NOTE ON IRREDUCIBLE QUARTIC CONGRUENCES*

BY

H. R. BRAHANA

Introduction. In the study of the metabelian subgroups in the holomorph of the abelian group of order p^n and type 1, 1, $\cdots$ it becomes necessary to classify irreducible quartic congruences belonging to the modular field defined by the prime p under the group of linear fractional transformations with coefficients belonging to the same field.† This classification is offered here because it does not depend on the group problem from which it arose, and because it is believed that the results should have application in many other connections.

The case $p=2$ is excluded from consideration; it usually requires special treatment. The case $p=3$ must also be excluded from any argument that depends on (3) or the form of the general quartic which follows (3). The theorem at the end of §1, which is established by an argument which is principally geometric, is valid for all odd primes. It is easy to show that when $p=3$ any irreducible quartic is conjugate to x^4+x+2 or to x^4+x^2+2.

1. Classification of quartics. We consider the irreducible quartic

$$x^4 - \gamma x^2 + \alpha x - \beta \equiv 0 \pmod{p}, \tag{1}$$

where α, β, γ are residues of the integers, mod p, and the group of linear fractional transformations

$$x = (ax' + b)/(cx' + d), \tag{2}$$

where a, b, c, d are in the same modular field. The congruence (1) defines a Galois field $GF(p^4)$ in which every quartic and every quadratic belonging to the $GF(p)$ is reducible. If λ is a root of (1), then its four roots are $\lambda, \lambda^p, \lambda^{p^2}, \lambda^{p^3}$. The marks of $GF(p^4)$ may be considered as points of a line, and (2) is a projective transformation of that line into itself. Any quartic into which (1) may be transformed by (2) has roots $\mu, \mu^p, \mu^{p^2}, \mu^{p^3}$ whose cross ratio is the same as that of the roots of (1). All six cross ratios σ of the roots of (1), corresponding to the ways in which $\lambda, \lambda^p, \lambda^{p^2}, \lambda^{p^3}$ may be arranged, satisfy the relation

$$I^3/J^2 = 108(1 - \sigma + \sigma^2)^3/[(\sigma + 1)^2(\sigma - 2)^2(2\sigma - 1)^2], \tag{3}$$

---

* Presented to the Society, April 6, 1934; received by the editors July 7, 1934.

† The connection between the two problems is indicated in the paper *On cubic congruences* which appears in the Bulletin of the American Mathematical Society, vol. 39 (1933), pp. 962–969.

where I and J are semi-invariants of (1).* For convenience we give the definitions of I and J for the quartic

$$a_0x^4 + 4a_1x^3 + 6a_2x^2 + 4a_3x + a_4 \equiv 0.$$

They are

$$(4) \qquad \begin{aligned} I &= a_0a_4 - 4a_1a_3 + 3a_2^2, \\ J &= a_0a_2a_4 - a_0a_3^2 - a_1^2a_4 + 2a_1a_2a_3 - a_2^3. \end{aligned}$$

Now since I and J are polynomials in the coefficients of the quartic, the absolute invariant $i = I^3/J^2$ of (1) is in the $GF(p)$, or, if $I \neq 0$ and $J = 0$, is infinity. If both I and J are zero, (1) has equal roots and in such quartics we are not interested here. Two quartics which are conjugate under the group (2) have the same absolute invariant i, and i may conceivably take on any one of the values $0, 1, 2, \cdots, p-1, \infty$.

We shall show first that two irreducible quartics belonging to the $GF(p)$ and having the same σ are conjugate under the group (2). Let λ and μ be respective roots of the two quartics. Then

$$(5) \qquad \mu = k_0 + k_1\lambda + k_2\lambda^2 + k_3\lambda^3,$$

where the k's are integers. The condition that there exist a transformation (2) which puts λ into μ is

$$k_0 + k_1\lambda + k_2\lambda^2 + k_3\lambda^3 \equiv (a\lambda + b)/(c\lambda + d).$$

Clearing of fractions, making use of the fact that λ is a root of (1) and of no congruence of lower degree with integer coefficients, we obtain a system of linear homogeneous congruences in a, b, c, d. The condition that the system have a solution different from 0, 0, 0, 0 is

$$(6) \qquad k_1k_3 + \gamma k_3^2 - k_2^2 \equiv 0.$$

Conversely, if (6) is satisfied there exists a solution with a, b, c, d all integers. The determinant of the transformation in the general case is

$$d^2(k_2^4 - \gamma k_2^2k_3^2 + \alpha k_2k_3^3 - \beta k_3^4)/(k_2^2k_3),$$

which cannot be zero unless k_2 and k_3 are both zero, or d is zero. If both k_2 and k_3 are zero, we have the solution $a = k_1$, $b = k_0$, $c = 0$, $d = 1$. If $d = 0$, a, b, and c cannot all be zero and hence $k_2 = 0$. In this case the determinant is $-bc = -\beta k_3c^2$ which is zero only if $k_3 = 0$. Consequently, if μ is not an integer and (6) is satisfied, there exists a non-singular transformation (2) with integer coefficients which puts λ into μ.

* Cf. Clebsch, *Theorie der Binären Algebraischen Formen*, Leipzig, 1872, p. 170. The difference in coefficients comes from the definitions of I and J given below.

Now since the coefficients of (2) are integers, if (2) transforms λ into μ it transforms λ^p into μ^p, etc., and consequently transforms (1) into the second quartic under consideration. Let us define the cross ratio of the ordered set $\lambda, \lambda^p, \lambda^{p^2}, \lambda^{p^3}$ as

$$\sigma(\lambda) = (\lambda - \lambda^p)(\lambda^{p^2} - \lambda^{p^3})/[(\lambda - \lambda^{p^3})(\lambda^{p^2} - \lambda^p)]. \tag{7}$$

If we set $\sigma(\lambda) = \sigma(\mu)$, substitute for μ from (5), and make use of the fact that λ is a root of (1), we obtain (6). Consequently, if μ is such that $\sigma(\lambda) = \sigma(\mu)$, then (6) is satisfied and there exist integers a, b, c, d such that (2)transforms λ into μ.

From the definition of $\sigma(\lambda)$ in (7) it is obvious that $\sigma(\lambda^{p^2}) = \sigma(\lambda)$, and that $\sigma(\lambda^p) = \sigma(\lambda)$ if and only if $\sigma(\lambda)$ is -1. Consequently every irreducible quartic is transformed into itself by an operator of order two of the group (2), and every irreducible quartic for which $\sigma(\lambda) = -1$ is transformed into itself by an operator of order four of the group (2). No operator of (2) other than those just described and powers of them can transform an irreducible quartic into itself, for if $T(x)$ is an operator of (2) and $T(\lambda) = \mu$, then $T(\lambda^p) = \mu^p$.

The order of (2) is $p(p^2-1)$. Every irreducible quartic such that $\sigma(\lambda) \neq -1$ is one of a set of $p(p^2-1)/2$ conjugates under (2). Let the number of such sets be k. Each other irreducible quartic belongs to a set of $p(p^2-1)/4$ conjugates, and there is not more than one such set. The number of irreducible quartics is $p^2(p^2-1)/4$.* From the relation

$$kp(p^2 - 1)/2 + mp(p^2 - 1)/4 = p^2(p^2 - 1)/4$$

where $m = 0$ or 1, it follows that $m = 1$ and $k = (p-1)/2$. We state the principal result in the following theorem:

The irreducible quartics belonging to a $GF(p)$ constitute $(p+1)/2$ sets of conjugates under the linear fractional group with coefficients in the $GF(p)$.

2. **Characterization in terms of the absolute invariant.** We have characterized the $(p+1)/2$ types of irreducible quartic in terms of the cross ratio of the roots in a given cyclic order. It follows from (3) that the absolute invariant i of an irreducible quartic is restricted to a set of not more than $(p+1)/2$ of the numbers $0, 1, 2, \cdots, p-1, \infty$. We shall show that two irreducible quartics of different types have different values for i, and therefore that the $(p+1)/2$ types are characterized by exactly $(p+1)/2$ values of the absolute invariant.

Since $[\sigma(\lambda)]^{p^2} = \sigma(\lambda^{p^2}) = \sigma(\lambda)$, it follows that $\sigma(\lambda)$ is always in the $GF(p^2)$ contained in the $GF(p^4)$ defined by the irreducible quartic. Also, since

* Dickson, *Linear Groups*, Leipzig, 1901, p. 18.

$[\sigma(\lambda)]^p = \sigma(\lambda^p)$ and is equal to $\sigma(\lambda)$ only if $\sigma(\lambda) = -1$, it follows that $\sigma(\lambda)$ is an integer only if $\sigma(\lambda) = -1$. When $\sigma(\lambda) = -1$, then $i = \infty$; the other possible values of $\sigma(\lambda)$ for $i = \infty$ are 2 and 1/2, neither of which can be the $\sigma(\lambda)$ of an irreducible quartic, being integers. There is therefore just one type with $i = \infty$, and we may confine our attention to the other $(p-1)/2$ types and assume that $\sigma(\lambda)$ is not an integer.

If our conjecture that the type is determined by the value of i is correct then of the six values of σ obtained by using a suitable value of i in (3) it should be possible to isolate two, either of which could be the $\sigma(\lambda)$ of an irreducible quartic. Let us suppose (3) to be written as a sextic polynomial equal to zero. Since the irreducible quartic has no multiple root and since harmonic quartics were disposed of in the preceding paragraph, it follows that the sextic we are dealing with now is one which corresponds to the "general" quartic or else to the equianharmonic quartic. The sextic has six distinct roots or two triple roots. Since σ is not an integer and is in the $GF(p^2)$, the sextic polynomial is the product of three quadratic factors belonging to and irreducible in the $GF(p)$. Let λ_1 be a root of the quartic and denote $\sigma(\lambda_1)$ by σ_1. Then $\sigma(\lambda_1^p) = 1/\sigma_1$. Since the sum of σ_1 and $1/\sigma_1$ is equal to its pth power it is in the $GF(p)$. Hence σ_1 and $1/\sigma_1$ satisfy a quadratic relation with integer coefficients. Since the sum of $(1-\sigma_1)$ and $1/(1-\sigma_1)$ has for a pth power the sum of $\sigma_1/(\sigma_1-1)$ and $(\sigma_1-1)/\sigma_1$, it follows that neither pair satisfies a quadratic relation with integer coefficients unless we are dealing with the equianharmonic case. Hence, if the sextic is written with 1 for the coefficient of σ^6, just one of its irreducible quadratic factors has the constant term equal to 1 or else the sextic is the cube of a quadratic. In either case the zeros of the quadratic factor with the constant term 1 are the two possible values of the cross ratio of $\lambda, \lambda^p, \lambda^{p^2}, \lambda^{p^3}$, where λ is a root of an irreducible quartic. Therefore,

Two irreducible quartics with the same value of the absolute invariant are conjugate under (2).

It follows from this theorem that there are $(p+1)/2$ values of i, including ∞, such that there exist irreducible quartics having those values of i. Any quartic with integer coefficients having for i a number not among those $(p+1)/2$ values is necessarily reducible. This agrees with the statement of the conditions for irreducibility of a quartic given by Dickson.* It is of some interest to note that there exists a quartic of the form (1) having for its ab-

* *Criteria for the irreducibility of functions in a finite field*, Bulletin of the American Mathematical Society, vol. 13 (1906), p. 7.

solute invariant any given integer or infinity, and to see why for certain values of i such a quartic is reducible.

Let us suppose that I and J are any two integers, and let us write (1) in the form

$$x^4 + 6a_2x^2 + 4a_3x + a_4 \equiv 0.$$

If we use (4) to express a_3 and a_4 in terms of a_2, I, and J, we have

$$a_4 = I - 3a_2^2, \text{ and } a_3^2 = Ia_2 - 4a_2^3 - J.$$

Writing the second congruence as

$$a_2^3 - Ia_2/4 + (J + a_3^2)/4 \equiv 0,$$

we note that as a_3 is allowed to run through the numbers of the $GF(p)$ we have $(p+1)/2$ cubic congruences of which no more than $(p+1)/3$ can be irreducible.* Hence, a_3 may be selected and then a_2 and a_4 determined so that the resulting quartic has the semi-invariants I and J. If I is fixed and J runs through the values $0, 1, 2, \cdots, p-1$ then i runs through the non-zero squares if I is a square or the not-squares if I is a not-square. If I, J, is $0, 1$, or $1, 0$ then i is 0 or ∞. An easy computation shows that there are exactly $(p-1)/2$ integers such that if i takes any one of those values the sextic is the product of two irreducible cubics or the product of six linear functions with integer coefficients.

The values of i which are suitable for irreducible quartics are readily determined from the fact that the discriminant of the quartic must be a not-square,† viz., I^3-27J^2 is a not-square. Since $I^3=iJ^2$, it follows that $i-27$ must be a not-square. As i runs through the numbers of the $GF(p)$, $(p-1)/2$ such i's are obtained, and the remaining one is $i=\infty$.

3. **Determination of a quartic of a given type.** Having given an i for which there exists an irreducible quartic it does not follow that every quartic having that value of i is irreducible. I and J may be selected in many ways. J may always be selected so that $-J$ is a square in the $GF(p)$. Then consider the quartic

$$x^4 + 4(-J)^{1/2}x + I \equiv 0. \tag{8}$$

It has semi-invariants I and J. The condition that it be reducible is found from Ferrari's method of solution of the quartic. The resolvent cubic is

$$t^3 - 4It + 16J \equiv 0. \tag{9}$$

---

* Cf. *On cubic congruences*, loc. cit., p. 968.

† Dickson, the second reference preceding.

This congruence is reducible and has one integral root t_1. The condition that (8) be reducible is that t_1 be a square if $i \neq \infty$, or that $-I$ be a square if $i = \infty$. In the latter case a proper choice of I makes (8) irreducible.

Suppose $i \neq \infty$ and (8) reducible. Then consider

$$x^4 + 6a_2x^2 + 4a_3x + a_4 \equiv 0, \tag{10}$$

where $a_4 = I - 3a_2^2$, and $a_3^2 = Ia_2 - 4a_2^3 - J$, the I and J being the same as in the last paragraph. The resolvent cubic of (10) may be readily shown to have the root $t_1 + 2a_2$, and (10) is reducible if $t_1 - 4a_2$ is a square. Since t_1 depends only on I and J there are $(p-1)/2$ values of a_2 such that $t_1 - 4a_2$ is not a square. Any of these values which makes the quantity $Ia_2 - 4a_2^3 - J$ a square in the $GF(p)$ gives an irreducible congruence (10) with integer coefficients. Since irreducible congruences with the given i have been shown to exist and since every quartic can be transformed into the form (10) by means of an operator of (2) it follows that a number a_2 exists satisfying the given conditions. We have thus a straightforward method of writing a member of each of the $(p+1)/2$ conjugate sets of irreducible quartics.

UNIVERSITY OF ILLINOIS,
URBANA, ILL.