leaves unaltered $x_1+\omega x_2+\omega^2 x_3$ is the identity I (§ 9). Thus the substitution I alone forms a group G_1 of order 1.

EXAMPLE 3. The rational functions occurring in the solution of the quartic equation (§ 4) furnish the following substitution groups on four letters:

a) The symmetric group G_{24} of all the substitutions on 4 letters.

b) The group to which the function $y_1=x_1x_2+x_3x_4$ belongs (Exs. 4–6, p. 14):

$$G_8 = \{I, (12), (34), (12)(34), (13)(24), (14)(23), (1324), (1423)\}.$$

c) Since $y_2 \equiv x_1x_3+x_2x_4$ is derived from $y_1 \equiv x_1x_2+x_3x_4$ by interchanging x_2 and x_3, the group of y_2 is derived from G_8 by interchanging x_2 and x_3 within its substitutions. Hence the group of y_2 is

$$G_8' = \{I, (13), (24), (13)(24), (12)(34), (14)(32), (1234), (1432)\}.$$

d) The group of $y_3 \equiv x_1x_4 + x_2x_3$, derived from G_8 by interchanging x_2 and x_4, is:

$$G_8'' = \{I, (14), (32), (14)(32), (13)(42), (12)(43), (1342), (1243)\}.$$

e) The function $x_1 + x_2 - x_3 - x_4$ belongs to the group

$$H_4 = \{I, (12), (34), (12)(34)\}.$$

Since all the substitutions of H_4 are contained in the group G_8, H_4 is called a **subgroup** of G_8. But H_4 is not a subgroup of G_8'.

f) The function $\psi \equiv y_1 + \omega y_2 + \omega^2 y_3$, or

$$\psi \equiv x_1x_2 + x_3x_4 + \omega(x_1x_3 + x_2x_4) + \omega^2(x_1x_4 + x_2x_3),$$

remains unaltered by the substitutions which leave y_1, y_2, and y_3 simultaneously unaltered and by no other substitutions. Hence the group of ψ is composed of the substitutions common to the three groups G_8, G_8', G_8'', forming their **greatest common subgroup**:

$$G_4 = \{I, r = (12)(34), s = (13)(24), t = (14)(23)\}$$

That these four substitutions form a group may be verified directly:

$$r^2 = I,\ s^2 = I,\ t^2 = I,$$

$$rs = sr = t,\ rt = tr = s,\ st = ts = r.$$

Hence any two of its substitutions are commutative. This **commutative group** G_4 is therefore a subgroup of G_8, G_8', and G_8''.

22. THEOREM. *Every substitution can be expressed as a product of transpositions in various ways.*

Any substitution can be expressed as a product of cycles on different letters (§ 18). A single cycle on n letters can be expressed as a product of $n-1$ transpositions:

$$(1234 \ldots n) = (12)(13)(14) \ldots (1n).$$

EXAMPLES. $(123)(456) = (12)(13)(45)(46)$,
$(132) = (13)(12) = (12)(23) = (12)(23)(45)(45)$.

23. THEOREM. *Of the various decompositions of a given substitution s into a product of transpositions, all contain an even number of transpositions* (*whence s is called an* **even substitution**), *or all contain an odd number of transpositions* (*whence s is called an* **odd substitution**).

A single transposition changes the sign of the **alternating function** *

$$\phi=(x_1-x_2)(x_1-x_3)(x_1-x_4)\ldots(x_1-x_n)$$
$$\cdot(x_2-x_3)(x_2-x_4)\ldots(x_2-x_n)$$
$$\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot$$
$$\cdot(x_{n-1}-x_n).$$

Thus (x_1x_2) affects only the terms in the first and second lines of the product, and replaces them by

$$(x_2-x_1)(x_2-x_3)(x_2-x_4)\ldots(x_2-x_n)$$
$$\cdot(x_1-x_3)(x_1-x_4)\ldots(x_1-x_n).$$

Hence, if s is the product of an even number of transpositions, it leaves ϕ unaltered; if s is the product of an odd number of transpositions, it changes ϕ into $-\phi$.

COROLLARY. The totality of even substitutions on n letters forms a group, called the **alternating group on n letters.**

EXAMPLE 1. The alternating group on 3 letters is (§§ 9, 19)

$$G_3^{(3)}=\{I,\quad (123),\quad (132)\}.$$

EXAMPLE 2. The alternating group on 4 letters is (§ 19)

$G_{12}^{(4)}=\{I,$ (12)(34), (13)(24), (14)(23), and the 8 cycles of three letters$\}$.

24. THEOREM. *The order of the alternating group on n letters is* $\frac{1}{2}\cdot n!$

Denote the distinct *even* substitutions by

$$(e)\qquad e_1,\ e_2,\ e_3,\ \ldots,\ e_k.$$

Let t be a transposition. Then the products

$$(o)\qquad e_1t,\ e_2t,\ e_3t,\ \ldots,\ e_kt$$

are all distinct (§ 17) and being *odd* are all different from the substitutions (e). Moreover, every odd substitution s occurs in

* It may be expressed as the determinant

$$\begin{vmatrix} 1 & x_1 & x_1^2 & \ldots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \ldots & x_2^{n-1} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 1 & x_n & x_n^2 & \cdot & x_n^{n-1} \end{vmatrix}.$$

the set (o), since st is even and hence identical with a certain e_i, so that

$$s = e_i t^{-1} = c_i t.$$

Hence the $2k$ substitutions given by (e) and (o) furnish all the $n!$ substitutions on n letters without repetitions. Hence $k = \frac{1}{2} \cdot n!$

25. As shown in § 21, every rational function $\phi(x_1, \ldots, x_n)$ *belongs* to a certain group G of substitutions on $x_1, \ldots, x_n$, namely, is unaltered by the substitutions of G and changed by all other substitutions on $x_1, \ldots, x_n$. We next prove the inverse theorem:

Given a group G of substitutions on $x_1, \ldots, x_n$, we can construct a rational function $\phi(x_1, \ldots, x_n)$ belonging to G.

Let $G = \{a \equiv I, b, c, \ldots, l\}$ and consider the function

$$V = m_1 x_1 + m_2 x_2 + \ldots + m_n x_n,$$

where $m_1, m_2, \ldots, m_n$ are all distinct. Then V is an $n!$-valued function. Applying to V the substitutions of G, we get

$$V_a \equiv V, V_b, \ldots, V_l. \tag{27}$$

all of which are distinct. Applying to (27) any substitution c of G, we get

$$V_{ac}, V_{bc}, \ldots, V_{lc}. \tag{28}$$

These values are a permutation of the values (27). since $ac, bc, \ldots, lc$ all belong to the *group* G and are all distinct (§ 17). Hence any symmetric function of $V_a, V_b, \ldots, V_l$ is unaltered by all the substitutions of G. By suitable choice of the parameter ρ, the symmetric function

$$\phi \equiv (\rho - V)(\rho - V_b)(\rho - V_c) \ldots (\rho - V_l)$$

will be altered by every substitution s not in G. Indeed,

$$\phi_s \equiv (\rho - V_s)(\rho - V_{bs})(\rho - V_{cs}) \ldots (\rho - V_{ls})$$

is not identical with ϕ since V_s is different from $V, V_b, V_c, \ldots, V_l$.

EXAMPLE 1. For $G = \{I, a = (x_1 x_2 x_3), b = (x_1 x_3 x_2)\}$, take

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

Then $V_a = \omega^2 V$, $V_b = \omega V$. Hence

$$V + V_a + V_b = (1 + \omega + \omega^2) V = 0, \; VV_a + VV_b + V_a V_b = 0, \; VV_a V_b = V^3.$$

The function V^3 belongs to G (see Ex. 1, § 21).

EXAMPLE 2. For $G=\{I, c=(x_2x_3)\}$, take the V of Ex. 1. Then

$$VV_c=(x_1+\omega x_2+\omega^2x_3)(x_1+\omega x_3+\omega^2x_2)=c_1^2-3c_2$$

is unaltered by all six substitutions on the three letters. But

$$\phi=(\rho-V)(\rho-V_c)=\rho^2-(2x_1-x_2-x_3)\rho+c_1^2-3c_2,$$

for $\rho\neq 0$, is changed by every substitution on the letters not in G. Hence, for any $\rho\neq 0$, ϕ belongs to G.

EXERCISES

Ex. 1. If ω is a primitive μth root of unity,

$$(x_1+\omega x_1+\omega^2x_3+\ \ldots\ +\omega^{\mu-1}x_\mu)^\mu$$

belongs to the cyclic group $\{I, a, a^2, \ldots, a^{\mu-1}\}$, where $a\equiv(x_1\,x_1\ldots x_\mu)$.

Ex. 2. Taking $V=x_1+ix_1-x_1-ix_4$ and $s=(x_1x_1)(x_3x_4)$, show that $VV_s\equiv i(x_1-x_3)^2+i(x_2-x_4)^2$ belongs to G_8 of § 21, that $V+V_s$ belongs to H_4 of § 21, while $(\rho-V)(\rho-V_s)$, for $\rho\neq 0$, belongs to the group $\{I, s\}$

Ex 3. Taking $V=x_1+ix_1-x_2-ix_4$ and $t=(x_1x_3)(x_2x_4)$, show that VV_t belongs to the group $\{I, t\}$

Ex. 4. If $a_1, a_2, \ldots, a_n$ are any distinct numbers, the function

$$V=x_1^{a_1}x_2^{a_2}\ldots\ x_n^{a_n}$$

is $n!$-valued, and $V+V_b+V_c+\ \ldots\ +V_l$ belongs to $\{I, b, c, \ldots, l\}$.

Ex. 5. If ϕ belongs to G and ϕ' belongs to G', constants a and a' exist such that $a\phi+a'\phi'$ belongs to the greatest common subgroup of G and G'.

26. THEOREM. *The order of a subgroup is a divisor of the order of the group.*

Consider a group G of order N and a subgroup H composed of the substitutions

$$h_1=I,\ h_2,\ h_3,\ \ldots,\ h_P. \tag{29}$$

If G contains no further substitutions. $N=P$, and the theorem is true. Let next G contain a substitution g_2 not in H. Then G contains the products

$$g_2,\ h_2g_2,\ h_3g_2,\ \ldots,\ h_Pg_2. \tag{30}$$

The latter are all distinct (§ 17), and all different from the substitutions (29), since $h_\alpha g_2=h_\beta$ requires that $g_2=h_\alpha^{-1}h_\beta=$ a sub-

stitution of H contrary to hypothesis. Hence the substitutions (29) and (30) give $2P$ distinct substitutions of G. If there are no other substitutions in G, $N=2P$ and the theorem is true. Let next G contain a substitution g_3 not in one of the sets (29) and (30). Then G contains

$$g_3, h_2g_3, h_3g_3, \ldots, h_Pg_3. \tag{31}$$

As before, the substitutions (31) are all distinct and all different from the substitutions (29). Moreover, they are all different from the substitutions (30), since $h_\alpha g_3 = h_\beta g_2$ requires that $g_3 = h_\alpha^{-1} h_\beta g_2$ shall belong to the set (30), contrary to hypothesis. We now have $3P$ distinct substitutions of G. Either $N=3P$ or else G contains a substitution g_4 not in one of the sets (29), (30) (31). In the latter case, G contains the products

$$g_4, h_2g_4, h_3g_4, \ldots, h_Pg_4, \tag{32}$$

all of which are distinct and all different from the substitutions (29), (30), (31), so that we have $4P$ distinct substitutions. Proceeding in this way, we finally reach a last set of P substitutions

$$g_\nu, h_2g_\nu, h_3g_\nu, \ldots, h_Pg_\nu, \tag{33}$$

since the order of H is finite (§ 9). Hence $N=\nu P$.

DEFINITION. The number $\nu=\dfrac{N}{P}$ is called the **index** of the subgroup H under G, and the relation is exhibited in the adjacent scheme.

$$\begin{matrix} G \\ \nu \\ H \end{matrix}$$

COROLLARY. The order of any group H of substitutions on n letters is a divisor of $n!$ Indeed H is a subgroup of the symmetric group $G_{n!}$ on n letters.

27. THEOREM. *The period of any substitution contained in a group G of order N is a divisor of N.*

If the group G contains a substitution s of period P, it contains the cyclic subgroup H of order P:

$$H=\{s, s^2, \ldots, s^{P-1}, s^P \equiv I\}.$$

Then, by § 26, P is a divisor of N.

COROLLARY.* If the order N of a group G is a *prime* number, G is a cyclic group composed of the first N powers of a substitution of period N.

28. As shown in § 26, the N substitutions of a group G can be arranged in a **rectangular array** with the substitutions of any subgroup H in the first row:

$$\begin{array}{lllll} h_1=I & h_2 & h_3 & \dots & h_P \\ g_2 & h_2g_2 & h_3g_2 & \dots & h_Pg_2 \\ g_3 & h_2g_3 & h_3g_3 & \dots & h_Pg_3 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ g_\nu & h_2g_\nu & h_3g_\nu & \dots & h_Pg_\nu \end{array}$$

Here $g_1=I, g_2, g_3, \dots, g_\nu$ are called the right-hand **multipliers**. They may be chosen in various ways: g_2 is any substitution of G not in the first row; g_3 any substitution of G not in the first and second rows; g_4 any substitution of G not in the first, second, and third rows; etc.

Similarly, a rectangular array for the substitutions of G may be formed by employing left-hand multipliers.

29. THEOREM. *If ψ is a rational function of $x_1, \dots, x_n$ belonging to a subgroup H of index ν under G, then ψ is ν-valued under G.*

Apply to ψ all the N substitutions of G arranged in a rectangular array, as in § 28. All the substitutions belonging to a row give the same value since

$$\psi_{h_i g_\alpha} = (\psi_{h_i})_{g_\alpha} = (\psi)_{g_\alpha} = \psi_{g_\alpha}.$$

Hence there result at most ν values. But, if

$$\psi_{g_\alpha} = \psi_{g_\beta} \qquad (\beta < \alpha),$$

then $\psi_{g_\alpha g_\beta^{-1}} = \psi$, so that $g_\alpha g_\beta^{-1}$ is a substitution h_i leaving ψ

* This result is a special case of the following theorems, proved in any treatise on groups:

If the order of a group is divisible by a *prime* number p, the group contains a subgroup of order p (Cauchy)

If p^t is the highest power of the prime number p dividing the order of a group, the group contains a subgroup of order p^t (Sylow).

unaltered. Hence $g_\alpha = h_i g_\beta$, contrary to the assumption made in forming the rectangular array.

DEFINITION. The ν distinct functions $\phi, \phi_{\sigma_2}, \phi_{\sigma_3}, \ldots, \phi_{\sigma_\nu}$ are called the **conjugate values** of ϕ under the group G.

Taking G to be the symmetric group $G_{n!}$, we obtain Lagrange's result:

The number of distinct values which a rational function of n letters takes when operated on by all $n!$ substitutions is a divisor of $n!$

EXAMPLE 1. To find the distinct conjugate values of the functions

$$\Delta \equiv (x_1-x_2)(x_2-x_3)(x_3-x_1), \quad \theta \equiv (x_1+\omega x_2+\omega^2 x_3)^3$$

under the symmetric group G_6 on 3 letters, we note that they belong to the subgroup $G_3 = \{I, a=(x_1x_2x_3), b=(x_1x_3x_2)\}$, as remarked in § 21, Ex. 1. The rectangular array and the conjugate values are:

$$\begin{array}{cccc|c|c} I, & a=(x_1x_2x_3), & b=(x_1x_3x_2) & \| & \Delta & \theta \\ c=(x_2x_3), & ac=(x_3x_1), & bc=(x_1x_2) & \| & -\Delta & \theta_c \end{array}$$

EXAMPLE 2. To obtain the conjugate values of $x_1x_2+x_3x_4$ under the symmetric group G_{24} on 4 letters, we rearrange the results of Exs. 4, 5, 6, page 14, and exhibit a rectangular array of the substitutions of G_{24} with those of G_8 in the first row:

$$\begin{array}{cccccccc|l} I, & (12), & (34), & (12)(34), & (13)(24), & (14)(23), & (1324), & (1423) & x_1x_2+x_3x_4 \\ (234), & (1342), & (23), & (132), & (143), & (124), & (14), & (1243) & x_1x_3+x_2x_4 \\ (243), & (1432), & (24), & (142), & (123), & (134), & (1234), & (13), & x_1x_4+x_2x_3 \end{array}$$

30. THEOREM. *The ρ distinct values which a rational function $\phi(x_1, \ldots, x_n)$ takes when operated on by all $n!$ substitutions are the roots of an equation of degree ρ whose coefficients are rational functions of the elementary symmetric functions*

$$(34) \quad c_1 = x_1+x_2+\ldots+x_n, \quad c_2 = x_1x_2+x_1x_3+\ldots+x_{n-1}x_n, \ldots,$$
$$c_n = x_1x_2\ldots x_n.$$

Let the ρ distinct values of $\phi(x_1, \ldots, x_n)$ be designated

$$(35) \qquad \phi_1 \equiv \phi, \quad \phi_2, \quad \phi_3, \quad \ldots, \quad \phi_\rho.$$

They are the roots of an equation $(y-\phi_1)(y-\phi_2)\ldots(y-\phi_\rho)=0$ whose coefficients $\phi_1+\phi_2+\ldots+\phi_\rho, \ldots, \pm\phi_1\phi_2\ldots\phi_\rho$ are symmetric functions of $\phi_1, \phi_2, \ldots, \phi_\rho$. After proving that they are symmetric

functions of $x_1, x_2, \ldots, x_n$, we may conclude (Appendix) that they are rational functions of the expressions (34). We have therefore only to prove that any substitution s on $x_1, \ldots, x_n$ merely interchanges the functions (35). Let s replace the functions (35) by respectively

$$\phi_1', \phi_2', \phi_3', \ldots, \phi_\rho'. \tag{36}$$

In the first place, each ϕ' is identical with a function (35). For, there exists a substitution t which replaces ϕ_1 by ϕ_i, and s replaces ϕ_i by ϕ_i', so that ts replaces ϕ_1 by ϕ_i'. Hence there is a substitution on $x_2, \ldots, x_n$ which replaces ϕ_1 by ϕ_i', so that ϕ_i' occurs in the set (35).

In the second place, the functions (36) are all distinct. For, if $\phi_i' \equiv \phi_j'$, we obtain, upon applying the substitution s^{-1}, $\phi_i \equiv \phi_j$, contrary to assumption.

DEFINITION. The equation having the roots (35) is called the **resolvent equation** for ϕ.

Compare the solution of the general cubic (§ 3) and general quartic (§ 5).

31. LAGRANGE'S THEOREM. *If a rational function $\phi(x_1, x_2, \ldots, x_n)$ remains unaltered by all the substitutions which leave another rational function $\psi(x_1, x_2, \ldots, x_n)$ unaltered, then ϕ is a rational function of ψ and $c_1, c_2, \ldots, c_n$.*

The function ψ belongs to a certain group

$$H = \{h_1 \equiv I, h_2, h_3, \ldots, h_P\}.$$

Let ν be the index of H under the symmetric group $G_{n!}$. Consider a rectangular array of the substitutions of $G_{n!}$ with those of H in the first row:

$$\begin{array}{cccc|c|c} I & h_2 & \ldots & h_P & \psi \equiv \psi_1 & \phi \equiv \phi_1 \\ g_2 & h_2 g_2 & \ldots & h_P g_2 & \psi_{g_2} \equiv \psi_2 & \phi_{g_2} \equiv \phi_2 \\ \cdot & \cdot & \cdot & \cdot & \cdot \quad \cdot \quad \cdot & \cdot \quad \cdot \quad \cdot \\ g_\nu & h_2 g_\nu & \ldots & h_P g_\nu & \psi_{g_\nu} \equiv \psi_\nu & \phi_{g_\nu} \equiv \phi_\nu \end{array}$$

Then $\psi_1, \psi_2, \ldots, \psi_\nu$ are all distinct (§ 29); but $\phi_1, \phi_2, \ldots, \phi_\nu$ need not be distinct since ϕ belongs to a group G which may be larger than H. Under any substitution s on $x_1, x_2, \ldots, x_n$, the functions

$\psi_1, \psi_2, \ldots, \psi_\nu$ are merely permuted (§ 30). Moreover, if s replaces ψ_i by ψ_j, it replaces ϕ_i by ϕ_j. Set

$$g(t) \equiv (t-\psi_1)(t-\psi_2)\ldots(t-\psi_\nu),$$

$$\lambda(t) \equiv g(t)\left(\frac{\phi_1}{t-\psi_1}+\frac{\phi_2}{t-\psi_2}+\ldots+\frac{\phi_\nu}{t-\psi_\nu}\right),$$

so that $\lambda(t)$ is an integral function of degree $\nu-1$ in t. Since $\lambda(t)$ remains unaltered under every substitution s, its coefficients are rational symmetric functions of $x_1, x_2, \ldots, x_n$ and hence are rational functions of the expressions (34). Taking $\psi_1 \equiv \psi$ for t, we get *

$$\lambda(\psi_1) = (\psi_1-\psi_2)(\psi_1-\psi_3)\ldots(\psi_1-\psi_\nu)\cdot\phi_1 = g'(\psi_1)\cdot\phi_1,$$

$$\phi = \frac{\lambda(\psi)}{g'(\psi)}. \tag{37}$$

The theorem may be given the convenient symbolic form:

If $\begin{matrix} G:\phi \\ | \\ H:\psi \end{matrix}$, *then* $\phi = Rat.\ Func.\ (\psi;\ c_1, \ldots, c_n)$.

Taking first $H=G$ and next $H=I$, we obtain the corollaries:

COROLLARY 1. *If two rational functions belong to the same group, either is a rational function of the other and* $c_1, c_2, \ldots, c_n$.

COROLLARY 2. *Every rational function of* $x_1, x_2, \ldots, x_n$ *is a rational function of any* $n!$*-valued function* (*such as* V *of* § 25) *and* $c_1, c_2, \ldots, c_n$.

EXAMPLE 1. The functions Δ and θ of Ex. 1, § 29, belong to the same group $G_3^{(3)}$. We may therefore express Δ in terms of θ. By §§ 2, 3,

$$3\sqrt{-3}\,\Delta = (x_1+\omega^2x_2+\omega x_3)^3-(x_1+\omega x_2+\omega^2x_3)^3 = \frac{(c_1^2-3c_2)^3}{\theta}-\theta.$$

The expression for $\theta \equiv \psi_1^3$ in terms of Δ is given in § 34 below.

* The relation (37) is valid as long as $x_1, x_2, \ldots, x_n$ denote indeterminate quantities, since $\psi_1, \ldots, \psi_\nu$ are algebraically distinct so that $g'(\psi)$ is not identically zero. In case special values are assigned to $x_1, \ldots, x_n$ such that two or more of the functions $\psi_1, \ldots, \psi_\nu$ become numerically equal, then $g'(\psi)=0$, and ϕ is not a rational function of $\psi, c_1, \ldots, c_n$. In this case, see Lagrange, *Œuvres*, vol. 3, pp. 374–388; Serret, *Algèbre*, II, pp. 434–441. But this subject is considered in Part II.

EXAMPLE 2. The function $y_1 \equiv x_1x_2+x_3x_4$ belongs to the group G_8 and $t \equiv x_1+x_2-x_3-x_4$ belongs to the subgroup H_4 (§ 21). Hence y_1 is a rational function of t and the coefficients a, b, c, d of the equation whose roots are x_1, x_2, x_3, x_4. By § 5, $y_1 = \frac{1}{4}(t^2-a^2+4b)$.

EXAMPLE 3. The function $\psi_1 \equiv x_1+\omega x_2+\omega^2 x_3$ has $3!=6$ values. Hence every rational function of x_1, x_2, x_3 is a rational function of ψ_1 and c_1, c_2, c_3. The expressions for x_1, x_2, x_3 themselves follow from the formulæ (11) of § 3. Thus

$$x_1 = \tfrac{1}{3}\left(c_1+\psi_1+\frac{c_1^2-3c_2}{\psi_1}\right).$$

32. THEOREM. *If* $\nu \Big| \begin{matrix} G:\phi \\ H:\psi \end{matrix}$, *then* ψ *satisfies an equation of degree* ν *whose coefficients are rational functions of* $\phi, c_1, \ldots, c_n$.

As in § 29, we consider the ν conjugate values of ψ under G:

$$\psi, \psi_{\sigma_2}, \psi_{\sigma_3}, \ldots, \psi_{\sigma_\nu}.$$

Under any substitution of the group G, these values are merely permuted amongst themselves. Hence any symmetric function of them is unaltered under every substitution of G and therefore, by Lagrange's Theorem, is a rational function of $\phi, c_1, \ldots, c_n$. The same is therefore true of the coefficients of the equation

$$(w-\psi)(w-\psi_{\sigma_2}) \ldots (w-\psi_{\sigma_\nu}) = 0.$$

CHAPTER IV.

THE GENERAL EQUATION FROM THE GROUP STANDPOINT.

33. In the light of the preceding theorems, we now reconsider Cardan's solution (§ 2) of the reduced cubic equation $y^3+py+q=0$. The determination of its roots y_1, y_2, y_3 depends upon the chain of resolvent equations:

$$\xi^2=\frac{q^2}{4}+\frac{p^3}{27}, \quad \text{where } \xi\equiv\frac{\sqrt{-3}}{18}(y_1-y_2)(y_2-y_3)(y_3-y_1);$$

$$z^3=-\frac{q}{2}+\xi, \quad \text{where } z\equiv\tfrac{1}{3}(y_1+\omega y_2+\omega^2 y_3);$$

$$y_1=z-\frac{p}{3z}; \quad y_2=\omega z-\frac{\omega^2 p}{3z}, \quad y_3=\omega^2 z-\frac{\omega p}{3z}.$$

Initially given are the elementary symmetric functions

$$y_1+y_2+y_3=0, \quad y_1y_2+y_1y_3+y_2y_3=p, \quad -y_1y_2y_3=q,$$

belonging to the symmetric group G_6 on y_1, y_2, y_3. Solving a quadratic resolvent equation, we find the two-valued function ξ, which belongs to the subgroup G_3 of G_6 (§ 21, Ex. 1). Solving next a cubic resolvent equation, we find the six-valued function z, which belongs to the subgroup G_1 of G_3 (§ 21, Ex. 2). Then y_1, y_2, y_3 are rational functions of z, p, q, since they belong to the respective groups

$$G_2'=\{I, (y_2y_3)\}, \quad G_2''=\{I, (y_1y_3)\}, \quad G_2'''=\{I, (y_1y_2)\},$$

each containing G_1 (also direct from § 31, Cor. 2). From the group standpoint, the solution is therefore expressed by the scheme:

$$\begin{array}{cccc} G_6:p,q & & & \\ 2\,| & & & \\ G_3:\xi & G_2':y_1 & G_2'':y_2 & G_2''':y_3 \\ 3\,| & | & | & | \\ G_1:z & G_1:z & G_1:z & G_1:z \end{array}$$

34. The same method leads to a solution of the general cubic

$$x^3-c_1x^2+c_2x-c_3=0.$$

To the symmetric group G_6 on x_1, x_2, x_3 belong the functions

$$x_1+x_2+x_3=c_1, \quad x_1x_2+x_1x_3+x_2x_3=c_2, \quad x_1x_2x_3=c_3.$$

To the subgroup $G_3=\{I, (x_1x_2x_3), (x_1x_3x_2)\}$ belongs the function

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

In view of Ex. 3, page 4, Δ is a root of the binomial resolvent

$$\Delta^2=c_1^2c_2^2+18c_1c_2c_3-4c_2^3-4c_1^3c_3-27c_3^2.$$

By § 3 and § 2, we have for $\psi_1=x_1+\omega x_2+\omega^2x_3$, $\psi_4=x_1+\omega^2x_2+\omega x_3$,

$$\psi_1^3+\psi_4^3= \quad 2c_1^3-9c_1c_2+27c_3,$$

$$\psi_1^3-\psi_4^3=-3\sqrt{-3}(x_1-x_2)(x_2-x_3)(x_3-x_1)=-3\sqrt{-3}\,\Delta.$$

$$\therefore \ \psi_1^3=\tfrac{1}{2}(2c_1^3-9c_1c_2+27c_3-3\sqrt{-3}\,\Delta),$$

$$\psi_4^3=\tfrac{1}{2}(2c_1^3-9c_1c_2+27c_3+3\sqrt{-3}\,\Delta).$$

After determining* ψ_1 by extracting a cube root, the value of ψ_4 is (§ 3)

$$\psi_4=(c_1^2-3c_2)\div\psi_1.$$

Then, as in § 3, x_1, x_2, x_3 are rationally expressible in terms of ψ_1:

$$x_1=\tfrac{1}{3}(c_1+\psi_1+\psi_4), \quad x_2=\tfrac{1}{3}(c_1+\omega^2\psi_1+\omega\psi_4), \quad x_3=\tfrac{1}{3}(c_1+\omega\psi_1+\omega^2\psi_4).$$

35. The solution given in § 5 of the general quartic equation

$$x^4+ax^3+bx^2+cx+d=0 \tag{12}$$

may be exhibited from the group standpoint by the scheme:

$$\begin{array}{l} G_{24}: a, b, c, d \\ \quad | \\ G_8 : y_1=x_1x_2+x_3x_4, \quad t^2=(x_1+x_2-x_3-x_4)^2 \\ \quad | \\ H_4 : t, \ x_1+x_2, \ x_3+x_4, \ x_1x_2, \ x_3x_4 \\ H_2: x_1-x_2 \quad H_2': x_3-x_4. \end{array}$$

Here $H_2=\{I, (x_3x_4)\}$, $H_2'=\{I, (x_1x_2)\}$, G_8 and H_4 being given in § 21.

* For another method see Ex. 4, page 41.

36. Lagrange's second solution of (12) is based upon the direct computation of the function $x_1+x_2-x_3-x_4$. Its six conjugate values under G_{24} are $\pm t_1$, $\pm t_2$, $\pm t_3$, where

$$t_1=x_1+x_3-x_3-x_4, \quad t_2=x_1+x_3-x_2-x_4, \quad t_3=x_1+x_4-x_2-x_3.$$

The resolvent sextic is therefore

$$(\tau^2-t_1^2)(\tau^2-t_2^2)(\tau^2-t_3^2)=0.$$

Its coefficients may be computed * easily by observing that

$$t_1^2=a^2-4b+4y_1, \quad t_2^2=a^2-4b+4y_2, \quad t_3^2=a^2-4b+4y_3,$$

as follows from § 5. Using the results there established, we get

$$t_1^2+t_2^2+t_3^2=3a^2-12b+4(y_1+y_2+y_3)=3a^2-8b,$$

$$t_1^2t_2^2+t_1^2t_3^2+t_2^2t_3^2=3(a^2-4b)^2+8(a^2-4b)(y_1+y_2+y_3)+16(y_1y_2+y_1y_3+y_2y_3)$$
$$=3a^4-16a^2b+16b^2+16ac-64d,$$

$$t_1^2t_2^2t_3^2=(a^2-4b)^3+4(a^2-4b)^2(y_1+y_2+y_3)+16(a^2-4b)(y_1y_2+y_1y_3+y_2y_3)+64y_1y_2y_3$$
$$=\{8c+a(a^2-4b)\}^2.$$

The resolvent becomes a cubic equation upon setting $\tau^2=\sigma$. Denote its roots by $\sigma_1=t_1^2$, $\sigma_2=t_2^2$, $\sigma_3=t_3^2$. Then

$$x_1+x_2-x_3-x_4=\sqrt{\sigma_1}, \quad x_1+x_3-x_2-x_4=\sqrt{\sigma_2},$$
$$x_1+x_4-x_2-x_3=\sqrt{\sigma_3}, \quad x_1+x_2+x_3+x_4=-a.$$

From these we get

$$(38)\quad \begin{cases} x_1=\tfrac{1}{4}(-a+\sqrt{\sigma_1}+\sqrt{\sigma_2}+\sqrt{\sigma_3}), & x_2=\tfrac{1}{4}(-a+\sqrt{\sigma_1}-\sqrt{\sigma_2}-\sqrt{\sigma_3}), \\ x_3=\tfrac{1}{4}(-a-\sqrt{\sigma_1}+\sqrt{\sigma_2}-\sqrt{\sigma_3}), & x_4=\tfrac{1}{4}(-a-\sqrt{\sigma_1}-\sqrt{\sigma_2}+\sqrt{\sigma_3}). \end{cases}$$

The signs of $\sqrt{\sigma_1}$ and $\sqrt{\sigma_2}$ may be chosen arbitrarily, while that of $\sqrt{\sigma_3}$ follows from

$$(39)\qquad \sqrt{\sigma_1}\sqrt{\sigma_2}\sqrt{\sigma_3}=t_1t_2t_3=4ab-8c-a^3.$$

Indeed, we may determine the sign in

$$t_1t_2t_3=\pm\{8c+a(a^2-4b)\}$$

* Compare Ex. 5, page 41.

by taking $x_1=1$, $x_2=x_3=x_4=0$, whence $a=-1$, $b=c=d=0$, $t_1t_2t_3=1$.

37. The following solution of the quartic is of greater interest as it leads directly to a 24-valued function V, in terms of which all the roots are expressed rationally. As in § 5, we determine y_1 and t, belonging to G_8 and H_4 respectively, by solving a cubic and a quadratic equation. To the subgroup

$$G_2=\{I, (x_1x_2)(x_3x_4)\}$$

of H_4 belongs the function $\psi=V^2$, while to G_1 belongs V, where

$$V=(x_1-x_2)+i(x_3-x_4).$$

Under H_4, ψ takes a second value $\psi_1=\{(x_1-x_2)-i(x_3-x_4)\}^2$. Then

$$z^2-(\psi+\psi_1)z+\psi\psi_1=0$$

is the resolvent equation for ψ. But

$$\psi\psi_1=\{(x_1-x_2)^2+(x_3-x_4)^2\}^2=\{a^2-2b-2y_1\}^2=\tfrac{1}{4}\{3a^2-8b-t^2\}^2,$$
$$\psi+\psi_1=2\{(x_1-x_2)^2-(x_3-x_4)^2\}=2(x_1-x_2+x_3-x_4)(x_1-x_2-x_3+x_4)$$
$$=2(4ab-8c-a^3)\div t,$$

in view of (39). After finding ψ and ψ_1, we get

$$V=\sqrt{\psi}.\quad V_1=\sqrt{\psi_1}=(x_1-x_2)-i(x_3-x_4),$$
$$V_1=\tfrac{1}{2}(3a^2-8b-t^2)\div V. \tag{40}$$

Having the four functions t, V, V_1, and $x_1+x_2+x_3+x_4=-a$, we get

$$\begin{cases} x_1=\tfrac{1}{4}(-a+t+V+V_1), & x_2=\tfrac{1}{4}(-a+t-V-V_1), \\ x_3=\tfrac{1}{4}(-a-t-iV+iV_1), & x_4=\tfrac{1}{4}(-a-t+iV-iV_1). \end{cases} \tag{41}$$

38. The solution of the general cubic (§ 34) and the solution of the general quartic (§ 37) each consists essentially in finding the value of a function which is altered by every substitution on the roots and which therefore belongs to the identity group G_1. Likewise, the general equation of degree n,

$$x^n-c_1x^{n-1}+c_2x^{n-2}-\ldots+(-1)^nc_n=0, \tag{42}$$

could be completely solved if we could determine *one* value of a function belonging to the group G_1; for example,

(43) $V=m_1x_1+m_2x_2+\ldots+m_nx_n$ (m's all distinct).

In fact, each x_i is a rational function of $V, c_1, \ldots, c_n$ by § 31. For the cubic and quartic, the scheme for determining such a function V was as follows:

$$\begin{array}{l} G_6: c_1,\ c_2,\ c_3 \\ 2 \mid \\ G_3: (x_1+\omega x_2+\omega^2 x_3)^3 \\ 3 \mid \\ G_1: x_1+\omega x_2+\omega^2 x_3 \end{array} \qquad \begin{array}{l} G_{24}: a, b, c, d \\ 3 \mid \\ G_8: x_1x_2+x_3x_4 \\ 2 \mid \\ H_4: x_1+x_2-x_3-x_4 \\ 2 \mid \\ G_2: (x_1-x_2+ix_3-ix_4)^2 \\ 2 \mid \\ G_1: x_1-x_2+ix_3-ix_4 \end{array}$$

The same plan of solution applied to (42) gives the following scheme:

$$\begin{array}{ll} G_{n!}: c_1, c_2, \ldots, c_n & \\ \lambda \mid & \\ H: \xi, & \xi^\lambda+R_1(c_1, \ldots, c_n)\xi^{\lambda-1}+\ldots=0 \\ \mu \mid & \\ K: \eta, & \eta^\mu+R_2(\xi, c_1, \ldots, c_n)\eta^{\mu-1}+\ldots=0 \\ \vdots & \\ M: \phi & \\ \rho \mid & \\ G_1: V, & V^\rho+R(\phi\ c_1, \ldots, c_n)V^{\rho-1}+\ldots=0. \end{array}$$

Such resolvent equations would exist in view of the theorem of § 32. In case the resolvent equations were all binomial, the function V (and hence $x_1, \ldots, x_n$) would be found by the extraction of roots of known quantities, so that the equation would be solvable by radicals. We may limit the discussion to binomial equations of *prime* degree, since $z^{pq}=A$ may be replaced by the chain of equations $z^p=u$, $u^q=A$. The following question therefore arises:

If $\nu \begin{array}{l} G: \phi \\ \mid \\ H: \psi \end{array}$, when will the resolvent equation for ψ take the form

(44) $$\psi^\nu=\text{Rat. Func. }(\phi, c_1, \ldots, c_n).$$

Since ν is assumed to be prime, there exists a primitive νth root of unity, namely a number ω having the properties

$$\omega^\nu = 1, \quad \omega^k \neq 1 \text{ for any positive integer } k < \nu.$$

Hence the roots of (44) may be written

$$\psi, \ \omega\psi, \ \omega^2\psi, \ \ldots, \ \omega^{\nu-1}\psi. \tag{45}$$

Let $\psi_1 \equiv \psi, \psi_2, \ldots, \psi_\nu$ denote the conjugate functions to ψ under G (their number is ν by § 29). Now ψ belongs to the group H by hypothesis. Let ψ_2 belong to the group H_2, ψ_3 to $H_3, \ldots, \psi_\nu$ to H_ν. Since the roots (45) differ only by constant factors, they belong to the same group. Hence a *necessary* condition is that

$$H = H_2 = H_3 = \ldots = H_\nu.$$

39. The first problem is to determine the group to which belongs the function ψ_s into which ψ is changed by a substitution s, when it is given that ψ belongs to the group

$$H = \{h_1 \equiv I, \ h_2, \ \ldots, \ h_P\}.$$

If a substitution σ leaves ψ_s unaltered, so that $\psi_{s\sigma} = \psi_s$, then

$$\psi_{s\sigma s^{-1}} = \psi_{ss^{-1}} = \psi.$$

Hence $s\sigma s^{-1} = h$, where h is a substitution of H. Then

$$\sigma = s^{-1}hs.$$

Inversely, every substitution $s^{-1}hs$ leaves ψ_s unaltered. Hence ψ_s belongs to the group

$$\{s^{-1}h_1s = I, \ s^{-1}h_2s, \ \ldots, \ s^{-1}h_Ps\},$$

which will be designated $s^{-1}Hs$. We may state the theorem:

If ψ belongs to the subgroup H of index ν under G, the conjugates

$$\psi, \ \psi_{g_2}, \ \ldots, \ \psi_{g_\nu},$$

of ψ under G, belong to the respective groups

$$H, \ g_2^{-1}Hg_2, \ \ldots, \ g_\nu^{-1}Hg_\nu.$$

DEFINITIONS. The latter groups are said to form a **set of conjugate subgroups** of G. In case they are all identical, H is called a **self-conjugate subgroup** of G (or an **invariant subgroup** of G).

Hence a necessary condition that the general equation of degree n shall be solvable by radicals under the plan of solution proposed in § 38 is that each group in the series shall be a self-conjugate subgroup of prime index under the preceding group.

Note that the group $G_1=\{I\}$ is self-conjugate under every group G since $g^{-1}Ig=I$.

EXAMPLE 1. Let G be the symmetric group G_6 on 3 letters and let H be the group $G_3=\{I, (x_1x_2x_3), (x_1x_3x_2)\}$. Let $g_2=(x_2x_3)$. Then

$$\psi=(x_1+\omega x_2+\omega^2x_3)^3, \quad \psi_{g_2}=(x_1+\omega^2x_2+\omega x_3)^3$$

form a set of conjugate functions under G. Now ψ belongs to H and ψ_{g_2} belongs to the group $\{I, (x_1x_3x_2), (x_1x_2x_3)\}$, whose substitutions are derived from those of H by interchanging the letters x_2 and x_3, since that interchange replaces ψ by ψ_{g_2}. To proceed by the general method, we would compute

$$(x_2x_3)^{-1}(x_1x_2x_3)(x_2x_3)=(x_1x_3x_2), \quad (x_2x_3)^{-1}(x_1x_3x_2)(x_2x_3)=(x_1x_2x_3).$$

By either method we find that the group of ψ and ψ_{g_2} are identical, so that G_3 is self-conjugate under G_6. Also, G_1 is self-conjugate under G_3. Hence the necessary condition that the general cubic shall be solvable by radicals is satisfied.

EXAMPLE 2. Consider the conjugate values x_1, x_2, x_3 of x_1 under G_6.

$$\begin{array}{cc|c} I, & (x_2x_3) & x_1 \\ g_2=(x_1x_2), & (x_2x_3)g_2=(x_1x_2x_3) & x_2 \\ g_3=(x_1x_3), & (x_2x_3)g_3=(x_1x_3x_2) & x_3 \end{array}$$

Hence $H=\{I, (x_2x_3)\}$ is not self-conjugate under G_6. Here

$$g_2^{-1}Hg_2=\{I, (x_1x_3)\}\neq H, \quad g_3^{-1}Hg_3=\{I, (x_1x_2)\}\neq H.$$

40. DEFINITIONS. Two substitutions a and a' of a group G are called **conjugate under** G if there exists a substitution g belonging to G such that $g^{-1}ag=a'$. Then a' is called the **transform** of a by g.

There is a simple method of finding $g^{-1}ag$ without performing the actual multiplication. Suppose first that a is a circular substitution, say $a=(\alpha\beta\gamma\delta)$, while g is any substitution, say

$$g=\begin{pmatrix} \alpha & \beta & \gamma & \delta & \dots & \lambda \\ \alpha' & \beta' & \gamma' & \delta' & \dots & \lambda' \end{pmatrix}.$$

$$\therefore\ g^{-1}=\begin{pmatrix} \alpha' & \beta' & \gamma' & \delta' & \dots & \lambda' \\ \alpha & \beta & \gamma & \delta & \dots & \lambda \end{pmatrix}, \quad g^{-1}ag=\begin{pmatrix} \alpha' & \beta' & \gamma' & \delta' & \varepsilon' & \dots & \lambda' \\ \beta' & \gamma' & \delta' & \alpha' & \varepsilon' & \dots & \lambda' \end{pmatrix}.$$

Hence $g^{-1}ag=(\alpha'\beta'\gamma'\delta')$ may be obtained by applying the substitution g to the letters of the cycle $a=(\alpha\beta\gamma\delta)$.

Let next $a=a_1a_2a_3\ldots$, where $a_1, a_2, \ldots$ are circular substitutions. Then

$$g^{-1}ag=g^{-1}a_1g\cdot g^{-1}a_2g\cdot g^{-1}a_3g\ldots$$

Hence $g^{-1}ag$ is obtained by applying g within the cycles of a.

Thus $$(123)^{-1}\cdot(12)(34)\cdot(123)=(23)(14).$$

COROLLARY. Since any substitution transforms an even substitution into an even substitution, the alternating group $G_{\frac{1}{2}n!}$ is a self-conjugate subgroup of the symmetric group $G_{n!}$.

41. THEOREM. *Of the following groups on four letters:*

$$G_{24},\ G_{12},\ G_4=\{I,\ (12)(34),\ (13)(24),\ (14)(23)\},$$
$$G_2=\{I,\ (12)(34)\},\ G_1=\{I\},$$

each is a self-conjugate subgroup of the preceding group.

By the Corollary of § 40, G_{12} is self-conjugate under G_{24}. To show that G_4 is self-conjugate under G_{12} (as well as under G_{24}), we observe that G_4 contains all the substitutions of the type $(\alpha\beta)(\gamma\delta)$, while the latter is transformed into a substitution of the form $(\alpha'\beta')(\gamma'\delta')$ by any given substitution on four letters. That G_2 is self-conjugate under G_4 follows from the fact that (12)(34), (13)(24), (14)(23) all transform (12)(34) into itself.*

42. The necessary condition (§ 39) that the general quartic

$$x^4+ax^3+bx^2+cx+d=0$$

shall be solvable by radicals is satisfied in view of the preceding theorem. We proceed to determine a chain of *binomial* resolvent equations of *prime* degree which leads to a 24-valued function

$$V=x_1-x_2+ix_3-ix_4,$$

* This also follows from § 21, Ex. (*f*), since $rs=sr$ gives $s^{-1}rs=r$.

in terms of which the roots x_1, x_2, x_3, x_4 are rationally expressible. Let

$$(20) \qquad y_1=x_1x_2+x_3x_4, \quad y_2=x_1x_3+x_2x_4, \quad y_3=x_1x_4+x_2x_3,$$

as in § 4. The scheme for the solution is the following:

$$\begin{array}{l} G_{24}: a, b, c, d \\ \sim \\ G_{12}: \Delta = (x_1-x_2)(x_1-x_3)(x_1-x_4)(x_2-x_3)(x_2-x_4)(x_3-x_4) \\ 3 \\ G_3: \phi_1=y_1+\omega y_2+\omega^2 y_3 \\ 2 \\ G_2: \lambda = \phi_1 \div (x_1+x_2-x_3-x_4) \\ 2 \\ G_1: V = x_1-x_2+ix_3-ix_4 \end{array}$$

Referring to formulæ (22), (23), (24) of § 7, and setting $P=-4I$, $Q=16J$, we get

$$\Delta = 16\sqrt{I^3-27J^2},$$

$$I \equiv d-\frac{ac}{4}+\frac{b^2}{12}, \quad J \equiv \frac{bd}{6}-\frac{c^2}{16}-\frac{a^2d}{16}+\frac{abc}{48}-\frac{b^3}{216}.$$

Hence Δ is a root of the binomial resolvent $\Delta^2=256(I^3-27J^2)$. The resolvent for ϕ_1 is the binomial equation

$$(\phi-\phi_1)(\phi-\omega\phi_1)(\phi-\omega^2\phi_1) \equiv \phi^3-\phi_1{}^3=0.$$

By Lagrange's Theorem, $\phi_1{}^3$ is a rational function of Δ, a, b, c, d. To determine this function, set $\phi_2=y_1+\omega^2y_2+\omega y_3$. Then (§§ 2, 7)

$$\phi_2{}^3-\phi_1{}^3=3\sqrt{-3}(y_1-y_2)(y_2-y_3)(y_3-y_1)=-3\sqrt{-3}\,\Delta,$$
$$\phi_2{}^3+\phi_1{}^3=2(y_1{}^3+y_2{}^3+y_3{}^3)+12y_1y_2y_3+3(\omega+\omega^2)\delta,$$

where $\delta \equiv y_1{}^2y_2+y_1y_2{}^2+y_1{}^2y_3+y_1y_3{}^2+y_2{}^2y_3+y_2y_3{}^2$ satisfies the relations

$$(y_1+y_2+y_3)(y_1y_2+y_1y_3+y_2y_3)=\delta+3y_1y_2y_3,$$
$$(y_1+y_2+y_3)^3=3\delta+6y_1y_2y_3+y_1{}^3+y_2{}^3+y_3{}^3.$$

$$\therefore \phi_2{}^3+\phi_1{}^3=2(y_1+y_2+y_3)^3-9(y_1+y_2+y_3)(y_1y_2+y_1y_3+y_2y_3)+27y_1y_2y_3$$
$$=2b^3-9b(ac-4d)+27(c^2+a^2d-4bd)=-432J.$$

upon applying the relations in § 5. Hence

$$\phi_1^3 = \tfrac{1}{2}3\sqrt{-3}\,\Delta - 216J.$$

In view of Lagrange's Theorem, y_1, y_2, and y_3 are rational functions of ϕ_1. These functions may be determined as follows:

$$\begin{aligned}\phi_1\phi_2 &= y_1^2+y_2^2+y_3^2+(\omega+\omega^2)(y_1y_2+y_1y_3+y_2y_3)\\ &= (y_1+y_2+y_3)^2-3(y_1y_2+y_1y_3+y_2y_3)\\ &= b^2-3ac+12d \equiv H.\end{aligned}$$

From $y_1+y_2+y_3=b$, $y_1+\omega y_2+\omega^2 y_3=\phi_1$, $y_1+\omega^2 y_2+\omega y_3=\dfrac{H}{\phi_1}$,

$$y_1=\tfrac{1}{3}\left(b+\phi_1+\frac{H}{\phi_1}\right),\quad y_2=\tfrac{1}{3}\left(b+\omega^2\phi_1+\frac{\omega H}{\phi_1}\right),\quad y_3=\tfrac{1}{3}\left(b+\omega\phi_1+\frac{\omega^2 H}{\phi_1}\right).$$

Setting $t \equiv x_1+x_2-x_3-x_4$, we obtain for $\lambda=\phi_1/t$ the binomial resolvent

$$\lambda^2 = \phi_1^2 \div (a^2-4b+4y_1),$$

upon replacing t^2 by its value given in § 5. Next, we have (§ 37)

$$\begin{aligned}V^2 &= (x_1-x_2)^2-(x_3-x_4)^2+2i(x_1-x_2)(x_3-x_4)\\ &= \frac{4ab-8c-a^3}{t}+2i(y_2-y_3)\\ &= \frac{\lambda}{\phi_1}(4ab-8c-a^3)+\tfrac{2}{3}\sqrt{3}\left(\phi_1-\frac{H}{\phi_1}\right).\end{aligned}$$

The values of x_1, x_2, x_3, x_4 are then given by (41) in connection with (40).

SERIES OF COMPOSITION OF THE SYMMETRIC GROUP ON n LETTERS.

43. DEFINITIONS. Let a given group G have a **maximal** self-conjugate subgroup H, namely, a self-conjugate subgroup of G which is not contained in a larger self-conjugate subgroup of G. Let H have a maximal self-conjugate subgroup K. Such a series of groups, terminating with the identity group G_1,

$$G,\ H,\ K,\ \ldots,\ M,\ G_1,$$

in which each group is a maximal self-conjugate subgroup of the preceding group, forms a **series of composition** of G. The numbers λ (the index of H under G), μ (the index of K under H), ..., ρ (the index of G_1 under M) are called the **factors of composition** of G.

If the series is composed of the groups G and G_1 alone, the group G is called **simple.** Thus a simple group is one containing no self-conjugate subgroup other than itself and the identity group. A group which is not simple is called a **composite group.**

EXAMPLE 1. For the symmetric group on 3 letters, a series of composition is G_6, G_3, G_1 (see Ex. 1, § 39). Since the indices 2, 3 are prime numbers, the self-conjugate subgroups are maximal (see § 26).

EXAMPLE 2. A series of composition of the symmetric group on 4 letters is G_{24}, G_{12}, G_4, G_2, G_1 (§ 41), the indices being prime numbers.

EXAMPLE 3. A cyclic group of prime order is a simple group (§ 26).

44. LEMMA. *If a group on n letters contains all circular substitutions on 3 of the n letters, it is either the symmetric group $G_{n!}$ or else the alternating group $G_{\frac{1}{2}n!}$.*

It is required to show that every *even* substitution s can be expressed as a product of circular substitutions on 3 letters. Let

$$s = t_1 t_2 \ldots t_{2\nu-1} t_{2\nu},$$

where $t_1, \ldots, t_{2\nu}$ are transpositions (§§ 22, 23), and $t_1 \neq t_2$. If t_1 and t_2 have one letter in common, then

$$t_1 t_2 = (\alpha\beta)(\alpha\gamma) = (\alpha\beta\gamma).$$

If, however, t_1 and t_2 have no letter in common, then

$$t_1 t_2 = (\alpha\beta)(\gamma\delta) = (\alpha\beta)(\alpha\gamma)(\gamma\alpha)(\gamma\delta) = (\alpha\beta\gamma)(\gamma\alpha\delta).$$

Similarly, $t_3 t_4$ is either the identity or else equivalent to one cycle on 3 letters or to a product of two such cycles.

Hence the group contains all *even* substitutions on the n letters.

45. THEOREM. *The symmetric group on $n > 4$ letters contains no self-conjugate subgroup besides itself, the identity G_1, and the alternating group $G_{\frac{1}{2}n!}$, so that the latter is the only maximal self-conjugate subgroup of $G_{n!}$ ($n > 4$).*

That the alternating group is self-conjugate under the symmetric group was shown in § 40.

Let $G_{n!}$ have a self-conjugate subgroup H which contains a substitution s not the identity I.

Suppose first that s contains cycles of more than 2 letters:

$$s=(abc\ldots d)(ef\ldots)\ldots$$

Let α, β, δ be any three of the n letters and $\gamma, \varepsilon, \ldots, \phi, \ldots$ the remaining $n-3$ letters. Then H contains the substitutions

$$s_1=(\alpha\beta\gamma\ldots\delta)(\varepsilon\phi\ldots)\ldots, \quad s_2=(\beta\alpha\gamma\ldots\delta)(\varepsilon\phi\ldots)\ldots,$$

the letters indicated by dots in s_1 being the same as the corresponding letters in s_2. The fact that s_1 (and likewise s_2) belongs to H follows since

$$\sigma=\begin{pmatrix} a & b & c & \ldots & d & e & f & \ldots \\ \alpha & \beta & \gamma & \ldots & \delta & \varepsilon & \phi & \ldots \end{pmatrix}$$

is a substitution on the n letters which transforms s into s_1 (§ 40), while any substitution σ of $G_{n!}$ transforms a substitution s of the *self-conjugate* subgroup H into a substitution belonging to H (§ 39). Since H is a group, it contains the product $s_2 s_1^{-1}$, which reduces to $(\alpha\beta\delta)$. Hence H contains a circular substitution on 3 letters chosen arbitrarily from the n letters. Hence H is either $G_{n!}$ or $G_{\frac{1}{2}n!}$ (§ 44).

Suppose next that s contains only transpositions and at least two transpositions. The case $s=(ab)(ac)\ldots=(abc)\ldots$ has been treated. Let therefore

$$s=(ab)(cd)(ef)\ldots(lm).$$

Let $\alpha, \beta, \gamma, \delta$ be any four of the n letters, and $\varepsilon, \phi, \ldots, \lambda, \mu$ the others. Then the self-conjugate subgroup H contains the substitutions

$$s_1=(\alpha\beta)(\gamma\delta)(\varepsilon\phi)\ldots(\lambda\mu), \quad s_2=(\alpha\gamma)(\beta\delta)(\varepsilon\phi)\ldots(\lambda\mu)$$

and therefore also the product $s_2 s_1^{-1}$, which reduces to $(\alpha\delta)(\beta\gamma)$.

Since $n>4$, there is a letter ρ different from $\alpha, \beta, \gamma, \delta$. Hence H contains $(\alpha\rho)(\beta\gamma)$ and therefore the product

$$(\alpha\delta)(\beta\gamma)\cdot(\alpha\rho)(\beta\gamma)=(\alpha\delta\rho).$$

It follows as before that H is either $G_{n!}$ or $G_{\frac{1}{2}n!}$.

Suppose finally that $s=(ab)$. Then the self-conjugate subgroup H contains every transposition, so that $H=G_{n!}$.

46. THEOREM. *The alternating group on $n>4$ letters is simple.*

Let $G_{\frac{1}{2}n!}$ have a self-conjugate subgroup H larger than the identity group G_1. Of the substitutions of H different from the identical substitution I, consider those which affect the least number of letters. All the cycles of any one of them must contain the same number of letters; otherwise a suitable power would affect fewer letters without reducing to the identity I. Again, none of these substitutions contains more than 3 letters in any cycle. For, if H contains

$$s=(1234\lambda\ldots\rho)(\ldots)\ldots,$$

then H contains its transform by the *even* substitution $\sigma=(234)$;

$$s_1=\sigma^{-1}s\sigma=(1342\lambda\ldots\rho)(\ldots)\ldots,$$

where the dots indicate the same letters as in s. Hence H would contain

$$ss_1^{-1}=(142),$$

affecting fewer letters than does s. Finally, none of the substitutions in question contain more than a single cycle. For, if H contains either t or s, where

$$t=(12)(34)\ldots,\quad s=(123)(456)\ldots,$$

it would contain the transform of one of them by the *even* substitution $\kappa=(125)$ and consequently either $t\cdot\kappa^{-1}t\kappa$ or $s^{-1}\cdot\kappa^{-1}s\kappa$. The latter leaves 4 unaltered and affects no letter not contained in s; the former leaves 3 and 4 unaltered and affects but a single letter 5 not contained in t. In either case, there would be a reduction in the number of letters affected.

The substitutions, different from I, which affect the least number of letters are therefore of one of the types (ab), (abc). The former is excluded as it is odd. Hence H contains a substitution

(abc). Let α, β, γ be any three of the n letters, $\delta, \varepsilon, \ldots, \nu$ the others. Then (abc) is transformed into $(\alpha\beta\gamma)$ by *either* of the substitutions

$$r=\begin{pmatrix} a & b & c & d & e & \ldots & n \\ \alpha & \beta & \gamma & \delta & \varepsilon & \ldots & \nu \end{pmatrix}, \quad s=\begin{pmatrix} a & b & c & d & e & \ldots & n \\ \alpha & \beta & \gamma & \varepsilon & \delta & \ldots & \nu \end{pmatrix},$$

where the dots in r indicate the same letters as in s. Since $r=s(\delta\varepsilon)$, one of the substitutions r, s is *even* and hence in $G_{\frac{1}{2}n!}$. Hence, for $n>4$, H contains all the circular substitutions on 3 of the n letters, so that $H=G_{\frac{1}{3}n!}$.

47. It follows from the two preceding theorems that, *for $n>4$, there is a single series of composition of the symmetric group on n letters: $G_{n!}$, $G_{\frac{1}{2}n!}$, G_1.* The theorem holds also for $n=3$, since the only subgroup of G_6 of order 3 is G_3, while the three subgroups of G_6 of order 2 are not self-conjugate (§ 39, Ex. 2). The case $n=4$ is exceptional, since G_{12} contains the self-conjugate subgroup G_4 (§ 41).

Except for $n=4$, the factors of composition of the symmetric group on n letters are 2 and $\frac{1}{2}n!$.

48. It was proposed in § 38 to solve the general equation of degree n by means of a chain of binomial resolvent equations of prime degrees such that a root of each is expressible as a rational function of the roots $x_1, x_2, \ldots, x_n$ of that general equation. As shown in §§ 38–39, a necessary condition is the existence of a series of groups

$$G_{n!}, H, K, \ldots, M, G_1, \tag{46}$$

each a self-conjugate subgroup of prime index under the preceding group. In the language of § 43, this condition requires that $G_{n!}$ shall have a series of composition (46) with the factors of composition all prime. By § 47, this condition is not satisfied if $n\geqq 5$, since $\frac{1}{2}n!$ is then not prime. But the condition is satisfied if $n=3$ or if $n=4$ (§ 39, Ex. 1; § 41). Under the proposed plan of solution, the general equation of degree $n>4$ is therefore not solvable by radicals, whereas the general cubic and general quartic equations are solvable by radicals under this plan (§ 34, § 42).

To complete the proof of the impossibility of the solution by radicals of the general equation of degree $n>4$, it remains to show that the proposed plan is the only possible method. This* was done by Abel (*Œuvres*, vol. 1, page 66) in 1826 by means of the theorem:

Every equation which is solvable by radicals can be reduced to a chain of binomial equations of prime degrees whose roots are rational functions of the roots of the given equation.

As the direct proof of this proposition from our present standpoint is quite lengthy, it will be deferred to Part II (see § 94), where a proof is given in connection with the more general theory due to Galois.

EXERCISES.

1. If $H=\{I, h_2, \ldots, h_P\}$ is a subgroup of G of index 2, H is self-conjugate under G.

Hint: The substitutions of G not in H may be written $g, gh_2, \ldots, gh_P$; or also $g, h_2g, \ldots, h_Pg$. Hence every $h_\beta g$ is some gh_α, so that for every h_β, $g^{-1}h_\beta g$ is some h_α.

2. The group G_8 of § 21 has the self-conjugate subgroups G_2, G_4, H_4, $C_4=\{I, (1324), (12)(34), (1423)\}$. The only remaining self-conjugate subgroups are G_1 and G_8.

3. If a group contains all the circular substitutions on $m+2$ letters, it contains all the circular substitutions on m letters. Hint:

$$(1\,2\,3\ldots m\,m+1\,m+2)^2(m\,m-1\ldots3\,2\,m+2\,1\,m+1)=(1\,2\,3\ldots m-1\,m).$$

4. Compute directly the function ϕ_1^3 of § 34 as follows:

$$\phi_1^3=x_1^3+x_2^3+x_3^3+6x_1x_2x_3+3\omega(x_1^2x_2+x_1x_3^2+x_2^2x_3)+3\omega^2(x_1x_2^2+x_1^2x_3+x_2x_3^2)$$
$$=x_1^3+x_2^3+x_3^3+6x_1x_2x_3-\tfrac{9}{2}(x_1^2x_2+x_1x_3^2+x_1^2x_3+x_1x_2^2+x_2^2x_3+x_2x_3^2)-\tfrac{3}{2}\sqrt{-3}\,\Delta,$$

since

$$x_1^2x_2-x_1x_2^2+x_1x_3^2-x_1^2x_3+x_2^2x_3-x_2x_3^2=-(x_1-x_2)(x_2-x_3)(x_3-x_1)=-\Delta.$$

Twice the remaining part of ϕ_1^3 equals $2c_1^3-9c_1c_2+27c_3$ by § 3.

5. Compute directly the coefficients in § 36 as follows:

$$t_1^2+t_2^2+t_3^2=3\Sigma x_i^2-2\Sigma x_ix_j=3a^2-8b,$$
$$t_1t_2t_3=\Sigma x_1^3+2\Sigma x_1x_2x_3-\Sigma x_1(x_2^2+x_3^2+x_4^2)$$
$$=2\Sigma x_1^3+2\Sigma x_1x_2x_3-\Sigma x_i\Sigma x_j^2=4ab-8c-a^3.$$

---

* For the simpler demonstration by Wantzel, see Serret, *Algèbre*, II, 4th or 5th Edition, p. 512.

SECOND PART.

GALOIS' THEORY OF ALGEBRAIC EQUATIONS.

CHAPTER V.

ALGEBRAIC INTRODUCTION TO GALOIS' THEORY.

49. Differences between Lagrange's and Galois' Theories. Heretofore we have been considering with Lagrange the **general equation** of degree n, that is, an equation with independent variables as coefficients and hence (see page 101) with independent quantities $x_1, x_2, \ldots, x_n$ as roots. Hence we have called two rational functions of the roots equal only when they are identical for all sets of values of $x_1, \ldots, x_n$.

But for an equation whose roots are definite constants, we must consider two rational functions of the roots to be equal when their numerical values are equal, and it may happen that two functions of different form have the same numerical value.

Thus the roots of $x^3+x^2+x+1=0$ are

$$x_1=-1, \quad x_2=+i, \quad x_3=-i \qquad (i\equiv\sqrt{-1}).$$

Hence the functions x_2^2, x_3^2, and x_1 are numerically equal although of different form. We may not apply to the equation $x_2^2=x_3^2$ the substitution $(x_1x_2x_3)$, since $x_3^2\neq x_1^2$. Again, the totality of the substitutions on the roots which leave the function x_2^2 numerically unaltered do not form a group, since the substitutions are I, (x_1x_3), (x_2x_3), $(x_1x_2x_3)$.

Again, the roots of $x^4+1=0$ are

$$x_1=\epsilon, \quad x_2=i\epsilon, \quad x_3=-\epsilon, \quad x_4=-i\epsilon \qquad \left(\epsilon\equiv\frac{1+i}{\sqrt{2}}\right).$$

Hence $x_1^2=\epsilon^2=i$, $x_2x_4=\epsilon^2=i$. The functions x_1^2 and x_2x_4 differ in form, but are equal numerically. Also, x_1^2 equals x_3^2, but differs from x_2^2 and x_4^2. The 12 substitutions which leave x_1^2 numerically unaltered are I,(23),(24),(34),(234),(243),(13),(13)(24),(213),(413), (4213), (4132), the first six leaving x_1^2 formally unaltered and the last six replacing x_1^2 by x_3^2. They do not form a group, since the product (13)(23) is not one of the set.

There are consequently essential difficulties in passing from the theory of the general equation to that of special equations. This important step was made by Galois.*

In rebuilding our theory, special attention must be given to the nature of the coefficients of the equation under discussion,

$$(1) \qquad x^n-c_1x^{n-1}+c_2x^{n-2}-\ldots+(-1)^nc_n=0.$$

Here $c_1, \ldots, c_n$ may be definite constants, or independent variables, or rational functions of other variables. Whereas, in the Lagrange theory, roots of unity and other constants were employed without special notice being taken, in the Galois theory, particular attention is paid to the nature of all new constants introduced.

50. Domain of Rationality. To specify accurately what shall be understood to be a solution to a given problem, we must state the nature of the quantities to be allowed to appear in the solution. For example, we may demand as a solution a real num-

* Évariste Galois was killed in a duel in 1832 at the age of 21. His chief memoir was rejected by the French Academy as lacking rigorous proofs. The night before the duel, he sent to his friend Auguste Chevalier an account of his work including numerous important theorems without proof. The sixty pages constituting the collected works of Galois appeared, fifteen years after they were written, in the *Journal de mathématiques* (1846), and in *Œuvres mathématiques D'ÉVARISTE GALOIS, avec une introduction par M. Émile Picard*, Paris 1897.

ber or we may demand a positive number; for constructions by elementary geometry, we may admit square roots, but not higher roots of arbitrary positive numbers. In the study of a given equation, we naturally admit into the investigation all the irrationalities appearing in its coefficients; for example, $\sqrt{3}$ in considering $x^2+(2-5\sqrt{3})x+2=0$. We may agree beforehand to admit other irrationalities than those appearing in the coefficients.

In a given problem, we are concerned with certain constants or variables

$$R', R'', \ldots, R^{(\mu)} \tag{2}$$

together with all quantities derived from them by a finite number of additions, subtractions, multiplications, and divisions (the divisor not being zero). The resulting system of quantities is called the *domain of rationality* * $(R', R'', \ldots, R^{(\mu)})$.

EXAMPLE 1. The totality of rational numbers forms a domain. It is contained in every domain R. For if ω be any element $\neq 0$ of R, then $\omega \div \omega = 1$ belongs to R; but from 1 may be derived all integers by addition and subtraction, and from these all fractions by division.

EXAMPLE 2. The numbers $a+bi$, where $i=\sqrt{-1}$, while a and b take all rational values, form a domain (i). But the numbers $a+bi$, where a and b take only integral values do not form a domain.

DEFINITION. An equation whose coefficients are expressible as rational functions with integral coefficients of the quantities $R', R'', \ldots, R^{(\mu)}$ will be said to be algebraically solvable (or solvable by radicals) with respect to their domain, if its roots can be derived from $R', R'', \ldots$ by addition, subtraction, multiplication, division, and extraction of a † root of any index, the operations being applied a finite number of times.

51. The term **rational function** is used in Galois' theory only

---

* *Rationalitätsbereich* (Kronecker), *Körper* (Weber), *Field* (Moore).

† If we admitted the extraction of all the pth roots, we would admit the knowledge of all the pth roots of unity. This need not be admitted in Galois' theory (see § 89, Corollary).

in connection with a domain of rationality R. An **integral rational function for** R of certain quantities $u, v, w, \ldots$ is an expression

$$(3) \qquad \sum_{i,j,k,\ldots} C_{ijk\ldots} u^i v^j w^k \ldots,$$

where $i, j, k, \ldots$ are positive integers, and each coefficient $C_{ijk}\ldots$ is a quantity belonging to R. The quotient of two such functions (3) is **a rational function for** R.

Thus, $3u+\sqrt{2}$ is a rational function of u in $(\sqrt{2})$, but not in (1).

52. Equality. As remarked in § 49, two expressions involving only constants are regarded as equal when their *numerical* values are the same. Consider two rational functions

$$\phi(u, v, w, \ldots), \quad \psi(u, v, w, \ldots)$$

with coefficients in a domain $R=(R', R'', \ldots, R^{(\mu)})$. In case R', R'', ... are all constants, we say that ϕ and ψ are **equal** if, for every set of numerical values $u_1, v_1, w_1, \ldots$ which $u, v, w, \ldots$ can assume, the resulting numerical values of ϕ and ψ are equal. In case $R', R'', \ldots, R^{(\mu)}$ depend upon certain independent variables $r', r'', \ldots, r^{(m)}$, we say that ϕ and ψ are equal if, for every set of numerical values which $u, v, w, \ldots, r', r'', \ldots, r^{(m)}$ may assume, the resulting numerical values of ϕ and ψ are equal. When not equal in this sense, ϕ and ψ are said to be **distinct** or **different.**

For example, if u and v are the roots of $x^2+2\rho x+1=0$, the functions $u+v$ and $-2\rho uv$ are rational functions in the domain (ρ), and these rational functions are equal.

DEFINITION. A rational function $\phi(x_1, \ldots, x_n)$ is said to be **unaltered** by a substitution s on $x_1, \ldots, x_n$ if the function $\phi_s(x_1, \ldots, x_n)$ is equal to ϕ in the sense just explained. For brevity, we shall often say that ϕ then remains *numerically* unaltered by s. If $x_1, x_2, \ldots, x_n$ are independent variables, as in Lagrange's theory, and if ϕ_s is identically equal to ϕ, i.e., for all values of $x_1, \ldots, x_n$, we say that ϕ remains *formally* unaltered by s. For examples, see § 49.

53. The preceding definitions are generalizations of those employed in the Lagrange theory. The so-called general equation

of degree n may be viewed as an extreme case of the equations (1) whose coefficients $c_1, \ldots, c_n$ are rational functions in the domain $(R', R'', \ldots, R^{(p)})$. In fact, since its coefficients are independent variables belonging to the domain, they may be taken to replace an equal number of the quantities $R', R'', \ldots$ defining the domain, so that the general equation appears in the form

$$x^n + R'x^{n-1} + R''x^{n-2} + \ldots + R^{(n)} = 0.$$

Its roots are likewise independent variables (p. 101), so that two rational functions of the roots are equal only when identically equal.

54. Reducibility and irreducibility. An integral rational function $F(x)$ whose coefficients belong to a domain R is said to be **reducible in** R if it can be decomposed into integral rational factors of lower degree whose coefficients likewise belong to R; **irreducible in** R if no such decomposition is possible.*

EXAMPLE 1. The function x^2+1 is reducible in the domain (i) since it has the factors $x+i$ and $x+i$, rational in (i). But x^2+1, which is a rational function of x in the domain of rational numbers, is irreducible in that domain.

EXAMPLE 2. x^4+1 is reducible in any domain to which either $\sqrt{2}$, or $\sqrt{-2}$, or i, or $\epsilon \equiv \frac{1+i}{\sqrt{2}}$, belongs, but is irreducible in all other domains. In fact, its linear factors are $x \pm \epsilon$, $x \pm i\epsilon = x \pm \epsilon^3$; while every quadratic factor is of the form $x^2 \pm i$, or $x^2 + ax \pm 1$, $a^2 = \pm 2$.

If $F(x)$ is reducible in R, $F(x)=0$ is said to be a **reducible equation in** R; if $F(x)$ is irreducible in R, $F(x)=0$ is said to be an **irreducible equation in** R.

55. THEOREM. *Let the equations $F(x)=0$ and $G(x)=0$ have their coefficients in a domain R and let $F(x)=0$ be irreducible in R. If one root of $F(x)=0$ satisfies $G(x)=0$, then every root of $F(x)=0$ satisfies $G(x)=0$ and $F(x)$ is a divisor of $G(x)$ in R.*

After dividing out the coefficients of the highest power of x, let

$$F(x) = (x-\xi_1)(x-\xi_2)\ldots(x-\xi_n), \quad G(x) = (x-\eta_1)\ldots(x-\eta_m).$$

* A method to decompose a given integral function by a finite number of rational operations has been given by Kronecker, *Werke*, vol. 2, p. 256.

At least one ξ equals an η. Let $\xi_1=\eta_1, \ldots, \xi_r=\eta_r$, while the remaining ξ's differ from each η. Then the function

$$H(x)\equiv(x-\xi_1)\ldots(x-\xi_r)\equiv(x-\eta_1)\ldots(x-\eta_r)$$

is the highest common factor of $F(x)$ and $G(x)$. But Euclid's process for finding this highest common factor involves only the operation division, so that the coefficients of $H(x)$ are rational functions of those of $F(x)$ and $G(x)$ and consequently belong to the domain R. Hence $F(x)=H(x)\cdot Q(x)$, where $H(x)$ and $Q(x)$ are integral functions with coefficients in R. Since $F(x)$ is irreducible in R, $Q(x)$ must be a constant, evidently 1. Hence $F(x)=H(x)$, so that $F(x)$ is a divisor of $G(x)$ in R.

COROLLARY I. If $G(x)$ is of degree $\leqq n-1$, then $G(x)\equiv 0$. A root of an irreducible equation in R does not satisfy an equation of lower degree in R.

COROLLARY II. If also $G(x)=0$ is irreducible, then $G(x)$ is a divisor of $F(x)$, as well as $F(x)$ a divisor of $G(x)$. *If two irreducible equations in R have one root in common, they are identical.*

CHAPTER VI.

THE GROUP OF AN EQUATION.

EXISTENCE OF AN $n!$-VALUED FUNCTION; GALOIS' RESOLVENT.

56. Let there be given a domain R and an equation

$$(1) \qquad f(x) \equiv x^n - c_1 x^{n-1} + c_2 x^{n-2} - \ldots + (-1)^n c_n = 0,$$

whose coefficients belong to R. We assume that its roots x_1, $x_2, \ldots, x_n$ are all distinct.* It is then possible to construct a rational function V_1 of the roots with coefficients in R such that V_1 takes $n!$ distinct values under the $n!$ substitutions on $x_1, \ldots, x_n$. Such a function is

$$V_1 \equiv m_1 x_1 + m_2 x_2 + \ldots + m_n x_n,$$

if $m_1, \ldots, m_n$ are properly chosen in the domain R. Indeed, the two values V_a and V_b, derived from V_1 by two distinct substitutions a and b respectively, are not equal for all values of $m_1, \ldots, m_n$, since $x_1, \ldots, x_n$ are all distinct. It is therefore possible to choose values of $m_1, \ldots, m_n$ in R which satisfy none of the $\frac{1}{2}n!(n!-1)$ relations of the form $V_a = V_b$.

Then from an equation $V_{a'} = V_a$ will follow $a' = a$.

As an example, consider the equation $x^3 + x^2 + x + 1 = 0$, with the roots

$$x_1 = -1, \quad x_2 = +i \equiv \sqrt{-1}, \quad x_3 = -i,$$

and let R be the domain of all rational numbers. The six functions

$$-m_1 + im_2 - im_3, \quad -m_1 - im_2 + im_3, \quad im_1 - m_2 - im_3,$$
$$-im_1 + im_2 - m_3, \quad -im_1 - m_2 + im_3, \quad im_1 - im_2 - m_3,$$

* Equal roots of $F(x) = 0$ satisfy also $F'(x) = 0$, whose coefficients likewise belong to R, and consequently also $H(x) = 0$, where $H(x)$ is the highest common factor of $F(x)$ and $F'(x)$. If $F(x) \div H(x) = Q(x)$, the equation $Q(x) = 0$ has its coefficients in R and has distinct roots. After solving $Q(x) = 0$, the roots of $F(x) = 0$ are all known.

arising from the 3! permutations of x_1, x_2, x_3, will all be distinct if no one of the following relations holds:

$$m_2-m_3=0,\quad m_1-m_2=0,\quad m_1-m_3=0,$$
$$(i+1)m_1-2im_2+(i-1)m_3=0,\qquad (i-1)m_1+(i+1)m_2-2im_3=0,$$
$$(i-1)m_1-2im_2+(i+1)m_3=0,\qquad (i+1)m_1+(i-1)m_2-2im_3=0,$$
$$-2im_1+(i-1)m_2+(i+1)m_3=0,\qquad -2im_1+(i+1)m_2+(i-1)m_3=0,$$

of which the last six differ only by permutations of m_1, m_2, m_3. We may, for example, take $m_3=0$ and any rational values $\neq 0$ for m_1 and m_2 such that $m_1 \neq cm_2$, where c is $1, \pm i, 1\pm i, \frac{1}{2}(1\pm i)$. Thus $m_1x_1+x_2$ is a six-valued function in R if m_1 is any rational number different from 0 and 1.

[In the domain (i), we may take $m_1x_1+x_2$, where $m_1 \neq 0, 1, \pm i, 1\pm i, \frac{1}{2}(1\pm i)$.]

57. The $n!$ values of the function V_1 are the roots of an equation

$$F(V)\equiv(V-V_1)(V-V_2)\ldots(V-V_{n!})=0, \tag{4}$$

whose coefficients are integral rational functions of $m_1, \ldots, m_n$, $c_1, \ldots, c_n$ with integral coefficients and hence belong to the domain R (§ 50). If $F(V)$ is reducible in R, let $F_0(V)$ be that irreducible factor for which $F_0(V_1)=0$; if $F(V)$ is irreducible in R, let $F_0(V)$ be $F(V)$ itself. Then

$$F_0(V)=0 \tag{5}$$

is an irreducible equation called the **Galois resolvent** *of equation* (1).

Recurring to the example of the preceding section, take

$$V_1=x_2-x_1,\quad V_2=x_2-x_3,\quad V_3=x_3-x_1.$$

Then the six values of V_1 are $\pm V_1, \pm V_2, \pm V_3$, where

$$V_1=i+1,\quad V_2=2i,\quad V_3=-i+1.$$

The equation (4) now becomes

$$(V^2-V_1^2)(V^2-V_2^2)(V^2-V_3^2)=(V^2-2i)(V^2+4)(V^2+2i)$$
$$=V^6+4V^4+4V^2+16=0.$$

The irreducible factors of $F(V)$ in the domain of rational numbers are

$$V^2+4=(V-V_2)(V+V_2),\quad V^2-2V+2=(V-V_1)(V-V_3),$$
$$V^2+2V+2=(V+V_1)(V+V_3).$$

The Galois resolvent (5) is therefore

$$F_0(V)\equiv V^2-2V+2=0.$$

[For the domain (i), the Galois resolvent is $V-V_1\equiv V-i-1=0$.]

58. THEOREM. *Any rational function, with coefficients in a domain R, of the roots of the given equation* (1) *is a rational function, with coefficients in R, of an $n!$-valued function V_1:*

$$\phi(x_1, x_2, \ldots, x_n) = \Phi(V_1). \tag{6}$$

Let first the coefficients $c_1, \ldots, c_n$ in equation (1) be arbitrary quantities so that the roots $x_1, \ldots, x_n$ are independent variables. We may then apply the proof in § 31 of Lagrange's Theorem, taking for ψ the function V_1 which is unaltered by the identical substitution alone, and obtain a relation

$$\phi = \lambda(V_1) \div F'(V_1), \tag{6'}$$

where $F'(V)$ is the derivative of $F(V)$ defined by (4). We next give to $c_1, \ldots, c_n$ their special values in R, so that $x_1, \ldots, x_n$ become the roots of the given equation. Since $F'(V_1) \neq 0$, relation (6') becomes the desired relation (6), expressing ϕ as a rational function of V_1 with coefficients in R.

COROLLARY. *If s be any substitution on the letters $x_1, \ldots, x_n$, then*

$$\phi_s(x_1, x_2, \ldots, x_n) = \Phi(V_s), \tag{7}$$

provided no reduction in the form of $\Phi(V_1)$ has been made by means of the equation $F_0(V_1) = 0$ of* § 57.

As an example, we recur to the equation $x^3+x^2+x+1=0$, and seek an expression for the function $\phi \equiv x_2$ in terms of $V_1 \equiv x_2 - x_1$. Then

$$F(V) = V^6+4V^4+4V^2+16, \quad F'(V) = 6V^5+16V^3+8V,$$

$$\lambda(V) = F(V)\left\{\frac{x_2}{V-V_1}+\frac{x_1}{V+V_1}+\frac{x_2}{V-V_2}+\frac{x_3}{V-V_3}+\frac{x_3}{V+V_2}+\frac{x_1}{V+V_3}\right\}$$
$$= -2V^5-4V^4-12V^3-8V^2-16V-48,$$

upon setting $x_1 = -1$, $x_2 = i$, $x_3 = -i$, $V_1 = i+1$, $V_2 = 2i$, $V_3 = -i+1$. Hence

$$x_2 = \frac{\lambda(V_1)}{F'(V_1)} = \frac{-2V_1^5-4V_1^4-12V_1^3-8V_1^2-16V_1-48}{6V_1^5+16V_1^3+8V_1} \equiv \Phi(V_1).$$

In verification, we find that

$$\lambda(V_1) = \lambda(i+1) = -48i-16, \quad F'(V_1) = 16i-48, \quad \Phi(V_1) = i = x_2.$$

* That such a reduction invalidates the result is illustrated in the example of § 59.

In view of the corollary, we should have

$$x_1=\Phi(-V_1),\quad x_2=\Phi(V_2),\quad x_3=\Phi(V_3),\quad x_3=\Phi(-V_2),\quad x_1=\Phi(-V_3).$$

To verify these results, we note that

$$\Phi(-V_1)=\frac{16i-48}{-16i+48}=-1,\quad \Phi(V_2)=\frac{-80}{80i}=i,\quad \Phi(-V_2)=\frac{-80}{-80i}=-i,$$

while $\Phi(V_3)$ and $\Phi(V_1)$, $\Phi(-V_3)$, and $\Phi(-V_1)$, x_3 and x_2, are conjugate imaginaries, and x_1 is real.

59. As a special case of the preceding theorem, *the roots of the given equation are rational functions of V_1 with coefficients in R:*

$$x_1=\psi_1(V_1),\ x_2=\psi_2(V_1),\ \ldots,\ x_n=\psi_n(V_1). \tag{8}$$

Hence the determination of V_1 is equivalent to the solution of the given equation.

Since each V_s is a rational function of $x_1, \ldots, x_n$ with coefficients in R, it follows that *all the roots of the Galois resolvent are rational functions with coefficients in R of any one root V_1.*

EXAMPLE. For the equation $x^3+x^2+x+1=0$, and $V_1=x_2-x_1$, we have

$$x_1=-1,\quad x_2=V_1-1,\quad x_3=-V_1+1,\quad V_2=2V_1-2,\quad V_3=-V_1+2.$$

Although x_2 and V_1-1 are numerically equal, the functions x_1 and $-V_1-1$, obtained by applying the substitution (x_1x_2), are not equal. The relation $x_2=V_1-1$ is a *reduced* form of $x_2=\Phi(V_1)$, obtained in virtue of the identity $V_1^2-2V_1+2=0$ (§ 57). Thus

$$-2V_1^5-4V_1^4-12V_1^3-8V_1^2-16V_1-48=-48V_1+32,$$
$$6V_1^5+16V_1^3+8V_1=16V_1-64,$$

$$\frac{-48V_1+32}{16V_1-64}=\frac{(-3V_1+2)(V_1+2)}{(V_1-4)(V_1+2)}=\frac{-3V_1^2-4V_1+4}{V_1^2-2V_1-8}=\frac{-10V_1+10}{-10}=V_1-1.$$

It happens, however, that the equality $x_2=V_1-1$ leads to an equality $x_3=V_3-1=-V_1+1$ upon applying the substitution (x_2x_3). The fact that the identical substitution and (x_2x_3), but no other substitutions on x_1, x_2, x_3, lead to an equality when applied to $x_2=V_1-1$ finds its explanation in the general theorems next established.

THE GROUP OF AN EQUATION.

60. Let the roots of Galois' resolvent (5) be designated

$$V_1, V_a, V_b, \ldots, V_l, \tag{9}$$

the substitutions by which they are derived from V_1 being

$$I, a, b, \ldots, l. \tag{10}$$

These substitutions form a group G, called the **group of the given equation** (1) *with respect to the domain of rationality R.*

The proof consists in showing that, if r and s are any two of the substitutions (10), the product rs occurs among those substitutions. Let therefore V_r and V_s be roots of (5). Then

$$F_0(V_r)=0.$$

Now V_r is a rational function of V_1 with coefficients in R:

$$V_r=\theta(V_1), \tag{11}$$

the function θ being left in its unreduced form as determined in § 58. Hence $F_0[\theta(V_1)]=0$, so that one root V_1 of the equation (5) irreducible in R satisfies the equation

$$F_0[\theta(V)]=0, \tag{12}$$

with coefficients in R. Hence (§ 55) the root V_s of (5) satisfies (12).

$$\therefore F_0[\theta(V_s)]=0.$$

In view of the corollary of § 58, it follows from (11) that

$$(V_r)_s \equiv V_{rs}=\theta(V_s).$$

Hence $F_0(V_{rs})=0$, so that V_{rs} occurs among the roots (9).

EXAMPLE. For the equation $x^3+x^2+x+1=0$ and the domain R of rational numbers, the Galois resolvent was shown in § 57 to be $V^3-2V+2=0$, having the roots V_1 and V_3. Since V_3 was derived from V_1 by the substitution (x_2x_3), the group of the equation $x^3+x^2+x+1=0$ with respect to R is $\{I, (x_2x_3)\}$.

For the domain (i), the Galois resolvent was shown to be $V-V_1=0$. Hence the group of the equation with respect to (i) is the identity.

61. The group G of order N of the equation (1) with the roots $x_1, x_2, \ldots, x_n$ possesses the following two fundamental properties:

A. *Every rational function $\phi(x_1, x_2, \ldots, x_n)$ of the roots which remains unaltered by all the substitutions of G lies in the domain R.*

B. *Every rational function $\phi(x_1, x_2, \ldots, x_n)$ of the roots which equals a quantity in R remains unaltered by all the substitutions of G.*

By a rational function $\phi = \phi(x_1, \ldots, x_n)$ of the roots is meant a rational function with coefficients in R. Then by § 58

$$(13) \qquad \phi = \Phi(V_1), \quad \phi_a = \Phi(V_a), \quad \phi_b = \Phi(V_b), \ldots, \quad \phi_l = \Phi(V_l),$$

where Φ is a rational function with coefficients in R.

Proof of A. If $\phi = \phi_a = \phi_b = \ldots = \phi_l$, it follows from (13) that

$$\phi = \frac{1}{N}\{\Phi(V_1) + \Phi(V_a) + \Phi(V_b) + \ldots + \Phi(V_l)\}.$$

The second member is a symmetric function of the N roots (9) of Galois' resolvent (5) and hence is a rational function of its coefficients which belong to R. Hence ϕ lies in R.

Proof of B. If ϕ equals a quantity r lying in R, we have, in view of (13), the equality

$$\Phi(V_1) - r = 0.$$

Hence V_1 is a root of the equation, with coefficients in R,

$$(14) \qquad \Phi(V) - r = 0.$$

Since one root V_1 of the irreducible Galois resolvent equation (5) satisfies (14), all the roots $V_1, V_a, \ldots, V_l$ of (5) satisfy (14), in view of § 55. Hence

$$\Phi(V_1) - r = 0, \quad \Phi(V_a) - r = 0, \quad \ldots, \quad \Phi(V_l) - r = 0.$$

It therefore follows from (13) that $\phi = \phi_a = \phi_b = \ldots = \phi_l$. Hence ϕ remains unaltered by all the substitutions of G.

62. By a **rational relation** between the roots $x_1, \ldots, x_n$ is meant an equality $\phi(x_1, \ldots, x_n) = \psi(x_1, \ldots, x_n)$ between two rational functions, *with coefficients in R.* Then $\phi - \psi$ is a rational function,

equal to the quantity zero belonging to R, and therefore (by B) is unaltered by every substitution s of G. Hence $\phi_s-\psi_s=\phi-\psi=0$, so that $\phi_s=\psi_s$. Hence the result:

Any rational relation between the roots remains true if both members be operated upon by any substitution of the group G.

EXAMPLE. For the domain of rational numbers, it was shown in § 60 that the equation $x^3+x^2+x+1=0$ has the group $\{I, (x_2x_3)\}$. The rational relation (§ 59, Example)

$$x_2=V_1-1\equiv x_2-x_1-1$$

leads to a true relation $x_3=x_3-x_1-1\equiv V_3-1$ under the substitution (x_2x_3). If we apply (x_1x_2), we obtain a false relation $x_1=x_1-x_2-1$.

63. THEOREM. *Properties* A *and* B *completely define the group G of the equation: any group having these properties is identical with G.*

Suppose first that we know of a group

$$G'=\{I, a', b', \ldots, m'\}$$

that every rational function of the roots $x_1, \ldots, x_n$, which remains unaltered by all the substitutions of G', lies in R. The equation

$$F'(V)\equiv(V-V_1)(V-V_{a'})(V-V_{b'})\ldots(V-V_{m'})=0$$

has its coefficients in R since they are symmetric functions of $V_1, V_{a'}, \ldots, V_{m'}$ and therefore unaltered by the substitutions of G'. Since $F'(V)=0$ admits the root V_1 of the irreducible Galois resolvent (5), it admits all the roots $V_1, V_a, \ldots, V_l$ of (5). Hence $I, a, \ldots, l$ occur among the substitutions of G', so that G is a subgroup of G'.

Suppose next that we know of a group

$$G''=\{I, a'', b'', \ldots, r''\}$$

that every rational function of $x_1, \ldots, x_n$ which lies in R remains unaltered by all the substitutions of G''. Then the rational function $F_0(V_1)$, being equal to the quantity zero lying in R, remains unaltered by $a'', b'', \ldots, r''$, so that

$$0=F_0(V_1)=F_0(V_{a''})=F_0(V_{b''})=\ldots=F_0(V_{r''}).$$

Hence $V_1, V_{a''}, \ldots, V_{r''}$ occur among the roots $V_1, V_a, \ldots, V_l$ of $F_0(V)=0$. Hence G'' is a subgroup of G.

If both properties hold for a group, $G' \equiv G''$; then G' contains G as a subgroup and G' is a subgroup of G. Hence $G' \equiv G'' \equiv G$.

It follows that *the group of a given equation for a given domain is unique.* In particular, the group of an equation is independent of the special $n!$-valued function V_1 chosen.

EXAMPLE. For the equation $x^3+x^2+x+1=0$ and the domain R of all rational numbers, the functions $\pm V_1$, $\pm V_2$, $\pm V_3$ of § 57 are each 6-valued. Employing V_1, we obtain the Galois resolvent

$$(V-V_1)(V-V_3)=V^2-2V+2=0$$

and the group $\{I, x_2x_3)\}$. Evidently no change results from the employment of V_3. If we employ either $-V_1$ or $-V_3$, we obtain the Galois resolvent

$$(V+V_1)(V+V_3)=V^2+2V+2=0$$

and the group $\{I, (x_2x_3)\}$. If we employ either V_2 or $-V_2$, we get

$$(V-V_2)(V+V_2)=V^2+4=0.$$

Since $V_2=x_2-x_3$, the substitution replacing V_2 by $-V_2$ is (x_2x_3), so that the group is again $\{I, (x_2x_3)\}$.

ACTUAL DETERMINATION OF THE GROUP G OF A GIVEN EQUATION.

64. Group of the general equation of degree n. Its coefficients $c_1, \ldots, c_n$ are independent variables, and likewise its roots (p. 101). We proceed to show that, *for a domain R containing the coefficients and any assigned constants, the group of the general equation of degree n is the symmetric group $G_{n!}$.* It is only necessary to show that the Galois resolvent $F_0(V)=0$ is of degree $n!$. In the relation $F_0(V_1)=0$, we replace V_1 and the coefficients $c_1, \ldots, c_n$ by their expressions in terms of $x_1, \ldots, x_n$. Since the latter are independent, the resulting relation must be an identity (see p. 101) and hence remain true after any permutation of $x_1, \ldots, x_n$. By suitable permutations, V_1 is changed into $V_2, \ldots, V_{n!}$ in turn, while $c_1, \ldots, c_n$, being symmetric functions, remain unaltered. Hence $F_0(V_2)=0$, $\ldots$, $F_0(V_{n!})=0$. Hence $F_0(V)=0$ has $n!$ distinct roots.

Another proof follows from § 63 by noting that properties A and B hold for the symmetric group $G_{n!}$ when $x_1, \ldots, x_n$ are inde-

pendent variables. Thus A states that every symmetric function of the roots is rationally expressible in terms of the coefficients.

65. To determine the group of a special equation, we usually resort to some device. It is generally impracticable to construct an $n!$-valued function and then determine the Galois resolvent (5); or to apply properties A and B directly, since they relate to an infinite number of rational functions of the roots. Practical use may, however, be made of the following lemma, involving a knowledge of a single rational function:

LEMMA. *If a rational function $\psi(x_1, \ldots, x_n)$ remains formally unaltered by the substitutions of a group G' and by no other substitutions, and if ψ equals a quantity lying in the domain R, and if the conjugates of ψ under $G_{n!}$ are all distinct, then the group of the given equation for the domain R is a subgroup of G'.*

In view of the first part of § 63, it is only necessary to show that every rational function $\phi(x_1, \ldots, x_n)$, which remains *numerically* unaltered by all the substitutions of G', lies in R. If G' is of order P, we can set

$$\phi = \frac{1}{P}(\phi_1 + \phi_2 + \ldots + \phi_P),$$

so that ϕ can be given a form such that it is *formally* unaltered by all the substitutions of G'. Then, by Lagrange's Theorem (§ 31), ϕ is a rational function of ψ and hence equals a quantity lying in R.

EXAMPLE 1. To find the group of $x^3-1=0$ for the domain R of all rational numbers. The roots are

$$x_1=1, \quad x_2=\tfrac{1}{2}(-1+\sqrt{-3}), \quad x_3=\tfrac{1}{2}(-1-\sqrt{-3}).$$

Taking $\psi=x_1$, it follows from the lemma that G is a subgroup of $G'=\{I, (x_2x_3)\}$. Since x_2 does not lie in R, G is not the identity (property A). Hence $G=G'$.

EXAMPLE 2. To find the group G of $y^3-7y+7=0$ for the domain R of all rational numbers.

For the cubic $y^3+py+q=0$, we have (§ 2)

$$D \equiv (y_1-y_2)^2(y_2-y_3)^2(y_3-y_1)^2 = -27q^2-4p^3.$$

For $p=-7$, $q=7$, we get $D=7^2$. Hence the function

$$\psi \equiv (y_1-y_2)(y_2-y_3)(y_3-y_1)$$

has a value ± 7 lying in R and its conjugates ϕ and $-\phi$ under G_6 are distinct. By the lemma, G is therefore a subgroup of the alternating group G_3, and hence either G_3 itself or the identity G_1. Now, if the group of the equation were G_1, its roots would lie in R. But * a rational root of an equation of the form $y^3-7y+7=0$, having integral coefficients and unity as the coefficient of the highest power, is necessarily an integer. By trial, ± 1, ± 7 are not roots. Hence the roots are all irrational. Hence the group G is G_3.

EXAMPLE 3. Find the group of $x^4+1=0$ for the domain of rational numbers.

We seek a rational function of the roots x_1, x_2, x_3, x_4 which equals a rational number. Let us try the function $y_1=x_1x_2+x_3x_4$. Specializing the result holding for the general quartic equation (§ 4), we find that, for the quartic $x^4+1=0$, the resolvent equation (16) for y_1 is

$$y^3-4y=0.$$

By a suitable choice of notation to distinguish the roots x_i, we may set

$$y_1=-2, \quad y_2=0, \quad y_3=+2.$$

Hence y_1 equals a rational number and its conjugates under G_{24} are all distinct. Hence G is a subgroup of G_8, the group to which $x_1x_2+x_3x_4$ belongs *formally* (§ 21). Similarly, by considering the conjugate functions $y_2=x_1x_3+x_2x_4$, and $y_3=x_1x_4+x_2x_3$, we find that G is a subgroup of G_8' and G_8''. Hence G is a subgroup of G_4 (§ 21). Hence G is G_4, G_1,

$$G_2=\{I, (x_1x_2)(x_3x_4)\}, \quad G_2'=\{I, (x_1x_3)(x_2x_4)\}, \quad \text{or } G_2''=\{I, (x_1x_4)(x_2x_3)\}.$$

Now $G \neq G_1$, since no root of $x^4+1=0$ is rational.

If G_2, consider $t_1 \equiv x_1+x_2-x_3-x_4$. For the general quartic equation $x^4+ax^3+bx^2+cx+d=0$, we have $t_1^2=a^2-4b+4y_1$ by § 5. Hence, for $x^4+1=0$, $t_1^2=-8$. Since t_1 is not rational, $G \neq G_2$.

If G_2'', consider $t_3 \equiv x_1+x_4-x_2-x_3$. In general, $t_3^2=a^2-4b+4y_3$. Here $t_3^2=+8$. Since t_3 is not rational, $G \neq G_2''$.

If G_2', consider $t_2 \equiv x_1+x_3-x_2-x_4$. In general, $t_2^2=a^2-4b+4y_2$. Here $t_2^2=0$. Since a conjugate $-t_2$ of t_2 equals t_2, no conclusion may be drawn from the use of t_2. But $\phi \equiv x_1x_3-x_2x_4$ is unaltered by G_2'. Now

$$\phi^2=(x_1x_3+x_2x_4)^2-4x_1x_2x_3x_4=y_2^2-4=-4.$$

Hence ϕ is not rational, so that $G \neq G_2'$.

The group of $x^4+1=0$ for the domain of rational numbers is therefore G_4.

EXERCISES.

Find for the domain of rational numbers the group of

1. $x^3+x^2+x+1=0$ (using the lemma, § 65).
2. $(x-1)(x+1)(x-2)=0$.

* Dickson, *College Algebra* (John Wiley & Sons), p. 198.

3. $x^3-2=0$. [x_1, x_2, x_3 and $(x_1-x_2)(x_2-x_3)(x_3-x_1)$ are irrational.]

4. $x^4+x^3+x^2+x+1=0$ with roots $x_1=\varepsilon$, $x_2=\varepsilon^2$, $x_3=\varepsilon^4$, $x_4=\varepsilon^3$, where ε is an imaginary fifth root of unity. Since the resolvent for $x_1x_2+x_3x_4$ is $y^3-y^2-3y+2=0$ with the roots 2, $\frac{1}{2}(-1\pm\sqrt{5})$, G is a subgroup of G_8'. The latter has the subgroup $C_4=\{I, (1234), (13)(24), (1432)\}$, to which belongs $\psi_1=x_1^2x_2+x_2^2x_3+x_3^2x_4+x_4^2x_1$. Here $\psi_1=\varepsilon^4+\varepsilon^3+\varepsilon+\varepsilon^2=-1$ is rational. The six conjugates to ψ_1 under G_{24} are distinct; they are obtained from ψ_1 by applying I, (12)(34), (12), (14), (23), (34); their values are -1, 4, $1+2\varepsilon+\varepsilon^3$, $1+2\varepsilon^3+\varepsilon^4$, $1+2\varepsilon^3+\varepsilon$, $1+2\varepsilon^4+\varepsilon^2$, respectively. Hence G is a subgroup of C_4. To $G_3'=\{I, (13)(24)\}$ belongs

$$(x_1-x_3+ix_2-ix_4)^2=(1+2i)(\varepsilon^3+\varepsilon^3-\varepsilon^4-\varepsilon)=\pm\sqrt{5}(1+2i).$$

Hence $G\neq G_3'$. Evidently $G\neq G_1$. Hence $G=C_4$.

5. Show that, for the domain $(1, i)$, the group of $x^4+1=0$ is G_3'.

6. Show that, for the domain $(1, \omega)$, $\omega=$imaginary cube root of unity, the group of $x^3-2=0$ is $C_3=\{I, (x_1x_2x_3), (x_1x_3x_2)\}$.

Hint: $(x_1+\omega x_2+\omega^2x_3)^3$ and $(x_1+\omega^2x_2+\omega x_3)^3$ have distinct rational values.

TRANSITIVITY OF GROUP; IRREDUCIBILITY OF EQUATION.

66. A group of substitutions on n letters is **transitive** if it contains a substitution which replaces an arbitrarily given letter by another arbitrarily given letter; otherwise the group is **intransitive.**

Thus the group $G_4=\{I, (x_1x_2)(x_3x_4), (x_1x_3)(x_2x_4), (x_1x_4)(x_2x_3)\}$ is transitive; I replaces x_1 by x_1, $(x_1x_2)(x_3x_4)$ replaces x_1 by x_2, $(x_1x_3)(x_2x_4)$ replaces x_1 by x_3, $(x_1x_4)(x_2x_3)$ replaces x_1 by x_4. Having a substitution s which replaces x_1 by any given letter x_i and a substitution t which replaces x_1 by any given letter x_j, the group necessarily contains a substitution which replaces x_i by x_j, namely, the product $s^{-1}t$.

The group $H_4=\{I, (x_1x_2), (x_3x_4), (x_1x_2)(x_3x_4)\}$ is intransitive.

67. THEOREM. *The order of a transitive group on n letters is divisible by n.*

Of the substitutions of the given group G, those leaving x_1 unaltered form a subgroup $H=\{I, h_2, \ldots, h_r\}$. Consider a rectangular array (§ 28) of the substitutions of G with those of H in the first row, choosing as g_2 any substitution replacing x_1 by x_2, as g_3 any substitution replacing x_1 by x_3, etc. Then all the substitutions of the second row and no others will replace x_1 by x_2,

all of the third row and no others will replace x_1 by x_3, etc. Since G is transitive, there are $\nu = n$ rows. But the order of G is divisible by ν (§ 26).

Examples of transitive groups: $G_3^{(3)}$, $G_6^{(3)}$, $G_{24}^{(4)}$, $G_{12}^{(4)}$, $G_8^{(4)}$, $G_4^{(4)}$.

The least order of a transitive group on n letters is therefore n. A transitive group on n letters of order n is called a **regular group.** Thus $G_3^{(3)}$ and $G_4^{(4)}$ are regular.

68. THEOREM. *If an equation is irreducible for the domain R, its group for R is transitive; if reducible, the group is intransitive.*

First, if $f(x)=0$ is irreducible in R, its group for R is transitive. For, if intransitive, G contains substitutions replacing x_1 by $x_1, x_2, \ldots, x_m$, but not by $x_{m+1}, \ldots, x_n$, the notation for the roots being properly chosen. Hence every substitution of G permutes $x_1, \ldots, x_m$ amongst themselves and therefore leaves unaltered any symmetric function of them. Hence the function $g(x) \equiv (x-x_1)(x-x_2)\ldots(x-x_m)$ has its coefficients in R, so that $g(x)$ is a rational factor of $f(x)$, contrary to the irreducibility of $f(x)$.

Let next $f(x)$ be reducible in R and let $g(x) \equiv (x-x_1)\ldots(x-x_m)$ be a rational factor of $f(x)$, m being $< n$. The rational relation $g(x_1)=0$ remains true if operated upon by any substitution of G (§ 62). Hence no substitution of G can replace x_1 by one of the roots $x_{m+1}, \ldots, x_n$; for, if so, $g(x)=0$ would have as root one of the quantities $x_{m+1}, \ldots, x_n$, contrary to assumption. Hence G is intransitive.

EXAMPLE 1. The equation $x^3-1=0$ is reducible in the domain R of rational numbers; its group for R is $\{I, (x_2x_3)\}$ by § 65, Ex. 1, and is intransitive. A like result holds for $x^3+x^2+x+1=0$ (§ 60).

EXAMPLE 2. The equation $y^3-7y+7=0$ is irreducible in the domain R of rational numbers, since its left member has no linear factor in R (§ 65, Ex. 2). Hence its group for R is transitive. By § 65, the group is $G_3^{(3)}$.

EXAMPLE 3. The equation $x^4+1=0$ is irreducible in the domain R of rational numbers (§ 54, Ex. 2). Hence its group for R is transitive, and so is of order at least 4. We may therefore greatly simplify the work in § 65, Ex. 3, for the determination of the group G.

EXAMPLE 4. The equation $x^4+1=0$ is reducible in the domain $(1, i)$. Its group G_2' is intransitive (see Ex. 5, page 58).

RATIONAL FUNCTIONS BELONGING TO A GROUP.

69. THEOREM. *Those substitutions* **of the group** *G of an equation which leave unaltered a rational function ϕ of its roots form a group.*

Let $I, a, b, \ldots, k$ be all the substitutions of G which leave ϕ unaltered (in the numerical sense, § 52). Apply to the rational relation $\phi = \phi_a$ the substitution b of the group G. Then (§ 62) $\phi_b = \phi_{ab}$. Hence $\phi_{ab} = \phi$, so that the product ab is one of the substitutions leaving ϕ unaltered. Hence the substitutions $I, a, b, \ldots, k$ form a group H.

No matter what group ϕ belongs to *formally* (§ 21), we shall henceforth say that ϕ **belongs to the group** H, a subgroup of G.

EXAMPLE. For the domain R of rational numbers the group of $x^4+1=0$ is

$$G_4 = \{I, (x_1x_2)(x_3x_4), (x_1x_3)(x_2x_4), (x_1x_4)(x_2x_3)\},$$

by § 65, Ex. 3. Of the 12 substitutions which leave x_1^2 numerically unaltered (§ 49), only I and $(x_1x_3)(x_2x_4)$ occur in G_4. Hence the function x_1^2 of the roots of $x^4+1=0$ belongs to the group $\{I, (x_1x_3)(x_2x_4)\}$.

70. THEOREM. *If H is any subgroup of the group G of a given equation for a domain R, there exists a rational function of its roots with coefficients in R which belongs to H.*

Let V_1 be any $n!$-valued function of the roots with coefficients in R (§ 56). Let $V_1, V_a, \ldots, V_k$ be the functions derived from V_1 by applying the substitutions of H. Then the product

$$\phi \equiv (\rho - V_1)(\rho - V_a) \ldots (\rho - V_k)$$

in which ρ is a suitably chosen quantity in R, is a rational function of the roots with coefficients in R which belongs to H (compare § 25).

71. THEOREM. *If a rational function ϕ of the roots of an equation belongs to a subgroup H of index ν under the group G of the equation for a domain R, then ϕ takes ν distinct values when operated upon by all the substitutions of G; they are the roots of a resolvent equation with coefficients in R,*

$$g(y) \equiv (y - \phi_1)(y - \phi_2) \ldots (y - \phi_\nu) = 0. \tag{15}$$

The proof that there are exactly ν distinct values of ψ under the substitutions of G is the same as in § 29, the term *distinct* now having the meaning given in § 52.

Any substitution *of the group* G merely permutes the functions $\psi_1, \psi_2, \ldots, \psi_\nu$ (compare § 30), so that any symmetric function of them is unaltered by all the substitutions of G and hence equals a quantity in R (Theorem A, § 61). Hence the coefficients of (15) lie in R.

REMARK. *The resolvent equation* (15) *is irreducible in* R.

Let $\gamma(y)$ be a rational factor of $g(y)$. Applying to the rational relation $\gamma(\psi_1)=0$ the substitutions of G, we get $\gamma(\psi_2)=0, \ldots, \gamma(\psi_\nu)=0$. Hence $\gamma(y)=0$ admits all the roots of $g(y)=0$, so that $\gamma(y) \equiv g(y)$.

EXAMPLE 1. For the domain R of rational numbers, the group G of $x^3+x^2+x+1=0$ is $\{I, (x_2x_3)\}$, by § 60. The conjugates to x_2-x_1 under G are $\psi_1=x_2-x_1$, $\psi_2=x_3-x_1$. They are the roots of

$$y^2-(\psi_1+\psi_2)y+\psi_1\psi_2=y^2-2y+2=0.$$

EXAMPLE 2. For the domain $(1, i)$, the group G of $x^4+1=0$ is $\{I, (x_1x_3)(x_2x_4)\}$, by Ex. 5, page 58, employing the notation of § 49 for the roots. The conjugates to x_1 under G are $\psi_1=x_1$, $\psi_2=x_3$. They are the roots of

$$y^2-(\varepsilon-\varepsilon)y+\varepsilon(-\varepsilon)=y^2-i=0.$$

It is irreducible in $(1, i)$, since $\sqrt{i}=(1+i) \div \sqrt{2}$.

72. LAGRANGE'S THEOREM GENERALIZED BY GALOIS. *If a rational function* $\phi(x_1, x_2, \ldots, x_n)$ *of the roots of an equation* $f(x)=0$ *with coefficients in a domain* R *remains unaltered by all those substitutions of the group* G *of* $f(x)=0$ *which leave another rational function* $\psi(x_1, x_2, \ldots, x_n)$ *unaltered, then* ϕ *is a rational function of* ψ *with coefficients in* R.

The function ψ belongs to a certain subgroup H of G, say of index ν. By means of a rectangular array of the substitutions of G with those of H in the first row, we obtain the ν distinct conjugate functions $\psi_1, \psi_2, \ldots, \psi_\nu$ and a set of functions $\phi_1, \phi_2, \ldots, \phi_\nu$, not necessarily distinct, but such that a substitution of G which

replaces ψ_i by ψ_j will replace ϕ_i by ϕ_j (compare § 31). If $g(t)$ be defined by (15), then

$$\lambda(t) \equiv g(t)\left(\frac{\phi_1}{t-\psi_1}+\frac{\phi_2}{t-\psi_2}+\ \dots\ +\frac{\phi_\nu}{t-\psi_\nu}\right)$$

is an integral function of t which remains unaltered by all the substitutions of G, so that its coefficients lie in R (§ 71). Taking $\psi_1 \equiv \psi$ for t, we get $\phi = \lambda(\psi) \div g'(\psi)$.

For examples, see § 58. The function V_1 is unaltered by the identical substitution only, which leaves unaltered any rational function.

REDUCTION OF THE GROUP BY ADJUNCTION.

73. For the domain $R=(1)$ of all rational numbers, the group of the equation $x^3+x^2+x+1=0$ is $G_2=\{I,\ (x_2x_3)\}$; while its group for the domain $R'=(1,\ i)$ is the identity G_1 (see § 60). In the language of Galois and Kronecker, we derive the domain $R'=(1,\ i)$ from the included domain $R=(1)$ by **adjoining** the quantity i to the domain R. By this adjunction the group G_2 of x^3+x^2+x+1 is **reduced** to the subgroup G_1. The adjoined quantity i is here a rational function of the roots, $i=x_2=-x_3$, in the notation of § 49 for the roots. The Galois resolvent $V^2-2V+2=0$ for R becomes reducible in R', viz., $(V-i-1)(V+i-1)=0$.

For the domain $R=(1)$, the group of $x^4+1=0$ is G_4; for the domain $(1,\ i)$, its group is the subgroup $G_2'=\{I,\ (x_1x_3)(x_2x_4)\}$, by § 65. By the adjunction of i to the domain R, the group is reduced to a subgroup G_2'. Here $i=x_1^2=x_3^2=-x_2^2=-x_4^2=x_2x_4$, in the notation of § 49. The subgroup of G_4 to which x_1^2 belongs is G_2'. If we afterwards adjoin $\sqrt{2}$, the roots will all belong to the enlarged domain $(1,\ i,\ \sqrt{2})$, so that the group reduces to the identity. For example, $x_1=(1+i)\div\sqrt{2}$.

For the domain $R=(1)$, the group of $x^3-2=0$ is G_6; for the domain $(1,\ \omega)$, ω being an imaginary cube root of unity, the group is the cyclic group C_3 (Exercises 3 and 6, page 58). Call the roots

$$x_1=\sqrt[3]{2},\quad x_2=\omega\sqrt[3]{2}\equiv\omega x_1,\quad x_3=\omega^2\sqrt[3]{2}\equiv\omega^2x_1.$$

Then $\omega=x_2/x_1$, a rational function belonging to C_3. In fact, $(x_1x_2x_3)$ replaces x_2/x_1 by $x_3/x_2=\omega=x_2/x_1$, $(x_1x_3x_2)$ replaces x_2/x_1 by $x_1/x_3=\omega^{-2}=\omega$; while these two substitutions and the identity are the only substitutions leaving x_2/x_1 unaltered. If we subsequently adjoin $\sqrt[3]{2}$, the roots all belong to the enlarged domain $(1,\ \omega,\ \sqrt[3]{2})$, so that the group reduces to the identity.

74. In general, we are given a domain $R=(R', R'', \ldots)$ and an equation $f(x)=0$ with coefficients in that domain. Let G be its group for R. Adjoin a quantity ξ. The irreducible Galois resolvent $F_0(V)=0$ for the initial domain R may become reducible in the enlarged domain $R_1=(\xi; R', R'', \ldots)$. Let $\lambda(V, \xi)$ be that factor of $F_0(V)$ which is rational and irreducible in R_1 and vanishes for $V=V_1$. If $V_1, V_a, \ldots, V_k$ are the roots of $\lambda(V, \xi)=0$, then $G'=\{I, a, \ldots, k\}$ is the group of $f(x)=0$ in R_1 (§ 57). Hence G' is a subgroup of G, including the possibility $G'=G$, which occurs if $F_0(V)$ remains irreducible after the adjunction of ξ, so that $\lambda(V, \xi)=F_0(V)$.

THEOREM. *By an adjunction, the group G is reduced to a subgroup G'.*

75. Suppose that, as in the examples in § 73, the quantity adjoined to the given domain R is a rational function $\phi(x_1, x_2, \ldots, x_n)$ of the roots with coefficients in R.

THEOREM. *By the adjunction of a rational function $\phi(x_1, \ldots, x_n)$ belonging to a subgroup H of G, the group G of the equation is reduced precisely to the subgroup H.*

It is to be shown that the group H has the two characteristic properties (§ 61) of the group of the equation for the new domain $R_1=(\psi; R', R'', \ldots)$. First, any rational function $\phi(x_1, \ldots, x_n)$ which remains unaltered by all the substitutions of H is a rational function of ψ with coefficients in R (§ 72) and hence lies in R_1. Second, any rational function $\phi(x_1, \ldots, x_n)$ which equals a quantity ρ in R_1 remains unaltered by all the substitutions of H. For the relation $\phi=\rho$ may be expressed as a rational relation in R and hence leads to a true relation when operated upon by any substitution of G (§ 62) and, in particular, by the substitutions of the subgroup H. The latter leave ψ, and hence also ρ, unaltered. Hence the left member ϕ of the relation remains unaltered by all the substitutions of H.

CHAPTER VII.

SOLUTION BY MEANS OF RESOLVENT EQUATIONS.

76. Before developing the theory further, it is desirable to obtain a preview of the applications to be made to the solution of any given equation $f(x)=0$. Suppose that we are able to solve the resolvent equation (15), one of whose roots is the rational function ϕ belonging to the subgroup H of the group G of $f(x)=0$. Since ϕ is then known, it may be adjoined to the given domain of rationality $(R', R'', \ldots)$. For the enlarged domain $R_1=(\phi; R', R'', \ldots)$, the group of $f(x)=0$ is H. Let $\chi(x_1, \ldots, x_n)$ be a rational function with coefficients in R_1 which belongs to a subgroup K of H. Suppose that we are able to solve the resolvent equation one of whose roots is χ. Then χ may be adjoined to the domain R_1. For the enlarged domain $R_2=(\chi, \phi; R', R'', \ldots)$, the group of $f(x)=0$ is K. Proceeding in this way, we reach a final domain R_k for which the group of $f(x)=0$ is the identity G_1. Then the roots $x_1, \ldots, x_n$, being unaltered by the identity, lie in this domain R_k (property A, § 61). The solution of $f(x)=0$ may therefore be accomplished if all the resolvent equations can be solved. To apply Galois' methods to the solution of each resolvent, the first step is to find its group for the corresponding domain of rationality.

77. Isomorphism. Let G be the group of a given equation $f(x)=0$ for a given domain R. Let $\phi(x_1, \ldots, x_n)$ be a rational function of its roots with coefficients in R and let ϕ belong to a subgroup H of index ν under G. Consider a rectangular array

of the substitutions of G with those of H in the first row, and the resulting functions conjugate to ψ:

$$\begin{array}{llll|l} h_1=I & h_2 & \dots & h_P & \psi_1=\psi \\ g_2 & h_2g_2 & \dots & h_Pg_2 & \psi_2=\psi_{g_2} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ g_\nu & h_2g_\nu & \dots & h_Pg_\nu & \psi_\nu=\psi_{g_\nu} \end{array}$$

Apply any substitution g of the group G to the ν conjugates

$$\psi,\ \psi_{g_2},\ \psi_{g_3},\ \dots,\ \psi_{g_\nu}. \tag{16}$$

The resulting functions

$$\psi_g,\ \psi_{g_2g},\ \psi_{g_3g},\ \dots,\ \psi_{g_\nu g} \tag{17}$$

are merely a permutation of the functions (16), as shown in § 29. Hence to any substitution g of the group G on the letters $x_1, \dots, x_n$, there corresponds one definite substitution

$$\gamma=\begin{pmatrix} \psi & \psi_{g_2} & \dots & \psi_{g_\nu} \\ \psi_g & \psi_{g_2g} & \dots & \psi_{g_\nu g} \end{pmatrix} \equiv \begin{pmatrix} \psi_{g_i} \\ \psi_{g_ig} \end{pmatrix}$$

on the letters (16). We therefore obtain * a set Γ of substitutions γ, not all of which are distinct in certain cases (Exs. 2 and 3 below).

THEOREM. *The set Γ of substitutions γ forms a group.*

For to g, g', and gg' correspond respectively

$$\gamma=\begin{pmatrix} \psi_{g_i} \\ \psi_{g_ig} \end{pmatrix},\quad \gamma'=\begin{pmatrix} \psi_{g_i} \\ \psi_{g_ig'} \end{pmatrix},\quad \gamma''=\begin{pmatrix} \psi_{g_i} \\ \psi_{g_igg'} \end{pmatrix}.$$

To compute the product $\gamma\gamma'$, we vary the order of the letters in the first line of γ' and have

$$\gamma'=\begin{pmatrix} \psi_{g_ig} \\ \psi_{g_ig\cdot g'} \end{pmatrix},\quad \gamma\gamma'=\begin{pmatrix} \psi_{g_i} \\ \psi_{g_igg'} \end{pmatrix}=\gamma''.$$

Hence if Γ contains γ and γ', it contains the product $\gamma\gamma'$.

Since Γ contains a substitution replacing ψ by ψ_{g_i} for any $i=1, \dots, \nu$, *the group Γ is transitive* (§ 66).

* For a definition of Γ without using the function ψ, see § 104.

DEFINITIONS. The group Γ is said to be **isomorphic** to G, since to every substitution g of G corresponds *one* substitution γ of Γ, and to the product gg' of any two substitutions of G corresponds the product $\gamma\gamma'$ of the two corresponding substitutions of Γ. If, inversely, to every substitution of Γ corresponds but one substitution of G, the groups are said to be **simply isomorphic**;* otherwise, **multiply isomorphic.***

EXAMPLE 1. Let $G=G_6^{(3)}$, $H=G_1$, $\psi=x_1+\omega x_2+\omega^2 x_3$. Set (compare § 9)

$$\psi_1=\psi, \quad \psi_2=\psi_a, \quad \psi_3=\psi_b, \quad \psi_4=\psi_c, \quad \psi_5=\psi_d, \quad \psi_6=\psi_e.$$

Then $a=(x_1x_2x_3)$ replaces ψ_1 by $\psi_2=\omega^2\psi_1$, and ψ_4 by $\psi_6=\omega\psi_4$. Hence a replaces ψ_2 by $\omega^4\psi_1=\psi_3$, ψ_3 by $\omega^6\psi_1=\psi_1$, ψ_6 by $\omega^2\psi_4=\psi_5$, ψ_5 by $\omega^3\psi_4=\psi_4$. Hence to a corresponds $\alpha=(\psi_1\psi_2\psi_3)(\psi_4\psi_6\psi_5)$. Similarly, we find that to $c=(x_2x_3)$ corresponds $\gamma=(\psi_1\psi_4)(\psi_2\psi_5)(\psi_3\psi_6)$. Hence to $b=a^2$ corresponds $\beta=\alpha^2$, to $d=a^{-1}ca$ corresponds $\delta=\alpha^{-1}\gamma\alpha$, to $e=b^{-1}cb$ corresponds $\varepsilon=\beta^{-1}\gamma\beta$. We have therefore the following holoedric isomorphism between G and Γ:

I	I
$a=(x_1x_2x_3)$	$\alpha=(\psi_1\psi_2\psi_3)(\psi_4\psi_6\psi_5)$
$b=(x_1x_3x_2)$	$\beta=(\psi_1\psi_3\psi_2)(\psi_4\psi_5\psi_6)$
$c=(x_2x_3)$	$\gamma=(\psi_1\psi_4)(\psi_2\psi_5)(\psi_3\psi_6)$
$d=(x_1x_3)$	$\delta=(\psi_2\psi_6)(\psi_3\psi_4)(\psi_1\psi_5)$
$e=(x_1x_2)$	$\varepsilon=(\psi_3\psi_5)(\psi_1\psi_6)(\psi_2\psi_4)$

It may be verified directly that to b, d, e correspond β, δ, ε, respectively.

Since I, a, β, γ, δ, ε replace ψ_1 by ψ_1, ψ_2, ψ_3, ψ_4, ψ_5, ψ_6, respectively, Γ is transitive.

EXAMPLE 2. Let $G=G_{12}^{(4)}$, $H=G_4$, $\psi=(x_1-x_2)(x_3-x_4)$. Set

$$\psi_1=\psi, \quad \psi_2=(x_1-x_3)(x_4-x_2), \quad \psi_3=(x_1-x_4)(x_2-x_3).$$

We obtain the following meriedric isomorphism between G and Γ:

I,	$(x_1x_2)(x_3x_4)$,	$(x_1x_3)(x_2x_4)$,	$(x_1x_4)(x_2x_3)$	I
$(x_2x_3x_4)$,	$(x_1x_3x_2)$,	$(x_1x_4x_3)$,	$(x_1x_2x_4)$	$(\psi_1\psi_2\psi_3)$
$(x_2x_4x_3)$,	$(x_1x_4x_2)$,	$(x_1x_2x_3)$,	$(x_1x_3x_4)$	$(\psi_1\psi_3\psi_2)$

The group Γ is transitive since it contains substitutions replacing ψ_1 by ψ_1, ψ_2, or ψ_3.

---

* Other terms are **holoedric** and **meriedric** for simple and multiple isomorphism.

78. Order of the group Γ. To find the number of distinct substitutions in Γ, we seek the conditions under which two substitutions γ and γ' of Γ are identical. Using the notation of § 77, the conditions are

$$\psi_{g_i g} = \psi_{g_i g'} \qquad (i=1, 2, \ldots, \nu),$$

if we set $g_1 = I$. Applying to this identity the substitution $g^{-1}g_i^{-1}$, we get

$$\psi = \psi_{g_i g' g^{-1} g_i^{-1}}.$$

Hence $g_i g' g^{-1} g_i^{-1} = h$, where h is some substitution leaving ψ unaltered and hence in the group H. Then

$$g'g^{-1} = g_i^{-1} h g_i \qquad (i=1, 2, \ldots, \nu).$$

But $g_i^{-1} h g_i$ belongs to the group $H_i \equiv g_i^{-1} H g_i$ of the function ψ_{g_i} (§ 39). Hence $g'g^{-1}$ belongs simultaneously to $H_1, H_2, \ldots, H_\nu$, and therefore to their greatest common subgroup J.

Inversely, any substitution σ of J leaves $\psi_1, \psi_2, \ldots, \psi_\nu$ unaltered and hence corresponds to the identity in Γ. Then g and $g' = \sigma g$ correspond to substitutions γ and γ' which are identical.

If G is of order k and if the greatest common subgroup J of $H_1, H_2, \ldots, H_\nu$ is of order j, then Γ is of order k/j.

EXAMPLE 1. For $G = G_6$, $H = G_1$, the order of Γ is 6 (§ 77, Ex. 1).

EXAMPLE 2. For $G = G_{12}^{(4)}$, $H = G_4$ (§ 77, Ex. 2), we have $H_1 = H_2 = H_3$, since G_4 is self-conjugate under G_{12} (§ 41). Hence $k=12$, $j=4$, so that the order of Γ is 3.

EXAMPLE 3. For $G = G_{24}^{(4)}$, $H_1 = G_8$, $\psi = x_1x_2 + x_3x_4$, we set (§ 29, Ex. 2)

$$\psi_1 = x_1x_2 + x_3x_4, \quad \psi_2 = x_1x_3 + x_2x_4, \quad \psi_3 = x_1x_4 + x_2x_3.$$

Then $H_1 = G_8$, $H_2 = G_8'$, $H_3 = G_8''$, $J = G_4$ (§ 21). Hence Γ is of order $\frac{24}{4} = 6$. This result may be verified directly. There are only 6 possible substitutions on 3 letters ψ_1, ψ_2, ψ_3. But the substitutions of G which lead to the identical substitution of Γ must leave ψ_1, ψ_2, ψ_3 all unaltered and hence belong to the greatest common subgroups G_4 of H_1, H_2, H_3. Hence exactly four substitutions of G correspond to each substitution of Γ, so that the order of Γ is $\frac{24}{4} = 6$. The four substitutions of any set form one row of the rectangular array for

G_{24} with the substitutions I, $(x_1x_2)(x_3x_4)$, $(x_1x_3)(x_2x_4)$, $(x_1x_4)(x_2x_3)$ of G_4 in the first row. As right-hand multipliers we may take

$$g_1=I,\quad g_2=(x_2x_3x_4),\quad g_3=(x_2x_4x_3),\quad g_4=(x_3x_4),\quad g_5=(x_2x_4),\quad g_6=(x_2x_3).$$

To the four substitutions of the first row, the four of the second row, . . . , correspond

$$I,\quad (\psi_1\psi_2\psi_3),\quad (\psi_1\psi_3\psi_2),\quad (\psi_2\psi_3),\quad (\psi_1\psi_3),\quad (\psi_1\psi_2).$$

79. Of special importance is the case in which $H_1, H_2, \ldots, H_\nu$ are identical, so that H *is self-conjugate under* G. Then $J=H$, so that the order k/j of Γ equals the index ν of H under G. Hence the number of distinct substitutions of Γ equals the number of letters $\psi_1, \ldots, \psi_\nu$ upon which its substitutions operate, or *the order and the degree of the group* Γ *are equal.* Moreover, Γ was seen to be transitive. Hence Γ is a *regular group* (§ 67).

DEFINITION.* When H is self-conjugate under G, the group Γ is called the **quotient-group** of G by H and designated G/H. In particular, the order of G/H is the quotient of the order of G by that of H.

EXAMPLE 1. By Examples 1 and 2 of § 77, the quotient-group G_6/G_1 is a regular group on six letters; the quotient-group G_{12}/G_4 is the cycle group $\{I, (\psi_1\psi_2\psi_3), (\psi_1\psi_3\psi_2)\}$, which is a regular group.

EXAMPLE 2. We may not employ the symbol G_{24}/G_8, since G_8 is not self-conjugate under G_{24} (§ 78, Ex. 3).

EXAMPLE 3. Consider the groups G_6 and G_3 on three letters. To G_3 belongs $\psi_1=(x_1-x_2)(x_2-x_3)(x_3-x_1)$; under G_6 it takes a second value $\psi_2=-\psi_1$ (§ 9). We obtain the following isomorphism between G_6 and Γ:

$$\begin{array}{lll|l} I, & (x_1x_2x_3), & (x_1x_3x_2) & I \\ (x_2x_3), & (x_1x_3), & (x_1x_2), & (\psi_1\psi_2) \end{array}$$

Since G_3 is self-conjugate under G_6, we have $\Gamma=G_6/G_3=\{I, (\psi_1\psi_2)\}$.

COROLLARY. *If* H *is a self-conjugate subgroup of* G *of prime index* ν, *then* Γ *is a cyclic group of order* ν (§ 27).

Illustrations are afforded by the groups G_{12}/G_4 and G_6/G_3 of Exs. 1 and 2.

REMARK. Any substitution group G is simply isomorphic with a regular group. In proof, we have merely to take as ψ any $n!$-valued function V_1, whence Γ will be of order equal to the order of G.

* Hölder, *Math. Ann.*, vol. 24, page 31.

80. Let H be a *maximal* self-conjugate subgroup of G (§ 43). The quotient-group $\Gamma=G/H$ is then *simple* (§ 43). For if Γ has a self-conjugate subgroup Δ distinct from both Γ and the identity G_1, there would exist, in view of the correspondence between G and Γ, a self-conjugate subgroup D of G, such that D contains H but is distinct from both G and H. This would contradict the hypothesis that H was maximal.

For example, if H is a self-conjugate subgroup of G of prime index ν, it is necessarily maximal. Then Γ is a cyclic group of prime order ν (Cor., § 79) and consequently a simple group.

81. The importance of the preceding investigation of the group Γ of substitutions on the letters $\psi_1, \psi_2, \ldots, \psi_\nu$ lies in the significance of Γ in the study of the resolvent equation

$$g(y)\equiv(y-\psi_1)(y-\psi_2)\ldots(y-\psi_\nu)=0, \tag{15}$$

whose coefficients belong to the given domain R. We proceed to prove the

THEOREM. *For the domain R, the group of the equation* (15) *is Γ.*

We show that Γ has the characteristic properties A and B of § 61. Any rational function $\rho(\psi_1, \psi_2, \ldots, \psi_\nu)$ with coefficients in R may be expressed as a rational function $r(x_1, x_2, \ldots, x_n)$ with coefficients in R:

$$\rho(\psi_1, \psi_2, \ldots, \psi_\nu)=r(x_1, x_2, \ldots, x_n). \tag{18}$$

From this rational relation we obtain a true relation (§ 62) upon applying any substitution g of the group G on $x_1, \ldots, x_n$. But g gives rise to a substitution γ of the group Γ on $\psi_1, \ldots, \psi_\nu$. Hence the resulting relation is

$$\rho_\gamma(\psi_1, \psi_2, \ldots, \psi_\nu)=r_g(x_1, x_2, \ldots, x_n). \tag{19}$$

To prove A, let $\rho(\psi_1, \ldots, \psi_\nu)$ remain unaltered by all the substitutions of Γ, so that $\rho_\gamma=\rho$, for any γ in Γ. Then, by (18) and (19), $r_g=r$, for any g in G. Hence r lies in the domain R (property A for the group G). Hence ρ lies in R.

To prove B, let ρ lie in the domain R. Then, by (18), r lies

in R. Hence $r_g = r$, for any g in G (property B for the group G). Hence, by (18) and (19), $\rho_\gamma = \rho$, so that ρ remains unaltered by all the substitutions γ of Γ.

COR. 1. Since Γ is transitive (§ 77), equation (15) is irreducible in R (§ 68). This was shown otherwise in § 71.

COR. 2. If the group H to which ϕ belongs is self-conjugate under G, the group of the resolvent (15) is regular (§ 79). The resolvent is then said to be a **regular equation**.

COR. 3. If H is a self-conjugate subgroup of G of prime index ν, the group of (15) is cyclic (§ 79, Corollary). The resolvent is then said to be a **cyclic equation** of prime degree ν.

COR. 4. If H is a maximal self-conjugate subgroup of G, the group of (15) is simple (§ 80). The resolvent is then said to be **a regular and simple equation.**

82. THEOREM. *The solution of any given equation can be reduced to the solution of a chain of simple regular equations.*

Let G be the group of the given equation for a given domain R, and let a series of composition (§ 43) of G be

$$G, H, K, \ldots, M, G_1,$$

the factors of composition being λ (index of H under G), μ (index of K under H), $\ldots$, ρ (index of G_1 under M). Let $\phi, \psi, \ldots, \chi, V$ be rational functions of the roots belonging to $H, K, \ldots, M, G_1$, respectively (§ 70). Then ϕ is a root of a resolvent equation of degree λ with coefficients in R, which is a simple regular equation (§ 81, Cor. 4). By the adjunction of ϕ to the domain R, the group G of the equation is reduced to H (§ 75). Then ψ is a root of a simple regular equation of degree μ with coefficients in the enlarged domain (ϕ, R). By the adjunction of ψ, the group is reduced to K. When, in this way, the group has reduced to the identity G_1, the roots $x_1, \ldots, x_n$ lie in the final domain reached (compare § 76).

In particular, *if the factors of composition $\lambda, \mu, \ldots, \rho$ are all prime numbers, the resolvent equations are all regular cyclic equations of prime degrees* (§ 81, Cor. 3).

83. THEOREM. *A cyclic equation of prime degree p is solvable by radicals.*

Let R be a given domain to which belong the coefficients of the given equation $f(x)=0$ with the roots $x_0, x_1, \ldots, x_{p-1}$, and for which the group of $f(x)=0$ is the cyclic group $G=\{I, s, s^2, \ldots, s^{p-1}\}$, where $s=(x_0x_1x_2\ldots x_{p-1})$. Adjoin to the domain R an imaginary pth root of unity * ω and let the group of $f(x)=0$ for the enlarged domain R' be G'. Consider the rational functions, with coefficients in R',

$$\theta_i \equiv x_0+\omega^i x_1+\omega^{2i}x_2+\ldots+\omega^{(p-1)i}x_{p-1}. \tag{20}$$

Under the substitution s, θ_i is changed into $\omega^{-i}\theta_i$. Hence $\theta_i^p \equiv \theta_i$ is unaltered by s and therefore by every substitution of G and of the *subgroup* G' (§ 74). Hence θ_i lies in the domain R' (§ 61). Extracting the pth root, we have $\theta_i=\sqrt[p]{\theta_i}$. Since the function (20) belongs to the identity group, it must be possible, by Lagrange's Theorem (§ 72), to express the roots $x_0, x_1, \ldots, x_{p-1}$ rationally in terms of θ_i. The actual expressions for the roots were found in the following elegant way by Lagrange. We have, by (20),

$$\begin{aligned}
&x_0+x_1 &&+x_2 &&+\ldots+x_{p-1}=c\\
&x_0+\omega x_1 &&+\omega^2x_2 &&+\ldots+\omega^{p-1}x_{p-1} &&=\sqrt[p]{\theta_1}\\
&x_0+\omega^2x_1 &&+\omega^4x_2 &&+\ldots+\omega^{2(p-1)}x_{p-1} &&=\sqrt[p]{\theta_2}\\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
&x_0+\omega^{p-1}x_1 &&+\omega^{2(p-1)}x_2 &&+\ldots+\omega^{(p-1)^2}x_{p-1} &&=\sqrt[p]{\theta_{p-1}}
\end{aligned}$$

where $c\equiv\sqrt[p]{\theta_0}$ is the negative of the coefficient of x^{p-1} in $f(x)=0$. Multiplying these equations by $1, \omega^{-i}, \omega^{-2i}, \ldots, \omega^{-(p-1)i}$, respectively, and adding the resulting equations, and then dividing by p, we get †

$$x_i=\frac{1}{p}\left\{c+\omega^{-i}\sqrt[p]{\theta_1}+\omega^{-2i}\sqrt[p]{\theta_2}+\ldots+\omega^{-(p-1)i}\sqrt[p]{\theta_{p-1}}\right\},$$

* As shown in § 89, ω can be determined by a finite number of applications of the operation *extraction of a single root of a known quantity.*

† Since $1+\omega^t+\omega^{2t}+\ldots+\omega^{(p-1)t}=0$ for $t=1, 2, \ldots, p-1$.

for $i=0, 1, \ldots, p-1$. The value of one of these $p-1$ radicals, say $\sqrt[p]{\theta_1}$, may be chosen arbitrarily; but the others are then fully determined, being rationally expressible in terms of that one. Indeed,

$$\sqrt[p]{\theta_i} \div (\sqrt[p]{\theta_1})^i \equiv \theta_i \div \theta_1^i$$

becomes $\omega^{-i}\theta_i \div (\omega^{-1}\theta_1)^i$ upon applying the substitution s and hence is unaltered by s, and is therefore in the domain R'.

84. From the results of §§ 82–83, we have the following

THEOREM. *If the group of an equation has a series of composition for which the factors of composition are all prime numbers, the equation is solvable by radicals, that is, by the extraction of roots of known quantities.*

The group property thus obtained as a sufficient condition for the algebraic solvability of a given equation will be shown (§ 92) to be also a necessary condition.

CHAPTER VIII.

REGULAR CYCLIC EQUATIONS; ABELIAN EQUATIONS.

85. Let $f(x)=0$ be an equation whose group G for a domain R consists of the powers of a circular substitution $s=(x_1x_2\ldots x_n)$:

$$G=\{I, s, s^2, \ldots, s^{n-1}\},$$

n being any integer. Since the cyclic group G is transitive and of order equal to its degree, it is *regular* (§ 67). Inversely, the generator s of a transitive cyclic group is necessarily a circular substitution on the n letters.*

The equation $f(x)=0$ then has the properties:

(a) It is irreducible, since its group is transitive (§ 68).

(b) All the roots are rational functions, with coefficients in R, of any one root x_1. Indeed, there are only n substitutions in the transitive group on n letters, and consequently a single substitution (the identity) leaving x_1 unaltered. Since x_1 belongs to the identity group, the result follows by Lagrange's Theorem (§ 72). Let $x_2=\theta(x_1)$. To this rational relation we may apply all the substitutions of G (§ 62). Hence

$$(21)\qquad x_2=\theta(x_1),\ x_3=\theta(x_2),\ \ldots,\ x_n=\theta(x_{n-1}),\ x_1=\theta(x_n).$$

DEFINITION. An irreducible equation for a domain R between whose n roots exist relations of the form (21), θ being a rational function with coefficients in R, is called an **Abelian equation**.†

---

* A non-circular substitution, as $t=(x_1x_2x_3)(x_4x_5)$, generates an intransitive group. Thus the powers of t replace x_1 by x_1, x_2, or x_3 only.

† More explicitly, uniserial Abelian (einfache Abel'sche, Kronecker). A more general type of "Abelian equations" was studied by Abel, *Œuvres*, I, No. XI, pp. 114–140.

86. THEOREM. *The group G of an Abelian equation is a regular cyclic group.*

Denote any substitution of the group G by

$$g=\begin{pmatrix} x_1 & x_2 & x_3 & \dots & x_n \\ x_\alpha & x_\beta & x_\gamma & \dots & x_\nu \end{pmatrix}.$$

Applying to the rational relations (21) the substitutions g (§ 62),

$$x_\beta=\theta(x_\alpha),\ x_\gamma=\theta(x_\beta),\ \dots,\ x_\alpha=\theta(x_\nu).$$

But, by (21), $\theta(x_\alpha)=x_{\alpha+1}$, holding also for $\alpha=n$ if we agree to set $x_i=x_{i+n}=x_{i+2n}=\dots$ It follows that

$$x_\beta=x_{\alpha+1},\ x_\gamma=x_{\beta+1},\ \dots,\ x_\alpha=x_{\nu+1}.$$

Since the equation is irreducible, its roots are all distinct. Hence, aside from multiples of n,

$$\beta=\alpha+1,\quad \gamma=\beta+1=\alpha+2,\quad \delta=\gamma+1=\alpha+3,\dots$$
$$\therefore\ g=\begin{pmatrix} x_1 & x_2 & x_3 & \dots & x_n \\ x_\alpha & x_{\alpha+1} & x_{\alpha+2} & \dots & x_{\alpha+n-1} \end{pmatrix}.$$

Since g replaces x_i by $x_{i+\alpha-1}$, it is the power $\alpha-1$ of the circular substitution $s=(x_1x_2x_3\dots x_n)$ which replaces x_i by x_{i+1}. Hence G is a subgroup of $G'=\{I,\ s,\ s^2,\dots,\ s^{n-1}\}$. But G is transitive, since the equation is irreducible. Hence $G=G'$.

EXAMPLE. The equation $x^4+x^3+x^2+x+1\equiv\dfrac{x^5-1}{x-1}=0$ has the roots

$$x_1=\epsilon,\quad x_2=\epsilon^2,\quad x_3=\epsilon^4,\quad x_4=\epsilon^3,$$

where ϵ is an imaginary fifth root of unity. Hence

$$x_2=x_1^2,\quad x_3=x_2^2,\quad x_4=x_3^2,\quad x_1=x_4^2.$$

Moreover, the equation is irreducible in the domain R of all rational numbers (§ 88). This may be verified directly by observing that the linear factors are $x-\epsilon^i$ and hence irrational, while

$$x^4+x^3+x^2+x+1\equiv(x^2+ax+r)(x^2+bx+r^{-1})$$

gives $a+b=1$, $ab+r+r^{-1}=1$, $ar^{-1}+br=1$, so that either

$$a=\tfrac{1}{2}(1\pm\sqrt{5}),\quad b=\tfrac{1}{2}(1\mp\sqrt{5}),\quad r=1,$$

or,
$$a=\frac{r}{r+1},\quad b=\frac{1}{r+1},\quad r^4+r^3+r^2+r+1=0.$$

Hence the group for R is a cyclic group. Compare Ex. 4, page 58.

87. Cyclotomic equation for the pth roots of unity, p being prime,

$$x^{p-1}+x^{p-2}+\ldots+x+1=0. \tag{22}$$

Let ϵ be one root of (22), so that $\epsilon^p=1$, $\epsilon\neq 1$. Then

$$\epsilon,\ \epsilon^2,\ \epsilon^3,\ \ldots,\ \epsilon^{p-1} \tag{23}$$

are all roots of (22) and are all distinct. Hence they furnish all the roots of (22). As shown in the Theory of Numbers, there exists,* for every prime number p, an integer g such that g^m-1 is divisible by p for $m=p-1$ but not for a smaller positive integer m. Such an integer g is called a **primitive root of** p. It follows that the series of integers

$$1,\ g,\ g^2,\ \ldots,\ g^{p-2},$$

when divided by p, yield in some order the remainders

$$1,\ 2,\ 3,\ \ldots,\ p-1.$$

Hence the roots (23) may be written

$$x_1=\epsilon,\ x_2=\epsilon^g,\ x_3=\epsilon^{g^2},\ \ldots,\ x_{p-1}=\epsilon^{g^{p-2}}.$$
$$\therefore\ x_2=x_1^g,\ x_3=x_2^g,\ \ldots,\ x_{p-1}=x_{p-2}^g,\ x_1=x_{p-1}^g,$$

the last relation following from the definition of g, thus:

$$(\epsilon^{g^{p-2}})^g=\epsilon^{g^{p-1}}=\epsilon^{1+qp}=\epsilon.$$

Hence the roots have the property indicated by formulæ (21). In view of the next section, we may therefore state the

THEOREM. *The cyclotomic equation for the imaginary pth roots of unity, p being prime, is an Abelian equation with respect to the domain of all rational numbers.*

---

* For example, if $p=5$, we may take $g=2$, since

$$2^1-1=1,\quad 2^2-1=3,\quad 2^3-1=7,\quad 2^4-1=15.$$

For $p=5$ the results of this section were found in the example of § 86.

88. Irreducibility of the cyclotomic equation (22) in the domain R of all rational numbers.* Suppose that

$$x^{p-1}+x^{p-2}+\ldots+x+1=\phi(x)\cdot\psi(x),$$

where ϕ and ψ are integral functions of degree $<p-1$ with integral † coefficients. Taking $x=1$, we get

$$p=\phi(1)\cdot\psi(1).$$

Since p is prime, one of the integral factors, say $\phi(1)$, must be ± 1. Since $\phi(x)=0$ has at least one root in common with (22), whose roots are (23), at least one of the expressions $\phi(\varepsilon^i)$ is zero. Hence

$$\phi(\varepsilon)\cdot\phi(\varepsilon^2)\cdot\phi(\varepsilon^3)\ldots\phi(\varepsilon^{p-1})=0. \tag{24}$$

For any positive integer s less than p, the series

$$\varepsilon^s,\ \varepsilon^{2s},\ \varepsilon^{3s},\ \ldots,\ \varepsilon^{(p-1)s} \tag{25}$$

is identical, apart from the order of the terms, with the series (23). For, every number (25) equals a number (23), and the numbers (25) are all distinct. In fact, if

$$\varepsilon^{rs}=\varepsilon^{ts},\ \text{whence}\ \varepsilon^{(r-t)s}=1,\quad (0\leqq r<p,\ 0\leqq t<p)$$

then $(r-t)s$, and consequently also $r-t$, is divisible by p, so that $r=t$. Hence (24) holds true when ε is replaced by ε^s. Hence

$$\phi(x)\cdot\phi(x^2)\ldots\phi(x^{p-1})=0$$

is an equation having all the numbers (23) as roots. Its left member is therefore divisible by $x^{p-1}+\ldots+x+1$, so that

$$\phi(x)\cdot\phi(x^2)\ldots\phi(x^{p-1})=Q(x)\cdot(x^{p-1}+x^{p-2}+\ldots+x+1),$$

where $Q(x)$ is an integral function with integral coefficients. Setting $x=1$, we get

$$[\phi(1)]^{p-1}=[\pm 1]^{p-1}=p\cdot Q(1).$$

Since ± 1 is not divisible by p, the assumption that $x^{p-1}+\ldots+x+1$ is reducible in R leads to a contradiction.

---

* The proof is that by Kronecker, *Crelle*, vol. 29; other proofs have been given by Gauss, Eisenstein (*Crelle*, vol. 39, p. 167), Dedekind (Jordan, *Traité des substitutions*, Nos. 413–414).

† If rational, then integral (Weber, *Algebra*, I, 1895, p. 27).

89. THEOREM. *Any Abelian equation is solvable by radicals.*

Let n be the degree of the Abelian equation. By § 86, its group G is a regular cyclic group $\{I, s, s^2, \ldots, s^{n-1}\}$ of order n. Set $n = p \cdot n'$, where p is prime. Set $s^p = s'$. Then the group

$$H = \{I, s', s'^2, \ldots, s'^{n'-1}\}$$

is a subgroup of G of prime index p. It is self-conjugate, since

$$s^{-\beta} s'^{\alpha} s^{\beta} = s^{-\beta} s^{\alpha p} s^{\beta} = s^{\alpha p} = s'^{\alpha}$$

by § 13. Hence H may be taken as the second group of a series of composition of G. Proceeding with H as we did with G, we finally reach the conclusion:

The factors of composition of a cyclic group of order n are the prime factors of n each repeated as often as it occurs in n.

In view of the remark at the end of § 82, it now follows that *any Abelian equation of degree n can be reduced to a chain of Abelian equations whose degrees are the prime factors of n.*

We may now show by induction that every Abelian equation of prime degree p is solvable by radicals. We suppose solvable all Abelian equations of prime degrees less than a certain prime p. Among them are the Abelian equations of prime degrees to which can be reduced the Abelian equation of degree $p-1$, giving an imaginary pth root of unity (§ 87). The latter being therefore known, every Abelian equation of degree p is solvable by radicals (§ 83). Now an Abelian equation of degree 2 is solvable by radicals. Hence the induction is complete.

It follows now that an Abelian equation of any degree is solvable.

COROLLARY. If p is a prime number, all the pth roots of unity can be found by a finite number of applications of the operation *extraction of a single root of a known quantity,* the index of each radical being a prime divisor of $p-1$.

90. LEMMA. *If p be prime, and if A be a quantity lying in a domain R but not the pth power of a quantity in R, then $x^p - A$ is irreducible in R.*

For, if reducible in R, so that

$$x^p - A = \phi_1(x) \cdot \phi_2(x) \ldots,$$

the several factors are of the same degree only when each is of degree 1, the only divisor of p. In the latter case, the roots would all lie in R, contrary to assumption. Let then ϕ_1 be of higher degree than ϕ_2 and set

$$\phi_1(x)=(x-x_1')\dots(x-x_{n_1}'),\quad \phi_2(x)=(x-x_1'')\dots(x-x_{n_2}''),$$

so that $n_1-n_2>0$. The last coefficients in the products are

$$\pm x_1'x_2'\dots x_{n_1}'=\pm\omega^{\sigma_1}x_1^{n_1},\quad \pm x_1''x_2''\dots x_{n_2}''=\pm\omega^{\sigma_2}x_1^{n_2},$$

respectively, since the roots of $x^p-A=0$ are

$$x_1,\quad \omega x_1,\quad \omega^2x_1,\quad \dots,\quad \omega^{p-1}x_1, \tag{26}$$

ω being an imaginary pth root of unity. But the last coefficients, and their quotient $\pm\omega^{\sigma}x_1^{m}$, where $m=n_1-n_2>0$, lie in R. Since p and m are relatively prime, integers μ and ν exist for which

$$m\mu-p\nu=1.$$

$$\therefore\ (\omega^{\sigma}x_1^{m})^{\mu}=\omega^{\sigma\mu}x_1^{p\nu+1}=\omega^{\sigma\mu}A^{\nu}x_1=A^{\nu}x',$$

where x' is one of the roots (26). Hence $A^{\nu}x'$, and consequently x', lies in R. Then A equals the pth power of a quantity x' in R, contrary to assumption. Hence x^p-A must be irreducible.

91. THEOREM. *A binomial equation of prime degree p,*

$$x^p-A=0,$$

can be solved by means of a chain of Abelian equations of prime degree.

Let R be the given domain to which A belongs. Adjoin ω and denote by R' the enlarged domain. Then the roots (26) satisfy the relations

$$x_2=\omega x_1,\quad x_3=\omega x_2,\quad \dots,\quad x_p=\omega x_{p-1},\quad x_1=\omega x_p,$$

of the type (21) of § 85, $\theta(x)$ being here the rational function ωx. The discussion in § 90 shows that x^p-A is either irreducible in the enlarged domain R' or else has *all* its roots in R'. In the former case, the group of $x^p-A=0$ for R' is a regular cyclic group (§ 86); in the latter case, the group for R' is the identity. But ω itself is determined by an Abelian equation (§ 87). Hence, in either case, $x^p-A=0$ is made to depend upon a chain of Abelian equations, whose degrees may be supposed to be prime (§ 89).

CHAPTER IX.

CRITERION FOR ALGEBRAIC SOLVABILITY.

92. We are now in a position to complete the theory of the algebraic solution of an arbitrarily given equation of degree n,

$$f(x)=0. \tag{1}$$

A group property expressing a sufficient condition for the algebraic solvability of (1) was established in § 84. To show that this property expresses a necessary condition, we begin with a discussion of equation (1) under the hypothesis that it is solvable by radicals, namely (§ 50), that its roots $x_1, \ldots, x_n$ can be derived from the initially given quantities $R', R'', \ldots$ by addition, subtraction, multiplication, division, and extraction of a root of any index. These indices may evidently be assumed to be prime numbers. If $\xi, \eta, \ldots, \psi$ denote all the radicals which enter the expressions for all the roots $x_1, x_2, \ldots, x_n$, the solution may be exhibited by a chain of binomial equations of prime degree;

$$\begin{gathered}\xi^\lambda=L(R', R'', \ldots), \quad \eta^\mu=M(\xi, R', R'', \ldots), \quad \ldots, \\ \psi^\rho=P(\ldots, \eta, \xi, R', R'', \ldots), \\ x_i=R_i(\psi, \ldots, \eta, \xi, R', R'', \ldots) \qquad (i=1, \ldots, n),\end{gathered}$$

$L, M, \ldots, P, R_i$ being rational functions with integral coefficients, in which some of the arguments $\xi, \eta, \ldots$ written may be wanting. By § 91, each of these binomial equations, and therefore also the complete chain, can be replaced by a chain of Abelian equations of prime degrees;

$$\begin{aligned}
&\Phi(y;\ R', R'', \ldots)=0, && \text{Abelian for domain } R;\\
&\Psi(z;\ y, R', R'', \ldots)=0, && \text{Abelian for } (y, R);\\
&\cdots\cdots\cdots && \cdots\cdots\cdots\\
&\theta(w;\ \ldots, z, y, R', R'', \ldots)=0, && \text{Abelian for } (\ldots, z, y, R);\\
&x_i=\Omega_i(w, \ldots, z, y, R', R'', \ldots) && (i=1, \ldots, n).
\end{aligned}$$

We begin by solving the first Abelian equation $\Phi(y)=0$ and adjoining one of its roots, say y, to the original domain R; the group G of (1) then reduces to a certain subgroup, say H, including the possibility $H=G$ (§ 74). Then we solve the second Abelian equation $\Psi(z)=0$ and adjoin one of its roots, say z, to the enlarged domain (y, R); the group H reduces to a certain subgroup, say J, including the possibility $J=H$. Proceeding in this way, until the last equation $\theta(w)=0$ has been solved and one of its roots, say w, has been adjoined, we finally reach the domain $(w, \ldots, z, y, R)$, with respect to which the group of (1) is the identity G_1, since all the roots x_i lie in that domain.

By every one of these successive adjunctions, either the group of equation (1) is not reduced at all or else the group is reduced to a self-conjugate subgroup of prime index. This theorem, due to Galois, is established as a corollary in the next section; its importance is better appreciated if we remark that each adjoined quantity is not supposed to be a rational function of the roots, in contrast with § 75, so that we shall be able to draw an important conclusion, due to Abel, concerning the nature of the irrationalities occurring in the expressions for the roots of a solvable equation (§ 94).

From this theorem of Galois, it follows that the different groups through which we pass in the process of successive adjunction of a root of each Abelian equation in the chain to which the given solvable equation was reduced must form a series of composition of the group G of the given equation having only prime numbers as factors of composition. Indeed, the series of groups beginning with G and ending with the identity G_1 are such that each is a self-conjugate subgroup of prime index under the preceding. Hence the sufficient condition (§ 84) for the algebraic solvability of a

given equation is also a necessary condition, so that we obtain Galois' criterion for algebraic solvability:

In order that an equation be solvable by radicals, it is necessary and sufficient that its group have a series of composition in which the factors of composition are all prime numbers.

93. Theorem of Jordan,* as amplified and proved by Hölder:†

For a given domain R let the group G_1 of an equation $F_1(x)=0$ be reduced to G_1' by the adjunction of all the roots of a second equation $F_2(x)=0$, and let the group G_2 of the second equation be reduced to G_2' by the adjunction of all the roots of the first equation $F_1(x)=0$. Then G_1' and G_2' are self-conjugate subgroups of G_1 and G_2 respectively, and the quotient-groups G_1/G_1' and G_2/G_2' are simply isomorphic.

Let $\psi_1(\xi_1, \xi_2, \ldots, \xi_n)$ be a rational function, with coefficients in R, of the roots of the first equation which belongs to the subgroup G_1' of the group G_1 of the first equation (§ 70). By hypothesis, the adjunction of the roots $\eta_1, \eta_2, \ldots, \eta_m$ of the equation $F_2(x)=0$ reduces the group G_1 to G_1'. Hence ψ_1 lies in the enlarged domain, so that

$$\psi_1(\xi_1, \xi_2, \ldots, \xi_n)=\phi_1(\eta_1, \eta_2, \ldots, \eta_m), \tag{27}$$

the coefficients of the rational function ϕ_1 being in R.

Let $\psi_1, \psi_2, \ldots, \psi_k$ denote all the numerically distinct values which ψ_1 can take under the substitutions (on $\xi_1, \ldots, \xi_n$) of G_1. Then G_1' is of index k under G_1 (§ 71). Let $\phi_1, \phi_2, \ldots, \phi_l$ denote all the numerically distinct values which ϕ_1 can take under the substitutions (on $\eta_1, \ldots, \eta_m$) of G_2. The k quantities ψ are the roots of an irreducible equation in R (§ 71); likewise for the l quantities ϕ. Since these two irreducible equations have a common root $\psi_1=\phi_1$, they are identical (§ 55, Cor. II). Hence $\psi_1, \ldots, \psi_k$ coincide in some order with $\phi_1, \ldots, \phi_l$; in particular, $k=l$.

If s_i is a substitution of G_1 which replaces ψ_1 by its conjugate ψ_i, then s_i transforms G_1', the group of ψ_1 by definition, into the group of ψ_i of the same order as G_1'. But ψ_i, being equal to a ϕ, lies in

* *Traité des substitutions*, pp. 269, 270. † *Math. Annalen*, vol. 34.

the domain $R' \equiv (R;\ \eta_1,\ \ldots,\ \eta_m)$, and hence is unaltered by the substitutions of the group G_1' of the equation $F_1(x)=0$ for that domain R' (§ 61, property B). Hence the group of ψ_i contains all the substitutions of G_1'; being of the same order, the group of ψ_i is identical with G_1'. *Hence G_1' is self-conjugate under G_1.* The group of the irreducible equation satisfied by ψ_1 is therefore the quotient-group G_1/G_1' (§ 79).

Let H_2 be the subgroup of G_2 to which belongs $\phi_1(\eta_1, \eta_2, \ldots, \eta_m)$. Since ϕ_1 is a root of an irreducible equation in R of degree $l=k$, the group H_2 is of index k under G_2 (§ 71). By the adjunction of ϕ_1 (or, what amounts to the same thing in view of (27), by the adjunction of ψ_1), the group G_2 of equation $F_2(x)=0$ for R is reduced to H_2 (§ 75). If not merely $\psi_1(\xi_1, \ldots, \xi_n)$, but all the ξ's themselves be adjoined, the group G_2 reduces perhaps further to a subgroup of H_2. Hence G_2' is contained in H_2. We thus have the preliminary result: If the group of $F_1(x)=0$ reduces to a subgroup of index k on adjoining all the roots of $F_2(x)=0$, then the group of $F_2(x)=0$ reduces to a subgroup of index k_1, $k_1 \geqq k$, on adjoining all the roots of $F_1(x)=0$.

Interchanging F_1 and F_2 in the preceding statement we obtain the result: If the group of $F_2(x)=0$ reduces to a subgroup of index k_1 on adjoining all the roots of $F_1(x)=0$, then the group of $F_1(x)=0$ reduces to a subgroup of index k_2, $k_2 \geqq k_1$, on adjoining all the roots of $F_2(x)=0$. Since the hypothesis for the second statement is identical with the conclusion for the first statement, it follows that

$$k_2=k, \quad k_1 \geqq k, \quad k_2 \geqq k_1,$$

so that $k_1=k$. Hence the group G_2' of the theorem is identical with the group H_2 of all the substitutions in G_2 which leave ϕ_1 unaltered. It follows that *G_2' is self-conjugate under G_2* (for the same reason that G_1' is self-conjugate under G_1). The irreducible equation in R satisfied by ϕ_1 has for its group the quotient-group G_2/G_2'.

But the two irreducible equations for R satisfied by ϕ_1 and ψ_1, respectively, were shown to be identical. Hence the groups

G_1/G_1' and G_2/G_2' differ only in the notations employed for the letters on which they operate, and hence are simply isomorphic.

COROLLARY. For the particular case in which the second equation is an Abelian equation of prime degree p, all of its roots are rational functions in R of any one root, so that by adjoining one we adjoin all its roots. *By the adjunction of any one root of an Abelian equation of prime degree p, the group of the given equation* $F_1(x)=0$ *either is not reduced at all or else is reduced to a self-conjugate subgroup of index p.*

94. If G_2 is simple and if the adjunction causes a reduction, then G_2 is reduced to the identity. Hence the group $G_2'=H_2$, to which belongs ϕ_1, is the identity. Hence the roots $\eta_1, \eta_2, \ldots, \eta_m$ of $F_2(x)=0$ are rational functions in R of ϕ_1 (§ 72) and therefore, in view of (27), of the roots $\xi_1, \ldots, \xi_n$ of $F_1(x)=0$.

If the group of an equation $F_1(x)=0$ *for a domain R is reduced by the adjunction of all the roots of an equation* $F_2(x)=0$ *whose group for R is simple, then all the roots of* $F_2(x)=0$ *are rational functions in R of the roots of* $F_1(x)=0$.

Since the group of a solvable equation $f(x)=0$ has a series of composition in which the factors of composition are all prime numbers, the equation can be replaced by a chain of resolvent equations each an Abelian equation of prime degree (end of § 82, § 85). The adjunction of a root of each resolvent reduces the group of the equation and the group of the resolvent is simple, being cyclic of prime order. Hence the roots of each Abelian resolvent equation are all rational functions of the roots of $f(x)=0$. But the radicals entering the solution of an Abelian equation of prime degree are rationally expressible in terms of its roots and an imaginary pth root of unity (§ 83),

$$\sqrt[p]{\theta_1}=x_0+\omega x_1+\omega^2 x_2+\ldots+\omega^{p-1}x_{p-1},\ldots$$

and hence are rationally expressible in terms of the roots of $f(x)=0$ and pth roots of unity. We therefore state Abel's Theorem:

The solution of an algebraically solvable equation can always be performed by a chain of binomial equations of prime degrees whose

roots are rationally expressible in terms of the roots of the given equation and of certain roots of unity.

The roots of an algebraically solvable equation can therefore be given a form such that all the radicals entering them are rationally expressible in terms of the roots of the equation and of certain roots of unity. This result was first shown empirically by Lagrange for the general quadratic, cubic, and quartic equations (see Chapter I).

The Theorem of Abel supplies the step needed to complete the proof of the impossibility of the algebraic solution of the general equation of degree $n>4$ (§ 48).

95. By way of illustrating Galois' theory, we proceed to give algebraic solutions of the general equations of the third and fourth degrees by chains of Abelian equations.

For the cubic $x^3-c_1x^2+c_2x-c_3=0$, let the domain of rationality be $R=(c_1, c_2, c_3)$. The group of the cubic for R is the symmetric group G_6 (§ 64). To the subgroup G_3 belongs

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

In view of Ex. 3, page 4, Δ is a root of the equation

$$\Delta^2=c_1^2c_2^2+18c_1c_2c_3-4c_2^3-4c_1^3c_3-27c_3^2. \tag{28}$$

Its second root $-\Delta$ is rationally expressible in terms of the first root Δ, and (28) is irreducible since Δ is not in R for general c_1, c_2, c_3. Hence (28) is Abelian (§ 85). By adjoining Δ to R, the group reduces to G_3 (§ 75). Solve the Abelian equation $\omega^2+\omega+1=0$ (§ 87) and adjoin ω to the domain (Δ, R). To the enlarged domain $R'=(\omega, \Delta, c_1, c_2, c_3)$ belong the coefficients of the function

$$\psi_1=x_1+\omega x_2+\omega^2x_3.$$

By § 34, ψ_1^3 has a value lying in R', namely,

$$\psi_1^3=\tfrac{1}{2}[2c_1^3-9c_1c_2+27c_3-3(\omega-\omega^2)\Delta].$$

This binomial is an Abelian equation for the domain R' (§ 91). By the adjunction of ψ_1, the group of the cubic reduces to the

identity. Hence x_1, x_2, x_3 lie in the domain $(\psi_1, \omega, \Delta, c_1, c_2, c_3)$. Thus, by § 34,

$$x_1=\tfrac{1}{3}\left(c_1+\psi_1+\frac{c_1^2-3c_2}{\psi_1}\right), \quad x_2=\tfrac{1}{3}\left(c_1+\omega^2\psi_1+\omega\frac{(c_1^2-3c_2)}{\psi_1}\right).$$

We may, however, solve the cubic without adjoining ω. In the domain (Δ, c_1, c_2, c_3), the cubic itself is an Abelian equation, since its group G_3 is cyclic (§ 85). By the adjunction of a root x_1 of this Abelian equation, the group reduces to the identity, so that x_2 and x_3 must lie in the domain $(x_1, \Delta, c_1, c_2, c_3)$. The explicit expressions for x_2 and x_3 are given by Serret, *Algèbre supérieure*, vol. 2, No. 511:

$$x_2=\frac{1}{2\Delta}\{(6c_2-2c_1^2)x_1^2+(9c_3-7c_1c_2+2c_1^3-\Delta)x_1+4c_2^2-c_1^2c_2-3c_1c_3+c_1\Delta\},$$

the value of x_3 being obtained by changing the sign of Δ throughout.

96. For the general quartic $x^4+ax^3+bx^2+cx+d=0$, the group for the domain $R=(a, b, c, d)$ is G_{24}. To the subgroup G_{12} belongs

$$\Delta=(x_1-x_2)(x_1-x_3)(x_1-x_4)(x_2-x_3)(x_2-x_4)(x_3-x_4).$$

Since Δ^2 is an integral function of a, b, c, d with rational coefficients (§ 42), we obtain Δ by solving an equation which is Abelian for R. After the adjunction of Δ, the group is G_{12}. To the *subgroup* G_4 *of* G_{12} belongs the function $y_1=x_1x_2+x_3x_4$. It satisfies the cubic resolvent equation (§ 4)

$$y^3-by^2+(ac-4d)y-a^2d+4bd-c^2=0. \tag{16}$$

The group of this resolvent for the domain (Δ, a, b, c, d) is a cyclic group of order 3 (§ 79, Cor.), so that the resolvent is Abelian. By the adjunction of y_1, the group of the quartic reduces to G_4. To the subgroup G_2 of G_4 belongs the function $t=x_1+x_2-x_3-x_4$. It is determined by the Abelian equation (§ 5)

$$t^2=a^2-4b+4y_1. \tag{29}$$

By the adjunction of t, the group reduces to G_2. To the identity subgroup G_1 of G_2 belongs x_1; it is a root of (17), § 4:

$$x^3+\tfrac{1}{2}(a-t)x+\tfrac{1}{2}y_1-(\tfrac{1}{2}ay_1-c)/t=0.$$

After the adjunction of a root x_1 of this Abelian equation, the group is the identity G_1. Hence (§ 72) all the roots lie in the domain $(x_1, t, y_1, \Delta, a, b, c, d)$. This is evident for x_2, since $x_1+x_2=-\frac{1}{2}(a-t)$. For x_3 and x_4, we have

$$x_3+x_4=x_1+x_2-t, \quad x_3-x_4=(y_2-y_3)\div(x_1-x_2),$$

while y_2 and y_3 are rationally expressible in terms of y_1, Δ, and the coefficients of (16), as shown at the end of § 95. In fact, $(y_1-y_2)(y_2-y_3)(y_1-y_3)$ has the value Δ by § 7.

97. Another method of solving the general quartic was given in § 42. For the domain $R=(\omega, a, b, c, d)$, where ω is an imaginary cube root of unity, the group is G_{24} (§ 64). After the adjunction of Δ, the group is G_{12}. To the self-conjugate subgroup G_4 belongs $\phi_1=y_1+\omega y_2+\omega^2 y_5$, where $y_1=x_1x_2+x_3x_4$, etc., so that ϕ_1 is a rational function of x_1, x_2, x_3, x_4, with coefficients in R. By § 42,

$$\phi_1^3=\tfrac{3}{2}(\omega-\omega^2)\Delta-216J,$$

so that ϕ_1 is determined by an equation which is Abelian for the domain $(\Delta, \omega, a, b, c, d)$. Then, by § 42, y_1, y_2, y_3 belong to the enlarged domain $(\phi_1, \Delta, \omega, a, b, c, d)$.

By the adjunction of t, a root of the binomial Abelian equation (29), the group reduces to G_2. By the adjunction* of both $i=\sqrt{-1}$ and $V=x_1-x_2+ix_3-ix_4$, which is a root of a binomial quadratic equation (§ 42), the group reduces to the identity G_1. The expressions for x_1, x_2, x_3, x_4 in terms of t, V, i, and a, are given by formula (41), in connection with (40), of § 37.

* Without adjoining i and V, we may determine $t_2=x_1+x_3-x_2-x_4$ from $t_2^3=a^2-4b+4y_2$. Then $t_3=x_1+x_4-x_2-x_3$ is known, since $t_1t_2t_3=4ab-8c-a^3$ by formula (39) of § 36, where $t_1=t$. Then

$$x_1=\tfrac{1}{4}(-a+t_1+t_2+t_3), \quad x_2=\tfrac{1}{4}(-a+t_1-t_2-t_3), \text{ etc.}$$

CHAPTER X.

METACYCLIC EQUATIONS; GALOISIAN EQUATIONS.

98. Analytic representation of substitutions. Given any substitution

$$s=\begin{pmatrix} x_0 & x_1 & x_2 & \dots & x_{n-1} \\ x_a & x_b & x_c & \dots & x_k \end{pmatrix},$$

so that $a, b, \dots, k$ form a permutation of $0, 1, \dots, n-1$, it is possible to construct a function $\phi(z)$ of one variable z such that

$$\phi(0)=a, \quad \phi(1)=b, \quad \phi(2)=c, \quad \dots, \quad \phi(n-1)=k.$$

Indeed, such a function is given by Lagrange's Interpolation-Formula,

$$\phi(z)=\frac{aF(z)}{zF'(0)}+\frac{bF(z)}{(z-1)F'(1)}+\dots+\frac{kF(z)}{(z-n+1)F'(n-1)},$$

where $F(z)\equiv z(z-1)(z-2)\dots(z-n+1)$ and $F'(z)$ is the derivative of $F(z)$. Then the substitution s is represented analytically as follows;

$$s=\begin{pmatrix} x_z \\ x_{\phi(z)} \end{pmatrix}.$$

We confine our attention to the case in which n is a prime number p, and agree to take $x_z=x_{z+p}=x_{z+2p}=\dots$. Then (as in § 86) the circular substitution $t=(x_0\, x_1\, x_2 \dots x_{p-1})$ may be represented in the form

$$t=\begin{pmatrix} x_z \\ x_{z+1} \end{pmatrix}.$$

Let G be the largest group of substitutions on $x_0, x_1, \dots, x_{p-1}$

under which the cyclic group $H=\{I, t, t^2, \ldots, t^{p-1}\}$ is self-conjugate. The general substitutions g of G and h of H may be written

$$g=\begin{pmatrix} x_z \\ x_{\phi(z)} \end{pmatrix}, \quad h=\begin{pmatrix} x_z \\ x_{z+a} \end{pmatrix}=t^a.$$

By hypothesis, $g^{-1}tg$ belongs to H and hence is of the form t^a.

$$g^{-1}=\begin{pmatrix} x_{\phi(z)} \\ x_z \end{pmatrix}, \quad g^{-1}t=\begin{pmatrix} x_{\phi(z)} \\ x_{z+1} \end{pmatrix}, \quad g^{-1}tg=\begin{pmatrix} x_{\phi(z)} \\ x_{\phi(z+1)} \end{pmatrix}.$$

But t^a replaces $x_{\phi(z)}$ by $x_{\phi(z)+a}$. Hence must

$$x_{\phi(z+1)}=x_{\phi(z)+a}.$$

Taking in turn $z=0, 1, 2, \ldots$, and writing $\phi(0)=b$, we get

$$x_{\phi(1)}=x_{b+a}, \quad x_{\phi(2)}=x_{\phi(1)+a}=x_{b+2a}, \quad x_{\phi(3)}=x_{\phi(2)+a}=x_{b+3a}, \quad \ldots$$

By simple induction, we get $x_{\phi(z)}=x_{b+za}$ for any integer z. Hence

$$g=\begin{pmatrix} x_z \\ x_{az+b} \end{pmatrix}. \tag{30}$$

Here a and $b\equiv\phi(0)$ are integers. Also a is not divisible by p, since $g^{-1}tg$ is not the identity. The distinct substitutions * g are obtained by taking the values

$$a=1, 2, \ldots, p-1; \quad b=0, 1, 2, \ldots, p-1.$$

The resulting $p(p-1)$ substitutions form a group called the **metacyclic group** of degree p. This follows from its origin or from

$$\begin{pmatrix} x_z \\ x_{az+b} \end{pmatrix}\begin{pmatrix} x_z \\ x_{az+\beta} \end{pmatrix}=\begin{pmatrix} x_z \\ x_{a(az+b)+\beta} \end{pmatrix}\equiv\begin{pmatrix} x_z \\ x_{aaz+(ab+\beta)} \end{pmatrix}.$$

REMARK. The only circular substitutions of period p in the metacyclic group are the powers of t. For $a=1$, (30) becomes t^b; for $a\neq 1$, (30) leaves one root unaltered, namely, that one whose index z makes $az+b$ and z differ by a multiple of p.

---

* Formula (30) does, indeed, define a substitution on $x_0, x_1, \ldots, x_{n-1}$,

$$\begin{pmatrix} x_0 & x_1 & x_2 & \ldots \\ x_b & x_{a+b} & x_{2a+b} & \ldots \end{pmatrix},$$

since $b, a+b, 2a+b, \ldots, (p-1)a+b$ give the remainders 0, 1, 2, .., $p-1$, in some order, when divided by p. In proof, the remainders are all different.

99. A metacyclic equation of degree p is one whose group G for a domain R is the metacyclic group of degree p. It is irreducible since G is transitive, its cyclic subgroup H being transitive. Again, all its roots are rational functions of two of the roots with coefficients in R. For, by the adjunction of two roots, say x_u and x_v, the group reduces to the identity. Indeed, if g leaves x_u and x_v unaltered, then

$$(au+b)-u, \quad (av+b)-v$$

are multiples of p, so that their difference $(a-1)(u-v)$ is a multiple of p, whence $a=1$, and therefore $b=0$. Hence the identity alone leaves x_u and x_v unaltered.

DEFINITION. For a domain R, an irreducible equation of prime degree whose roots are all rational functions of two of the roots is called a **Galoisian equation.**

Hence *a metacyclic equation is a Galoisian equation.*

100. Given, inversely, a Galoisian equation of prime degree p, we can readily determine its group G for a domain R. The equation being irreducible, its group is transitive, so that the order of G is divisible by p (§ 67). Hence G contains a cyclic subgroup H of order p (see foot-note to § 27). Let x_0 and x_1 denote the two roots in terms of which all the roots are supposed to be rationally expressible. Among the powers of any circular substitution of period p, there is one which replaces x_0 by x_1. Hence, by a suitable choice of notation for the remaining roots, we may assume that H contains the substitution

$$t=(x_0\, x_1\, x_2 \ldots x_{p-1}).$$

To show that H is self-conjugate under G, it suffices to prove that any circular substitution, contained in G,

$$r=(x_{i_0}\, x_{i_1}\, x_{i_2} \ldots x_{i_{p-1}})$$

is a power of t; for, the transform of t by any substitution of G will then belong to H (§ 40). Since every two adjacent letters in r are different, $i_{s+1}-i_s$ is never a multiple of p and hence, for at

least two values μ and ν of z chosen from the series $0, 1, \ldots, p-1$, gives the same remainder when divided by p. Hence

$$x_{i_{\mu+1}-i_\mu} = x_{i_{\nu+1}-i_\nu}, \text{ say } = x_k.$$

Since r is a power of a circular substitution replacing x_0 by x_1, we may assume that $i_0=0$, $i_1=1$. The hypothesis then gives

$$x_{i_a} = \theta_a(x_{i_0}, x_{i_1}) \qquad (a=0, 1, \ldots, p-1),$$

where θ_a is a rational function with coefficients in R. Applying to these rational relations the substitutions $r^\mu t^{-i_\mu}$ and $r^\nu t^{-i_\nu}$ of the group G, we obtain, by § 62,

$$x_{i_{a+\mu}-i_\mu} = \theta_a(x_0, x_k), \quad x_{i_{a+\nu}-i_\nu} = \theta_a(x_0, x_k).$$

Hence the subscripts in the left members are equal, so that

$$i_{a+\mu}-i_{a+\nu} = i_\mu - i_\nu = c \qquad (a=0, 1, \ldots, p-1),$$

omitting multiples of p. Hence every subscript in r exceeds by c the $(\mu-\nu)$th subscript preceding it. Hence r is a power of t.

Since G has a self-conjugate cyclic subgroup H, it is contained in the metacyclic group of degree p (§ 98).

The group of a Galoisian equation of prime degree p is a subgroup of the metacyclic group of degree p.

101. A metacyclic equation is readily solved by means of a chain of two Abelian equations. Let $\psi = R(x_0, x_1, \ldots, x_{p-1})$ belong to the subgroup H of G. Then

$$\psi_1 = \psi, \psi_2 = R(x_0, x_2, x_4, \ldots, x_{2p-2}), \ldots, \psi_{p-1} = R(x_0, x_{p-1}, x_{2p-2}, \ldots, x_{(p-1)^2})$$

are the $p-1$ values of ψ under G. But ψ_i is changed into ψ_{ki} by the substitution which replaces x_z by x_{kz}. It follows that the $p-1$ values of ψ are permuted cyclically under the $p(p-1)$ substitutions of G. The group of the resolvent equation

$$(w-\psi_1)(w-\psi_2)\ldots(w-\psi_{p-1}) = 0$$

is therefore a cyclic group of order $p-1$, so that the resolvent is an Abelian equation (§ 85). By the adjunction of ψ, the group

of the original equation reduces to the cyclic group H, so that it is Abelian in the enlarged domain.

The method applies also to any Galoisian equation. Its group G is a subgroup of the metacyclic group and yet contains H as a subgroup. The order of G is therefore pd, where d is a divisor of $p-1$. The two auxiliary Abelian equations are then of degrees d and p respectively. Applying § 89, we have the results:

A Galoisian equation can be solved by a chain of Abelian equations of prime degree and hence is solvable by radicals.

EXAMPLE 1. Let A be a quantity lying in a given domain R but not the pth power of a quantity in R. Then the equation

$$x^p - A = 0$$

is irreducible in R (§ 90). Its roots are

$$x_0, \quad x_1 = \omega x_0, \quad x_2 = \omega^2 x_0, \quad \ldots, \quad x_{p-1} = \omega^{p-1} x_0.$$

All the roots are rationally expressible in terms of x_0 and x_1:

$$x_i = \left(\frac{x_1}{x_0}\right)^i x_0 \qquad (i = 0, 1, \ldots, p-1).$$

The equation is therefore a Galoisian equation. For the function ψ belonging to the cyclic subgroup H we may take

$$\frac{x_1}{x_0} = \frac{x_2}{x_1} = \ldots = \frac{x_0}{x_{p-1}} = \omega.$$

The resolvent equation $\omega^{p-1} + \ldots + \omega + 1 = 0$ is indeed Abelian (§ 87). After the adjunction of ω, $x^p - A = 0$ becomes an Abelian equation (§ 91).

EXAMPLE 2. To solve the quintic equation *

$$y^5 + py^3 + \tfrac{1}{5}p^2 y + r = 0, \tag{e}$$

set $y = z - \dfrac{p}{5z}$. Then (compare the solution of the cubic, § 2)

$$z^5 - \frac{p^5}{5^5 z^5} + r = 0.$$

$$\therefore z^5 = -\frac{r}{2} + \sqrt{Q}, \quad Q \equiv \frac{r^2}{4} + \left(\frac{p}{5}\right)^5.$$

If ϵ is an imaginary fifth root of unity, the roots of (e) are

$$y_1 = A + B, \quad y_2 = \epsilon A + \epsilon^4 B, \quad y_3 = \epsilon^2 A + \epsilon^3 B, \quad y_4 = \epsilon^3 A + \epsilon^2 B, \quad y_5 = \epsilon^4 A + \epsilon B,$$

where

$$A = \sqrt[5]{-\frac{r}{2} + \sqrt{Q}}, \quad B = \sqrt[5]{-\frac{r}{2} - \sqrt{Q}}.$$

* Compare Dickson's *College Algebra*, pages 189 and 193.

Evidently A and B may be expressed as linear functions of y_1 and y_2. Hence y_3, y_4, y_5 are rational functions of y_1 and y_2 with coefficients in the domain $R=(\epsilon, p, r)$. For general p and r, equation (e) is irreducible in R, since no one of its roots lies in R and since it has no quadratic factor in R (as may be shown from the form of the roots). Hence (e) is a Galoisian equation.

102. LEMMA. *If L is a self-conjugate subgroup of K of prime index ν and if k is any substitution of K not contained in L, then k^ν, and no lower power of k, belongs to L, and the period of k is divisible by ν.*

By the Corollary of § 79, the quotient-group K/L is a cyclic group

$$\{I, \gamma, \gamma^2, \ldots, \gamma^{\nu-1}\}.$$

Hence to k corresponds a power of γ, say γ^κ, where κ is not divisible by ν. Then to k^ν corresponds $(\gamma^\kappa)^\nu=I$, so that k^ν belongs to L. If $0<m<\nu$, k^m does not belong to L, since $(\gamma^\kappa)^m=I$ requires that κm be divisible by the prime number ν.

Let the period μ of k be written in the form

$$\mu=q\nu+\tau \qquad (0\leqq\tau<\nu).$$

Since $k^\nu=h$, a substitution of L, we get $I=k^\mu=h^q k^\tau$. Hence $k^\tau=h^{-q}$, so that $\tau=0$, in view of the earlier result concerning powers of k. Hence μ is divisible by ν.

103. THEOREM (Galois). *Every irreducible equation of prime degree p which is solvable by radicals is a Galoisian equation.*

Let G be the group of the equation for a domain R and let

$$G, H, \ldots, J, K, L, \ldots, G_1 \tag{31}$$

be a series of composition of G. Since the equation is solvable by radicals, the factors of composition are all prime numbers (§ 92). Since the equation is irreducible in R, G is transitive (§ 68), so that its order is divisible by p (§ 67). Hence (foot-note to § 27), G contains a circular substitution of period p, say $t=(x_0\, x_1 \ldots x_{p-1})$. Let K denote the last group in the series (31) which contains t. Then the group L, immediately following K, and of prime index ν under K, does not contain t. Since $t^p=I$ belongs to L, while no lower power of t belongs to L, it follows from § 102 that $\nu=p$.

To show that L is the identity G_1, suppose that L contains a substitution s replacing x_α by a different letter x_β. Then $u \equiv st^{\alpha-\beta}$ leaves x_α unaltered and belongs to K. Since $\alpha-\beta$ is not divisible by p and since t does not belong to L, it follows that u does not belong to L. By the Lemma of § 102, the period of u is divisible by $\nu=p$. This is impossible since u is a substitution on p letters, one of which remains unaltered.

Since $L=G_1$ and the index of L under K is p, the group K is the cyclic group of order p formed by the powers of t. Since the group J immediately preceding K in the series (31) contains the cyclic group K as a self-conjugate subgroup, J is contained in the metacyclic group of degree p (§ 98). By the remark at the end of § 98, J contains no circular substitutions of period p other than the powers of t. If J' be the group immediately preceding J in the series (31), so that J is self-conjugate under J', the transform of t by any substitution of J' belongs to J and is a circular substitution of period p, and therefore is a power of t. Hence the cyclic group K is self-conjugate under J', as well as under J. Hence J' is contained in the metacyclic group (§ 98). Proceeding in this way until we reach the group G, we find that G is contained in the metacyclic group. The theorem therefore follows from § 101.

CHAPTER XI.

AN ACCOUNT OF MORE TECHNICAL RESULTS.

104. Second definition of the group Γ of § 77. To show that Γ is completely defined by the given groups G and H and is entirely independent of the function ψ used in defining it, we define a group Γ_1 independently of functions belonging to H and prove that $\Gamma_1 = \Gamma$.

Consider a rectangular array of the substitutions of G with those of the subgroup H in the first row:

$$(32) \qquad \begin{array}{c|cccc} r_1 & g_1 = I & h_2 & \dots & h_t \\ r_2 & g_2 & h_2 g_2 & \dots & h_t g_2 \\ \dots & \dots & \dots & \dots & \dots \\ r_\nu & g_\nu & h_2 g_\nu & \dots & h_t g_\nu \end{array}$$

where r_j denotes the jth row of the array. Let g be any substitution of G. Since $g_1 g, \dots, g_\nu g$ lie in the array (32), we may write

$$(33) \qquad g_1 g = h_{\alpha'} g_\alpha, \quad g_2 g = h_{\beta'} g_\beta, \quad \dots, \quad g_\nu g = h_{\kappa'} g_\kappa.$$

Hence the products of the substitutions in the array (32) by g on the right-hand may be written (retaining the same order):

$$(34) \qquad \begin{array}{c|cccc} r_\alpha & h_{\alpha'} g_\alpha & (h_2 h_{\alpha'}) g_\alpha & \dots & (h_t h_{\alpha'}) g_\alpha \\ r_\beta & h_{\beta'} g_\beta & (h_2 h_{\beta'}) g_\beta & \dots & (h_t h_{\beta'}) g_\beta \\ \dots & \dots & \dots & \dots & \dots \\ r_\kappa & h_{\kappa'} g_\kappa & (h_2 h_{\kappa'}) g_\kappa & \dots & (h_t h_{\kappa'}) g_\kappa \end{array}$$

Now $h_{\alpha'}, h_2 h_{\alpha'}, \dots, h_t h_{\alpha'}$ form a permutation of $h_1 = I, h_2, \dots, h_t$. Hence the substitutions in the first row of (34) are identical, apart from their order, with those of the αth row of (32). Similarly

for the other rows. Hence the multiplication of (32) on the right by g gives rise to the following permutation of the *rows*:

$$\gamma = \begin{pmatrix} r_1 & r_2 & \dots & r_\nu \\ r_\alpha & r_\beta & \dots & r_\kappa \end{pmatrix}.$$

To identify the group Γ_1 of these substitutions γ with the group Γ given by the earlier definition, we note that to g corresponds, under the earlier definition,

$$\begin{pmatrix} \psi_{g_1} & \psi_{g_2} & \dots & \psi_{g_\nu} \\ \psi_{g_1 g} & \psi_{g_2 g} & \dots & \psi_{g_\nu g} \end{pmatrix} = \begin{pmatrix} \psi_{g_1} & \psi_{g_2} & \dots & \psi_{g_\nu} \\ \psi_{g_\alpha} & \psi_{g_\beta} & \dots & \psi_{g_\kappa} \end{pmatrix},$$

since, by (33), $\psi_{g_1 g} = \psi_{h_{\alpha'} g_\alpha} = \psi_{g_\alpha}$, etc. But this substitution differs from γ only in notation. Hence $\Gamma_1 = \Gamma$.

EXAMPLE 1. Let G be the cyclic group $\{I, c, c^2, c^3, c^4, c^5\}$, where $c^6 = I$, and let H be the subgroup $\{I, c^3\}$. The array is

$$\begin{array}{c|cc} r_1 & I & c^3 \\ r_2 & c & c^4 \\ r_3 & c^2 & c^5 \end{array}$$

To c corresponds $(r_1 r_2 r_3)$. Hence $\Gamma = \{I, (r_1 r_2 r_3), (r_1 r_3 r_2)\}$.

EXAMPLE 2. Let G be the alternating group $G_{12}^{(4)}$ and let H be the commutative subgroup G_4 (§ 21, Ex. *f*). The rectangular array for G is given in § 77, Ex. 2. Multiplying its substitutions on the right by $(x_1x_2)(x_3x_4)$, we obtain the array

$(x_1x_2)(x_3x_4)$,	I,	$(x_1x_4)(x_2x_3)$,	$(x_1x_3)(x_2x_4)$
$(x_1x_2x_4)$,	$(x_1x_4x_3)$,	$(x_1x_3x_2)$,	$(x_2x_3x_4)$
$(x_1x_2x_3)$,	$(x_1x_3x_4)$,	$(x_2x_4x_3)$,	$(x_1x_4x_2)$

Hence each row as a whole remains unaltered, so that to $(x_1x_2)(x_3x_4)$ corresponds the identity. A like result follows for $(x_1x_3)(x_2x_4)$ and for the product $(x_1x_4)(x_2x_3)$ of the two. But $(x_2x_3x_4)$ applied as a right-hand multiplier gives rise to the permutation $(r_1r_2r_3)$ of the rows, as follows immediately from the formation of the rectangular array by means of the right-hand multipliers $(x_2x_3x_4)$ and $(x_2x_3x_4)^2$. Hence $\Gamma = \{I, (r_1r_2r_3), (r_1r_3r_2)\}$.

105. Constancy of the factors of composition. By the criterion of § 92, an equation is solvable by radicals if, and only if, the group G of the equation has a series of composition in which the factors of composition are all prime numbers. In applying the

criterion, it might be necessary to investigate all the series of compositions of G to decide whether or not there is one series with the factors of composition all prime. The practical value of the criterion is greatly enhanced by the theorem of C. Jordan:*

If a group has two different series of composition, the factors of composition for one series are the same, apart from their order, as the factors of composition for the other series.

EXAMPLE 1. Let G_8, G_4, H_4 be defined as in § 21; G_2, G_2', G_2'' as in Example 3 of § 65; and let

$C_4 = \{I, (x_1x_3x_2x_4), (x_1x_2)(x_3x_4), (x_1x_4x_2x_3)\}$, $H_2 = \{I, (x_1x_2)\}$, $H_2' = \{I, (x_3x_4)\}$. Then G_8 has the following series of compositions:

$$G_8, G_4, G_2, G_1; \quad G_8, G_4, G_2', G_1; \quad G_8, G_4, G_2'', G_1;$$
$$G_8, C_4, G_2, G_1; \quad G_8, H_4, G_2, G_1; \quad G_8, H_4, H_2, G_1; \quad G_8, H_4, H_2', G_1.$$

In each case the factors of composition are 2, 2, 2.

EXAMPLE 2. Let C_{12} be the cyclic group formed by the powers of the circular substitution $a = (x_1x_2x_3 \ldots x_{12})$. Its subgroups are

$$C_6 = \{I, a^2, a^4, a^6, a^8, a^{10}\}, \qquad C_4 = \{I, a^3, a^6, a^9\},$$
$$C_3 = \{I, a^4, a^8\}, \qquad C_2 = \{I, a^6\}, \quad C_1 = \{I\}.$$

The only series of composition of C_{12} are the following:†

$$C_{12}, C_6, C_3, C_1; \quad C_{12}, C_6, C_2, C_1; \quad C_{12}, C_4, C_2, C_1.$$

The factors of composition are respectively 2, 2, 3; 2, 3, 2; 3, 2, 2.

106. Constancy of the factor-groups. In a series of composition of G,

$$G, G', G'', \ldots, G_1,$$

each group is a maximal self-conjugate subgroup of the preceding group (§ 43). The succession of quotient-groups

$$G/G', G'/G'', G''/G''', \ldots$$

forms a series of **factor-groups** of G. Each factor-group is simple (§ 80). The theorem of Jordan on the constancy of the numerical

* *Traité des substitutions*, pp. 42–48. For a shorter proof, see Netto-Cole, *Theory of Substitutions*, pp. 97–100.

† Every subgroup is self-conjugate since $a^{-i}a^ja^i = a^j$ (§ 13).

factors of composition is included in the following theorem of Hölder:*

For two series of composition of a group, the factor-groups of one series are identical, apart from their order, with the factor-groups of the other series.

Thus, in Example 1 of § 105, the factor-groups are all cyclic groups of order 2. In Example 2, the factor-groups for the respective series are

$$K_2, K_2, K_3; \quad K_2, K_3, K_2; \quad K_3, K_2, K_2,$$

where K_2 and K_3 are cyclic groups of orders 2 and 3 respectively. That C_6/C_2 is the cyclic group K_3 follows from § 104, Ex. 1, by setting $a^2=c$. That C_{12}/C_4 is K_3 follows readily from § 104.

107. Hölder's investigation† on the reduction of an arbitrary equation to a chain of auxiliary equations is one of the most important of the recent contributions to Galois' theory. The earlier restriction to *algebraically* solvable equations is now removed. As shown in § 82, the solution of a given equation can be reduced to the solution of a chain of simple regular equations by employing rational functions of the roots of the given equation. The groups of the auxiliary equations are the simple factor-groups G of the given equation. Can any one of these simple groups be avoided by employing *accessory irrationalities*, namely, quantities not rational functions of the roots of the given equation? That this question is to be answered in the negative is shown by Hölder's result that the factor-groups of G must occur among the groups of the auxiliary simple equations however the latter be chosen. Any auxiliary compound may first be replaced by a chain of equivalent simple equations. The number of factor-groups of G therefore gives the minimum number of necessary auxiliary simple equations. If this minimum number is not exceeded, then Hölder's theorem states that all the roots of all the auxiliary equations are

* Hölder, *Math. Ann.*, vol. 34, p. 37; Burnside, *The Theory of Groups*, p. 118; Pierpont, *Galois' Theory of Algebraic Equations*, *Annals of Math.*, 1900, p. 51.

† *Mathematische Annalen*, vol. 34, p. 26; Pierpont, *l. c.*, p. 52.

rational functions of the roots of the given equation and the quantities in the given domain of rationality.

Hölder's proof of these results, depending of course upon the constancy of the factor-groups of G, is based upon the fundamental theorem of § 93.

The special importance thus attached to simple groups has led to numerous investigations of them. Several infinite systems of simple groups have been found and a table of the known simple groups of composite orders less than one million has been prepared.*

For full references and for further developments of Galois' theory, the reader may consult *Encyklopädie der Mathematischen Wissenschaften*, I, pp. 480–520.

* Dickson, *Linear Groups*, pp. 307–310, Leipzig, 1901.

APPENDIX.

RELATIONS BETWEEN THE ROOTS AND COEFFICIENTS OF AN EQUATION.

Let $x_1, x_2, \ldots, x_n$ denote the roots of an equation $f(x)=0$ in which the coefficient of x^n has been made unity by division. Then

$$f(x) \equiv (x-x_1)(x-x_2)\ldots(x-x_n),$$

as shown in elementary algebra by means of the factor theorem. Writing $f(x)$ in full, and expanding the second member, we get

$$\begin{aligned} x^n - c_1x^{n-1} + c_2x^{n-2} - \ldots + (-1)^n c_n \equiv x^n - (x_1+x_2+\ldots+x_n)x^{n-1} \\ + (x_1x_2+x_1x_3+x_2x_3+\ldots+x_{n-1}x_n)x^{n-2} \\ - \ldots + (-1)^n x_1x_2\ldots x_n. \end{aligned}$$

Equating coefficients of like powers of x, we get

$$(i) \quad x_1+x_2+\ldots+x_n=c_1,\ x_1x_2+\ldots+x_{n-1}x_n=c_2,\ \ldots,\ x_1\ldots x_n=c_n.$$

These combinations of $x_1, \ldots, x_n$ are called the **elementary symmetric functions** of the roots. Compare Exs. 5 and 6 of page 4.

FUNDAMENTAL THEOREM ON SYMMETRIC FUNCTIONS.*

Any integral symmetric function of $x_1, x_2, \ldots, x_n$ can be expressed in one and only one way as an integral function of the elementary symmetric functions $c_1, c_2, \ldots, c_n$.

A term $x_1^{m_1}x_2^{m_2}x_3^{m_3}\ldots$ is called **higher** than $x_1^{n_1}x_2^{n_2}x_3^{n_3}\ldots$ if the first one of the differences $m_1-n_1, m_2-n_2, m_3-n_3, \ldots$, which

* The proof is that by Gauss, *Gesammelte Werke*, III, pp. 37, 38.

does not vanish, is *positive*. Then $c_1, c_2, c_3, \ldots, c_i$ have for their highest terms $x_1, x_1x_2, x_1x_2x_3, \ldots, x_1x_2 \ldots x_i$, respectively. In general, the function $c_1^{\alpha}c_2^{\beta}c_3^{\gamma} \ldots$ has for its highest term

$$x_1^{\alpha+\beta+\gamma+\cdots} x_2^{\beta+\gamma+\cdots} x_3^{\gamma+\cdots} \ldots$$

Hence it has the same highest term as $c_1^{\alpha'}c_2^{\beta'}c_3^{\gamma'} \ldots$ if, and only if,

$$\alpha+\beta+\gamma+ \ldots = \alpha'+\beta'+\gamma'+ \ldots, \quad \beta+\gamma+ \ldots = \beta'+\gamma'+ \ldots,$$
$$\gamma+ \ldots = \gamma'+ \ldots,$$

which require that $\alpha=\alpha'$, $\beta=\beta'$, $\gamma=\gamma', \ldots$

Let S be a given symmetric function. Let its highest term be

$$h \equiv a\, x_1^{\alpha} x_2^{\beta} x_3^{\gamma} x_4^{\delta} \ldots x_n^{\nu} \quad \ldots (\alpha \geqq \beta \geqq \gamma \geqq \delta \ldots \geqq \nu).$$

We build the symmetric function

$$\sigma \equiv a\, c_1^{\alpha-\beta} c_2^{\beta-\gamma} c_3^{\gamma-\delta} \ldots c_n^{\nu}.$$

In its expansion in terms of $x_1, \ldots, x_n$ by means of formulæ (*i*), its terms are all of the same degree and the highest term is evidently h. The difference

$$S_1 \equiv S - \sigma$$

is a symmetric function simpler than S, since the highest term h has been cancelled. Let the highest term of S_1 be

$$h_1 \equiv a_1\, x_1^{\alpha_1} x_2^{\beta_1} x_3^{\gamma_1} x_4^{\delta_1} \ldots$$

A symmetric function with a still lower highest term is given by

$$S_2 \equiv S_1 - a_1\, c_1^{\alpha_1-\beta_1} c_2^{\beta_1-\gamma_1} c_3^{\gamma_1-\delta_1} \ldots$$

Since the degrees of S_1 and S_2 are not greater than the degree of S, and since there is only a finite number of terms $x_1^{m_1}x_2^{m_2}x_3^{m_3} \ldots$ of a given degree which are lower than the term h, we must ultimately obtain, by a repetition of the process, the symmetric function 0;

$$0 \equiv S_k - a_k\, c_1^{\alpha_k-\beta_k} c_2^{\beta_k-\gamma_k} c_3^{\gamma_k-\delta_k} \ldots$$

We therefore reach the desired result

$$S = a_1\, c_1^{\alpha-\beta} c_2^{\beta-\gamma} \ldots + a_2\, c_1^{\alpha_1-\beta_1} c_2^{\beta_1-\gamma_1} \ldots + \ldots + a_k c_1^{\alpha_k-\beta_k} c_2^{\beta_k-\gamma_k} \ldots$$

To show that the expression of a symmetric function S in terms of $c_1, \ldots, c_n$ is unique, suppose that S can be reduced to both $\phi(c_1, c_2, \ldots, c_n)$ and $\psi(c_1, c_2, \ldots, c_n)$, where ϕ and ψ are different integral functions of $c_1, \ldots, c_n$. Then $\phi - \psi$, considered as a function of $c_1, \ldots, c_n$, is not identically zero. After collecting like terms in $\phi - \psi$, let $bc_1^{\alpha}c_2^{\beta}c_3^{\gamma}\ldots$ be a term with $b \neq 0$. When expressed in $x_1, \ldots, x_n$, it has for its highest term

$$b\, x_1^{\alpha+\beta+\gamma+\cdots} x_2^{\beta+\gamma+\cdots} x_3^{\gamma+\cdots} \ldots$$

As shown above, a different term $b'c_1^{\alpha'}c_2^{\beta'}c_3^{\gamma'}\ldots$ has a different highest term. Hence of these highest terms one must be higher than the others. Since the coefficient of this term is not zero, the function $\phi - \psi$ cannot be identically zero in $x_1, \ldots, x_n$. This contradicts the assumption that $S \equiv \phi$, $S \equiv \psi$, for all values of $x_1, \ldots, x_n$.

COROLLARY. *Any integral symmetric function of $x_1, \ldots, x_n$ with integral coefficients can be expressed as an integral function of $c_1, \ldots, c_n$ with integral coefficients.*

Examples showing the practical value of the process for the computation of symmetric functions are given in Serret, *Algèbre supérieure*, fourth or fifth edition, vol. 1, pp. 389–395.

ON THE GENERAL EQUATION.

Let the coefficients $c_1, c_2, \ldots, c_n$ be indeterminate quantities. The roots $x_1, x_2, \ldots, x_n$ are functions of $c_1, \ldots, c_n$; the notation $x_1, \ldots, x_n$ is definite for each set of values of $c_1, \ldots, c_n$. We proceed to prove the theorem:*

If a rational, integral function of $x_1, \ldots, x_n$ with constant coefficients equals zero, it is identically zero.

Let $\psi[x_1, \ldots, x_n] = 0$. Let $\xi_1, \ldots, \xi_n$ denote indeterminates and $\sigma_1, \ldots, \sigma_n$ their elementary symmetric functions $\xi_1 + \ldots + \xi_n$, $\ldots$, $\xi_1 \cdot \xi_2 \ldots \xi_n$. Then

* This proof by Moore is more explicit than that by Weber, *Algebra*, II (1900), § 566.

$$\Pi\psi[\xi_{s_1}, \ldots, \xi_{s_n}] = \Psi[\sigma_1, \ldots, \sigma_n],$$

the product extending over the $n!$ permutations $s_1, \ldots, s_n$ of $1, \ldots, n$, and Ψ denoting a rational, integral function. Hence

$$\Pi\psi[x_{s_1}, \ldots, x_{s_n}] = \Psi[c_1, \ldots, c_n] = 0,$$

since one factor $\psi[x_1, \ldots, x_n]$ is zero. Since $c_1, \ldots, c_n$ are indeterminates, $\Psi[c_1, \ldots, c_n]$ must be identically zero, i.e., formally in $c_1, \ldots, c_n$. Consider $c_1, \ldots, c_n$ to be functions of new indeterminates $y_1, \ldots, y_n$. Then

$$\Psi[c_1(y_1, \ldots, y_n), \ldots, c_n(y_1, \ldots, y_n)] \equiv 0$$

formally in $y_1, \ldots, y_n$. Hence, by a change of notation,

$$\Psi[\sigma_1(\xi_1, \ldots, \xi_n), \ldots, \sigma_n(\xi_1, \ldots, \xi_n)] \equiv 0$$

formally in $\xi_1, \ldots, \xi_n$. Hence, for some factor,

$$\psi[\xi_{s_1}, \ldots, \xi_{s_n}] \equiv 0$$

formally in $\xi_1, \ldots, \xi_n$. As a mere change of notation,

$$\psi[\xi_1, \ldots, \xi_n] \equiv 0.$$

As an application, we may make a determination of the group of the general equation more in the spirit of the theory of Galois than that of § 64. If, in the domain $R = (c_1, \ldots, c_n)$, a rational function $\phi(x_1, \ldots, x_n)$ with coefficients in R has a value lying in R, there results a relation

$$\psi[x_1, \ldots, x_n] = 0,$$

upon replacing $c_1, \ldots, c_n$ by the elementary symmetric functions of $x_1, \ldots, x_n$. By the theorem above, $\psi[x_{s_1}, \ldots, x_{s_n}] = 0$, so that

$$\phi(x_{s_1}, \ldots, x_{s_n}) = \phi(x_1, \ldots, x_n).$$

8 III 28

INDEX.

(The numbers refer to pages.)