CHAPTER IX

THE GALOIS THEORY OF EQUATIONS

SUPPOSE that there is given a cubic equation, say

$$x^3 + a x^2 + b x + c = 0.$$

This equation will always have three roots, which will be real or complex numbers, and which we will denote by α, β, γ.

To find α, β, γ it is of course necessary to solve the equation, and this may not be an easy procedure, but there are certain functions of the roots α, β, γ which can be determined easily without solving the equation.

If we are given a function of the roots, say $\alpha^2 \beta$, we can in general form five other functions, e.g. $\alpha^2 \gamma$, $\beta^2 \alpha$, $\beta^2 \gamma$, $\gamma^2 \alpha$, $\gamma^2 \beta$ by taking a different arrangement of the roots α, β, γ, i.e. by operating on the function with a permutation interchanging the roots. The six operations of the symmetric group give six functions which are all distinct in this case.

It may happen that all the operations of the group leave the function unchanged, as, e.g. when the function is $(\alpha + \beta + \gamma)$ or $\alpha \beta \gamma$. Such functions are called symmetric functions. Any symmetric function of the roots can be expressed directly in terms of the coefficients in the equation without solving the equation.

Thus the equation

$$x^3 + a x^2 + b x + c = 0$$

must be exactly the same as the equation

$$(x - \alpha)(x - \beta)(x - \gamma) = 0,$$

and expanding the latter and comparing the coefficients of the various powers of x,

$$\alpha + \beta + \gamma = -a,$$
$$\alpha \beta + \beta \gamma + \gamma \alpha = b,$$
$$\alpha \beta \gamma = -c.$$

In terms of these any other symmetric function can be expressed. Thus

$$\alpha^2 + \beta^2 + \gamma^2 = (\alpha + \beta + \gamma)^2 - 2\,(\alpha\,\beta + \beta\,\gamma + \gamma\,\alpha)$$
$$= a^2 - 2\,b.$$

Now it may happen that we can find a function of the roots that is changed by some of the permutations but is left unchanged by others. Then the permutations which leave it unchanged will form a subgroup of the symmetric group, and the function is said to *belong to this subgroup.*

Thus there is a subgroup of order two which contains the identity and the interchange $(\alpha\,\beta)$. Examples of functions which belong to this subgroup are $(\alpha^2 + \beta^2)$, $(\alpha + \beta)$, γ, $\alpha\,\gamma + \beta\,\gamma$.

These functions of the roots cannot be expressed in terms of the coefficients a, b, c, without solving the equation, but they have the remarkable property that any one of them can be expressed in terms of any other, with the aid of the coefficients.

Thus $$(\alpha + \beta) = -\,a - \gamma,$$
$$(\alpha^2 + \beta^2) = (\alpha + \beta)^2 - 2\,\alpha\,\beta$$
$$= (a + \gamma)^2 - 2\,c/\gamma,$$
$$\alpha\,\gamma + \beta\,\gamma = -\,a\,\gamma - \gamma^2.$$

To express, say, γ in terms of $(\alpha^2 + \beta^2)$ is not so easy, but can nevertheless be accomplished. Thus

$$\gamma^2 = \alpha^2 + \beta^2 + \gamma^2 - (\alpha^2 + \beta^2) = a^2 - 2b - (\alpha^2 + \beta^2),$$

and since $$\gamma^3 + a\,\gamma^2 + b\,\gamma + c = 0,$$
then $$\gamma\,(\gamma^2 + b) = -\,a\,\gamma^2 - c,$$
so that $$\gamma = -\,(a\,\gamma^2 + c)/(\gamma^2 + b).$$

This expresses γ in terms of γ^2, which in its turn has already been expressed in terms of $(\alpha^2 + \beta^2)$.

Now there are three subgroups of the symmetric group, each of order two, and of the same type as the one we are considering. These are:

$$G_1;\ I,\ (\alpha\,\beta);$$
$$G_2;\ I,\ (\beta\,\gamma);$$
$$G_3;\ I,\ (\gamma\,\alpha).$$

Any of these subgroups can be transformed into any other by an operation of the symmetric group. They are called *conjugate subgroups*, and the set of three is a *class of conjugate subgroups.*

The other subgroup of the symmetric group of order six is the subgroup of order three consisting of the elements

$$G;\ I,\ (\alpha\,\beta\,\gamma),\ (\alpha\,\gamma\,\beta).$$

This is different because there is no other subgroup conjugate to it. Every transform of G gives the same subgroup G, and it is called a *self conjugate subgroup.*

An example of a function of the roots which belongs to this subgroup is

$$(\alpha-\beta)(\alpha-\gamma)(\beta-\gamma)=\alpha^2\beta+\beta^2\gamma+\gamma^2\alpha-\alpha\beta^2-\beta\gamma^2-\gamma\alpha^2.$$

The ratio of the order of the group to the order of the subgroup is called the *index* of the subgroup.

We will now consider how the properties of these subgroups can be used in the solution of equations.

It is well known that, in general, the solution of an algebraic equation of degree greater than one involves irrational numbers. Hence to find the solution, even of a quadratic, some process must be employed which obtains an irrational number. The simplest process which yields an irrational number is the extraction of roots, that is the finding of the square root, cube root or n-th root of a given number. We say that an equation is *solvable* if by finding n-th roots of numbers a certain number of times we can reach an expression which satisfies the equation. It is well known that any quadratic equation can be solved by the extraction of one square root. Hence the quadratic equation is solvable.

Now if those functions of the roots of an equation which correspond to a given group H are known, and the group H has a subgroup G of index r, then the functions which belong to the group G can be obtained by solving an equation of degree r. Further, if G is a self conjugate subgroup of H and r is a prime number, it can be shown that this equation can be put in the form

$$x^r=k,$$

and thus the step from the functions belonging to H to the functions belonging to G can be made by the extraction of one r-th root. Hence, if H is the symmetric group on n

symbols, we can solve the n-th degree equation if we can find a sequence of subgroups

$$H,\ G_1,\ G_2,\ .\ .\ .\ ,\ G_r = I$$

ending in the group of order one which consists of the identity, such that each group is an invariant subgroup of the preceding group, of prime index. Further, only when such a sequence of subgroups can be obtained is the general n-th degree equation solvable.

For the cubic equation such a sequence exists, for we can take H as the symmetric group, then G as the invariant subgroup of order 3, and finally the identity.

A function belonging to the group G is

$$D = (\alpha - \beta)\ (\alpha - \gamma)\ (\beta - \gamma) = \alpha^2 \beta + \beta^2 \gamma + \gamma^2 \alpha - \alpha \beta^2 - \beta \gamma^2 - \gamma \alpha^2.$$

Clearly D^2 is a symmetric function. This can be expressed in terms of a, b, c and is in fact

$$D^2 = -27c^2 - 4b^3 + a^2b^2 + 18abc - 4a^3c.$$

From this D is found by the extraction of the root, and since $\alpha^2 \beta + \beta^2 \gamma + \gamma^2 \alpha + \alpha \beta^2 + \beta \gamma^2 + \gamma \alpha^2$ is a symmetric function and hence is known, we can also find $\alpha^2 \beta + \beta^2 \gamma + \gamma^2 \alpha$, and all such functions as are unchanged when α, β, γ are permuted cyclically.

It is now required to find, say, $\alpha^2 \beta$ by the extraction of a cube root. The permutation S which permutes α, β, γ cyclically, satisfies $S^3 = I$. We therefore make it correspond to the complex number ω, which is a cube root of unity, $\omega = \frac{1}{2}(-1 + i\sqrt{3})$.

We obtain thus from $\alpha^2 \beta$ by the operator $(I + \omega S + \omega^2 S^2)$ the quantity

$$U = \alpha^2 \beta + \omega \beta^2 \gamma + \omega^2 \gamma^2 \alpha.$$

Then

$$\begin{gathered} U^3 = \alpha^6 \beta^3 + \beta^6 \gamma^3 + \gamma^6 \alpha^3 \\ + 3\ \omega\ \alpha \beta \gamma (\alpha^3 \beta^2 + \beta^3 \gamma^2 + \gamma^3 \alpha^2) \\ 3\ \omega^2\ \alpha \beta \gamma (\alpha^2 \beta^2 + \beta^2 \gamma^3 + \gamma^2 \alpha^3) \\ 6\ \alpha^3 \beta^3 \gamma^3. \end{gathered}$$

These expressions all belong to the group G and can all be evaluated. Further, since $\alpha^2 \beta$ belongs to the group of order one, each of α, β, γ can be expressed in terms of it.

Now this method would be a very clumsy and laborious method to use in practice. Neat and concise methods like the following are generally employed. For the general cubic

$$x^3 + a x^2 + b x + c = 0$$

replace $(x + \frac{1}{3} a)$ by x to obtain a cubic in which the term in x^2 is absent, say

$$x^3 + p x + q = 0.$$

Then if $x = y + z$ the equation can be written

$$y^3 + z^3 + 3 y z (y + z) + p (y + z) + q = 0.$$

Further, suppose that y and z are restricted so that

$$3 y z + p = 0.$$

Then

$$y^3 + z^3 = - q,$$
$$y^3 z^3 = - p^3/27,$$

so that y^3 and z^3 are the roots of

$$\lambda^2 + q \lambda - p^3/27 = 0$$

regarded as a quadratic equation in λ. When y^3 is found from this by the extraction of a square root, then y can be found from y^3 by the extraction of a cube root. Further $z = - p/3y$, and the three roots of the cubic are

$$y + z, \ \omega y + \omega^2 z, \ \omega^2 y + \omega z$$

where ω is the complex cube root of unity.

These two methods are, however, fundamentally the same. The second is just a simplified and neat form of the first. It applies only to the cubic, however, and has no application to any other equation.

The first method, however, is perfectly general and can be used to solve any solvable equation.

For the quartic equation with roots α, β, γ, δ, the appropriate group is the symmetric group on the four symbols α, β, γ, δ. The 24 operations of this group separate into five classes which correspond to the partitions of 4. The orders of the classes are as follows:

Class:	(1^4),	$(1^2 2)$,	(13),	(4),	(2^2).
Order:	1,	6,	8,	6,	3.

This symmetric group has a self-conjugate subgroup of order 12, which consists of the classes (1^4), (13) and (2^2). We denote the symmetric group by H, and this group of order 12, which is called the *alternating group*, by G_1.

The group G_1 has a self-conjugate subgroup of order 4, which we denote by G_2, which is composed of the elements from the classes (1^4) and (2^2), i.e. the elements I, $(\alpha\,\beta)\,(\gamma\,\delta)$, $(\alpha\,\gamma)\,(\beta\,\delta)$, $(\alpha\,\delta)\,(\beta\,\gamma)$. These elements are all self-conjugate in G_2, and hence there are self-conjugate subgroups of order 2, e.g. G_3 consisting of I and $(\alpha\,\beta)\,(\gamma\,\delta)$.

To solve a quartic equation with roots α, β, γ, δ we obtain first a function of the roots belonging to G_1. The simplest of such functions is

$$\begin{aligned}D = {} & \alpha^3\beta^2\gamma + \alpha^3\gamma^2\delta + \alpha^3\delta^2\beta + \beta^3\gamma^2\alpha + \beta^3\alpha^2\delta + \beta^3\delta^2\gamma \\ & + \gamma^3\alpha^2\beta + \gamma^3\beta^2\delta + \gamma^3\delta^2\alpha + \delta^3\alpha^2\gamma + \delta^3\gamma^2\beta + \delta^3\beta^2\alpha \\ & - \alpha^3\gamma^2\beta - \alpha^3\delta^2\gamma - \alpha^3\beta^2\gamma - \beta^3\alpha^2\gamma - \beta^3\delta^2\alpha - \beta^3\gamma^2\delta \\ & - \gamma^3\beta^2\alpha - \gamma^3\delta^2\beta - \gamma^3\alpha^2\delta - \delta^3\gamma^2\alpha - \delta^3\beta^2\gamma - \delta^3\alpha^2\beta \\ = {} & (\alpha-\beta)\,(\alpha-\gamma)\,(\alpha-\delta)\,(\beta-\gamma)\,(\beta-\delta)\,(\gamma-\delta).\end{aligned}$$

Then D^2 is clearly a symmetric function and can be expressed in terms of the coefficients in the equation, and extraction of the square root gives the value of D.

Putting $D = D_1 - D_2$ where these represent respectively the positive and negative terms, clearly $D_1 + D_2$ is a symmetric function expressible in terms of the known coefficients and hence can be found D_1 and D_2.

The simplest function* belonging to the group G_2 is $(\alpha\,\beta + \gamma\,\delta)$. This group is of index 3 in G_1 and the conjugate expressions are $(\alpha\,\gamma + \beta\,\delta)$, $(\alpha\,\delta + \beta\,\gamma)$. Hence put

$$Z = (\alpha\,\beta + \gamma\,\delta) + \omega\,(\alpha\,\gamma + \beta\,\delta) + \omega^2\,(\alpha\,\delta + \beta\,\gamma)$$

where ω is the complex cube root of unity $\frac{1}{2}(-1 + i\sqrt{3})$. Then

$$\begin{aligned}Z^3 = \Sigma\,\alpha^3\beta^3 + 3\,\Sigma\,\alpha^2\beta^2\gamma\,\delta + \omega\,[D_1 + 2\,\alpha\,\beta\,\gamma\,\delta\,\Sigma\,\alpha\,\beta] \\ \omega^2\,[D_2 + 2\,\alpha\,\beta\,\gamma\,\delta\,\Sigma\,\alpha\,\beta].\end{aligned}$$

This can be expressed in terms of the symmetric functions and D. Hence Z can be found by the extraction of a cube root. From Z the values of $(\alpha\,\beta + \gamma\,\delta)$, $(\alpha\,\gamma + \beta\,\delta)$, $(\alpha\,\delta + \beta\,\gamma)$ can be deduced.

To proceed to the group G_3 we put

$$w = \alpha\,\beta - \gamma\,\delta.$$

Then $w^2 = (\alpha\,\beta + \gamma\,\delta)^2 - 4\,\alpha\,\beta\,\gamma\,\delta$ is known, and the extraction of a square root gives the value of w, from which $\alpha\,\beta$ may be determined. The function $(\alpha + \beta)$ belonging to the

* Strictly, this function belongs to a group of order 8 which is mentioned below, and which includes G_2 as a subgroup. The other 4 operations are excluded, however, by the use of D.

same subgroup as $\alpha\beta$ can be expressed in terms of $\alpha\beta$, and the roots α and β are determined by solving the known quadratic equation

$$x^2 - (\alpha + \beta)\, x + \alpha\beta = 0.$$

This shows that any quartic equation can be solved by the extraction of roots. Once again, to use the above method as described to solve a given numerical quartic equation would prove awkward and cumbersome, but once it is known that an equation is solvable it is comparatively straightforward to devise a neater and more usable method.

In actual practice it is more convenient to proceed from the symmetric group to the group of order 8 comprising

$$I,\ (\alpha\,\beta),\ (\gamma\,\delta),\ (\alpha\,\beta)\ (\gamma\,\delta),\ (\alpha\,\gamma)\ (\beta\,\delta)$$
$$(\alpha\,\delta)\ (\beta\,\gamma),\ (\alpha\,\gamma\,\beta\,\delta),\ (\alpha\,\delta\,\beta\,\gamma).$$

This group is of index 3 in the symmetric group, but is not self-conjugate, and gives rise to a cubic equation called the *auxiliary cubic*. It is not of the form $y^3 = c$, since the subgroup is not self-conjugate, but is quite a general cubic equation. It is solvable since every cubic is solvable.

The group of order 8 has the self-conjugate subgroup consisting of I, $(\alpha\,\beta)$, $(\gamma\,\delta)$, $(\alpha\,\beta)\,(\gamma\,\delta)$. The transition to this subgroup is equivalent to the factorization of the quartic into two quadratics, from which the solution follows.

Thus if the quartic is

$$x^4 + 4\,a\,x^3 + 6\,b\,x^2 + 4\,d\,x + e = 0,$$

this is put in the form

$$(x^2 + 2\,a\,x + y)^2 - [(4a^2 + 2g - 6b)\,x^2 + (4ay - 4d)\,x + y^2 - e] = 0.$$

If y satisfies a certain cubic equation, the auxiliary cubic, then the expression in the square bracket becomes an exact square, so that the equation is of the form

$$(x^2 + 2ax + y)^2 - (px + q)^2 = 0,$$

whence the factorization and solution follows.

Notice that $y = \frac{1}{2}\,(\alpha\,\beta + \gamma\,\delta)$, which is a function of the roots belonging to the above group of order 8.

The appropriate group for the general quintic or fifth degree equation is the symmetric group of order $5! = 120$. This group has a self-conjugate subgroup of order 60, the alternating group. But it can be shown that this alternating group has no invariant subgroup. Hence the procedure fails,