ON THE RUFFINI–ABELIAN THEOREM.

BY PROFESSOR J. PIERPONT.

Gauss having rigorously established in 1799 the fundamental theorem of algebra that every equation of degree n possesses n roots real or imaginary,* it was natural to inquire more closely into the nature of these quantities. When n was less than five, it had long been known that these roots could in every case be expressed as explicit algebraic functions of the coefficients; further it was known that for every degree equations existed of more or less special nature for which this was still true. The unsuccessful attempts of the foremost mathematicians of the century which was just closing to find such expressions for the equation of degree five, when the coefficients were left indeterminate, had rendered it very doubtful if the roots of the general equation of degree greater than four possessed this property. Between the years 1799 and 1813 an Italian mathematician, Ruffini,† made several attempts to establish the justice of these doubts; but his reasoning although highly interesting and valuable is not conclusive, and the question remained open until the publication of Abel's ‡ celebrated argument in 1826, where he proved that it was impossible to express the roots of an equation of degree greater than four, as explicit algebraic functions of the coefficients when these last were left indeterminate.

Abel's demonstration, however, is not all that could be desired. In the first place, as he was ignorant of Ruffini's beautiful researches, the substitution-theoretical part of his paper is unnecessarily roundabout; secondly, in the algebraical part Abel unnecessarily complicates his proof with a classification of functions according to order and degree. Here he commits an error which caused as acute a mind as Hamilton to declare that "it renders it difficult to judge of the validity of his subsequent reasoning." In this, however, Hamilton was misled, the classification in question being entirely superfluous here, however important in other

* GAUSS, Werke, vol. III. Compare also the interesting paper by Bôcher, BULLETIN, May, 1895.

† Cf. BURKHARDT. Supplement of the *Zeitschrift für Mathematik u. Physik*, vol. 37.

‡ *Oeuvres Complètes*, 2d edition, vol. I., p. 66. It is interesting to compare this with Abel's first attempt which forms the third paper of the new edition.

algebraical investigations. In any case it was highly desirable that a theorem of such far-reaching importance and which stands as it were at the very gateway of any algebraical theory of the roots of higher equations, should be demonstrated in a simple, direct and rigorous manner. Such a demonstration was published by Kronecker in the Monatsberichte* of the Berlin Academy for 1879. This paper has not received the attention of writers of treatises on algebra which it deserves; such standard modern treatises† as Serret, Petersen, Carnoy, all contain demonstrations of the theorem which are imperfect. Serret's demonstration is in its algebraical part almost a word for word reproduction of Abel's memoir and thus contains the unfortunate error noted by Hamilton; the demonstration given by Petersen and Carnoy is vitiated by the same tacit postulate made by Ruffini in the Modena treatise of 1813.

Since the publication of Kronecker's paper in 1879, no other proof has appeared, and yet it seems to me that Kronecker in following Abel too closely in the substitution-theoretical part of his demonstration has not given the simplest proof possible; on the other hand, in the algebraical part, in condensing to the utmost the demonstration, he presupposes that his readers are familiar with the form of proof given by Abel. I propose then in the following lines to give a demonstration of the Ruffini-Abelian Theorem which shall be as direct and *self-contained* as possible; in doing this I hope to render a service to a large class of readers whose studies have led them away from algebraical theories, but who would be glad to see this celebrated theorem demonstrated without implying more or less familiarity with the higher parts of algebra. To aid in this I give at the end of this paper § 8 an illustrative example worked out in detail. In addition to this demonstration I give two others: one, a modification of Ruffini's form; the second, Kronecker's modification of Abel's form. As will be observed, the three forms of demonstration have their algebraical part, essentially due to Abel, in common, while the substitution-theoretical part increases in complexity.

§ 1

We begin by giving a few definitions and establishing one or two elementary theorems.

* p. 205 *Vereinfachung des Abel'schen Beweises*, etc.

† SERRET: *Algèbre supérieure* 5th ed. PETERSEN: *Theorie der algebraischen Gleichungen.* CARNOY: *Cours d'Algèbre supérieure.*

We say $f(\lambda, \mu, \nu\cdots)$ is an integral function of the quantities $\lambda, \mu, \nu, \cdots$ when its calculation requires only the operations of addition, subtraction and multiplication in regard to these quantities; every such function is of the type $\Sigma C\lambda^a \mu^b \nu^c \cdots$ where the coefficients C do not involve $\lambda, \mu, \nu\cdots$ and the exponents $a, b, c\cdots$ are positive integers. The function $f(\lambda, \mu, \nu \cdots)$ is said to be a rational function of $\lambda, \mu, \nu\cdots$ when its calculation requires only the operations of addition, subtraction, multiplication and division in regard to them; every such function is the quotient of two integral functions of $\lambda, \mu, \nu\cdots$ and is thus of the type

$$f(\lambda, \mu, \nu\cdots) = \frac{f_1(\lambda, \mu, \nu\cdots)}{f_2(\lambda, \mu, \nu\cdots)}$$

f_1, f_2, being integral. A function $f(a, b, c, \cdots; \lambda, \mu, \nu\cdots)$ may be an integral function in regard to certain quantities $\lambda, \mu, \nu\cdots$ and rational in regard to certain others, $a, b, c\cdots$; if f involves only the quantities $a, b, c\cdots \lambda, \mu, \nu\cdots$ and certain rational numbers, we say $f(a, b, c\cdots\lambda, \mu, \nu\cdots)$ is an integral function of $\lambda, \mu, \nu \cdots$ whose coefficients are rational functions of $a, b, c\cdots$ with rational-number coefficients, or more shortly f is an integral function of $\lambda, \mu, \nu\cdots$ with coefficients rational in $a, b, c\cdots$.

Let $\varphi(\xi, a, b, c\cdots)$ be an integral function of ξ whose coefficients are rational in $a, b, c\cdots$; if $\xi_1, \xi_2, \xi_3\cdots$ be the values of ξ for which $\varphi = 0$,

$$\varphi(\xi) = A(\xi-\xi_1)(\xi-\xi_2)(\xi-\xi_3)\cdots\cdots;$$

similarly if $\eta_1\ \eta_2\ \eta_3\cdots\cdots$ be the zeros of $\psi(\eta, a', b', c'\cdots)$

$$\psi(\eta) = B(\eta-\eta_1)(\eta-\eta_2)(\eta-\eta_3)\cdots\cdots$$

If some of the η's are equal to some of the ξ's as

$$\eta_1 = \xi_1,\ \eta_2 = \xi_2, \cdots\cdots \eta_\mu = \xi_\mu$$

then φ and ψ have a common divisor

$$\delta = (\xi-\xi_1)\cdots(\xi-\xi_\mu)$$

As δ can be obtained by the process of finding the greatest common divisor, and as this process never requires other than rational operations on the coefficients of φ, ψ which are rational in the quantities $a, b, c\cdots a', b', c'$, it follows that δ is an integral function of ξ with coefficients rational in $a, b, c\cdots a', b', c'\cdots$. The function $f(\xi, a, b, c\cdots)$ is said to be irreducible in regard to certain quantities $\lambda, \mu, \nu\cdots$ when it is not the product of factors whose coefficients are rational in $\lambda, \mu, \nu, \cdots$; in the same way the equation $f(\xi) = 0$ is said to

be irreducible under the same circumstances. From this definition it follows that if $f(\xi, a, b, c\cdots)$ be irreducible in regard to $a, b, c\cdots$and certain quantities $\lambda, \mu, \nu\cdots$and have a divisor δ in common with $\varphi(\xi, a, b, c\cdots\lambda, \mu, \nu\cdots)$ then φ is divisible by f. For δ as we saw is of the form $\delta(\xi, a, b, c\cdots\lambda, \mu, \nu\cdots)$; which being a factor common to f and φ, requires that f possess a factor whose coefficients are rational in $a, b, c\cdots\lambda, \mu, \nu\cdots$which is impossible unless $f=\delta$, that is unless φ is divisible by f. Hence:

THEOREM I: If

$$f(\xi, a, b, c\cdots)=\xi^m + A_1\xi^{m-1} + \cdots + A_m=0$$

be irreducible in regard to $a, b, c\cdots\lambda, \mu, \nu\cdots$, and if at the same time ξ satisfy the equation of *less* degree

$$\xi^\mu + B_1\xi^{\mu-1} + \cdots + B_\mu=0 \qquad \mu<m$$

where the B are rational in $a, b, c\cdots\lambda, \mu, \nu\cdots$then

$$B_1=0 \quad B_2=0\cdots\cdots B_\mu=0$$

We turn now to the substitution theory.
The number of permutations of n things

$$1, 2, 3\cdots\cdots n$$

is $n!$; let

$$l_1 \; l_2 \; l_3\cdots\cdots l_n$$

denote one of these permutations; the operation which replaces 1 by l_1, 2 by $l_2\cdots n$ by l_n is called a substitution and is denoted by the symbol

$$s=\begin{pmatrix} 1 & 2 & 3\cdots n \\ l_1 & l_2 & l_3\cdots l_n \end{pmatrix}$$

where the order of the top row is indifferent if only the l_1 is under 1, l_2 under 2 etc., in each case. As to each of the $n!$ permutations corresponds a substitution, there are $n!$ substitutions affecting the n things $1, 2\cdots n$. I shall speak of them as the substitutions of the symmetric group G or as the substitutions of G. One of these substitutions is

$$\begin{pmatrix} 1 & 2 & 3\cdots n \\ 1 & 2 & 3\cdots n \end{pmatrix}$$

which leaving each element unchanged is called the identical substitution and denoted briefly by 1. Let $s, t, u,\cdots$

be certain substitutions, the operation arising from operating first with s, then with t is denoted by $s.t$ and is called the product of s, t; similarly $s\,t\,u$ is the resulting operation arising from operating first with s, then with t finally with u.

A substitution which replaces each element of the top row by the following, finally the last by the first is called a cycle or a circular substitution; thus

$$\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix},\quad \begin{pmatrix}4&2&1&5&3\\2&1&5&3&4\end{pmatrix}$$

are such. Every substitution is the product of cycles, thus

$$\begin{pmatrix}1&2&3&4&5&6&7\\3&1&7&5&6&4&2\end{pmatrix}=\begin{pmatrix}1&3&7&2\\3&7&2&1\end{pmatrix}\begin{pmatrix}4&5&6\\5&6&4\end{pmatrix}$$

$$\begin{pmatrix}1&2&3&4&5&6&7&8&9&10&11\\10&8&3&6&7&5&4&9&2&1&11\end{pmatrix}=\begin{pmatrix}1&10\\10&1\end{pmatrix}\begin{pmatrix}2&8&9\\8&9&2\end{pmatrix}\begin{pmatrix}3\\3\end{pmatrix}\begin{pmatrix}4&6&5&7\\6&5&7&4\end{pmatrix}\begin{pmatrix}11\\11\end{pmatrix}$$

A circular substitution of two elements as (12) is a transposition. To every substitution s corresponds *one* substitution t such that $s\,t=1$; thus if

$$s=\begin{pmatrix}1&2&3&4\\4&3&1&2\end{pmatrix}$$

the substitution t is

$$t=\begin{pmatrix}4&3&1&2\\1&2&3&4\end{pmatrix}$$

for s converts

$$1\ 2\ 3\ 4$$

into $\quad 4\ 3\ 1\ 2$

respectively but each element of this last row is converted by t into

$$1\ 2\ 3\ 4$$

respectively, so the joint effect of s and t, or $s.t$ is to leave each element unchanged $\therefore\ s\,t=1$. The substitution t is called the inverse of s and denoted by s^{-1}, so that $s\,s^{-1}=1$. For brevity also we put $s.s=s^2$, $s.s.s=s^3$, etc.

Let $x_1\ x_2\cdots x_n$ be the roots of $x^n+a_1\,x^{n-1}+\cdots+a_n=0$, and let $\varphi\,(x_1, x_2\cdots x_n;\ \lambda, \mu,\cdots)$ be a rational function of $x_1\,x_2\cdots x_n$ and certain quantities $\lambda, \mu,\cdots$; if φ remain invariant *in form*, however we permute the indices 1, 2, $3\cdots n$, or what is the same thing, for all the substitutions of the symmetric group G, φ is said to be a rational symmetric function of $x_1\,x_2\cdots x_n$.

An elementary theorem of algebra is the following:

THEOREM II. Every rational symmetric function $\varphi(x_1\ x_2,\cdots x_n\ ;\ \lambda,\ \mu,\ \nu)$ of the roots $x_1\ x_2\cdots x_n$ of the equation $x^n + a_1 x^{n-1} +\cdots+ a_n = 0$, is a rational function of the coefficients $a_1,\ a_2\cdots a_n$ and the quantities $\lambda,\ \mu,\ \nu\cdots$.

The function $f(\lambda, \mu, \nu\cdots.)$ is said to be an explicit algebraical function of $\lambda, \mu, \nu\cdots$ when its calculation requires in addition to the rational operations only the extraction of roots in regard to the quantities $\lambda, \mu, \nu\cdots$.

We shall call the equation

$$(a) \qquad f(x) = x^n + a_1 x^{n-1} +\cdots+ a_n = 0$$

general when its coefficients are independent variables, and it shall possess an algebraic solution when their exists an explicit algebraic function of the coefficients which satisfies it. We propose to prove that when n is greater than four, no such function exists by showing that the admission of its existence leads to a contradiction.

§ 2

In fact let us seek the most general form of an explicit algebraical function of the coefficients $a_1\ a_2\cdots a_n$. It may be obtained as Ruffini remarked as follows:

Taking a rational function of the a's as $f_1(a_1\ a_2\cdots a_n)$ we extract a p_1^{th} root; calling this radical R_1 we form a rational function of the a's and of R_1 as $f_2(a_1\cdots a_n, R_1)$ and extract a p_2^{th} root; calling this radical R_2 we form a rational function of the a's and of R_1 and R_2 as $f_3(a_1\ a_2\cdots a_n\ ;\ R_1\ R_2)$, and extract a p_3^{th} root which we call R_3; proceeding in this way every explicit algebraical function x_0 will be defined by the *suite* of equations:

$$(A) \qquad \begin{gathered} R_1^{p_1} = f_1(a_1\ a_2\cdots a_n),\ R_2^{p_2} = f_2(a_1\cdots a_n\ ;\ R_1),\cdots \\ R_\lambda^{p_\lambda} = f_\lambda(a_1 a_2\cdots a_n; R_1 R_2\cdots R_{\lambda-1}),\ x_0 = f(a_1 a_2\cdots a_n, R_1, R_2\cdots R_\lambda) \end{gathered}$$

the functions f being all rational in regard to the quantities within the parentheses.

We proceed now to show how the *suite* may be simplified without losing its generality. In the first place the exponents p_k may be taken to be primes, since the extraction of an mn^{th} root may be effected by the extraction of an m^{th}, and from that an n^{th} root. Another simplification arises by observing that no loss of generality is incurred by considering f_k to be an integral function of the radicals $R_1\ R_2\cdots R_{-1k}$ with coefficients rational in $a_1, a_2,\cdots a_n$.

For let for example $f(a_1 \cdots a_n, u)$ be a rational function of u with coefficients rational in $a_1 \cdots a_n$, and

$$u^p = g(a_1 \cdots a_n) \tag{1}$$

then f is of the form

$$f = \frac{b_0 + b_1 u + b_2 u^2 + \cdots + b_{p-1} u^{p-1}}{c_0 + c_1 u + c_2 u^2 + \cdots + c_{p-1} u^{p-1}} = \frac{\varphi(u)}{\psi(u)} \tag{2}$$

the coefficients b, c being rational in the a's. It is to be noticed that neither φ nor ψ contains powers of u higher than $p-1$, since all higher powers may be reduced by observing that

$$u^p = g \quad u^{p+1} = u^p . u = g . u, \quad u^{p+2} = u^p . u^2 = g\, u^2 \cdots$$

and g is rational in the a's.

The expression (2) may be made integral in regard to u as follows: let the p roots of (1) be

$$u, \quad u_1 = \omega u \quad u_2 = \omega^2 u \cdots u_{p-1} = \omega^{p-1} u$$

where $\omega\ \omega^2 \cdots$ are the roots of the equation

$$\frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1 = 0 \tag{3}$$

The product

$$P = \psi(u)\, \psi(u_1) \cdots \psi(u_{p-1})$$

is a symmetric function of the roots of (1) and is thus a rational function $P(a_1 \cdots a_n)$ of $a_1 \cdots a_n$; further the product

$$Q = \psi(u_1)\psi(u_2) \cdots \psi(u_{p-1})$$

considered as a function of ω is symmetric in the roots of (3) and is thus an integral function $Q(a_1, \cdots a_n; u)$ of u with coefficients rational in $a_1 \cdots a_n$. We have thus, multiplying numerator and denominator by Q,

$$f = \frac{\varphi Q}{\psi Q} = \frac{\varphi Q}{P};$$

and the right hand member is now an integral function of u with coefficients rational in $a_1 \cdots a_n$. Thus every rational function $f(a_1 \cdots a_n, u)$ can be expressed as an integral function of u, with coefficients rational in $a_1\, a_2 \cdots a_n$.

Precisely the same reasoning applies to a rational function $f(a_1\, a_2 \cdots a_n, u, v)$ where

$$v^q = h(a_1 \cdots a_n, u) \tag{4}$$

the function h being an integral function of u with coefficients rational in $a_1 a_2 \cdots a_n$. In fact arranging according to ascending power of v

$$f(u, v) = \frac{l_0 + l_1 v + l_2 v^2 \cdots + l_{q-1} v^{q-1}}{m_0 + m_1 v + m_2 v^2 + \cdots + m_{q-1} v^{q-1}} = \frac{\lambda(v)}{\mu(v)}$$

where the coefficients l, m, as rational functions of $a_1 \cdots a_n$, u may be taken as integral functions of u with coefficients rational in $a_1 \cdots a_n$. Making the denominator $\mu(v)$ symmetric in respect to the roots

$$v, v_1, v_2 \cdots\cdots v_{q-1}$$

of (4) by multiplying numerator and denominator by $\mu(v_1) \cdots \mu(v_{q-1})$ we see that

$$f(u, v) = \frac{\lambda(v)\,\mu(v_1) \cdots \mu(v_{q-1})}{\mu(v)\,\mu(v_1) \cdots \mu(v_{q-1})}$$

is an integral function of u, v, with coefficients rational in $a_1 \cdots a_n$. These considerations being applicable to rational functions of any number of radicals, we see that without loss of generality we may assume that the functions f in (A) are integral functions in regard to $R_1 R_2 \cdots$ with coefficients rational in respect to $a_1 a_2 \cdots a_n$.

Finally we observe that we can assume that the equations

$$R_k^{p_k} = f_k \qquad k = 1, 2 \cdots \lambda \tag{5}$$

are irreducible in respect to

$$a_1 \cdots a_n;\ R_1, R_2 \cdots R_{k-1} \tag{6}$$

For if (5) be reducible let

$$(X - R_k)(X - R_k') \cdots (X - R_k^{(\mu-1)}) \tag{7}$$

be a factor rational in respect to the quantities (6), $R_k, R_k' \cdots R_k^{(\mu-1)}$ being roots of (5); then the absolute term of (7) or

$$R_k R_k' \cdots R_k^{(\mu-1)} = \omega R_k^{\mu}, \qquad \omega^{p_k} = 1$$

is rational in (6), or if λ satisfy $\lambda \mu \equiv 1 \mod p_k$, $\omega^{\lambda} R_k$ is rational in (6); that is R_k is rational in ω and the quantities (6). But as the determination of ω, as is well known, depends upon the solution of a *suite* of binomial equations whose degrees are the prime factors of $p_k - 1$, the assumption that the equations of the *suite* (A) are irreducible in the above sense, involves no loss of generality.

Thus to sum up: every explicit algebraical function of $a_1\ a_2 \cdots\ a_n$ is represented by the *suite* (A) where f_k is an integral function of the radicals $R_1, R_2 \cdots R_{k-1}$ whose coefficients are rational in $a_1\ a_2 \cdots\ a_n$; the equations $R_k^{p_k} = f_k$ are irreducible in respect to $a_1 \cdots\ a_n$; $R_1 \cdots\ R_{k-1}$; the exponents p_k are primes, finally

$$(b) \qquad x_0 = \Sigma A_h R_\lambda^h \qquad h = 0, 1 \cdots p_\lambda - 1$$

where A_h is an integral function of $R_1 \cdots\ R_{\lambda-1}$, with coefficients rational in $a_1 \cdots\ a_n$.

§ 3

We impose now the condition that the explicit algebraical function x_o shall satisfy the equation (a); this will give us a relation between the roots $x_o\ x_1 \cdots$ and the radical R_λ which will indicate a method of simplifying the suite (A) still further. Raising x_o to the various powers, and substituting these values of $x_0, x_0^2, x_0^3, \cdots x_0^n$ in (a), we have the equation.

$$(1) \qquad 0 = B_0 + B_1 R_\lambda + B_2 R_\lambda^2 + \cdots + B_{p_{\lambda-1}}\ R_\lambda^{p_\lambda - 1}$$

and making use of

$$(2) \qquad R^{p_\lambda} = f_\lambda$$

to reduce powers of R_λ higher than $p_{\lambda-1}$; the coefficients B are rational in

$$a_0\ a_1 \cdots a_n,\ R_1, R_2 \cdots, R_{\lambda-1}$$

and hence by theorem I., the coefficients B all vanish.* Thus (1) is satisfied when we replace R_λ by αR_λ where $\alpha^{p_\lambda} = 1$. Hence the expressions obtained from (b) when we replace there R_λ by $\alpha^k R_\lambda$, that is

$$(3) \qquad x_k = \Sigma A_h \alpha^{hk} R_\lambda^h \qquad k = 0, 1 \cdots p_\lambda - 1$$

satisfy (1) and are thus roots of (a). Here all the coefficients A cannot vanish, let A_h be one of these; if we multiply both sides of the p_λ equations (3) respectively by α^{-h}, $\alpha^{-2h} \cdots \alpha^{-(p_\lambda - 1)h}$, and add, we get, remembering that

$$1 + \alpha^r + \alpha^{2r} + \cdots + \alpha^{(p_\lambda - 1)r} = 0$$

the equation

$$(4) \qquad \Sigma \alpha^{-hk} x_k = p_\lambda A_h R_\lambda^h$$

which gives us the relation in question.

*We have assumed the *suite* to embrace only irreducible equations; in practice it is convenient to defer the elimination of reducible elements till this stage where we have the means of deciding concerning reducibility.

This relation shows us how we may express x_o as an integral function of certain radicals

$$P_1, P_2 \cdots\cdots P_\lambda$$

where these radicals enjoy the peculiar property of being integral functions of $x_o\, x_1 \cdots\cdots x_{n-1}$ and certain roots of unity $\alpha, \beta \cdots \omega$ with rational-number coefficients. In fact put†

$$P_\lambda = p_\lambda A_h R_\lambda^h; \tag{5}$$

this equation together with (2) shows that R_λ is a rational function of P_λ and the quantities $R_1, \cdots R_{\lambda-1}$, since the assumption that (2) is irreducible in respect to $R_1 \cdots R_{\lambda-1}\ P_\lambda$ is, on account of (3) inadmissible. (Theorem I). As R_λ is rational in respect to these quantities so is x_o. That P_λ satisfies a binomial equation of the type

$$P_\lambda^{p_\lambda} = g_\lambda\,(a_1 \cdots a_n, R_1 R_2 \cdots R_{\lambda-1})$$

is evident; for

$$P_\lambda^{p_\lambda} = p_\lambda^{p_\lambda} A_\lambda^{p_\lambda} R_\lambda^{p_\lambda h} = p_\lambda^{p_\lambda} A_\lambda^{p_\lambda} f_\lambda^{\,h}$$

which is a rational function of $a_1 \cdots a_n\ R_1 \cdots R_{\lambda-1}$ which we denote by g_λ.

The radical R_λ being replaced by P_λ, we proceed now to show how we may replace $R_{\lambda-1}$ by $P_{\lambda-1}$. Put

$$\xi_0 = P_\lambda^{p_\lambda} = (\Sigma \alpha^{-h\,k} x_k)^{p_\lambda}$$

and let $\xi_0\, \xi_1\, \xi_2 \cdots$ be the $n!$ functions (different or not) arising from applying the $n!$ substitutions of the symmetric group to ξ_0. Form now the equation

$$\Phi(\xi) = (\xi - \xi_o)\ (\xi - \xi_1) \cdots\cdots = 0,$$

its coefficients being symmetric in $x_o, x_1, \cdots x_n$ are rational in the coefficients $a_1 \cdots a_n$.

Now a moment's reflection shows that the reasoning applied to the equations

$$f(x) = 0, \qquad x_0 = f_\lambda\,(a_1 \cdots a_n;\ R_1 \cdots R_\lambda)$$

† This step could obviously be omitted if for $h = 1$, A_h is a rational number.

can be applied word for word to the equations

$$\Phi(\xi)=0, \qquad \xi_0=g_\lambda(a_1\cdots a_n;\ R_1\cdots R_{\lambda-1})$$

In fact referring to the reasoning just made in regard to x_0, R_λ we see that we may write

$$(b') \qquad \xi_0=\Sigma A_r' R_{\lambda-1}^r \qquad r=0,1\cdots p_{\lambda-1}1.$$

which is the equation analogous to (b).

This value of ξ_0 substituted in $\Phi=0$ gives

$$(1') \qquad 0=B_0'+B_1'R_{\lambda-1}+\cdots B'_{p-1}R_{\lambda-1}^{p-1}$$

which is analagous to (1). This shows that the quantities

$$(3') \qquad \xi=\Sigma A_r'\beta^{rs}R_{\lambda-1}^r \qquad s=0,1\cdots p_{\lambda-1}-1, \qquad \beta^{p_{\lambda-1}}=1$$

also satisfy $\Phi=0$. These equations now give as before the relation

$$(4') \qquad \Sigma\beta^{-rs}x_s=p_{\lambda-1}A_r'R_{\lambda-1}^r$$

analogous to (4). It follows thus, if we put

$$P_{\lambda-1}=p_{\lambda-1}A_r'R_{\lambda-1}^r$$

that $R_{\lambda-1}$ is a rational function of $R_1, R_2,\cdots R_{\lambda-2}$ and $P_{\lambda-1}$ while on the one hand $P_{\lambda-1}$ satisfies a binomial equation of the type

$$P_{\lambda-1}^{p_{\lambda-1}}=g_{\lambda-1}(a_1\cdots a_n;\ R_1, R_2, R_{\lambda-2})$$

and on the other is an integral function of $\xi_0\ \xi_1\cdots$and β. But $\xi_0\ \xi_1\cdots$are integral functions of $x_0\ x_1\cdots$and α, hence $P_{\lambda-1}$ is an integral function of $x_0\ x_1\cdots x_{n-1}$ and the roots of unity α, β; the coefficients of these functions being rational numbers. Returning now to the expression for x_0, namely:

$$x_0=f(a_1\cdots a_n, R_1\cdots R_{\lambda-1}, R_\lambda),$$

we see that we are in the position to replace the radicals $R_{\lambda-1}$, R_λ by the radicals $P_{\lambda-1}$, P_λ. The same reasoning being applicable to the remaining radicals we have the following:

THEOREM III. If an equation is algebraically solvable, we can always give the explicit algebraic expression for a root such a form that all the radicals entering it are integral functions of the roots $x_0\ x_1\cdots x_{n-1}$ and certain roots of unity $\alpha, \beta,\cdots\omega$, the coefficients of these functions being rational numbers;

the radicals themselves are determined by a *suite* of be nomial equations

$$(B) \qquad P_1^{p_1} = g_1(a_1 \cdots a_n) P_2^{p_2} = g_2(a_1 \cdots a_n;\ P_1) \cdots\cdots P_\lambda^{p_\lambda} = g_\lambda\,(a_1 \cdots a_n; P_1\, P_2 \cdots P_{\lambda-1})$$

while x_0 is given by

$$(C) \qquad x_0 = g\,(a_1 \cdots a_n;\ P_1\ P_2 \cdots P_\lambda),$$

the functions g being integral functions of $P_1 \cdots\cdots P_\lambda$ with coefficients rational in $a_1 \cdots a_n$.

§ 4.

The theorem just proved affords us a sure foundation to construct the substitution-theoretical part of the demonstration; we give first a form due to Ruffini.* Consider the rational integral function of the roots†

$$\varphi\ (x_1\ x_2 \cdots x_n)$$

defined by the first equation of (B); let $\varphi_s\ \varphi_{s^2} \cdots\cdots$ be the values of φ after application of $s\ s^2 \cdots$ where

$$s = \begin{pmatrix} 1\,2\,3\,4\,5 \\ 2\,3\,4\,5\,1 \end{pmatrix},$$

then since $g_1\,(a_1 \cdots a_n)$ is a symmetric function of the roots it remains unchanged for s. Applying then s to the identity

$$\varphi^{p_1} = g_1\,(a_1 \cdots a_n)$$

it becomes $\varphi_s^{p_1} = g_1$ whence

$$(1) \qquad \varphi_s = \beta\,\varphi \quad \text{where } \beta^{p_1} = 1$$

Applying s to the identity (1) it becomes

$$\varphi_{s^2} = \beta\varphi_s = \beta^2\varphi$$

similarly $\varphi_{s^3} = \beta^3\varphi$, $\varphi_{s^4} = \beta^4\varphi$ and $\varphi_{s^5} = \beta^5\varphi$; but as $s^5 = 1$, $\varphi_{s^5} = \varphi$ and $\beta^5 = 1$.

In the same way, if

$$\sigma = \begin{pmatrix} 1\ 2\ 3 \\ 2\ 3\ 1 \end{pmatrix}$$

*Cf. my paper in *Monatshefte für Mathematik und Physik*, vol. 6, for fuller information concerning this form of proof used by Ruffini in the Modena work already referred to.

† We designate these now by the indices 1, 2...n, as more convenient.

$\varphi_\sigma = \gamma\varphi$ where, as $\sigma^3=1$, $\gamma^3=1$

Hence the application of σ to the identity (1) gives

$$\varphi_{s\sigma} = \beta\varphi_\sigma = \beta\gamma\varphi$$

whence we conclude as above that $(\beta\gamma)^5=1$ since $(s\sigma)^5=1$. Similarly if

$$\rho = \begin{pmatrix} 3 & 4 & 5 \\ 4 & 5 & 3 \end{pmatrix}$$

then $\varphi_\rho = \varphi_{\rho^2} = \varphi$; but since $\rho\sigma = s$, $\varphi_{\rho\sigma} = \varphi_s = \varphi$; hence $\beta=1$ since $\varphi_s = \beta\varphi$. That is φ remains not only unaltered for σ and ρ, but also for s. Consider now the rational function of the roots

$$\psi\,(x_1 x_2 \cdots x_n)$$

defined by the second equation of the *suite B*. The right hand side of the identity

$$\psi^{p_2} = g_2\,(a_1 \cdots a_n;\ \varphi)$$

remaining unaltered for the substitutions s, σ, ρ we can reason in regard to ψ precisely as we did concerning φ: hence ψ is unchanged for these substitutions. Proceeding in this way we see that all the radicals $P_1\ P_2 \cdots P_\lambda$ remain unaltered for s; but applying s to the identical relation (C) viz:

$$x_1 = g\,(a_1 \cdots a_n;\ P_1 P_2 \cdots P_\lambda)$$

we observe that the right hand side remains unaltered whereas the left hand side does not which is an absurdity. The assumption that there exist an explicit algebraical function of the coefficients $a_1\ a_2 \cdots a_n$ which satisfies (A), leads thus to a contradiction.

§ 5

An interresting modification of Ruffini's proof is the following: We just saw that P_ν ($\nu=1, 2$) remain unaltered by the circular substitution $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$; as the indices 1,2,3,4,5 employed in showing this were any five of the n indices, it follows that P_ν remain unaltered for every circular substitution of three indices. These substitutions we shall call the substitutions of the alternate group which we denote shortly by Γ. We propose to show that P_ν remain unaltered

for no other substitutions of the symmetric group G; having established this it follows that the radical P_2 is rational in P_1 which violates the hypothesis made in regard to the *suite B*. In the first place P_1 must change its value for every transposition $\tau=(\lambda, \mu)$ for if it remain unaltered for *any* transposition we show that it remains unaltered for *every* transposition; as every substitution is the product of cycles and as $\begin{pmatrix} 1\ 2\ 3\cdots m \\ 2\ 3\ 4\cdots 1 \end{pmatrix}$ is the product of transpositions $(12)(13)\cdots(1\,m)$, P_1 would remain unaltered for every substitution, and then being symmetric functions of the roots, it would be rational in $a_1 a_2 \cdots a_n$.

Suppose then P_1 remain unaltered for τ, let λ be any substitution of G, then P_1 remains unaltered for $\varphi=\lambda^{-1}\tau\lambda$; for since $P_{\lambda^{-1}\tau}=P_{\lambda^{-1}}$ we have $P_{\lambda^{-1}\tau\lambda}=P_{\lambda^{-1}\lambda}=P_1$

Now, by properly choosing λ, ρ can represent any transposition $(l_\lambda\, l_\mu)$; for let

$$\lambda=\begin{pmatrix} 1\ 2\ 3\cdots n \\ l_1\ l_2\ l_3\cdots l_n \end{pmatrix}$$

then λ^{-1} converts

(1) $$l_1\, l_2\, l_3\cdots l_\lambda\cdots l_\mu\cdots l_n$$

respectively into

$$1\ 2\ 3\cdots\lambda,\cdots\mu\cdots n$$

which τ converts respectively into

$$1\ 2\ 3\cdots\mu\cdots\lambda\cdots n$$

which finally λ converts into

(2) $$l_1\, l_2\, l_3\cdots l_\mu\cdots l_\lambda\cdots l_n\,;$$

that is the substitution $\rho=\lambda^{-1}\tau\lambda$ converts (1) into (2) so that ρ leaving every index except l_λ, l_μ unaltered and merely transposing these

$$\rho=(l_\lambda, l_\mu)$$

Thus every transposition alters P_1; but every pair of transpositions leaves it unchanged, since every such pair is of the type

$$(1\ 2)\ (3\ 4) \text{ or } (1\ 2)\ (2\ 3),$$

but the first being equal to $\begin{pmatrix} 1\ 2\ 3 \\ 2\ 3\ 1 \end{pmatrix}\begin{pmatrix} 3\ 1\ 4 \\ 1\ 4\ 3 \end{pmatrix}$ and the second equal to $\begin{pmatrix} 1\ 3\ 2 \\ 3\ 2\ 1 \end{pmatrix}$, both are substitutions of Γ. From this we

conclude that if any substitution s be the product of m transpositions, it will alter or leave unaltered the radical P_1 according as m is odd or even. This shows that however s be decomposed into a product of transpositions, their number is always odd or always even, and we say s is an odd or even substitution according as m is. As I' contains all the even substitutions of G, P_1 and hence P_2 also is altered for every substitution not in I'. The number of substitutions I' in G is $\frac{1}{2}\,n\,!$; for let

$$s_1=1,\ s_2,\ s_3\cdots s_m \tag{1}$$

be the even substitution, and

$$t_1\ t_2\ t_3\cdots t_\mu$$

be the odd; then,

$$t_1,\ s_2t_1,\cdots\cdots s_m\ t_1 \tag{2}$$

are distinct and odd, hence $\mu \geqq m$; also

$$t_1\cdot t_1,\ t_2\,t_1,\ t_3\,t_1,\cdots t_\mu\ t_1$$

are distinct and even, hence $m \geqq \mu \therefore m=\mu=\frac{1}{2}\ n\,!$ This shows that P_ν acquire but two values for the substitutions of G; for they remain unchanged for (1) while they both change for the substitutions (2) into P_ν', and there are no other substitutions in G.

We now conclude easily that P_2 is rational in P_1. As P_1 is root of a binominal equation, it follows that $P_1'=-P_1$; also the coefficients of

$$\Phi\,(x)=(P_2+P_2')\,x+P_1\,(P_2-P_2')$$

being unaltered for the substitutions of G, are rational in $a_1\ a_2\cdots a_n$; denotingthem by A, B, we have

$$\Phi\,(x)=A\,x+B$$

But
$$\Phi\,(P_1)=A\,P_1+B=2\,P_1\,P_2,$$

hence
$$P_2=\frac{A\,P_1+B}{2\,P_1}$$

and P_2 is rational in P_1 and the coefficients $a_1\cdots a_n$.

§ 6.*

We turn now to Kronecker's form of Abel's proof. From the preceding paragraph we take as proven that P_1 is un-

* In anticipation of questions of priority, I remark that this paragraph formed part of a paper I had the honor to read before the Yale Mathematical Club, December 4, 1894. No changes except of the most insignificant nature have been made in the text.

altered for the substitution of I', and that every rational function of the roots unaltered for Γ is rational in P_1. Consider the rational function of the roots $\psi(x_1 x_2 \cdots x_n) = P_2$ defined by the second equation of the *suite* (B)

$$\psi^{p_2} = g_2(P_1). \tag{1}$$

The $\frac{1}{2}n!$ functions (different or not)

$$\psi\, \psi_1\, \psi_2 \cdots\cdots \tag{2}$$

which arise from ψ on applying to it the $\frac{1}{2}n!$ substitution of I' must all be of the form

$$\omega\psi, \qquad \omega^{p_2} = 1$$

since the right hand side of (1) remains unaltered for these substitutions. Thus if ψ remain unaltered for one substitution

$$\sigma = \begin{pmatrix} 1, 2, 3 \cdots n \\ l_1\, l_2\, l_3 \cdots l_n \end{pmatrix}$$

of I' besides the identical substitution, all the conjugate functions (2) must also remain unaltered for σ. But such a substitution must exist since $\frac{1}{2}n! > p_2$; in fact the coefficients of the equation

$$\Phi(x) = (x-\psi)(x-\psi_1)(x-\psi_2)\cdots \tag{3}$$

being symmetric in (2) are unchanged for the substitutions of I' and are thus rational in P_1.

But $\Phi = 0$ having the root $x = \psi$ in common with the irreducible equation

$$P_2^{p_2} = g_2(P_1) \tag{4}$$

is satisfied by all the roots of (4) and hence $\frac{1}{2}n! \equiv p_2$; as p_2 is prime $\frac{1}{2}n! > p_2$.

We now show that the conjugate functions (2) remaining unaltered by σ a substitution different from the identical substitution, remain unaltered for every substitution

$s = \begin{pmatrix} 1\ 2 \cdots n \\ h_1\, h_2 \cdots h_n \end{pmatrix}$ of I' and $P_2 = \psi$ is thus rational in P_1 which

is contrary to hypothesis. To do this Kronecker remarks that ψ remains unaltered for every substitution ρ of I' which changes

$$l_{h_k} \text{ into } h_{l_k} \qquad k = 1, 2 \cdots n$$

In fact $\rho=\sigma^{-1}s^{-1}\sigma s$, for σ^{-1} changes l_{hk} into h_k which s^{-1} changes into k which is changed by σ into l_k which finally s changes into h_{lk}. But that $\psi_\rho = \psi$ is manifest since by hypothesis $\psi_\sigma = \psi$ and hence $\psi_{\sigma^{-1}}=\psi$ also, but then $\psi_{\sigma^{-1}s^{-1}} = \psi_{s^{-1}}$ and $\psi_{\sigma^{-1}s^{-1}\sigma} = \psi_{s^{-1}\sigma} = \psi_{s^{-1}}$, hence finally $\psi_{\sigma^{-1}s^{-1}\sigma s} = \psi_{s^{-1}s} = \psi$. Thus if ψ remain unaltered for σ it also remains unaltered for ρ; which enables us to show that ψ is unchanged for at least one circular substitution of three elements. For whatever σ may be it is of one of the five following types:

1° σ contains at least one cycle of more than three letters and is of the form

$$\sigma_1=\begin{pmatrix}1&2&3\cdots m\\2&3&4\cdots 1\end{pmatrix} c_1\, c_2\cdots\cdots$$

where $c_1\, c_2\cdots$ denote other cycles of σ_1

2° it contains two or more cycles of three elements, but no cycle of more elements, and

$$\sigma_2=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\begin{pmatrix}4&5&6\\5&6&4\end{pmatrix} c_1\, c_2\cdots$$

3° it contains only one cycle of three elements and one or more transpositions

$$\sigma_3=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\begin{pmatrix}4&5\\5&4\end{pmatrix} c_1\, c_2\cdots$$

4° it contains only transpositions, but of these at least three

$$\sigma_4=(1\ 2)\ (3\ 4)\ (5\ 6)\, c_1\, c_2\cdots$$

5° it contains only two transpositions

$$\sigma_5=(1\ 2)\ (3\ 4)\ (5)\cdots$$

Put now $\rho_\lambda=\sigma_\lambda^{-1}\sigma_\lambda^{-1}\sigma_\lambda s_\lambda$

$$s_1=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\quad s_2=\begin{pmatrix}1&4&5\\5&4&1\end{pmatrix}\quad s_3=\begin{pmatrix}1&2&4\\2&4&1\end{pmatrix}\quad s_4=\begin{pmatrix}1&3&5\\3&5&1\end{pmatrix}=s_5$$

then

$$\rho_1=\begin{pmatrix}1&2&4\\2&4&1\end{pmatrix}\quad \rho_2=\begin{pmatrix}1&4&5&2&6\\4&5&2&6&1\end{pmatrix}\quad \rho_3=\begin{pmatrix}1&2&5&3&4\\2&5&3&4&1\end{pmatrix}$$

$$\rho_4=\begin{pmatrix}1&3&5\\3&5&1\end{pmatrix}\begin{pmatrix}2&6&4\\6&4&2\end{pmatrix},\quad \rho_5=\begin{pmatrix}1&3&5&4&2\\3&5&4&2&1\end{pmatrix}$$

which shows that all the cases may be reduced to 1°. Hence ψ remains unaltered for some circular substitution of three elements

$$\tau=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$$

But if ψ remain unchanged for τ it will also remain invariant for

$$(5)\qquad \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix},\quad \begin{pmatrix}1&2&4\\2&4&1\end{pmatrix},\quad \begin{pmatrix}1&2&5\\2&5&1\end{pmatrix},\quad \cdots\begin{pmatrix}1&2&n\\n&2&1\end{pmatrix}$$

For let $t=\begin{pmatrix}1&2&\nu\\2&\nu&1\end{pmatrix}$, then ψ being invariant for τ is for $t^{-1}\tau\, t^{-1}=\omega$ and hence for ω; but $\omega=\begin{pmatrix}2&\nu&3\\\nu&3&2\end{pmatrix}$ and hence

$$\omega^2=\begin{pmatrix}2&3&\nu\\3&\nu&2\end{pmatrix}\qquad \nu=4,5\cdots n$$

Every substitution of I' is the product of the substitutions of (5), for every substitution of I' is the product of a certain number of pairs of transpositions

$$(1\ 2)\quad (1\ 3)\quad \cdots(1\ n).$$

Let (1λ) (1μ) be such a pair, then as

$$(1\lambda)\ (1\mu)=\begin{pmatrix}1&2&\lambda\\2&\lambda&1\end{pmatrix}\begin{pmatrix}1&2&\lambda\\2&\lambda&1\end{pmatrix}\begin{pmatrix}1&2&\mu\\\mu&2&1\end{pmatrix}$$

ψ remains unaltered for every substitution of I'.

This demonstration, while longer than either of the two preceding ones, is interesting from a historical view, as the lemma on the conjugate functions ψ contains as a corollary Cauchy's theorem, which is fundamental in Abel's proof. In fact let

$$\varphi_1\quad \varphi_2\quad \cdots\varphi_m$$

be the m distinct values which a rational function φ of $x_1\, x_2\cdots x_n$ assumes for the substitutions of I'; as no substitution of I' leaves *all* the φ's unchanged every substitution of I' will give rise to a permutation of the above m indices; as there are only $m!$ permutation of m things this number must be certainly as great as $\frac{1}{2}n!$ and

$$m!\geqq\tfrac{1}{2}n!$$

Now if $m < n$ then not only is $m! < n!$ but also $m! < \frac{1}{2} n!$ which is impossible. Thus every rational function φ of $x_1 x_2 \cdots x_n$ which takes on more than two values, takes on at least n values; which is Cauchy's theorem.

§ 7.

It being demonstrated that the general equation of degree $n > 4$ possesses no algebraic solution when the coefficients are regarded as independent variables, it lies very near to inquire whether there are equations with constant coefficients, say with rational-number coefficients, which do not possess an algebraic solution. To this very important question the Ruffini-Abelian theorem gives no reply; however in looking over the reasoning employed in the last three paragraphs we observe that its correctness depends upon the obvious fact that every rational equation

$$\Phi(x_1 x_2 \cdots x_n \alpha, \beta \cdots) = 0 \tag{1}$$

between the roots and certain roots of unity $\alpha, \beta \cdots$, the coefficients being rational numbers, remains true on applying to it any substitution of the alternate group Γ. The question is thus reduced to this: do there exist equations of every degree, whose coefficients are rational numbers such that every relation (1) still subsists on applying any substitution of Γ? That this is so has been shown by Hilbert.* Hence not only has the *general* equation of degree > 4 no algebraic solution, but there exists an infinity of equations of every degree with integral coefficients which possess this property.

§ 8.

We close by giving an illustration of §§ 2, 3 applied to the explicit algebraic function

$$x = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$$

root of the cubic

$$x^3 + px + q = 0 \tag{1}$$

Here

$$R_1^2 = f_1(p, q) = \frac{q^2}{4} + \frac{p^3}{27}; \quad R_2^3 = f_2(p, q, R_1) = -\frac{q}{2} + R_1$$

$$R_3^3 = f_3(p, q, R_1, R_2) = -\frac{q}{2} + R_1 \tag{α}$$

$$x_0 = R_2 + R_3 \tag{2}$$

* CRELLE, vol. 110, p. 104.

We proceed to replace the *suite* (α) by a *suite* (β) of the type (B) of § 3. Raising (2) to the 2nd and 3rd powers and substituting in (1) we get

$$R_3^3 + 3\,R_2 R_3^2 + (3\,R_2^2 + p)\,R_3 + (R_2^3 + p\,R_2 + q) = 0$$

or reducing by aid of

$$R_3^3 = f_3 = -\frac{q}{2} - R_1 \qquad R_2^3 = -\frac{q}{2} + R_2$$

we get

$$3\,R_2 . R_3^2 + (3\,R_2^2 + p)\,R_3 + p\,R_2 = 0$$

As the coefficients of this equation are not zero, the last equation of (α) cannot be reducible and R_3 must be rational in the preceding radicals. In fact we know that

$$R_3 = -\frac{p}{3\,R_2}$$

Equation (2) becomes thus

$$x_0 = R_2 - \frac{{}^1/_3\,p}{R_1 - \frac{1}{2}q} R_2^2 \tag{3}$$

The denominator here is $-R_1 - \frac{1}{2}q$ whose conjugate value is $-R_1 - \frac{1}{2}q$; hence multiplying numerator and denominator of the second term of the right member of (3) by this last, (3) becomes

$$x_0 = R_2 - \frac{9}{p^2}(R_1 + \tfrac{1}{2}q)\,R_2^2 \tag{4}$$

which is an integral function of R_1, R_2 with coefficients rational in p, q. The value of x_0 given by (4) substituted in (1) gives

$$0 = B_0 + B_1 R_2 + B_2 R_2^2,$$

where

$$B_0 = R_1 - \frac{q}{2} - \frac{3^6}{p^6}\cdot\frac{p^6}{3^6}(R_1 + \tfrac{1}{2}q)$$

$$B_1 = -\frac{3^3}{p^2}\frac{p^3}{3^3} + p$$

$$B_2 = \frac{3^5}{p^4}\frac{p^3}{3^3}(1 + \tfrac{1}{2}q) - \frac{3^2}{p}\left(R_1 + \frac{q}{2}\right)$$

which are all identically equal to zero. Hence not only is (4) a root of (1) but so also are the quantities which we

deduce from it in replacing R_2 by ωR_2 and $\omega^2 R_2$ ($\omega^3 = 1$). Denoting these roots respectively by $x_0 x_1 x_2$ we have

$$x_0 = R_2 - \frac{3^2}{p^2}(R_1 + \tfrac{1}{2}q) R_2^2$$

$$x_1 = \omega R_2 - \frac{3^3}{p^2}(R_1 + \tfrac{1}{2}q)\omega^2 R_2^2$$

$$x_2 = \omega^2 R_2 - \frac{3^2}{p^2}(R_1 + \tfrac{1}{2}q)\omega R_2^2$$

As the coefficicnt of R_2 is here 1 we do not need to replace R_2 by a new radical. Solving we get

$$R_2 = \tfrac{1}{3}\Sigma \omega^{-k} x_k \qquad k = 0, 1, 2$$
$$= \frac{x_0 + \omega^2 x_1 + \omega x_2}{3}$$

The suite (α) is now replaced by

$$R_1^2 = f_1 \quad R_2^3 = f_2$$
(β) $$x_0 = g(p, q, R_1, R_2,)$$
$$= R_2 - \frac{9}{p^2}(R_1 + \tfrac{1}{2}q) R_2^2$$

and the first step has been accomplished.

We have now to reason in the same way in regard to the remaining radical R_1. To this end we form the equation $\varphi(\xi) = 0$ whose roots are the values of

$$\xi_0 = R_2^3 = \left(\frac{x_0 + \omega^2 x_1 + \omega x_2}{3}\right)^3$$

As ξ_0 acquires only two distinct values, Φ will be the cube of an integral function of ξ with coefficients rational in p, q; this is easily found to be

$$\varphi(\xi) = \xi^2 + q\xi - \tfrac{1}{27}p^3,$$

Substituting here the value of ξ given in (β), $\varphi(\xi) = 0$ becomes

$$(R_1 - \tfrac{q}{2})^2 + q(R_1 - \tfrac{q}{2}) - \tfrac{1}{27}p^3 = 0,$$

or

$$B_0 + B_1 R_1 = 0$$

where

$$B_0 = \tfrac{1}{4}q^2 + \tfrac{1}{4}q^2 - \tfrac{1}{2}q^2 + \tfrac{1}{27}p^3 - \tfrac{1}{27}p^3$$
$$B_1 = q - q$$

vanish identically; whence not only

$$\xi_0 = R_1 - \frac{q}{2}$$

but also

$$\xi_1 = -R_1 - \frac{q}{2}$$

is a root of $\varphi = 0$.
Whence

$$R_1 = \tfrac{1}{2}(\xi_0 - \xi_1) = \tfrac{1}{2 \cdot 3^3}\left[(x_0 + \omega^2 x_1 + \omega^2 x_2)^3 - (x_0 + \omega x_1 + \omega^2 x_2)^3\right]$$

$$= -\frac{\sqrt{-3}}{2.9}\sqrt{\triangle},$$

where $\triangle = (x_0 - x_1)^2 (x_1 - x_2)^2 (x_1 - x_2)^2$ is the discriminant of (1). Thus the *suite* (β) has the character (B).

YALE UNIVERSITY,
NEW HAVEN, CONN.

ON CERTAIN SUB-GROUPS OF THE GENERAL PROJECTIVE GROUP.

BY PROFESSOR HENRY TABER.

[Read at the January meeting of the Society, 1896.]

§ 1

In what follows a linear transformation homogeneous in n variables as

$$\begin{aligned} x_1' &= a_{11} x_1 + a_{12} x_2 + \cdots + a_{1n} x_n, \\ x_2' &= a_{21} x_1 + a_{22} x_2 + \cdots + a_{2n} x_n, \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ x_n' &= a_{n1} x_1 + a_{n2} x_2 + \cdots + a_{nn} x_n, \end{aligned}$$

will be denoted by the single letter A. If x_1, x_2, etc., are the Cartesian coördinates of a point in n-fold space, the transformation A is a homogeneous strain; and the totality of transformations A constitutes the group of homogeneous strains in n-fold space. If we consider only transformations A of non-zero determinant, we obtain Lie's *general linear homogeneous group*. The group of transformations A of determinant $+1$ is termed by Lie the *special linear homogeneous group*.