THEORY OF ALGEBRAIC EQUATIONS.

INTRODUCTION TO THE

THEORY OF ALGEBRAIC EQUATIONS.

BY

LEONARD EUGENE DICKSON, Ph.D.,

ASSISTANT PROFESSOR OF MATHEMATICS IN
THE UNIVERSITY OF CHICAGO.

PREFACE.

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

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

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

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

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

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

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

CHICAGO, *August*, 1902

TABLE OF CONTENTS.

APPENDIX.

THEORY OF ALGEBRAIC EQUATIONS.

FIRST PART.

THE LAGRANGE-ABEL-CAUCHY THECRY 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

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

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

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

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

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

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

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

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

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

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

The other two cube roots are then

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

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

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

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

Then

(6) $$\omega^2+\omega+1=0\quad \omega^3=1.$$

In view of the relation

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

a particular cube root $\sqrt[3]{-\frac{1}{2}q-\sqrt{R}}$ 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 tne 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

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

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

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

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

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 $\sqrt[3]{-\frac{1}{2}q+\sqrt{R}}+\sqrt[3]{-\frac{1}{2}q-\sqrt{R}}$, where all combinations of the cube roots are taken, are the roots of the cubics

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

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

6 Show that $x_1+x_2+x_3=c_1$, $x_1x_2+x_1x_3+x_2x_3=c_2$, $x_1x_2x_3=c_3$, using Ex. 5. How may these results be derived directly from equation (1)?

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

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

These functions differ only in the permutations of x_1, x_2, x_3. As there are just six permutations of three letters, these functions give all that can be obtained from ψ_1 by permuting x_1, x_2, x_3. For this reason, ψ_1 is called a *six-valued* function.

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

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

Hence the *resolvent* sextic becomes

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

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

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

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 fiunctions 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

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

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

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

$$(19)\qquad x_1+x_2-x_3-x_4=t,\quad x_1x_2+x_3x_4=y_1.$$

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

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

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

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

5. Without having recourse to Ferrari's device, the two quadratic equations whose roots are tho four roots of the general quartio 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) aro the roots of $(-y_1)(y-y_2)(y-y_3)=0$, or

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

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

$$y_1+y_2+y_3=x_1x_2+x_3x_4+x_1x_3+x_2x_4+x_1x_4+x_2x_3=b,$$

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

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

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

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

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

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 ana x_3+x_4 are found from the relations

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

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

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

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

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

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

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

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

in view of (20). Hence

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

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

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

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

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

CHAPTER II.

SUBSTITUTIONS; RATIONAL FUNCTIONS.

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

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

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

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

The substitution which leaves every letter unaltered,

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Applying the substitution a to the function ψ, we get ψ_a; applying the substitution c to ψ_a, we get ψ_d. Hence $\psi_{ac} = \psi_d$. Likewise $\psi_{ab} = \psi_I = \psi$, $\psi_{ba} = \psi$.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

EXAMPLES. From the example in § 10, we get

$a^2 = b,\quad a^3 = a^2 a = ba = I,$ whence a is of period 3;
$b^2 = a,\quad b^3 = b^2 b = ab = I,$ 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),

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

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