CHAPTER I

GALOISIAN GROUPS AND RESOLVENTS

1. Suppose that $c_1, c_2, \dots c_n$ form a set of assigned algebraic quantities, and that

$$f(x) = x^n + c_1 x^{n-1} + \dots + c_r x^{n-r} + \dots + c_n.$$

If we can find another set of algebraic quantities $x_1, x_2, \dots x_n$ such that

$$\Sigma x_i = -c_1, \quad \Sigma x_i x_j = c_2, \dots, \quad x_1 x_2 \dots x_n = (-)^n c_n \dots\dots (1),$$

we shall have identically

$$f(x) = (x - x_1)(x - x_2) \dots (x - x_n).$$

Under these circumstances (supposing that the algebra we are using is the ordinary one)

$$f(x) = 0$$

for $x = x_1, x_2, \dots x_n$ and for no other values of x.

Thus every solution of (1) leads to the complete solution of the equation $f(x) = 0$. Conversely the complete solution of $f(x) = 0$ in the form $x = \xi_1, \xi_2, \dots \xi_n$ leads to the complete solution of (1), considered as a system of simultaneous equations, in the form

$$x_1, x_2, \dots x_n = \xi_a, \xi_b, \dots \xi_l,$$

where $\xi_a, \xi_b, \dots \xi_l$ represents, in turn, every permutation of $\xi_1, \xi_2, \dots \xi_n$.

If the values $\xi_1, \xi_2, \dots \xi_n$ are all distinct, $f(x) = 0$ has no multiple roots, and the solutions of the simultaneous equations are all distinct, and are $n!$ in number.

If $f(x) = 0$ has multiple roots, its solution may be made to depend upon an equation without multiple roots. Suppose, for example, that $f(x)$ has a root r of multiplicity α; then the first derived function $f_1(x)$, that is to say df/dx, has a root r of multiplicity $(\alpha - 1)$. Hence if $\phi = \mathrm{dv}(f, f_1)$, the highest common factor of f and f_1, the equation

$f/\phi = 0$ has coefficients which are rational functions of $c_1, c_2, \ldots c_n$, and its roots are the distinct roots of $f(x)$, each occurring only once. Moreover, if $f_i = d^i f/dx^i$, we can, by finding dv (f_1, f_2), dv (f_2, f_3) and so on, determine by rational operations the exact multiplicity of any repeated root of $f = 0$: hence the complete solution of $f/\phi = 0$ leads to that of $f = 0$. In all that follows it will be assumed that f has no multiple roots.

2. It has been proved in various ways that the roots of $f(x) = 0$ actually exist; that is to say, if real or complex values be assigned, at pleasure, to the coefficients, then there are exactly n determinate real or complex numbers $x_1, x_2, \ldots x_n$ such that

$$f(x) = \Pi\,(x - x_i)$$

for all values of x. Another theorem which will be assumed throughout is that every rational symmetric function of the roots can be expressed as a rational function of the coefficients.

3. What gives special interest to the subject in hand is that the actual determination of the roots of a given equation is a problem which differs in complexity according to the assumptions made with regard to the coefficients, and the value of n. Thus, if $n < 5$, and the coefficients are left arbitrary, it is possible to construct an explicit algebraic function of the coefficients which is a root of the equation. For $n > 4$, this is no longer the case; a fact first proved by Abel, who also perceived the real reason for the limitation, namely, the special properties of the group of permutations of n different things when $n < 5$.

When the coefficients are numerically given, the rational roots, if any exist, can be found by trial, and the values of the irrational ones can be found by approximation. With these processes of approximation, however, we shall not be concerned; our main problem is, in fact, the following :

Given a particular equation with numerical coefficients, it is required to find the simplest set of irrational quantities such that all the roots of the given equation can be expressed as finite rational functions, in an explicit form, of the set of irrationals. What is to be understood by the *simplest* set of auxiliary irrationals will appear as we proceed.

4. Before entering upon the general theory, it will be useful to consider the case of a cubic equation with arbitrary coefficients, and roots α, β, γ. Since the value of $\alpha + \beta + \gamma$ is known, it will be sufficient

if we can find the values of two other independent linear functions of the roots. If we take an arbitrary linear function $\alpha + l\beta + m\gamma$, this will, in general, assume six values by the permutation of α, β, γ: these values will be the roots of an equation

$$y^6 + m_1 y^5 + \ldots + m_6 = 0,$$

the coefficients of which are rational in l, m and known quantities. Let us try to make this a quadratic in y^3. Then if ω is a complex cube root of unity, there will be six roots of the form

$$y_1,\ \omega y_1,\ \omega^2 y_1,\ y_2,\ \omega y_2,\ \omega^2 y_2.$$

Assuming, as an identity independent of α, β, γ,

$$\alpha + l\beta + m\gamma = \omega(\beta + l\gamma + m\alpha),$$

we have $l = \omega$, $m = \omega^2$: so that we obtain a function

$$y_1 = \alpha + \omega\beta + \omega^2\gamma,$$

the values of which, when α, β, γ are interchanged, become

$$\begin{aligned} y_2 &= \alpha + \omega^2\beta + \omega\gamma, \\ y_3 &= \omega^2\alpha + \omega\beta + \gamma = \omega^2 y_2, \\ y_4 &= \omega\alpha + \omega^2\beta + \gamma = \omega y_1, \\ y_5 &= \omega\alpha + \beta + \omega^2\gamma = \omega y_2, \\ y_6 &= \omega^2\alpha + \beta + \omega\gamma = \omega^2 y_1. \end{aligned}$$

Consequently

$$y_1^3 + y_2^3 = (\alpha + \omega\beta + \omega^2\gamma)^3 + (\alpha + \omega^2\beta + \omega\gamma)^3 = A,$$

a quantity symmetrical in α, β, γ, and therefore rational in the coefficients of the given cubic; in fact,

$$A = 2\Sigma\alpha^3 - 3\Sigma\alpha^2\beta + 12\alpha\beta\gamma = -2c_1^3 + 9c_1c_2 - 27c_3.$$

Similarly $\qquad y_1 y_2 = \Sigma\alpha^2 - \Sigma\alpha\beta = c_1^2 - 3c_2 = B,$

another rational function of the coefficients: so that y_1^3, y_2^3 are the roots of the rational equation

$$y^6 - Ay^3 + B^3 = 0.$$

Let $\qquad \theta = \left\{\frac{A + \sqrt{(A^2 - 4B^3)}}{2}\right\}^{\frac{1}{3}}$

with a fixed determination of the radicals involved. Then we may put

$$\begin{aligned} \alpha + \beta + \gamma &= -c_1, \\ \alpha + \omega\beta + \omega^2\gamma &= \theta, \\ \alpha + \omega^2\beta + \omega\gamma &= B/\theta, \end{aligned}$$

and hence

$$3\alpha = -c_1 + \theta + B/\theta = -c + \theta + \frac{A - \sqrt{(A^2 - 4B^3)}}{2B^2}\theta^2,$$
$$3\beta = -c_1 + \omega^2\theta + \omega B/\theta = \ldots,$$
$$3\gamma = -c_1 + \omega\theta + \omega^2 B/\theta = \ldots.$$

By giving θ all its six values, we obtain all the six permutations of α, β, γ.

It will be noticed that the success of this method depends on finding a power of a linear function of the roots which is a two-valued function of the coefficients; this has been done with the help of an auxiliary number ω which is a root of the rational quadratic $\omega^2 + \omega + 1 = 0$.

In a similar way for the general quartic

$$(\alpha - \beta + \gamma - \delta)^2$$

is a three-valued function of the coefficients, and may be explicitly found by means of an auxiliary rational cubic; after this the solution of the quartic may be completed.

5. If, after the manner of Lagrange, we try to extend this process to a quintic, we take ϵ, a complex fifth root of unity, and form the rational equation satisfied by

$$(x_1 + \epsilon x_2 + \epsilon^2 x_3 + \epsilon^3 x_4 + \epsilon^4 x_5)^5.$$

The degree of this is 24, and it is only in special cases that it can be solved in a manner similar to that which is applicable in the foregoing examples. Thus the method breaks down; at the same time, a generalisation of the process, due to Galois, is of the highest importance in the whole of the theory.

6. Galois begins by considering the rational equation satisfied by the most general linear function of the roots. Let $u_1, u_2, \ldots u_n$ be a set of absolutely undetermined symbols, subject merely to the ordinary algebraic laws of combination; and for the sake of brevity let $n! = \mu$. If we put

$$v_1 = u_1x_1 + u_2x_2 + \ldots + u_nx_n = \sum_{i=1}^{i=n} u_i x_i,$$

where $x_1, x_2, \ldots x_n$ are the roots (all different) of $f(x) = 0$, we can obtain from v_1, by interchanging the roots in all possible ways, μ essentially different expressions $v_1, v_2, \ldots v_\mu$

The product

$$\prod_{i=1}^{i=\mu} (v - v_i) = v^\mu + b_1 v^{\mu-1} + \ldots + b_\mu = F(v),$$

where v is a new indeterminate, is an integral function of v with coefficients which are integral and rational in $c_1, c_2, \dots c_n$ as well as in $u_1, u_2, \dots u_n$ because $F(v)$ is a symmetrical function of the roots of f.

The equation $F(v) = 0$ is called the *complete Galoisian resolvent* of $f(x) = 0$. Its discriminant is a rational integral function of $c_1, c_2, \dots c_n, u_1, u_2, \dots u_n$, which does not vanish identically: so that we may, if we please, assign numerical values to the parameters $u_1, u_2, \dots u_n$ without making any two roots of the resolvent equal to each other. In particular, these numerical values may be ordinary real integers.

7. The most important property of F is that *any rational function of the roots of f can be expressed as a rational function of any one of the roots of F.*

Let the given rational function be $\phi(x_1, x_2, \dots x_n)$, and let

$$\phi_1 (= \phi), \phi_2, \dots \phi_\mu$$

be the expressions obtained from ϕ by applying the substitutions which derive $v_1, v_2, v_3, \dots v_\mu$ from v_1. These expressions ϕ_i are not necessarily all different in form; and two which have different forms may have the same value. But it must be remembered that ϕ_i is derived from ϕ_1 by the same permutation which changes v_1 to v_i.

Consider the expression

$$\psi(v) = \left\{ \frac{\phi_1}{v - v_1} + \frac{\phi_2}{v - v_2} + \dots + \frac{\phi_\mu}{v - v_\mu} \right\} F(v);$$

$\psi(v)$ is an integral function of v, in general of degree $(\mu - 1)$, but possibly lower, and it is a symmetric function of $x_1, x_2, \dots x_n$. Hence the coefficients of $\psi(v)$ can be expressed as rational functions of $c_1, c_2, \dots c_n$; and if, after doing this, we put $v = v_1$, it follows from the above identity that

$$\psi(v_1) = \phi_1 F'(v_1),$$

or

$$\phi_1 = \frac{\psi(v_1)}{F'(v_1)} = R(v_1; c_1, c_2, \dots c_n; u_1, u_2, \dots u_n),$$

where R denotes a rational function of the quantities in the bracket. This equality reduces to an absolute identity if on the right-hand side we replace $v_1, c_1, \dots c_n$ by their expressions in terms of $x_1, x_2, \dots x_n, u_1, u_2, \dots u_n$.

The discriminant of F is

$$\Delta = F'(v_1) F'(v_2) \dots F'(v_\mu),$$

and the quotient $\Delta/F'(v_1)$ is expressible as a rational integral function of v_1: hence we may also put ϕ into the form

$$\phi = \frac{\psi(v_1)\,F'(v_2)\,F'(v_3)\ldots F'(v_\mu)}{\Delta} = \frac{J(v_1)}{\Delta},$$

where $J(v_1)$ is a rational integral function of v_1.

It should be observed also that ϕ_i can be expressed as the same function of v_i that ϕ_1 is of v_1.

Finally, ϕ_1 is expressible as a rational function of *any* root of $F(v)$. Thus if we choose v_i, all we have to do is to replace, in the foregoing proof,

$$v_1, v_2, \ldots v_\mu$$

by

$$s_i(v_1), s_i(v_2), \ldots s_i(v_\mu),$$

where s_i is the perfectly definite substitution which converts v_1 to v_i. In general, ϕ is not the same rational function of v_i as it is of v_1.

8. Several important consequences immediately follow from the theorem just proved. In the first place, we may put $\phi = v_i$, and thus infer that

All the roots of the Galoisian resolvent may be expressed as rational functions of any one of them.

An equation having this property is called a *normal* equation; the Galoisian resolvent is accordingly a normal equation. It must be remembered that the same equation may be normal from one point of view and not from another, if, in the definition, we understand "rational function" to mean "rational function with rational coefficients." By a *field of rationality* we shall understand the aggregate of all the expressions obtainable from a finite set of symbols $t_1, t_2, \ldots t_m$ by a finite set of rational operations; that is to say, all the expressions which can be reduced to the form

$$\frac{\phi(t_1, t_2, \ldots t_m)}{\psi(t_1, t_2, \ldots t_m)},$$

where ϕ, ψ are finite polynomials with ordinary whole numbers for their coefficients. The elements $t_1, t_2, \ldots t_m$ may be partly undetermined parameters, or *umbræ*, partly determinate numbers; those which are numerical may be irrational arithmetically, but are here considered rational in the sense of being given or determined. The simplest field of rationality is that of ordinary rational numbers; this is contained in every other field.

If t_{m+1} is any algebraic number or symbol not contained in the field $(t_1, t_2, \ldots t_m)$, the field $(t_1, t_2, \ldots t_m, t_{m+1})$ is said to be obtained from

the former field by the *adjunction* of t_{m+1}: this term is specially employed when t_{m+1} is a numerical quantity.

In the case of the Galoisian resolvent we may say, then, that it is a normal equation in the field

$$(c_1, c_2, \dots c_n ; u_1, u_2, \dots u_n).$$

9. If, in the theorem of Art. 7, we put $\phi = x_i$, we arrive at the proposition that

Every root of an equation without multiple roots can be expressed as a rational function of any one root of its Galoisian resolvent.

If rational values are given to the parameters $u_1, u_2, \dots u_n$, the resolvent equation becomes normal in the field $(c_1, c_2, \dots c_n)$. Moreover if $c_1, c_2, \dots c_n$ are given, not as symbols, but as actual numbers, the resolvent becomes a definite numerical equation. Unless this equation has multiple roots, it is still true that the knowledge of the value of any one root of the resolvent leads to the complete solution of $f = 0$; because to calculate the function $\psi(v)$ of Art. 7 in its rational form it is sufficient to know the *values* of the elementary symmetric functions of $x_1, x_2, \dots x_n$, and these are given by f.

10. The total resolvent $F(v)$ may or may not be reducible without adjunction; in the second case $f(x) = 0$ is said to be an equation without *affection*.

The irreducible factors of the resolvent of an affected equation are all of the same degree.

Let $\psi_1(v)$, $\psi_2(v)$ be any two such factors: let v_1 be any root of $\psi_1(v) = 0$, and v_2 any root of $\psi_2(v) = 0$. Then (Art. 7) v_2 can be expressed as an integral function, $J(v_1)$, of v_1. If the Tschirnhausen transformation $y = J(x)$ is applied to $\psi_1(x) = 0$, we obtain an equation $\chi(y) = 0$ of the same degree as $\psi_1 = 0$ which has a solution $y = v_2$ in common with $\psi_2(y) = 0$: hence $\chi(y)$ is divisible by $\psi_2(y)$, and the degree of ψ_1 cannot be less than that of ψ_2. By a similar argument, the degree of ψ_2 cannot be less than that of ψ_1; therefore the degrees must be equal.

If h is the degree of each irreducible factor, we have an identity

$$F(v) = \psi_1(v)\, \psi_2(v) \dots \psi_m(v),$$

with

$$mh = \mu,$$

so that m and h are conjugate factors of μ.

Every one of the equations $\psi_i(v) = 0$ is normal, and they are all Tschirnhausen transformations of any one of them. Each may be

called a *primary* resolvent of $f(x)=0$. The knowledge of any one root of a primary resolvent leads to the complete solution of $f(x)=0$.

11. A simple example will help to illustrate the results so far obtained. Let the given equation be

$$x^3-x^2+x-1=0,$$

and let a, b, c be used instead of u_1, u_2, u_3.

The complete resolvent is $F=\phi\chi\psi$,

where

$$\phi=(v-a)^2+(b-c)^2,\quad \chi=(v-b)^2+(c-a)^2,\quad \psi=(v-c)^2+(a-b)^2.$$

One root of $\phi=0$ is $a-bi+ci$, and from this the roots $1, i, -i$ of the original equation are obtained. If we put

$$v_1=a-bi+ci,$$

then

$$\pm\frac{v_1-a}{b-c},\ 1,$$

give the roots of $f=0$ as rational functions of v_1.

12. The reducibility of F shows the existence of asymmetrical functions of $x_1, x_2, \dots x_n$ which nevertheless have rational values. The coefficients of the terms of a primary resolvent $\psi(v)$, considered as a polynomial in $v, u_1, u_2, \dots u_n$, are all rational; but when expressed in terms of $x_1, x_2, \dots x_n$ they cannot all be symmetrical, otherwise every permutation of the roots of f would leave $\psi(v)$ unaltered, and this is not the case.

13. Consider now a primary resolvent

$$\psi_1(v)=(v-v_1)(v-v_2)\dots(v-v_h).$$

Any one of its roots, say v_i, can be derived from v_1 by a perfectly definite permutation of $x_1, x_2, \dots x_n$: let this be called s_i. Including the identical substitution s_1, we have in connection with ψ_1 just h substitutions $s_1, s_2, \dots s_h$. It is a most important theorem that *these substitutions form a group*; that is to say, for every pair of substitutions s_a, s_b (the same or different) we have $s_a s_b=s_c$, where s_c is a definite substitution of the same set.

It follows from Art. 7 that since v_b and v_1 are both roots of $F(v)=0$, there is an integral function $J(v)$ such that

$$s_b(v_1)=v_b=J(v_1).$$

Moreover it appears from the same article that

$$J(v_a)=s_a(v_b)=s_a\{s_b(v_1)\}.$$

But since the equations

$$\psi_1(v) = 0, \quad \psi_1\{J(v)\} = 0$$

have a common root v_1, and the first is irreducible, while both are rational, each root of the first is a root of the second, and in particular

$$\psi_1\{J(v_a)\} = 0\ ;$$

that is to say, $s_a\{s_b(v_1)\}$ is a root of $\psi_1(v) = 0$, and is therefore equal in value to $s_c(v_1)$, where s_c is a substitution of the set $s_1, s_2, \dots s_h$. But this equality in value must also be a coincidence in form, on account of the arbitrary nature of the parameters $u_1, u_2, \dots u_n$. Hence

$$s_b s_a = s_c,$$

it being understood that $s_b s_a$ means the result of first applying s_b and then applying s_a. In a similar way $s_a s_b = s_d$; but s_d is, in general, different from s_c.

14. If ψ_2 is any other of the primary resolvents, there will, in the same way, be a group of substitutions connected with it. This is, in fact, the same group as the one associated with ψ_1. For suppose that

$$\psi_2(v) = (v - v_{h+1})(v - v_{h+2}) \dots (v - v_{2h})\ :$$

then v_{h+1} can be expressed in the form

$$v_{h+1} = J(v_1),$$

and by the usual argument it follows that

$$\psi_2 = \{v - J(v_1)\}\{v - J(v_2)\} \dots \{v - J(v_h)\}.$$

The notation may be so arranged that

$$J(v_i) = v_{h+i} \qquad (i = 1, 2, \dots h),$$

and this being so, we conclude that

$$v_{h+i} = s_i(v_{h+1}),$$

because v_{h+i} is derived from v_{h+1} by the change of v_1 into v_i, and the only substitution which does this is s_i.

The group $(s_1, s_2, \dots s_h)$ is called *the Galoisian group* of the equation $f(x) = 0$. If the complete resolvent is irreducible without adjunction, $h = n!$ and the Galoisian group consists of all the permutations of $x_1, x_2, \dots x_n$.

15. We will now select any one of the primary resolvents, denote it by $\psi(v)$, and call it simply, for the present, *the* resolvent of $f(x)$. Assuming nothing about $f(x)$ except that its coefficients are actually given, $F(v)$ and subsequently $\psi(v)$ can be found by rational operations. The degree of $\psi(v)$ in v at once gives the order of the Galoisian group.

But we can go further than this, and determine, from an examination of ψ, the elements $s_1, s_2, \dots s_h$ which form the group. The notation may be so arranged that

$$\psi = (v - v_1)(v - v_2) \dots (v - v_h),$$

$$v_1 = u_1x_1 + u_2x_2 + \dots + u_nx_n.$$

Now the change of v_1 into v_2 effected by the substitution s_2 may also be effected by a substitution σ_2 operating on the parameters $u_1, u_2, \dots u_n$. For instance, if

$$v_1 = u_1x_1 + u_2x_2 + u_3x_3 + u_4x_4 + u_5x_5 + u_6x_6,$$

$$v_2 = u_1x_2 + u_2x_4 + u_3x_6 + u_4x_1 + u_5x_3 + u_6x_5,$$

then $$s_2 = (x_1x_2x_4)(x_3x_6x_5), \quad \sigma_2 = (u_1u_4u_2)(u_3u_5u_6).$$

In general, if s_i contains the cycle $(x_ax_b \dots x_kx_l)$, σ_i contains the cycle $(u_lu_k \dots u_bu_a)$ and there is a one-one correspondence between the substitutions s_i and the substitutions σ_i. If σ_i is applied to $\psi(v)$ in its rational form, the result is a function $\chi(v)$ of the same order, which has a root v_i, and therefore coincides with $\psi(v)$. Thus there are at least h distinct permutations σ, forming a group, which leave $\psi(v)$ formally unaltered. The same argument applies to the other primary resolvents obtained from F, and since there are only hm substitutions σ altogether, it follows that there are precisely h substitutions σ which leave ψ formally unaltered; from each of these we can deduce uniquely a substitution s belonging to the Galoisian group.

For instance, in the example of Art. 11, if we take ψ as the resolvent,

$$\sigma_1 = 1, \quad \sigma_2 = (ab),$$

and the corresponding Galoisian group is

$$s_1 = 1, \quad s_2 = (x_1x_2).$$

After obtaining the elements of the Galoisian group

$$G = (s_1, s_2, \dots s_h),$$

its properties, as a group of substitutions, or more generally as an abstract group, may be investigated. These are, in themselves, wholly independent of the values of $x_1, x_2, \dots x_n$.

16. It will now be supposed that the coefficients of f are numerical; and, as explained in Art. 8, any quantity in the field $(c_1, c_2, \dots c_n)$ will be considered rational, no matter whether the coefficients c_i are arithmetically rational or not. It will now be proved that

Every rational function of the roots of f which is unchanged **in numerical value** *by the substitutions of the Galoisian group has*