Value sets of functions over finite fields

by

S. D. Cohen (Glasgow)

1. Introduction and general results. Let \( F \) be a finite field of order \( q \) and characteristic \( p \). Where necessary adjoin \( \infty \) to \( F \) as a possible value of a variable or function in the obvious way (see [2], \S\ 4). For any rational function \( f = f_1/f_2 \) in \( E(x) \), where \( f_1 \) and \( f_2 \) are co-prime polynomials, define \( V(f) \) to be the set of values taken by \( f \) in \( F \) and \( \deg f \), the degree of \( f \), to be \( \max(\deg f_1, \deg f_2) \).

Our chief object in this paper is to discuss the extent to which a function \( f \) of bounded degree is determined by \( V(f) \). More precisely, we consider when \( V(y) \subseteq V(f) \) can hold for two functions \( f \) and \( g \). In fact, we solve the problem completely for functions \( f \) of degree not exceeding \( 4 \). For details of the results see \S\ 2.

The remainder of this section is devoted to a summary of the various general results which bring together and extend work discussed by the author in [1] and [2] and by M. Fried in [6], [8] and [10] and which form the abstract background from which the specific functions of \S\ 2 will emerge.

Accordingly, let \( h(x, y) \) be a polynomial in \( x \) with coefficients in \( F(y) \). We shall say that \( h \) is \( x \)-soluble (in \( F \)) if, for every \( y \) in \( F \), \( h(x, y) = 0 \) is soluble with \( x \) in \( F \). For the application to value sets we shall set \( h(x, y) = f_1(x) - g(x)f_2(x) \), where \( f = f_1/f_2 \) and \( g \) are rational functions in \( E(x) \). (We shall frequently abuse notation and write \( f(x) - g(y) \) for this polynomial or even for the numerator of the rational function \( f(x) - g(y) \).)

Returning to the case of a general \( h \), which need not even be irreducible, we outline a proof of the following result.

Proposition 1.1. Let \( h(x, y) \) be a separable polynomial of degree \( m \) in \( x \) with coefficients in \( F(y) \) of degree \( \leq n \). Let \( h(x, y) = 0 \) have roots \( \alpha_1, \ldots, \alpha_m \) in a splitting field \( K \) over \( F(y) \). Let \( \bar{F} \) denote the algebraic closure of \( F \) in \( K \) and \( G(K, F(y)) \), etc., the subset of the galois group \( G(K, F(y)) \)
of \( K \) over \( F(y) \) comprising automorphisms whose restrictions to \( F \) fix precisely \( F \). If

\[
G^s(K, F(y)) = \bigcup_{i=1}^m G^s_i(K, F(x, y)),
\]

then \( h \) is \( x \)-soluble. Conversely, if \( g > 0(m, n) \) and \( h \) is \( x \)-soluble, then \((1.1)\) holds.

Proof. We can assume that \( h \) is square-free. For brevity, put \( G = G(K, F(y)), G^s = G^s(K, F(y)) \), \( G^s_i = G^s_i(K, F(x, y)) \), \( i = 1, \ldots, m \), \( G^s = \bigcup_{i=1}^m G^s_i \). Also, for any \( y_0 \) in \( F \), let \( A(y_0) \) denote the conjugacy class in \( G \) which has the defining property of the Frobenius automorphism of some prime in \( K \) dividing \( y_0 \). Clearly \( A(y_0) \) exists; it is uniquely defined if \( y - y_0 \) is unramified in each \( F(x, y) \), i.e., if \( h(x, y) \) is square-free. Then, in fact, \( A(y_0) \subseteq G^s \) and indeed, \( G^s \) is unramified if and only if \( h(x, y) = 0 \) is soluble in \( F \). (see Lemma 3 of [1] and [2]). Moreover, even if \( y - y_0 \) is ramified, then \( h(x, y) = 0 \) is soluble in \( F \) if and only if \( h(x, y) = 0 \) is soluble in \( F \) (see Lemma 3 of [1] and [2]). Hence, \((1.1)\) holds.

Actually, in the last sentence of the above proof, it suffices to assume that \( h \) is \( x \)-soluble with, at most, \( k \)-soluble exceptions where \( 0 \leq k < 1 \) (see [2] p. 59). Consequently, the hypothesis of the second part can be weakened as in the following theorem.

**Theorem 1.2.** In the situation of Proposition 1.1, suppose that \( h \) is \( x \)-soluble except for at most \( k \)-soluble values of \( y \) in \( F \), where \( k > 0 \) and \( 0 \leq k < 1 \). If \( g > 0 \) and \( \delta(h) \), then \((1.1)\) holds and actually \( h \) is \( x \)-soluble in \( F \). In particular, if \( f \) and \( g \) are functions of degree \( \leq m, n \) respectively and \( g > c \), then \( V(f) \), \( V(g) \), \( V(f) \), \( V(g) \) implies \( V(y) \in V(f) \).

The final assertion of Theorem 1.2 completely resolves a conjecture and a conditional result of Fried ([5], Conjecture 3, [8], Corollary 2). It should have been proved in [2] but was obscured there by our not taking \( h(x, y) = f(x) - g(y) \). In fact, the discussion was equivalent to putting \( h(x, y) = f(x) - g(y) \), so that values \( y \) of \( y \) for which \( g(x) - y \) are not square-free had to be left out of the considerations.

In discussing possible occurrences of \((1.1)\), it may be convenient to separate the cases in which \( h \) is irreducible (in \( F[x, y] \)) or reducible, respectively. Alternative conditions for an irreducible \( h \) to be \( x \)-soluble are provided in the next result (cf. [2], Lemma 4 and Theorem 3, [8], Proposition 1).

**Proposition 1.3.** In the situation of Proposition 1.1, let \( h \) be irreducible in \( F(x, y) \). Suppose that \( g > c(m, n) \). Then the following are equivalent:

(i) \( h \) is \( x \)-soluble in \( F \);

(ii) \( h(x, y) \) is reducible in \( F(x, y) \), but has no absolutely irreducible factors except \( (x - y) \) in \( F(x, y, z) \), where \( h(x, y) = 0 \).

Indeed, for any \( g \), (iii) implies (i) and (ii).

Proof. We use the notation employed in proving Proposition 1.1. Note that the condition that \( h(x, y) \) is reducible in \( F(x, y) \) is equivalent to the condition that \( F(x, y) = F' \) for all \( i = 1, \ldots, m \) (cf. (4.10) of [3]). Hence, Lemma 4 of [2] shows that (iii) is equivalent to each of \( G^s_i = G^s_i \), and (b) the \( G^s_i \) are pairwise disjoint. By Proposition 1.1, (i) and (iii) are equivalent as required, while it follows from Theorem 1.2 that (ii) \( \Rightarrow \) (i). Finally, suppose (i) holds. Then (a) and (b) are true. Hence every member of \( A(y_0) \) belongs to precisely one \( G^s_i \). By [1], Lemma 5, if \( h(x, y) \) is square-free, then \( h(x, y) = 0 \) has a unique solution in \( F \). This completes the proof.

Note. It will follow from the examples of Theorem 2.1 (II) below that the exceptional \( y \) in (ii) may definitely give rise to multiple solutions of \( h(x, y) = 0 \) in \( F \). Thus some modification appears to be necessary in statement (12.2) of [8].

Condition (1.1) for \( h \) to be \( x \)-soluble is, at first sight, a very restrictive one. Indeed, it implies that \( G = G(K, F(y)) \) is admissible in the following sense: \( G \) can be represented as a permutation group on \( 1, \ldots, m \) and is a cyclic extension of a normal subgroup \( \bar{G} \); moreover, if \( G^s \) is the subset of \( G \) every member of which generates \( G \), then \( G^s = \bigcup_{i=1}^m G^s_i \), where \( G^s_i \) denotes the stabilizer of \( i \) in \( G^s \). Indeed, for \( h \) to be irreducible (and so absolutely irreducible, by Proposition 1.3 (iii)), an admissible \( G \) has additionally to be transitive, and, since \( F \neq \bar{F} \), the cyclic extension \( \bar{G} \) must be non-trivial. (In the irreducible case, Fried, [11], p. 153, has given a description of an admissible \( G \) corresponding to Proposition 1.3.)

Accordingly, in order to find all \( x \)-soluble \( h \) of given degree \( m \) in \( x \), it is first necessary to find all admissible \( G \) contained in the symmetric group \( S_m \). This is straightforward for \( m \leq 4 \); there are two non-trivial possibilities with \( G \) transitive and one with \( G \) intransitive; in effect, these are dealt with in §§ 5-7 below. More generally, the known examples of permutation polynomials, namely cyclic and Chebyshev polynomials (see [9]), indicate that \( G \) may be a cyclic or metacyclic group. But there are other possibilities even when \( G \) is transitive. Indeed, \( G \) need not even be soluble, as shown by the following example pointed out to the author.
by J. Saxl, in which \( m = 28 \). Take \( G = \text{PGL}(2, 8), \ G = \text{PGL}(2, 8) \) so that \( |G| = 1512 \), \( G \) is simple and \( G/\overline{G} \) is cyclic of order 3. As for the intransitive (reducible) case, Fried ([10]), pp. 211, 227) has announced examples (with \( h(x, y) = f(x) - g(y), f, g \) polynomials) which imply the existence of admissible \( G \) with \( G/\overline{G} \) trivial (so that \( F = \overline{F} \)).

Having found an admissible \( G \), we would next like to find all \( h \) if any for which \( G = G[H, P(y)] \) (in the obvious correspondence). In the irreducible case, this includes what Fried ([11]) has called the "general Schur problem" and is very difficult. For general \( h \) we give a solution only in the case that the total degree of \( h \) (in \( x \) and \( y \)) does not exceed 3 (§ 8). However, if \( h(x, y) \) is of the form \( f(x) - g(y) \), we can invoke properties of the discriminant and, in this way, obtain a complete solution provided \( \deg f \leq 4 \). These are the results listed in § 2 and proved in §§ 3–7.

Finally, in § 9, we shall consider some non-trivial examples of sets of functions \( f_j \) which cover \( F \), i.e. for which \( \bigcup V(f_j) = F \).

2. Results on value sets. We describe here our main results on the existence of pairs of function \( f(x), g(x) \) in \( F(x) \) for which \( V(g) \subseteq V(f) \).

Define a permutation function \( P \) over \( F \) to be one for which \( V(P) = F \). Then, trivially, \( V(g) \subseteq V(P) \) for any function \( g \). Now obviously a non-singular, linear fractional transformation \( L \) in \( F(x) \) is a permutation function. However, there are others, e.g. the monomials \( x^n \) provided \( (n, q - 1) = 1 \) and the Chebyshev polynomials \( T_n \) for certain values of \( n \), see [9]. These can be included in a more general class of functions of the form \( f = \hat{f}(Q) \) for which \( V(f) = V(Q) \). The main result, which follows, shows that, in addition to such functions, there are some interesting pairs of functions \( f, g \) with \( \deg f \leq 4 \) for which \( V(g) \subseteq V(f) \). In its statement and throughout we use the following notation. \( L \) denotes a non-singular linear fractional transformation; \( P \) is a permutation function; \( \lambda \) is an arbitrary non-square in \( F \); \( \overline{F} \) denotes the field of order \( \lambda^4 \).

**Theorem 3.1.** Let \( f, g \) be rational functions in \( F(x) \). Then \( V(g) \subseteq V(f) \) if either (I) or (II) below holds.

(I). \( f = \hat{f}(Q), g = \hat{f}(R) \) for some \( \hat{f}, Q, R \) in \( F(x) \) with
\[(2.1) \quad \hat{V}(f(Q)) = V(\hat{f}).\]
In particular, (2.1) is satisfied whenever \( Q \) is a permutation function and \( \hat{f} \) is any function.

(II). \( \alpha = \text{char}(F) \geq 3 \) and \( f = LQ \hat{f} \overline{P}, g = LQ \hat{g} \overline{P} \), where \( L, P \) and \( R \) are in \( F(x) \) and \( \hat{f}, \hat{g} \) are one of the following pairs:

(i) \( f^{*} = x^3 - 3a^2 + 2, g^{*} = 4/(3a^2 + 1) \);

(ii) \( f^{*} = a^3 - 3a, g^{*} = 2a\lambda(2a + \lambda)/[\lambda(2a^3 + 1)],\)

\[(2.2) \quad g^{*} = 2\lambda[\alpha(x^3 + \lambda) + 2(\alpha^2 - 3a^2)]/(\beta(2a^3 + 1)).\]

where \( (\alpha, \beta) \) is a chosen pair in \( F \times F \) for which \( -3(\alpha^2 - \beta^2) \) is a non-zero square in \( F \);

(iii) \( q = 1 \mod 3 \) and
\[f^{*}(x) = (x^3 + 3\alpha^2)/3(x^3 - 1), \quad g^{*}(x) = \alpha^3\]

where \( \mu \) is any non-cube in \( F \);

(iv) \( f^{*}(x) = x^3 + 3\alpha^2, \)
\[g^{*}(x) = 108\mu^2(\mu^3 - 1)/[\mu^3 - 3], \quad \text{if} \quad q = 1 \mod 3, \]
\[108\mu^2(\mu^3 - 3)/[(x^3 + 3\alpha^2)^3 - 3\alpha^2(x + 3\alpha^2)], \quad \text{if} \]
\[q = -1 \mod 3, \]

where \( \mu \) is any non-cube in \( F \) and \( \nu \) is any non-cube in \( F^2 \) whose conjugate over \( F \) is \( \pm \nu^{-1} \);

(v) \( \alpha = 0, 1, 1 \) and \( f^{*}(x) = [(x^3 + 3a - 3)/4(a^2 + 3x)] + 3a - 1, \)
\[g^{*}(x) = \frac{[(x^3 + 3a - 3)/4(a^2 + 3x)] + 3a - 1}{[x^3 + 3a - 3]^3 + 3a - 1}, \quad \text{if} \quad q = 1 \mod 3, \]
\[\frac{[(x^3 + 3a - 3)/4(a^2 + 3x)] + 3a - 1}{[x^3 + 3a - 3]^3 + 3a - 1}, \quad \text{if} \]
\[q = -1 \mod 3, \]

where \( \mu \) is any non-cube in \( F \) and \( \nu \) is a non-cube in \( F^2 \) whose conjugate over \( F \) is \( \nu^{-1} \) or \( -\nu^{-1} \) according as \( \nu \) is or is not a square in \( F \), respectively.

Conversely, suppose that \( \deg f \leq 4, \deg g \leq 4 \) and that \( q > 0(\alpha, \beta) \) with \( \alpha = \text{char}(F) \geq 3 \). Then \( V(g) \subseteq V(f) \) implies that either (I) or (II) holds.

Remarks. (a) That (I) implies \( V(g) \subseteq V(f) \) is obvious. The sufficient (II) will emerge during the demonstration of the converse which, of course, is the harder task. (Note that, if \( \deg f \leq 4 \), then, in (II), we must have \( P = L \).)

Actually, the case in which \( f \) and \( g \) are cubic polynomials was partially considered by McCann and Williams [14] who showed that, if \( q = \geq 7 \), then \( V(f) = V(g) \) implies that \( g = f(\lambda) \) or \( f = P \).

(b) For some values of \( q \) we can explicitly simplify the form of the function \( g^* \) in (ii). For \( q = 1 \) or \( -1 \) is a square in \( F \), we may choose \( \alpha = 1, 0 \) with \( \alpha = 1, 0 \), respectively. Thus, we shall take (2.2)
\[g^*(x) = \frac{1}{\lambda(2a + \lambda)} \quad \text{if} \quad q = -1 \mod 3, \]
\[\frac{4a}{\lambda(2a + \lambda)}, \quad \text{if} \quad q = 1 \mod 12.\]

(c) The \( g^* \) of (iv) and (v) are in \( F(x) \) despite the fact that, if \( q = \geq 7 \), then \( V = \overline{V} \) and \( \nu \) lie in \( F^\overline{N} \). In (iv), for example, \( \nu \) could also be described as one of the \( \overline{\nu}(0) \) non-cubes in \( F^\overline{N} \) which are \( 2(\overline{\nu}(0))^{-1} \) roots of unity in \( F^\overline{N} \).
(d) Actually, in the excluded cases \( a = 0 \), \( 1 \), (v) remains valid but (after suitable linear transformations) reduces to (iii) and (iv), respectively.

(e) As regards (iii), since \( \mu \) can be any non-cube in \( F \), we also have \( V(\mu \omega^a) \subseteq V(f^*) \). Indeed, we have

\[
V(f^*) \supseteq V(\mu \omega^a) \cup V(\mu \omega^a).
\]

In particular \( |V(f^*)| = 3g/2 \), \( |V(\mu \omega^a)| = 3g/2 \).

(i) In case (II), the containment \( V(f) \subseteq V(f^*) \) are all proper. This is apparent from (2.8) in case (ii). Otherwise, in cases (i) and (ii), we have, approximately, \( |V(f)| = 2g/3 \), \( |V(\mu \omega^a)| = g \), while in cases (iv), \( |V(f) = 2g/3 \), \( |V(\mu \omega^a)| = g \).

(g) If the degree of \( f \) is allowed to exceed 4, it remains to describe which other exceptional cases require to be added to (II). Certainly, if \( f(x) = g(y) \) is reducible then, as mentioned in \( \S \), Fied [19] has asserted that there are algebraic number fields \( K \) and polynomials \( f \) and \( g \), defined over \( K \) and not linearly related such that \( V(f(\text{mod} \ p)) = V(g(\text{mod} \ p)) \) for almost all prime ideals \( p \) of \( K \). On the other hand, if \( f(x) = g(y) \) is irreducible, then, although there are additional admissible possibilities (in the sense of \( \S \)) for the galois group of \( h(x, y) \), these may never be realised by \( h \) of the form \( f(x) - g(y) \).

Of course an explicit classification of all functions satisfying (I) is desirable. We provide such for \( \deg f \leq 4 \). First we describe the permutation functions. We shall show that only the non-trivial ones are of degree 3. (Of course, the non-existence of permutation polynomials of degrees 2 and 4 is well known.) In particular, we shall show that there is a class of permutation functions of degree 3 which includes no polynomials.

**Theorem 2.3**. Let \( f \) be a permutation function of degree \( \leq 4 \). Suppose that \( g > e \) (absolute) and \( p > 3 \). Then \( f = L \) or \( f = L \circ f^* \circ L \), where

\[
f^*(x) = \begin{cases} \omega^a, & \text{if } g = -1 \text{ (mod } 3), \\ \omega^3 / (3x^2 + \lambda), & \text{if } g = 1 \text{ (mod } 3). \end{cases}
\]

Next, we show that (I) may hold with \( F \neq F \) even when \( H(f) \leq 4 \).

**Theorem 2.5**. Suppose that \( \deg f \leq 4 \) and \( \deg g \leq 6 \). If \( g > 4 \) (absolute) and \( p > 3 \), then \( V(f) = V(g) \) if and only if \( g = f(\text{mod} \ p) \) or \( f = L \circ f^* \circ L \), where \( f^* \) and \( g^* \) are one of the following pairs:

(i) \( f^*(x) = \omega^a, g^*(x) = a \) and \( g = -1 \) (mod 4);

(ii) \( f^*(x) = (\omega^a + \lambda)/\omega^2, g^*(x) = (\omega^a + \lambda)/\omega; \)

(iii) \( f^*(x) = (\omega^a + \lambda)^2/2(\omega^a - \lambda), g^*(x) = (\omega^a + \lambda)/\omega. \)

3. Auxiliary results. When \( h \) has degree \( \leq 4 \) in \( \omega \), some of the results of \( \S \) can be rephrased in a manner involving its discriminant. In fact, if \( h(x, y) = f(x) - g(y) \), we shall find that, by considering the shape of the discriminant, the functions \( f \) and \( g \) can be normalised, thereby greatly simplifying the argument.

Accordingly, let \( h(x, y) \) be a square-free polynomial of degree \( m \geq 2 \) with coefficients in \( F(y) \) and zeros \( x_1, \ldots, x_m \) in a splitting field. Let \( D_r(h) \) denote the discriminant \( a^{m-1} \prod_{i \neq j} (x_i - x_j) \) of \( h \), where \( a = a(h) \) is its leading coefficient. Further, for any \( f \) in \( F(x) \), we shall also, without fear of ambiguity, use \( D_r(f) \) to denote the polynomial \( D_r(f(\text{mod} \ g)) \) in \( F(y) \), where \( f(x) = f_1(x)/f_2(x) \) and \( f_1 \) and \( f_2 \) are co-prime polynomials with \( f_1 \) monic. We summarise some relevant properties of \( D_r \) which are due essentially to the fact that the extension \( F(x, y) / F(y) \), where \( f(x) = y \), has genus 0. They are actually valid for any field \( F \) whose characteristic \( > m \). In our case, assume \( p > m \).

In the first place, \( \deg D_r \leq 2m - 2 \). Put \( r = 2m - 2 - \deg D_r \). Suppose that \( D_r \) has prime decomposition \( \bigoplus_{i=1}^s \mathcal{P}^*_{i} \in F[y] \) where \( a \neq 0 \) in \( F \) and the \( \mathcal{P} \) are monic irreducibles. Formally adjoining a linear polynomial denoted (temporarily) by \( \mathcal{P}_m \) which vanishes at \( \infty \) and put \( D_r = \bigoplus_{i=1}^s \mathcal{P}^*_{i} \mathcal{P}_m^* \).

Refer to the set of ordered pairs of the form \( (\deg \mathcal{P}, r) \) (with multiplicities) as included in the ramification data of \( f \) over \( F \). Its significance is as follows. Let \( \gamma \) be any root of \( \mathcal{P}(y) = 0 \) in \( F \), the algebraic closure of \( F \). Let the zeros of \( f_1 - y \mathcal{P}_m \) in \( F \) have multiplicities \( e_1, e_2, \ldots \), with the convention that, if \( e_m = m - \deg f_1 \) is non-zero, then \( e_m \) is included. Then, of course, \( \sum_{i=1}^m e_i = m \), but in fact, we shall have \( \sum_{i=1}^m (e_i - 1) = r_i \). The collections \( E(\mathcal{P}) = (e_1, e_2, \ldots) \) complete the ramification data of \( f \). Note that \( \deg(\mathcal{P}^*_i) = m - r_i \). Since \( \mathcal{P}(y) = F[L(y)] \) for any \( L \in F(x) \) (adjoining \( \infty \) to \( F \), if necessary), it is clear from the above interpretation of the ramification data, that it is preserved under compositions of the form \( L \circ f \circ L \) with \( L_1, L_2 \in F(x) \). Further, if the pair \( (1, r) \) is included in the ramification data, then by replacing \( f \) by \( L(f) \) for appropriate \( L \), we can assume that \( \mathcal{P} \) appears in \( \mathcal{P}_r \), so that \( f_2 \) has prime decomposition of the form \( f_2 = \beta P^*_1 P^*_2 \cdots \) \( (\gamma > 0) \) where \( \sum_{i=1}^m (e_i - 1) \leq r_i \). In this situation, if \( \deg F_1 = 1 \), we can replace \( f \) by \( f(L) \) and assume that \( \deg f_2 = m - e_1 \).

To complete the preliminaries we state a vital lemma, which follows immediately from a more general result of the author [3].

**Lemma 3.1**. Suppose that \( r = 2 \) or 3 and \( p > 3 \). Let \( A \) and \( B \) be rational functions in \( F(x) \) with \( A \neq 0 \) and \( r \) the \( r \)-th power in \( F(x) \). Suppose that \( A(B) \) is an \( r \)-th power in \( F(x) \). If \( r = 2 \), then \( A = Q A_1^2 \), where \( A_1 \in F(x) \) and \( Q \) is a polynomial of degree \( \leq 2 \) in \( F(x) \). If \( r = 3 \), then \( A = LA_1^3 \), where \( L, A_1 \in F(x) \).
An explicit description of those $A, B$ for which $A(B)$ is an $r$th power (for any $r$) is given in [3].

4. The quadratic case. If $\deg f = 1$ then, of course, the results of § 2 are trivial. The case $\deg f = 2$ is disposed of in the following theorem.

**Theorem 4.1.** Let $h(x, y)$ in $F(x, y)$ have degree $2$ in $x$ and degree $n$ in $y$. Suppose $g > 0$ (in $F$) and $p > 2$. Then $h$ is $x$-soluble in $F$ if and only if it is reducible in $F(x)$. In particular, suppose $g$ and $f$ are functions in $F(x)$ with $\deg f = 2$, $\deg g = n$. Then the following are equivalent:

(i) $V(g) \subseteq V(f)$;
(ii) $g = f(R)$ for some $R$ in $F(x)$.

If also $\deg g = 2$, then the following are each equivalent to (i) or (ii).

(iii) $V(g) = V(f)$;
(iv) $g = f(L)$;
(v) $D_{\omega}(f) = \Delta f^{2}(f)$, where $v(y) \in F(y)$.

Proof. Condition (iii) of Proposition 1.3 can never hold if $m = 2$ and the first part is clear. If $h(x, y) = f(x) - g(y)$, then reducibility of $h$ is equivalent to (ii) so that (i) and (ii) are equivalent. Finally, suppose that $\deg g = 2$. The following implications are obvious: (ii)$\Rightarrow$(iv)$\Rightarrow$(iii)$\Rightarrow$(i)$\Rightarrow$(ii). Hence (i)$\Rightarrow$(iv) are equivalent. Moreover, (iv)$\Rightarrow$(v) while (v)$\Rightarrow$(iii) is an easy property of the discriminant.

5. Functions of degree 3. In the cubic case we use Proposition 1.3 in the following form.

**Proposition 5.1.** Suppose, in Proposition 1.3, that $h$ is a cubic in $x$ and $p > 3$. Then the following can be added to the list of equivalent conditions (i)-(iii):

(iv) $D_{\omega}(f) = \Delta f^{2}(f)$, where $v(y) \in F(y)$.

Proof. For a given $y$ in $F$, $h(x, y)$ has a unique zero (of multiplicity 1) in $F$ if and only if $D_{\omega}(f)$ is a non-square in $F$. Thus (iv)$\Rightarrow$(ii) while (ii)$\Rightarrow$(iv) (for large $g$) follows from a result of Perel'muter [18].

We now take $h(x, y) = f(x) - g(y)$ and proceed to prove the results of § 1 with $\deg f = 3$. Trivially, in this case, (i) of Theorem 2.1 occurs if and only if $D_{\omega} = 0$. We can assume $h$ irreducible.

Suppose therefore that $V(g) \subseteq V(f)$. This property clearly survives the operation of replacing $f$ and $g$ by $L_{0} = L_{1}$ and $L_{0} = L_{2}$, respectively. By Proposition 5.1, $D_{\omega}(f)$ is a square in $F(y)$. Hence, by Lemma 3.1, $\Delta f^{2}(f)$ is a square apart from a factor of degree at most 2. If $\deg f = 2$, then $\Delta f^{2}(f)$ has a square factor, while if $\deg f = 3$, then $\Delta f^{2}(f)$ divides $D_{\omega}$, where $\omega$ is the linear factor $D_{\omega}$ of § 3. Hence, in either case, $D_{\omega}$ has a square factor. We use $D_{1}, D_{2}, D_{\omega}$ to denote distinct linear polynomials (possibly $D_{\omega}$) and $\omega$ to denote an irreducible quadratic polynomial in $F[y]$ and consider the three possibilities for $\omega$.

(a) $D_{\omega} = L_{1}^{2}L_{2}^{2}$. As in § 3, we may assume that, in fact, $D_{\omega} = D_{\omega}^{\infty}$ and that $f$ is a polynomial. Indeed, by linear transformations we may take $D_{\omega}(g) = y^{3}$, whence $L_{0} = L_{1} = L_{2}$. So assume $f(x) = ax^{2}$. Then $D_{\omega}(g) = -27a^{2}$ and hence $\omega$ is a non-square in $F$ (i.e. $g = -1$ (mod 3)) and $f$ is a permutation polynomial.

(b) $D_{\omega} = L_{0}^{2}$. In this case we may assume that $D_{\omega}(g) = y^{3} - \lambda$. Thus, replacing $f$ by $L_{0} = L_{1}$, then $\Delta_{\omega} = (a_{1} \omega + \lambda a_{2})(a_{2} \omega + \lambda a_{3})$, $L_{1} = a_{3}/a_{2}$, we obtain

$$f(x) + \sqrt[3]{\lambda} f(x) = (x + \sqrt[3]{\lambda})^{3},$$

whence $f(x) = (x^{3} + 3\lambda x)/(3\omega^{2} + \lambda)$. Accordingly, $D_{\omega}(g) = -108\omega^{3}(y^{3} - \lambda)^{3}$, $\omega$ is a square in $F$ and $g = 1$ (mod 3). Moreover, by Proposition 4.1, this $f$ is a permutation function.

(c) $D_{\omega} = L_{0}^{2}L_{1}^{2} = L_{2}^{2}$. As before we may assume that $D_{\omega} = D_{\omega}^{\infty}$ and indeed that $f$ is a polynomial. In fact, by a linear transformation of $x$, we may take $f(x) = x^{3} - 3\lambda x$, where $\eta = 1$ or $\lambda$. Put $g(\eta) = 2\eta$. Then $D_{\omega}(g^{\eta}) = -108\eta^{4}(x^{3} - \eta)$. Hence $(-3\lambda)(x^{3} - \eta)$ is a square in $F(y)$ and

$$V(g) \subseteq S := \{2\eta : -(3\lambda)(x^{3} - \eta)\}$$

Now, for the moment suppose $\eta = 1$ and put $g(\eta) = 4(3\lambda x^{2} + 1)^{-1} - 2$. Then $D_{\omega}(g) = -(12\lambda)(y - 1)/(y + 1)$ and evidently $V(g_{\omega}) = S$. Hence

$$V(g) \subseteq V(f) \Leftrightarrow V(g) \subseteq V(g_{\omega}) \Leftrightarrow g_{\omega} = g_{\omega}(R),$$

for some $R \in F[x]$, by Theorem 4.1 (ii). The necessity and sufficiency of (i) of Theorem 3.1 (II) follows.

Next suppose that $\eta = \lambda$ and that $\alpha$ and $\beta$ in $F$ are such that $(-3\lambda)(\alpha^{3} - \beta^{3})$ is a non-zero square in $F$. Put

$$g_{\omega}(y) = 2\alpha[y^{3} + \lambda y^{2} + 3\beta y + \lambda](\beta^{3} y^{3} + \lambda) + 2\alpha y].$$

Then $D_{\omega}(g_{\omega})/(3\lambda)(y^{3} - \lambda)$ is a square in $F(y)$. By comparing this with (5.3) and using the argument of the $\eta = 1$ case, we see that $V(g) \subseteq V(f) \Leftrightarrow g = g_{\omega}(R)$. To complete the proof, it remains to show that, if $g^{*}$ is also given by (5.3) with another pair $(\alpha, \beta)$, then $g^{*} = g_{\omega}(E)$. By Theorem 4.1 (iii)-(v), this is so.
6. Functions of degree 4, the irreducible case. We suppose now that
\( h(x, y) = \sum h_i x^i \) \( (h_4 \neq 0) \) is a quartic polynomial in \( x \) with coefficients in \( F(y) \). Its classical cubic resolvent, namely
\[ x^3 - h'_3 x^2 + (h'_1 h'_4 - 4h'_3) x - h'_4 h'_1 + 4h'_3 h'_1 - h'_2, \]
where \( h'_i = h_i / h_4 \), will be denoted by \( \mathcal{A}_h(x, y) \). In the first instance we suppose that \( h \) is irreducible; thus, for example, Proposition 1.3 is applicable. Recall that \( F' \) denotes the field of order \( q^2 \).

**Proposition 6.1.** In the situation of Proposition 1.1, suppose that \( h \) has degree 4 in \( x \) and is irreducible over \( F(x, y) \) and that \( q > 3 \). Then \( h \) is \( x \)-soluble in \( F \) if and only if \( \mathcal{A}_h(x, y) \) is irreducible in \( F(x, y) \), but reducible in \( F^2(x, y) \). In particular, if \( h \) is \( x \)-soluble in \( F \) and \( q > 3 \), then

(i) \( h \) is \( x \)-soluble in \( F^2 \) and

(ii) \( D_h(g) = h'_3 D_{\mathcal{A}_h}(g) \) is a square in \( F(g) \).

**Proof.** We use the notation of Proposition 1.1. Suppose \( h \) is \( x \)-soluble in \( F \). Since \( h \) is irreducible, then \( F' \neq F \) and \( G(K, F') \) is divisible by 4. Indeed, by Proposition 1.3 (iii), \( G(K, F') \) is divisible by 3. In fact, since \( G(K, F(y)) \) is a cyclic extension of \( G(K, F') \), we must have \( G(K, F(y)) = A \) and \( G(K, F') = V = \{ \alpha, \beta, (\alpha + \beta), (\alpha + \beta - 27) \} \). Thus \( F' = F^2 \), accordingly (ii) holds and (i) follows from Proposition 1.3 (iii). Moreover, by (13), Theorem 43, \( \mathcal{A}_h \) is irreducible in \( F(x, y) \), but reducible in \( F^2(x, y) \). Conversely, if this last fact holds then \( G(K, F(y)) = A \) and \( G(K, F^2(y)) = V \). But \( A - V \) comprises only 3-cycles and so (2.1) is satisfied and consequently \( h \) is \( x \)-soluble. This completes the proof.

From Proposition 6.1, the \( x \)-solubility of \( h \) depends on the reducibility of the cubic \( \mathcal{A}_h \). Accordingly, we need a result which follows easily from "Cadd's formulas" for the solution of a cubic equation (see [12], p. 258).

**Lemma 6.2.** Let \( \mathcal{A}(x) = \alpha x^2 + \beta x + \gamma \) where \( \alpha, \beta \) (not both zero) belong to a field \( \Omega \) of characteristic \( > 3 \). Suppose that the discriminant \( D \) of \( \mathcal{A} \) is a square in \( \Omega \). Then \( \mathcal{A}(x) = 0 \) has one (and so all) solutions in \( \Omega \) if and only if \( \theta \) belongs to the field \( \Omega(\sqrt{D}) \). In particular, \( \theta = -\frac{1}{3} \left[ \theta + \sqrt{D(\theta - 27)} \right] \)

\[ \text{belongs to } \Omega(\sqrt{D} - 3) \backslash \{0\}. \]

We now specialize to the case \( h(x, y) = f(x) - g(y) \), where \( f \) has degree 4, but still assume \( f \) irreducible. As far as the results of §2 are concerned, we shall show that \( V(g) \subseteq V(f) \) if and only if \( f \) and \( g \) are given by one of (III)-(v) of Theorem 2.1 (II).
and if $\overline{\mu}$, its conjugate over $F(y)$, is $1$. In fact, we must have $\overline{\mu} = \delta(T + \sqrt{-3})(T - \sqrt{-3})^3$, where $\delta$ is a non-cube in $F$ such that $\delta^2 = \delta + 1$ and $T \in F(y)$. This leads to

$$g(y) = 108\delta(T + 3)^3/(3(T + \sqrt{-3})(T - \sqrt{-3})^3)^3 + 108(T + 3)^3/\delta(T + \sqrt{-3})^3 - \overline{\mu}^{-1}(T - \sqrt{-3})^3)^2,$$

where $\overline{\mu} = \delta + \nu$ as described in (iv) of Theorem 2.1 (II); in particular $\nu \in F$ since $\delta^2 + 1 = 1$. Hence $g(y) = g^*(T(y))$, as required. Since the steps are reversible, this completes the proof in this case.

(b) $\mathcal{E}_x$ and $\mathcal{E}_y$ divide $\mathcal{E}$ and $\mathcal{E}_1$, $\mathcal{E}_2$ with $E(\mathcal{E}_1) = E(\mathcal{E}_2) = \{1, 3\}$. In the usual way take $\mathcal{E}_2 = \mathcal{E}_x$ and deg $f_1 = 1$. A linear transformation in $x$ and multiplication by a constant enable us to concentrate our attention on the function $f(x) = (x^2 + 4x^3)/(4x + a)$, where $a \in \mathbb{F}_p$. Whenever $a \neq 0$, (otherwise $f$ is not in its lowest terms). Put $g(y) = x + 2x - 2$ and let $Q(u)$ be the resultant cubic of $f(x) - u$. We have

$$Q(u) = x^3 + 4x(a - 4)x + 16u(a - u)$$

and

$$D(u) = D_x(u) = 256u^2[-27(a - u)^2 - 2u(a - 4)] = 256u^2Q(u),$$

say. Moreover, taking $\mathcal{E}$ as the polynomial (6.5) in Lemma 6.2, we have

$$\theta = -2u[[u - 2]u + VQ(u)]^{-2}]^{13}/\overline{\mu}.$$

Now $Q(u)$ has a repeated factor (in $F(u)$) if and only if $u = -2, 4$ or $16$. However, $u = 16$ has been excluded. Moreover, if $u = 4$ and $\overline{\mu}$ is taken to be $V - 27(u - 2)$, then, in fact, $\theta = 2[2u(u - 4)]^{13}$. But Lemma 3.1 with $r = 3$ implies that $2u(u - 4)$ can never be a cube in $F(u)$ for any $u$ and, so, by Lemma 6.2 and Proposition 6.1, we cannot have $VQ(u) \subseteq F(u)$. Next, putting $u = -2$, we obtain $Q(u) = -27(u - 2)^2$. Since $D(u)$ is a square in $F(u)$, we must have $\overline{\mu}^{-1}(T + \sqrt{-3}) = 1/3$. Further, taking $VQ(u) = V - 27(u - 2)$ in (6.6), we require $(-32u)^{13}$ to be in $F(u)$, but not in $F(y)$. Clearly, this is the case if and only if $u = 2\mu R^p$ for some $R \in F$ and non-cube $\mu$ in $F$, i.e., if and only if $u = 2g^*(R)$, where $g^*$ is given by (iii) of Theorem 2.1 (II). Conversely, for $f^*$ and $g^*$ as given above, the above argument shows that $VQ(u) \subseteq F(u)$ for any $g^*$ with $p > 3$ and that actually, $\mathcal{E}_2 = \mathcal{E}_x$, where $E(\mathcal{E}_2) = E(\mathcal{E}_x) = \{1, 3\}$. This implies that $\mathcal{E}_2 = \mathcal{E}_x$, where $E(\mathcal{E}_2) = E(\mathcal{E}_x) = \{1, 3\}$. To conclude this case, it suffices to show that $Q(u)$ cannot be square-free. For suppose $Q(u) = -27(u - a)(u - b)$, where $a, b \in F$ with $a \neq b$. Then $(u - a)(u - b) = \nu^2$, where $\nu \in F(y)$. Thus $u = (b\nu - a)(a - 1)^2$ and we may take $VQ(u) = \overline{\mu}^{-1}$ if $u \neq 0$. From (6.6) it follows that

$$\theta = -2[2[2u(u - 4)]^{13}/(u^3 - 1) + 2u^3]^{13}/\overline{\mu}$$

belongs to $F(y)$. If $2a \neq a + b$, the rational function in braces in (6.7) is in its lowest terms and so has no cube root in $F(y)$ for any $v$ by Lemma 3.1. Indeed, even if $2a = a + b$, then $a \neq b$ and we would require $(b \nu - a)(a - 1)^2$ to have a cube root in $F(y)$ which again contradicts Lemma 3.1 since $a \neq b$. Hence $Q(u)$ is not square-free.

Thus

$$D(u) = D(y) = -27.21^{13}(4u^3 - 2u - 2) = -27.21^{13}Q(u),$$

say. Now, if $a = 0$, we have case (b) again. So assume that $a \neq 0$, thus $Q(u)$ is square-free. Putting $u = R^{-1}(R + a^2 - 3a - 1)$. Then $Q(u) = (R^2 + a^2)^2/\overline{\mu}$. If $\theta$ is given by (6.6) with $\mathcal{E} = \mathcal{E}_2$ and $VQ(u) = (R^3 - a^3)/\overline{\mu}$, we find that

$$\theta = 4(R - a^3)/\overline{\mu}.$$
(a) \( S_f = P^2 \mathbb{Z} \). By Proposition 6.1 (ii), even in \( F^2 \) we have \( V(g) \subseteq V(f) \). Moreover, in \( F^3 \), \( S_f = P^2 \mathbb{Z} \mathbb{F}_3^2 \) say. So, by (b) and (c), there exist \( L_i, L_i' \) in \( \mathbb{F}_3 \) such that \( f^*(x) = (x^4 + x^2)/\mu(x) = x^4 + x \), then
\[
\begin{align*}
|L_i| &= \log f^* \circ L_i, \\
|L_i'| &= \log \mu^* \circ L_i.
\end{align*}
\]
Now \( f, g, \mu^* \) and \( g^* \) are actually in \( F(x) \). Consequently, (6.9) yields
\[
\begin{align*}
L_i^* &= L_i^* \circ \mu(i), \\
L_i'^* &= L_i^* \circ \mu'(i),
\end{align*}
\]

where \( L_i^* = L_i^* \circ L_i, L_i'^* = L_i^* \circ L_i' \). This is a permutation polynomial in \( \mathbb{F}_3 \). For large \( q \), the only other possibility permitted by Theorem 2.1 (with \( \sigma = 3 \)) is that \( L_i^* = L_i \mathbb{F}_3 \) for some \( L_i \) in \( \mathbb{F}_3 \). Clearly this implies that \( L_i^* = L_i \mathbb{F}_3 \), and \( g^*(x) = x \) is not a permutation polynomial in \( \mathbb{F}_3 \). For large \( q \), the only other possibility permitted by Theorem 2.1 (with \( \sigma = 3 \)) is that \( L_i^* = L_i \mathbb{F}_3 \) for some \( L_i \) in \( \mathbb{F}_3 \). Clearly this implies that \( L_i^* = L_i \mathbb{F}_3 \), and \( g^*(x) = x \) is not a permutation polynomial in \( \mathbb{F}_3 \). For large \( q \), the only other possibility permitted by Theorem 2.1 (with \( \sigma = 3 \)) is that \( L_i^* = L_i \mathbb{F}_3 \) for some \( L_i \) in \( \mathbb{F}_3 \). Clearly this implies that \( L_i^* = L_i \mathbb{F}_3 \), and \( g^*(x) = x \) is not a permutation polynomial in \( \mathbb{F}_3 \). For large \( q \), the only other possibility permitted by Theorem 2.1 (with \( \sigma = 3 \)) is that \( L_i^* = L_i \mathbb{F}_3 \) for some \( L_i \) in \( \mathbb{F}_3 \). Clearly this implies that \( L_i^* = L_i \mathbb{F}_3 \), and \( g^*(x) = x \) is not a permutation polynomial in \( \mathbb{F}_3 \).

(b) \( S_f = P^2 \mathbb{Z} \mathbb{F}_3^2 \). Using Proposition 6.2 (ii) to work in \( \mathbb{F}_3 \), we have \( S_f = P^2 \mathbb{Z} \mathbb{F}_3^2 \mathbb{F}_3^2 \), which necessarily \( B(L_i) = B(L_i') \). But this is impossible by case (c).

(c) \( \mathbb{Z} \mathbb{F}_3^2 \). We must have \( B(L_i) = \{1, 3\} \). Replace \( F \) by \( F^3 \) so that now \( V(S) \subseteq F \) and \( \mathbb{Z} \mathbb{F}_3^2 \mathbb{F}_3^2 \), \( B(L_i) = \{1, 3\} \), \( i = 1, 2, 3 \). Then although \( V(g) \subseteq V(f) \) will now be false, we still must have \( V(D_f) \) (where \( u = g(y) \)) in \( F(y) \). Further, as in case (b), \( f = L_i^* \circ L_i \), where \( f_0(x) = (x^4 + x^2)/\mu(x) \) and \( \theta \) (given by (6.6)) is in \( F(y) \). The argument of case (b) forces \( \mu = -2 \). But then \( B(L_i) \) (say) must be \( \{2, 2\} \) and we have a contradiction.

This exhausts the possibilities for \( S_f \). Hence the discussion of Theorem 2.1 for deg \( f = 4 \) is complete in the "irreducible case."
so \( V(g) = V(f) \) if and only if \( g_1 = F' \).

(iv) \( \hat{f}(x) = x^3, f_1(x) = (x^3 - \lambda)/x \). Here
\[
(f(x) - g(y) = (x^3 - ax_1(y) - \lambda)(x^3 + ax_1(y) - \lambda),
\]
the two factors having identical discriminants so that Proposition 7.1 cannot be satisfied.

(b) \( \deg \hat{f} = 4 \). Here \( f_1 = L \) and we may assume, in fact, that \( f = \hat{f} \). Let \( K \) be the common splitting field of \( f(x) - t \) and \( \hat{g}(x) - t \) over \( F(t) \) with corresponding isomorphic Galois groups \( \mathcal{G}(f), \mathcal{G}(g) \), respectively. Let \( y \) be a zero of \( g(x) - t \) and put \( v = g_1(y) \). Thus \( \hat{g}(v) = v \) and so \( v \in K \). By Proposition 7.1, \( [K(y) : F(y)] = 4 \) (although \( [K(y) : F^2(y)] = 2 \). By the theorem of normal rationalities, \( r \) is divisible by 4. But \( [\mathcal{G}(g)] = 2 \mathcal{H}(g) \) where \( r \mathcal{H}(g) \). On the other hand, \( [\mathcal{G}(f)] = 24 \). The only consistent conclusion is that \( r = 4 \), \( \deg g = 6 \) and \( \mathcal{G}(f) = S_4 \), the symmetric group. Thus \( \hat{G}(g) \) is a transitive subgroup of \( S_4 \) isomorphic to \( S_4 \). The situation just described seems unlikely; nevertheless there are circumstances where it would occur for the assumption that \( f(x) - \hat{g}(v) \) is reducible, namely when \( \hat{g}(v) \) is \( S^2(x) \), where \( S \) is the cubic resolvent of \( f \). However, the additional hypothesis that \( f(x) - \hat{g}(v) \) is reducible enables us to reach a contradiction as follows. Consider the subgroup \( V \) of \( \hat{G}(f) \) whose members fix a prescribed root of \( f(x) = t \). Then \( V \cong S_3 \). Regarding \( V \) as a subgroup of \( \hat{G}(g) \) and using the fact that \( f(x) - \hat{g}(v) \) is reducible, we see that for suitable numbering of the roots \( \hat{g}(v) = t \) we have
\[
V = \{(123)(456), (123)(465), (12)(34), (13)(40), (23)(56), (1)\}.
\]

However, there is no way \( V \) could be one of precisely four conjugate subgroups of any transitive subgroup of \( S_4 \). So this case is, after all, impossible.

It may be helpful to point out that, in the above, the known example \([4]\) of a pair \((f, g)\) with \( f(x) - g(y) \) reducible and \( \deg \hat{f} = 4 \) (namely, \( f(x) = (x^3 - 1)^3 \), \( g(x) = -3x^2(x^3 - 1) \)) is eliminated by the demand that \( [K(y) : F(y)] = 4 \).

8. \( a \)-soluble polynomials of degree \( 3 \). For general polynomials \( h(x, y) \) of degree 3 or 4 in \( x \), the normalisation procedure achieved in \( \S \) 5–6 for the case \( h(x, y) = f(x) - g(y) \) is not available. However, we can characterise those polynomials \( h \) of total degree 3 in \( F[x, y] \) which are \( a \)-soluble, thus extending work of Mordell [15]. We use Proposition 5.1 in the following form.

**Lemma 8.1.** Suppose that in Proposition 5.1, \( h \) has the form
\[
h(x, y) = x^3 + h_1(y)x + h_0(y), \quad h_0 \neq 0.
\]

Then (5.1) holds if and only if \( g = -1 \) (mod 3) \( and \( h_1 = 0 \) or
\[
h_3 = -3(A^3 + 3B^2), \quad h_3 = 2A(A^3 + 3B^2),
\]
where \( A, B \neq 0 \) \( \in \mathcal{F}(y) \).

**Proof.** If \( h_1 = 0 \), then \( D_{h_1} = -27h_3^2 \) and (5.1) holds if and only if \( v = 3 \not\in \mathcal{F} \).

If \( h_1 \neq 0 \), put \( h_2 = -2h_3A/3 \). Then
\[
D_{h_2}(y) = 12h_2^2( -1/3A - A^3)
\]
and (5.1) holds if and only if \(-1/3A - A^3 = 3B^2 \). The result follows.

Before stating our theorem, we note that if \( h \) is \( a \)-soluble, then so is
\[
h_1(x, y) = ah_0(x + cy + d, ey + f), \quad ab \neq 0,
\]
and we say that \( h_1 \) and \( h \) are \( a \)-equivalent.

**Theorem 8.2.** Let \( h(x, y) \) in \( F[x, y] \) be a polynomial of total degree 3 and suppose that \( h > h_0 \) (absolute) and \( p > 3 \). Then \( h \) is \( a \)-soluble if and only if it has a factor linear in \( x \) or is \( a \)-equivalent to a polynomial of one of the following types:

I. \( x^3 - g(y) \), II. \( x^3 + y^3 - 2g_1(y) \), \( \{1, q = -1 \) (mod 3),
III. \( x^3 + 3x^2 + y(3x^3 + y) \), IV. \( x^3 + 3x^2 + y(3x^3 + y + 1)^2 \), \( \{1, q = -1 \) (mod 3),
V. \( x^3 + (3x^3 + 2)(3y^2 + 1) \)
We denote the form \( h(x, y) \) by \( h \). From Theorem 4.1 we may assume that \( h \) is irreducible of degree 3 in \( x \) and so is \( a \)-equivalent to a polynomial of the form (8.1) also of total degree 3. By Lemma 8.1, either \( h \) is \( a \)-equivalent to \( I \) for some \( g \) or is \( a \)-equivalent to (8.3)
\[
x^3 - 33(x^3 + 3x^3 + 2)(3y^2 + 1) \quad (x^3 + 3x^3 + 2)(3y^2 + 1),
\]
where \( A, B, C \) and the coefficients of (8.3) are all non-zero polynomials in \( F[y] \). We may suppose also that \( A, C \) and \( F = A^3 + 3B^2 \) are co-prime.
Since \( \mathcal{O}^A \), then \( A \) and \( C \) are co-prime and so \( \mathcal{O}^A \mathcal{O} \). However, \( A \) and \( B \) are also co-prime, for, if not, we would have \( A \) linear and both \( A^3 + 3B^2 \) and \( C \) in \( F \). But then
\[
A^3 + 3B^2 \quad (x^3 - 3x^3 + 2)(3y^2 + 1) \in \mathcal{O}, \quad a = 1 + 33A^3 \in \mathcal{O},
\]
which has discriminant \( h(18B^2) \) and so is reducible, whence \( h \) is reducible.
Now write \((8.3)\) as \(x^3 - 3CGx^2 + 2AG\), where \(C\) and \(G\) are \(C^{-1}E \in \text{End}(F)\) and \(\deg C + \deg G \leq 2\), \(\deg A + \deg G \leq 3\). We consider the various possibilities for \(C\) and \(G\). Let \(\bar{F}\) be the algebraic closure of \(F\) and put \(\delta = x - 3\lambda\) in \(\bar{F}\).

(a) \(\deg G = 0\). Thus \(\deg C = 1\) and \(\deg B = 3\) or 6. Since \(A\) and \(B\) are co-prime, then so are \(A + dB\) and \(A - dB\). Therefore, in \(\bar{F}(y)\), \(A + dB = C_1\) where \(C_1\) divides \(C\). But then, since \(G \in \text{End}(F)\), \(x(y, x)\) has a factor in \(\bar{F}(x, y)\) of \(x + 1\) or \(x + (x^2 + 2G/3)\) (by Cartan's Formula) which contradicts the fact that \(h\) is absolutely irreducible (Proposition 1.2 (iii)).

(b) \(\deg G = \deg G = 1\). This case is impossible for it would imply that \(B\) has degree 1 yet is divisible by \(C^n\).

(c) \(\deg G = 0\), \(\deg G = 1\). For this \(\deg A = \deg B = \deg E = 1\) so that \(\delta \in \bar{F}\), i.e. \(c = 1\) (mod 3). Replacing \(x\) by \(x - ay + b\) for suitable \(a \neq 0\), \(b \in F\), we may take \(A(y) = y, B(y) = (y + 1)^2\). Now the transformation \(x \rightarrow \frac{1}{2}(x + y + 1), y \rightarrow \frac{1}{2}(y + 1)\) shows that \(h\) is \(\alpha\)-equivalent to \((\alpha + (x^2 - 2g)(2y + 1))\). Now the transformation \(x \rightarrow \frac{1}{2}(x + y + 1), y \rightarrow \frac{1}{2}(y + 1)\) shows that \(h\) is \(\alpha\)-equivalent to \(2x^3 - 2(y^2 + 3y + 1)\).

A further transformation \(x \rightarrow x + y\) indicates that \(h\) is \(\alpha\)-equivalent to \(x^3\) but with \(\eta = -3\lambda(= \delta^3)\). To get \(x \rightarrow \delta y\) in the case \(c = 1\) (mod 3), apply the extra transformation \(x \rightarrow \delta x, y \rightarrow \delta (y + 1) - 1\).

A similar discussion reveals that if \(\deg A = 1\), \(\deg B = 0\), then \(h\) is \(\alpha\)-equivalent to \(\delta x, y \rightarrow \delta (y + 1) - 1\).

The sufficiency of \(x^3 - 3\lambda(x + 1)^2\) is obvious from the above and Lemma 8.1. Thus the proof is complete.

From Theorem 8.2, it is easy to guess which cubics \(h\) are both \(\alpha\)-solvable and \(\eta\)-solvable in \(F\). Formal verification of Mordell's result [15] (stated below) is indeed possible from this starting point and probably represents a shorter and less intricate method than that of Mordell. Nevertheless, the proof is not actually immediate and, for brevity, is omitted.

**Theorem 8.3 (Mordell).** Let \(h(x, y)\) in \(F[x, y]\) have total degree 3. Suppose that \(g > g_0\) and \(p > 3\). Then \(h\) is both \(\alpha\)-solvable and \(\eta\)-solvable in \(F\) if and only if \(h\) has a factor linear in \(x\) and a factor linear in \(y\) or one of \(h(x, y)\) and \(h(y, y)\) is of the form \((8.3)\) with \(c = 0\), where \(h_1\) is one of \(I-III\) in Theorem 8.2 with \(g(y, x) = x^2 + 3\lambda + 1\).

9. Covering sets. We shall call a set of functions \(\{f_i(x)\}\) in \(F(x)\) a covering set if \(\cup V(f_i) = F\). Here are some simple examples.

(i) \(\{f_1\}, f_1 = P\) for some \(i\).

(ii) \(\{x^r, y^r, \ldots, r^{-1}x^r\}\), where \(r\mid q - 1\) and \(\gamma \in F\) is a non-\(\alpha\)-th power for any divisor \(a\) of \(r\) with \(a > 1\).

(iii) \(\{(x^a - \lambda)/2z, 2z/(x^a - \lambda)\}\) (see § 7).

Using exponential sums, Mordell [16], [17], has constructed a non-trivial covering set comprising a function of degree 4 and a function of degree 3. However, the natural approach to covering sets may be to use the following result which follows immediately from Proposition 1.1. (For related work on the more general problem \(V(f) \subseteq \bigcup V(f_i)\), see [5], [9], § 4.)

**Proposition 9.1.** In the situation of Proposition 1.1, let

\[ h(x, y) = \prod_{i=1}^{m} (f_i(x) - y). \]

Suppose that

\[ G^*(K, F(y)) = \bigcup_{i=1}^{m} \bigcup_{x_i} G(x_i, F(x_i)), \]

where the inner union is over all roots \(x_i\) of \(f_i(x) = y\). Then \(\{f_i\}\) is a covering set for \(F\).

Using Proposition 9.1 and previous results in this paper, we can demonstrate some examples of covering sets valid for any \(F\) with \(p > 3\).

(iv) Mordell's covering set

\[ \{f_1, f_2\} = \{(x^3 + ax^2 + bx, (x^3 + 2ax^2 - a^2x - b)/2ax)\}, \quad b \neq 0, \]

follows easily from Proposition 9.1 since \(f_2(x) = y\) is the cubic resolvent of \(f_1(x) - y\). Another covering set arising in this way is

\[ \{(x^3 + ax^2 + bx, x, (x^3 + 2ax^2 - b)/2ax)\}, \quad ab \neq 0. \]

(v) From (i) of Theorem 2.1 (II) (cf. Theorem 8.2 (vi)), we get the pair

\[ \{(x^3 - 3x + 2)/3, 3e^2\}. \]

(vi) From (iii) of Theorem 2.1 (II) we get the pair

\[ \{f_1, f_2\} = \{(x^3 + 2ax - 4)/2x - 4, ax^2\}. \]

However, although this is a covering set for all \(q\), the manner of the covering depends on \(q\). For, of course, if \(q = -1\) (mod 3), then \(f_1 = P\) and we have a trivial covering set of type (i). On the other hand, if \(q = 1\) (mod 3), then \(\{V(f_1) \cap V(f_2)\} = \{q/12\}\).

(vii) Finally, we exhibit a non-trivial covering set of three functions. Put

\[ \{f_1, f_2, f_3\} = \{(ax^2 - 4x^2, -4x^2(ax^2 - 1, 1, (a - 1)^2/(a^2 + 1)). \]
(As noted earlier (§ 7), \( f_1(x) - f_2(y) \) is reducible.) Then the roots of \( f_i(x) = y, i = 1, 2, 3 \), can be written as \( \{a_1, -a_1, a_2, -a_2, \beta_1, -\beta_1, \beta_2, -\beta_2, \gamma, \gamma^{-1} \} \), respectively, where \( \beta_i = \frac{1}{2}(a_i \pm a_2), i = 1, 2, \) and
\[
\gamma = -(2y-1)^{-1}(1-2a_2 a_4 a_1^{-1}).
\]
Moreover, \( G^*(K, F(y)) \) is the whole galois group \( G \), say, and has order 8. If the roots of each \( f_i(x) = y \) are numbered in the order given, then the action of \( G \) as a permutation of these roots is as follows:

<table>
<thead>
<tr>
<th>( f_1 )</th>
<th>( f_2 )</th>
<th>( f_3 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>(1)</td>
<td>(1)</td>
<td>(1)</td>
</tr>
<tr>
<td>(12)</td>
<td>(14) (23)</td>
<td>(12)</td>
</tr>
<tr>
<td>(34)</td>
<td>(13) (24)</td>
<td>(12)</td>
</tr>
<tr>
<td>(12) (34)</td>
<td>(12) (34)</td>
<td>(1)</td>
</tr>
<tr>
<td>(13) (24)</td>
<td>(34)</td>
<td>(12)</td>
</tr>
<tr>
<td>(14) (23)</td>
<td>(12)</td>
<td>(12)</td>
</tr>
<tr>
<td>(1324)</td>
<td>(1324)</td>
<td>(1)</td>
</tr>
<tr>
<td>(1324)</td>
<td>(1423)</td>
<td>(1)</td>
</tr>
</tbody>
</table>

Thus \( \{f_1, f_2, f_3\} \) is a covering set by Proposition 9.1.

References