BIQUADRATIC EQUATIONS WITH PRESCRIBED GROUPS

by

Benjamin Nelson Moyls

A Thesis submitted in Partial Fulfilment of

The Requirements for the Degree of

MASTER OF ARTS

in the Department

of

MATHEMATICS

accepted

The University of British Columbia

September, 1941.

TABLE OF CONTENTS

ACKNOWLEDGMENT

The writer wishes to express his thanks to Dr. Ralph Hull of the Department of Mathematics at the University of British Columbia for his advice and guidance. His numerous criticisms and suggestions proved invaluable in the preparation of this thesis.

Ben Moyls

Sept. 1941.

BIQUADRATIC EQUATIONS WITH

PRESCRIBED GROUPS

I. INTRODUCTION.

One of the problems of the Galois theory of equations is that of determining values in a field F, of the coefficients of an equation

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

such that the equation will have a specified Galois group with respect to F. In some cases, at least, it is possible to find parametric representations of the equations having a specified Galois group. This means that the coefficients $a_1, \ldots, a_n$, can be expressed in terms of parameters such that, when the parameters are assigned values in F, the resulting values of $a_1, \ldots, a_n$ are the coefficients of an equation which has the specified Galois group with respect to F, and with the further property that all such equations can be so obtained. The values which may be assigned to the parameters are usually not completely arbitrary, but are subject to restrictions which ensure that the equation shall actually have the specified Galois group and not a subgroup of it. In other cases it is convenient to employ two or more different sets of parameters, corresponding to different forms for the coefficients, which together give the totality of equations having the specified group.

Seidelmann [1] has found parametric representations for cubic equations with the cyclic group, and for biquadratic equations with various groups. He introduced appropriate parameters into the forms taken by the roots of the equations, according to the Galois group of the equation, and calculated the forms of the coefficients from these.

Another general method of attacking the problem, called the "rational" method in contrast with Seidelmanns "irrational" method, has been discussed by Frl. E. Noether [2]. She showed that the existence of a parametric form for the equations with a specified Galois group depends upon the existence of a minimal basis for the rational functions of n variables which are unaltered by the specified group of permutations of the variables. A minimal basis for such functions belonging to a group, or, briefly, a minimal basis for the group, is a set of rational functions of the variables which are:

(a) unaltered by the permutations of the group,

(b) algebraically independent,

(c) such that every rational function of the variables which is unaltered by the permutations of the group is expressible as a rational function of the basis functions. For example, the elementary symmetric functions of n variables form a minimal basis for the symmetric group of permutations of the variables. Seidelmann's results indirectly

---

1) Seidelmann, F; "Die Kub. und Biquad. Gleichungen mit Affekt" Math. Annalen, 1918, pp. 230-233.

2) Noether, E: "Gleichungen mit Vorgeschriebener Gruppen" Math. Annalen, 1918, pp. 221-229.

yield minimal bases for the groups he considers, and Breuer[3] has determined minimal bases for certain metacyclic groups.

It is the purpose of this thesis to apply the rational methods suggested by Noether to the determination of the reduced biquadratic equations

$$x^4 + a_2 x^2 + a_3 x + a_4 = 0, \qquad (2)$$

having specified Galois groups with respect to the field R of rational numbers. The groups to be studied are described in the next section. For each group in turn, a minimal basis is then exhibited, the coefficients of the equation are expressed in terms of the basis functions which serve as the required parameters, and then restrictions to be placed upon the values in R, which may be assigned to the parameters, are studied. Since the existence of one minimal basis for a group implies the existence of infinitely many, a variety of parametric forms for the equations can be obtained. The general plan has been followed of using a minimal basis which seems likely to yield especially simple parametric forms for the coefficients of the equations. In some cases alternative minimal bases must be employed, in order to obtain those equations having the specified groups which correspond to exceptional values for the parameters first employed. Certain of the minimal bases used were suggested by Noether, that for the cyclic group by Dr. Hull.

The results obtained are equivalent to those of Seidelmann, although in a different form which is simpler than his in some cases.

---

3) Breuer, S: "Matazyklische Minimalbasis und Komplexe Primzahlen" Journal für Mathematik, bd. 156, 1927, pp. 13-42.

Certain modifications of the forms would be required if a coefficient field other than R were used.

II. The Groups.

The Galois group of an irreducible biquadratic equation, with respect to the field R, is a transitive group of permutations on four variables. We confine attention to the equations which are said to have an "affect", that is, have a Galois group other than the symmetric group itself. We denote the variables, and the roots of a biquadratic equation by x_0, x_1, x_2 and x_3, and a permutation such as $(x_0 x_1 x_2)$ by (012), as usual. The groups to be considered are as follows:

(a) The Quartic Group (Die Vierergruppe):

$$Q : \left[I,\ (01)(23),\ (02)(13),\ (03)(12) \right]$$

(b) The Octic Groups:

$$O : \left[Q,\ Q(13) \right]$$

$$O' : \left[Q,\ Q(12) \right]$$

$$O'' : \left[Q,\ Q(23) \right]$$

(c) The Alternating Group:

$$A : \left[Q,\ Q(123),\ Q(132) \right]$$

(d) The Cyclic Groups:

$$C : \left[I,\ (0123),\ (02)(13),\ (0321) \right]$$

$$C' : \left[I,\ (0231),\ (03)(12),\ (0132) \right]$$

$$C'' : \left[I,\ (0312),\ (01)(23),\ (0213) \right]$$

There is no loss of generality or completeness in dealing only with the groups Q, O, A and C, since the groups O' and O'' are equivalent to O, and correspond merely to a re-numbering of the variables, and, similarly for C , C$'$ and C$''$. It it to be noted that C is the cyclic subgroup of order 4 of O.

III. Biquadratic Equations with the Quartic Group.

A basis for the Quartic group can be constructed as follows:

Let

$$
\begin{aligned}
4u_0 &= x_0 + x_1 + x_2 + x_3 \\
4u_1 &= x_0 + x_2 - x_2 - x_3 \\
4u_2 &= x_0 - x_1 + x_2 - x_3 \\
4u_3 &= x_0 - x_1 - x_2 + x_3
\end{aligned}
\qquad (3)
$$

Then

$$
\begin{aligned}
x_0 &= u_0 + u_1 + u_2 + u_3 \\
x_1 &= u_0 + u_1 - u_2 - u_3 \\
x_2 &= u_0 - u_1 + u_2 - u_3 \\
x_3 &= u_0 - u_1 - u_2 + u_3
\end{aligned}
\qquad (4)
$$

The permutations (01)(23), (02)(13), (03)(12) of x's in the group Q, send u_0, u_1, u_2, u_3 into u_0, u_1, $-u_2$, $-u_3$; u_0, $-u_1$, u_2, $-u_3$; and u_0, $-u_1$, $-u_2$, u_3, respectively. It follows that the basis functions

$$
\alpha_0 = u_0, \qquad \alpha_2 = \frac{u_3 u_1}{u_2},
$$

$$
\alpha_1 = \frac{u_2 u_3}{u_1}, \qquad \alpha_3 = \frac{u_1 u_2}{u_3}, \qquad (5)
$$

are unaltered by all the permutations of the x's in Q. The α's are easily seen to be algebraically independent since this is true of the x's and the u's. Finally, a rational function of the x's is a rational function of the u's, and is unaltered by all the permutations of Q if and only if the numerator and denominator consist of terms:

$$
t = c\, u_0^{e_0}\, u_1^{e_1}\, u_2^{e_2}\, u_3^{e_3},
$$

which are themselves unaltered by Q.

Under the permutations of Q, t becomes, respectively:

$$t,\ (-1)^{e_2+e_3}\,t,\ (-1)^{e_1+e_3}\,t,\ \text{and}\ (-1)^{e_1+e_2}\,t.$$

Hence, if t is unaltered by Q; (e_2+e_3), (e_1+e_3), (e_1+e_2) must all be even. Let $e_0 = f_0$, $e_2+e_3 = 2f_1$, $e_1+e_3 = 2f_2$, $e_1+e_2 = 2f_3$, where f_0, f_1, f_2, and f_3 are integers. Then evidently

$$t = c\,\alpha_0^{f_0}\alpha_1^{f_1}\alpha_2^{f_2}\alpha_3^{f_3}$$

This completes the proof that α_0, α_1, α_2, and α_3 form a minimal basis for Q.

To express the elementary symmetric functions of the x's in terms of the α's, we first determine:

$$\begin{aligned}
E_1 &= u_0 \\
E_2 &= 6u_0^2 - 2(u_1^2+u_2^2+u_3^2) \\
E_3 &= 4u_0^3 - 4u_0\,(u_1^2+u_2^2+u_3^2) + 8u_1u_2u_3 \\
E_4 &= (u_1^4+u_2^4+u_3^4) - 2(u_1^2u_2^2+u_1^2u_3^2+u_2^2u_3^2) \\
&\qquad + (\text{functions of } u_0)
\end{aligned} \tag{6}$$

But from equations (5):

$$\begin{aligned}
u_1^2 &= \alpha_2\alpha_3 \\
u_2^2 &= \alpha_3\alpha_1 \qquad\qquad u_1u_2u_3 = \alpha_1\alpha_2\alpha_3 \\
u_3^2 &= \alpha_1\alpha_2
\end{aligned} \tag{7}$$

Hence in terms of the α's

$$\begin{aligned}
E_2 &= 6\alpha_0^2 - 2(\alpha_1\alpha_2+\alpha_1\alpha_3+\alpha_2\alpha_3) \\
E_3 &= 4\alpha_0^3 - 4\alpha_0\,(\alpha_1\alpha_2+\alpha_1\alpha_3+\alpha_2\alpha_3) + 8\alpha_1\alpha_2\alpha_3 \\
E_4 &= (\alpha_1^2\alpha_2^2+\alpha_1^2\alpha_3^2+\alpha_2^2\alpha_3^2) - 2(\alpha_1^2\alpha_2\alpha_3+\alpha_2^2\alpha_3\alpha_1+\alpha_3^2\alpha_1\alpha_2) \\
&\qquad + (\text{powers of } \alpha_0)
\end{aligned} \tag{8}$$

Consider now a reduced biquadratic equation

$$x^4 + a_2x^2 + a_3x + a_4 = 0, \tag{2}$$

having the Quartic group Q with respect to R, and whose roots are x_0, x_1, x_2, and x_3. By the Galois theory, a function of the roots which is unaltered by Q has a rational value. In particular, the functions α_0, α_1, α_2, and α_3 have rational values, provided no single u_i is zero, $i = 1,2,3$. Hence with this restriction on the u's equation (2) can be expressed in the form

$$
\begin{aligned}
&x^4 + a_2 x^2 + a_3 x + a_4 = 0, \\
&\quad a_2 = -2\,(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3) \\
&\quad a_3 = -8\,\alpha_1\alpha_2\alpha_3 \qquad\qquad (9) \\
&\quad a_4 = (\alpha_1^2\alpha_2^2 + \alpha_1^2\alpha_3^2 + \alpha_2^2\alpha_3^2) - 2(\alpha_1^2\alpha_2\alpha_3 + \alpha_2^2\alpha_3\alpha_1 + \alpha_3^2\alpha_1\alpha_2)
\end{aligned}
$$

where the α's have values in R.

Conversely, suppose rational values are assigned to the α's in (9). Then, since the α's are functions of the x's, form a basis for the group Q, and are rational, it follows that every function belonging to Q has a rational value. Hence, by the Galois theory, the group of the equation in (9) is either Q or a subgroup of Q. The restrictions on the α's which exclude the latter possibility are most easily found by considering the roots of (9). These are

$$
\begin{aligned}
x_0 &= \sqrt{\alpha_2\alpha_3} + \sqrt{\alpha_1\alpha_3} + \sqrt{\alpha_1\alpha_2} \\
x_1 &= \sqrt{\alpha_2\alpha_3} - \sqrt{\alpha_1\alpha_3} - \sqrt{\alpha_1\alpha_2} \qquad (10) \\
x_2 &= -\sqrt{\alpha_2\alpha_3} + \sqrt{\alpha_1\alpha_3} - \sqrt{\alpha_1\alpha_2} \\
x_3 &= -\sqrt{\alpha_2\alpha_3} - \sqrt{\alpha_1\alpha_3} + \sqrt{\alpha_1\alpha_2}
\end{aligned}
$$

It is evident that no proper subgroup of Q is transitive; hence equation (9) is reducible in R if its group is a subgroup of Q. For example, if its group is $[I, (01)(23)]$, it is reducible into two quadratic factors such that $x_0 + x_1$, $x_0 x_1$, $x_2 + x_3$, $x_2 x_3$ are all rational. This means that $\alpha_2\alpha_3$ must be the square of some number in R. Similarly, if the group is $[I, (02)(13)]$, $\alpha_1\alpha_3$ must be a square; if $[I, (03)(12)]$, $\alpha_1\alpha_2$ must be a square; and if (I), $\alpha_2\alpha_3$, $\alpha_1\alpha_3$, $\alpha_1\alpha_2$, must all be squares. In other words, if the equation in (9) is to have the group C and not one of its subgroups, the product of any two of the α's must not be the square of a number in R.

We have chosen a minimal basis which gives, if not the simplest parametric representation of the coefficients of (2), at least a symmetric one. We have now to consider the possibility of the u's (u_1, u_2, u_3) vanishing. First it is obvious that no two u's can be zero simultaneously, for then (2) is reducible and cannot have the Quartic group. This is not the case, however, when only one of the u's is zero. Suppose, for example, $u_2 = 0$. We then have a singular[4)] value for the parameter α_2, which corresponds to a parametric representation for the group Q which is not included in (9). To cover this case we must consider an alternative basis:

$$\begin{aligned} \alpha_0' &= u_0, & \alpha_1' &= u_1^2, \\ \alpha_2' &= u_1 u_2 u_3 = 0, & \alpha_3' &= u_3^2, \end{aligned} \tag{12}$$

which leads to the parametric representation:[5)]

$$x^4 + 2(\alpha_1' + \alpha_3')x + (\alpha_1' - \alpha_3')^2 = 0 \tag{13}$$

where α_1' and α_3' range over all values in R for which $\alpha_1'\alpha_3'$ is not a square. It is clear that the cases where $u_1 = 0$ or $u_3 = 0$ lead to the same form of equation (13). Moreover, equation (13) is distinct from and supplementary to the equation in (9). We sum up the Quartic case then in

---

4) Cf. Noether: Op. Cit., p.229.

5) The procedure for deriving this formal representation and proving its validity is similar to that for (9).

Theorem 1: The equations

$$x^4 - 2(\Sigma\alpha_1\alpha_2)x^2 - 8\alpha_1\alpha_2\alpha_3\ x + (\Sigma\alpha_1^2\alpha_2^2 - 2\,\Sigma\alpha_1^2\alpha_2\alpha_3) = 0$$
$$x^4 + 2(\alpha_1' + \alpha_3')x^2 + (\alpha_1' - \alpha_3')^2 = 0 \tag{14}$$

together include all biquadratic equations with the Quartic group Q when $\alpha_1, \alpha_2, \alpha_3$; α_1', α_3' range over all values of R for which the product of any two α's, and the product of α_1', α_3' are not the squares of numbers in R.

IV. Biquadratic Equations with an Octic Group.

A rational function of x_0, x_1, x_2, x_3, which is unaltered by the Octic group $0 \equiv [Q, Q(13)]$, is also unaltered by the Quartic group Q. But in addition it is unaltered by the permutation (13) on the x's. Now such a function, as shown in Section III, is also a rational function of $\alpha_0, \alpha_1, \alpha_2, \alpha_3$. Moreover, since the permutation (13) on the x's merely interchanges α_1 and α_3, and does not alter α_0 and α_2, a rational function of the x's unaltered by 0 must be symmetric in α_1 and α_3, when expressed in terms of the α's. In other words it is expressible as a rational function of the symmetric functions $\alpha_1+\alpha_3$ and $\alpha_1\alpha_3$ of α_1 and α_3, with coefficients which are rational functions of α_0 and α_2. Hence the functions

$$\beta_0'' = \alpha_0, \qquad \beta_1'' = \alpha_1 + \alpha_3,$$
$$\beta_2'' = \alpha_2, \qquad \beta_3'' = \frac{\alpha_1\alpha_3}{\alpha_1+\alpha_3}, \quad \alpha_1 + \alpha_3 \neq 0 \tag{15}$$

form a minimal basis for 0. This basis was chosen because it was homogeneous; thus we hoped that it would lead to a fairly symmetric parametric representation of the coefficients of the reduced quartic equation (2). The results:

$$x^4 + a_2 x^2 + a_3 x + a_4 = 0$$
$$a_2 = -(\beta_1''\beta_2'' + \beta_1''\beta_3'')$$
$$a_3 = -8(\beta_1''\beta_2''\beta_3'') \qquad (16)$$
$$a_4 = (\beta_1''\beta_2'' - \beta_1''\beta_3'')^2 - 4\beta_1''\beta_2''^2\beta_3'',$$

whose derivation is similar to that of the case which follows, are, however, not general. For even when β_1'', β_2'', β_3'' take on all rational values (with certain restrictions to bar out subgroups of O), the totality of biquadratic equations with the group O is not represented by equation (16), since the exceptional case, $\alpha_1+\alpha_3=0$, is automatically excluded when we employ the basis (15). Moreover (2) may have the Octic group O when $\alpha_1+\alpha_3=0$.

Hence we use the functions:

$$\beta_0 = \alpha_0, \quad \beta_1 = \alpha_1 + \alpha_3,$$
$$\beta_2 = \alpha_2, \quad \beta_3 = \alpha_1\alpha_3, \qquad (17)$$

which by the same argument as that for (15), form a minimal basis for the group O.

Now suppose that x_0, x_1, x_2, and x_3 are the roots of a reduced biquadratic equation having the group O with respect to R. The functions β in (17) are unaltered by O, and hence have rational values, provided, as in Section III, no single u_i is zero. After constructing the elementary symmetric functions in terms of the β's, we see that, when no u is zero by itself, the equation having the Octic group with respect to R has the form:

$$x^4 + a_2 x^2 + a_3 x + a_4 = 0$$
$$a_2 = -2(\beta_1\beta_2 + \beta_3)$$
$$a_3 = -8\beta_2\beta_3 \qquad (18)$$
$$a_4 = \beta_3^2 + \beta_2^2(\beta_1^2 - 4\beta_3) - 2\beta_1\beta_2\beta_3$$

where the β 's are rational.

Conversely, an equation (15) with the β 's rational, has a Galois group with respect to R which is either O or a subgroup of O.

Now the proper subgroups of O which we need to consider are the Quartic, the Cyclic, and the group $K \equiv [I, (02), (13), (02)\times(13)]$; and subgroups of these. If the Galois group of (15) is the Quartic group Q or one of its subgroups, the functions $x_0x_1 + x_2x_3$, $x_0x_2 + x_1x_3$ and $x_0x_3 + x_1x_2$, which are incidentally the roots of the resolvent cubic of (15), must all be rational. In terms of the β 's, this means that $\beta_1^2 - 4\beta_3$ must be the square of a number in R. If the group of (15) is the Cyclic group C_4 or a subgroup of it, the function $x_0^2x_1 + x_1^2x_2 + x_2^2x_3 + x_3^2x_0$ must be rational; and if the group K, $x_0 + x_2 - x_1 - x_3$ must be rational.

The conditions on the β 's may be summed up by saying that, if equation (18) is to have the Octic group O and not one of its proper subgroups, then $\beta_1^2 - 4\beta_3$, $\frac{\beta_1^2}{\beta_3} - 4$, β_3 must not be the squares of numbers in R.

We must now consider the singular values of the parameters β which arise when any u vanishes. There is obviously no difficulty when $u_1 = 0$, or $u_3 = 0$, or any two of the u's equal zero simultaneously, for then the group of (18) is a subgroup of the Octic. Let us suppose then that u_2 alone vanishes. Employing the α''s defined in (12) we construct the basis functions:

$$\begin{aligned} \beta_0' &= \alpha_0', & \beta_1' &= \alpha_1' + \alpha_3' \\ \beta_2' &= \alpha_2'; & \beta_3' &= \alpha_1'\alpha_3' \end{aligned} \qquad (19)$$

It is easily verified that the β''s form a rational minimal basis for O which gives the parametric representation:

$$x^4+2\beta_1'x^2+(\beta_1'^2-4\beta_3') = 0 \qquad (20)$$

where β_1' and β_3' have rational values. To ensure that (20) has not a proper subgroup of 0 for its Galois group, $\beta_1'^2-4\beta_3'$ and β_3' must not be squares. To complete the Octic case then, we combine (18) and (20) in

Theorem 2: The equations

$$\begin{gathered} x^4-2(\beta_1\beta_2+\beta_3)x^2-8\beta_2\beta_3x+[\beta_3^2+\beta_2^2(\beta_1^2-4\beta_3)-2\beta_1\beta_2\beta_3]=0 \\ x^4+2\beta_1'x^2+(\beta_1'^2-4\beta_3')=0 \end{gathered} \qquad (21)$$

together include all biquadratic equations with the Octic group 0, when β_1, β_2 and β_3 ; β_1', β_3' range over all values of R for which $\beta_1^2-4\beta_3$, β_3 , $\frac{\beta_1^2}{\beta_3}-4$ and $\beta_1'^2-4\beta_3'$, β_3' are not the squares of numbers in R.

NOTE: It will be observed that the pure equation

$$x^4+a_4 = 0 \qquad (22)$$

has the Octic group when a_4 is not a square[6], and the Quartic group when a_4 is a square.

V. Biquadratic Equations with the Alternating Group.

As in the case of the Octic group, a rational function of the independent variables x_0, x_1, x_2, x_3 which is unaltered by the Alternating group, is also unaltered by the Quartic group. In addition, however, it is unaltered by the permutations (123), (132) on the x's. Moreover, this rational function of the x's is also a rational function of the α's; and since the cyclic permutations (123), (132) on the x's effect the same permutations on the α's, it follows that any rational function of the x's which is unaltered by the Alternating group may be

---

6) Cf. Seidelmann, F.; Op. Cit., p. 232.

expressed as a rational cyclic function of α_1, α_2 and α_3 with coefficients which are rational functions of α_0. We find it convenient to introduce the irrationality ω, where ω is a primitive cube root of unity.

Let

$$\begin{aligned} y_0 &= \alpha_0 \\ 3y_1 &= \alpha_1 + \alpha_2 + \alpha_3 \\ 3y_2 &= \alpha_1 + \omega\alpha_2 + \omega^2\alpha_3 \\ 3y_3 &= \alpha_1 + \omega^2\alpha_2 + \omega\alpha_3 \end{aligned} \qquad (22)$$

Solving for the α's:

$$\begin{aligned} \alpha_1 &= y_1 + y_2 + y_3 \\ \alpha_2 &= y_1 + \omega^2 y_2 + \omega y_3 \\ \alpha_3 &= y_1 + \omega y_2 + \omega^2 y_3 . \end{aligned} \qquad (23)$$

From what has been said above, it is clear that

$$\gamma_0 = y_0, \qquad \gamma_2 = y_2 y_3$$
$$\gamma_1 = y_1, \qquad \gamma_3 = y_2^3 + y_3^3 \qquad (24)$$

forms a rational minimal basis for the group A.

In terms of the γ's, the elementary symmetric functions of the x's turn out to be

$$\begin{aligned} E_2 &= -6(\gamma_1^2 - \gamma_2) \\ E_3 &= 8(\gamma_1^3 + \gamma_3 - 3\gamma_1\gamma_2) \\ E_4 &= -3[\gamma_1^4 - 4\gamma_1\gamma_3 + 3\gamma_2^2 - 3\gamma_1^2\gamma_2) \end{aligned} \qquad (25)$$

Now consider $x_0, x_1, x_2,$ and x_3 as the roots of a reduced biquadratic equation having the group A with respect to R. The functions γ in (24) are unaltered by A, and hence have rational values. We need make no provision here for any of the u's vanishing, for, if one of them vanishes it can be shown that equation (2) reduced to the form

$$x^4 + a_2 x^2 + a_4 = 0$$

which has either the Quartic or Octic group; and if two or more of

u_1, u_2 or u_3 vanish there is a still further reduction of the group. Hence an equation with the Alternating group A with respect to R has the form

$$
\begin{aligned}
&x^4 + a_2 x^2 + a_3 x + a_4 = 0 \\
&a_2 = -6(\gamma_1^2 - \gamma_2) \\
&a_3 = -8(\gamma_1^3 + \gamma_3 - 3\gamma_1\gamma_2) \qquad\qquad (26) \\
&a_4 = -3(\gamma_1^4 - 4\gamma_1\gamma_3 + 3\gamma_2^2 - 3\gamma_1^2\gamma_2)
\end{aligned}
$$

and conversely, an equation(26) with rational γ's has either the group A or a subgroup of A.

The possible subgroups of A which (26) may have are the Quartic group, and those four groups which are cyclic on three of the roots of (26).

If the group is the Quartic, the roots of the resolvent cubic of (26) must all be rational; if the group is one of the four groups which are cyclic on three of the roots, the other root must be rational and equation (26) reducible. We are now ready to state

Theorem 3: The equation

$$x^4 - 6(\gamma_1^2 - \gamma_2)x^2 - 8(\gamma_1^3 + \gamma_3 - 3\gamma_1\gamma_2)x - 3(\gamma_1^4 - 4\gamma_1\gamma_3 + 3\gamma_2^2 - 3\gamma_1^2\gamma_2) = 0 \qquad (27)$$

includes all biquadratic equations which have the alternating group A; $\gamma_1, \gamma_2, \gamma_3$ may take on all values in R for which (27) is irreducible, and for which the resolvent cubic equation of (27):

$$y^3 - a_2 y^2 - 4a_4 y + (4a_2 a_4 - a_3^2) = 0 \qquad (28)$$

with a_2, a_3, a_4 defined as in (26), has not all three roots rational.

As a point of interest we mention a perhaps more practical criterion for fourth degree equations with the alternating group. If the Galois group of equation (2) is the alternating group A for the field R, then the square root of the discriminant of (2), namely,

$$P = (x_0 - x_1)(x_0 - x_2)(x_0 - x_3)(x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$$

must have a rational value; and conversely, if P has a rational value, it is unchanged by the Galois group of (2), which must thus be the Alternating group A or one of its subgroups. Hence

Theorem 4: The equation

$$x^4 + a_2 x^2 + a_3 x + a_4 = 0 \qquad (2)$$

embraces all biquadratic equations with the Alternating group when the a's take on all values in R for which:

(a) the discriminant $\Delta = 4(4a_4 - \frac{1}{3}a_2^2)^3 - 27(\frac{8}{3}a_2 a_4 - a_3^2 - \frac{2}{27}a_2^3)^2$ is equal to the square of a number in R,

(b) equation (2) has no rational root, and

(c) the resolvent cubic has not all its roots rational.

VI. Biquadratic Equations with a Cyclic Group.

In order to construct a minimal basis for the cyclic group $C \equiv [\, I, (0123), (02)(13), (0321)\,]$, it is convenient to introduce, temporarily, the irrationality i, where $i = \sqrt{-1}$.

Let

$$\begin{aligned} 4z_0 &= x_0 + x_1 + x_2 + x_3 \\ 4z_1 &= x_0 + ix_1 - x_2 - ix_3 \\ 4z_2 &= x_0 - x_1 + x_2 - x_3 \\ 4z_3 &= x_0 - ix_1 - x_2 + ix_3 \end{aligned} \qquad (29)$$

Then

$$\begin{aligned} x_0 &= z_0 + z_1 + z_2 + z_3 \\ x_1 &= z_0 - iz_1 - z_2 + iz_3 \\ x_2 &= z_0 - z_1 + z_2 - z_3 \\ x_3 &= z_0 + iz_1 - z_2 - iz_3 \end{aligned} \qquad (30)$$

The permutation $S = (0123)$, which generates C, carries z_0, z_1, z_2, and z_3

into $z_0, -iz_1, -z_2$, and iz_3, respectively. By means of the z's, it is easy to construct functions of the x's which are unaltered by S, and hence by C; for example, the functions;

$$z_2^2,\ z_1^4,\ z_3^4,\ z_1^2/z_2,\ z_3^2/z_2,\ z_1^2 z_2,\ z_3^2 z_2,\ z_1 z_3.$$

All of these functions of the x's have coefficients in R (i), but not all coefficients are in R. We first find a minimal basis for the rational functions $\Phi(x)$ of the x's, unaltered by C, with coefficients in R (i); and subsequently, find a minimal basis consisting of functions with coefficients in R.

It is clear, by (2), that a function $\Phi(x)$ is expressible as a rational function of the z's with numerator and denominator consisting of terms of the form

$$t = cz_0^{e_0}\ z_1^{e_1}\ z_2^{e_2}\ z_3^{e_3}$$

which are unaltered by C. The permutations $S = (0123)$, S^2, S^3 send t into $(-1)^{e_2}(i)^{-e_1+e_3}\ t$, $(-1)^{e_1+e_3}t$, and $(-1)^{e_2}(i)^{e_1-e_3}\ t$; respectively. Since t is unaltered by C, we must have $(e_1 + e_3)$ and thus $(e_1 - e_3)$, and $(e_2 \pm \frac{e_1-e_3}{2})$ even. Let $e_1 + e_3 = 2f_2$, $e_2 + \frac{e_1 - e_3}{2} = 2f_1$, $e_2 - \frac{e_1-e_3}{2} = 2f_3$,

Then $$t = c\ z_0^{e_0}\ (z_1 z_3)^{e_1-2f_1} (z_1^2 z_2)^{f_1} (z_3^2 z_2)^{f_3}$$

It follows that the functions

$$\varphi_0 = z_0,\quad \varphi_2 = z_1 z_3,\quad \varphi_1 = z_1^2 z_2,\quad \varphi_3 = z_3^2 z_2 \qquad (31)$$

which are themselves unaltered by C, and are readily seen to be algebraically independent since the z's are, form a minimal basis for the functions $\Phi(x)$.

It is now not difficult to construct, by means of the φ's, the required minimal basis, with rational coefficients, for the group C. First, it is clear that the functions:

$$\sigma_0 = \varphi_0, \qquad \sigma_1 = \tfrac{1}{2}\left[(1+i)\varphi_1 + (1-i)\varphi_3\right]$$
$$\sigma_2 = \varphi_2, \qquad \sigma_3 = \tfrac{1}{2}\left[(1-i)\varphi_1 + (1+i)\varphi_3\right] \tag{32}$$

also form a minimal basis for the functions $\Phi(x)$. Moreover, the σ's as functions of the x's, have coefficients in R. This is easily verified for $\sigma_0 = \varphi_0$ and $\sigma_2 = \varphi_2$, and is true for σ_1 and σ_3 since the replacement of i by -i in the coefficients of the x's interchanges z_1 and z_3, leaves z_2 unaltered, and hence interchanges φ_1 and φ_3.

Let f(x) be a rational function of the x's with rational coefficients. Then f(x) is also a $\Phi(x)$, and hence is a rational function of the φ's with coefficients in R(i). Such a function of the φ's evidently has rational coefficients, as a function of the x's, if and only if it is unaltered by the replacement of i by -i. Let $t = d\,\varphi_0^{g_0}\varphi_1^{g_1}\varphi_2^{g_2}\varphi_3^{g_3}$ be a term of the numerator or denominator of f(x), and let $\bar{t}$ be the expression obtained from t by the replacement of i by -i. Then $\bar{t} = \bar{d}\,\varphi_0^{g_0}\varphi_1^{g_3}\varphi_2^{g_2}\varphi_3^{g_1}$, where $\bar{d}$ is the conjugate of d in R(i). If t has rational coefficients, as a function of the x's, $t=\bar{t}$; whence $d=\bar{d}$, $g_1 = g_3$. Thus $t = d\,\varphi_0^{g_0}\varphi_2^{g_2}(\varphi_1\varphi_3)^{g_1} = d\,\sigma_0^{g_0}\sigma_2^{g_2}\left(\frac{\sigma_1^2+\sigma_3^2}{4}\right)^{g_1}$

which is a rational function of the σ's with rational coefficients. If $t \neq \bar{t}$, then the numerator, or denominator, of f(x) must contain $\bar{t}$ when it contains t; that is, it contains

$$t + \bar{t} = \varphi_0^{g_0}\varphi_2^{g_2}\left(d\,\varphi_1^{g_1}\varphi_3^{g_3} + \bar{d}\,\varphi_1^{g_3}\varphi_3^{g_1}\right)$$

It is a simple matter to show that the expression in parenthesis is a polynomial in σ_1 and σ_3 with rational coefficients. This completes the proof that the σ's form a rational minimal basis for C, since f(x) is thus expressible as a rational function of the σ's.

In terms of the z's, the elementary symmetric functions of the x's are:

$$E_2 = 6z_0^2 - 2z_2^2 - 4z_1 z_3$$

$$E_3 = 4z_0^3 - 4z_0(z_2^2 + 2z_1 z_3) + 4z_2(z_1^2 + z_3^2) \tag{33}$$

$$E_4 = z_0^4 - 2z_0^2(z_2^2 + 2z_1 z_3) + 4z_0 z_2(z_1^2 + z_3^2) + (z_2^2 - 2z_1 z_3)^2 - (z_1^2 + z_3^2)^2$$

Thus

$$E_2 = -\left[\frac{\sigma_1^2 + \sigma_3^2}{2\sigma_2^2} + 4\sigma_2\right]$$

$$E_3 = 4(\sigma_1 + \sigma_3) \tag{34}$$

$$E_4 = \left[\left(\frac{\sigma_1^2 + \sigma_3^2}{4\sigma_2^2} - 2\sigma_2\right)^2 - \frac{4\sigma_2^2(\sigma_1 + \sigma_3)^2}{(\sigma_1^2 + \sigma_3^2)}\right]$$

Now let x_0, x_1, x_2, x_3 be the roots of the reduced biquadratic equation

$$x^4 + a_2 x^2 + a_3 x + a_4 = 0, \tag{2}$$

whose group with respect to R is C. It is clear that the σ's are functions of the roots, which are unchanged by the permutations of C and therefore have rational values. Hence the coefficients of (2) can be expressed in the form

$$a_2 = -\left[\frac{\sigma_1^2 + \sigma_3^2}{2\sigma_2^2} + 4\sigma_2\right]$$

$$a_3 = -4(\sigma_1 + \sigma_3) \tag{35}$$

$$a_4 = \left[\left(\frac{\sigma_1^2 + \sigma_3^2}{4\sigma_2^2} - 2\sigma_2\right)^2 - \frac{4\sigma_2^2(\sigma_1 + \sigma_3)^2}{(\sigma_1^2 + \sigma_3^2)}\right]$$

where the σ's have values in R.

As in the case of the Quartic group, it is readily shown that, conversely, if rational values are assigned to the σ's in (35), the group of equation (2) is either C or one of its subgroups.

The only proper subgroup of C which we need to consider is the intransitive group $[I, (02)(13)]$. If (2) is to have this group, then it must be reducible into two quadratic factors such that $x_0 + x_2$, $x_0 x_2$, $x_1 + x_3$, $x_1 x_3$ are all rational. This leads to a restriction on the σ's which is included in

<u>Theorem 4:</u> The equation

$$x^4 - \left[\frac{\sigma_1^2+\sigma_3^2}{2\sigma_2^2} + 4\sigma_2\right]x^2 - 4(\sigma_1+\sigma_3)x + \left[\left(\frac{\sigma_1^2+\sigma_3^2}{4\sigma_2^2} - 2\sigma_2\right)^2 - \frac{4\sigma_2^2(\sigma_1+\sigma_3)^2}{(\sigma_1^2+\sigma_3^2)}\right] = 0 \quad (36)$$

ranges over all fourth degree equations with the cyclic group C when σ_1, σ_2, σ_3 are assigned all values in R such that $\left[\frac{\sigma_1^2+\sigma_3^2}{4\sigma_2^2}\right]$ is not the square of a number in R.

BIBLIOGRAPHY

1. Seidelmann, F: "Die Gesamtheit der kubischen und biquadratischen Gleichungen mit Affekt bei beliebigen Rationalitätsbereich."

Mathematische Annalen, 1918, pp. 230-233.

2. Noether, E: "Gleichungen mit Vorgeschriebener Gruppen"

Mathematische Annalen, 1918, pp. 221-229.

3. Breuer, S: "Metazyklische Minimalbasis und complexe Primzahlen"

Journal für Mathematik, bd. 156, 1927, pp. 13-42.

4. Dickson, L.E: "Modern Algebraic Theories."

Benj. Sanborne & Co., New York, 1930.

5. Carmichael, R.D: "Introduction to Theory of Groups of Finite Order.

Ginn and Co., New York, 1937.