[9] N. Nakagoshi, *The structure of the multiplicative group of residue classes modulo* p^{N+1}, Nagoya Math. J. 73 (1979), pp. 41–60.

[10] C. J. Parry and C. D. Walter, *The class number of pure fields of prime degree*, Mathematika 23 (1976), pp. 220–226; 24 (1977), p. 133.

[11] R. W. van der Waall, *On the conductor of the non-Abelian simple character of the Galois group of a special field extension*, Symposia Math. 15 (1975), pp. 389–395.

[12] H. Wada, *On cubic Galois extensions of* $Q(\sqrt{-3})$, Proc. Japan Acad. 46 (1970), pp. 397–400.

[13] H. Yokoi, *On the divisibility of the class number in an algebraic number field*, J. Math. Soc. Japan 20 (1968), pp. 411–418.

DEPARTMENT OF MATHEMATICS
TOYAMA UNIVERSITY
Gofuku 3190, Toyama 930, Japan

Received on 17.6.1982
and in revised form on 28.2.1983 (1312)

ACTA ARITHMETICA
XLIV (1984)

Irreducible discriminant components of coefficient spaces

by

M. FRIED (Irvine, Cal.)* and J. SMITH (Boston, Mass.)

1. Introduction and notation. Let A_R^n and A_C^n be two copies of affine n-space defined over Q. The *Noether cover* is the Galois cover (with group S_n) associated to the map $A_R^n \xrightarrow{\Phi_n} A_C^n$ that sends $(y(1), \dots, y(n))$ to the n-tuple of symmetric functions

$$(x(1), \dots, x(n)) = \Big(\dots, (-1)^i \sum_{j(1)<\dots<j(i)} y(j(1))\cdot \dots \cdot y(j(i)), \dots\Big).$$

For $\{i(1), \dots, i(u)\} = I$ a subset of $\{1, 2, \dots, n\}$, the *coefficient locus* $X(I)$ is defined by the equations $x(i) = 0$ for all $i \notin I$.

The *discriminant locus* is the image in A_C^n of the points of A_R^n for which two or more entries are equal. We identify the irreducible components of the intersection of $X(I)$ with the discriminant locus. If the elements of I have no common divisor, besides some trivial components (hyperplanes), this intersection is irreducible (Theorem 3.1).

Cohen [1] has shown that the Galois group of the cover induced by certain subvarieties of $X(I)$ is S_n. An easy consequence of the above irreducibility is a less sharp result: the group of the cover induced over $X(I)$ is S_n. Examples show (§ 4) that our results may remain valid for all of Cohen's subvarieties.

For F a field, $\bar{F}$ is a fixed algebraic closure of F. Let $A_R^n(\bar{F})$ denote the n-tuples of elements $(y(1), \dots, y(n)) \in (\bar{F})^n$. The subscript R (for "roots") indicates that the n-tuple is regarded as an ordering on the roots of the monic polynomial

$$\prod_{i=1}^{n} (y - y(i)) = p(y) = y^n + \sum_{i=1}^{n} x(i)\cdot y^{n-i}.$$

Let $A_C^n(\bar{F})$ denote another copy of affine n-space: the subscript C (for "coefficients") indicates that the points of $A_C^n(\bar{F})$ correspond to the coefficients of monic polynomials of degree n.

For X defined by equations with coefficients in F ([3], p. 181), X is F-

* Supported by N.S.F. Grant MCS 80-03253.

irreducible if X is not the union of two proper closed disjoint subsets of X defined over F. It is reduced if each F-irreducible component appears with multiplicity one.

Denote by D_n the discriminant locus of A^n_C. For $\{i(1), \ldots, i(u)\} = I$ a subset of $\{1, 2, \ldots, n\}$ the *coefficient locus* corresponding to I is the F-linear space $X(I)$ of A^n_C defined by the equations $x(i) = 0$ for all $i \notin I$. We explicitly identify the components of the intersection of $X(I)$ with D_n. Under the hypotheses that $n \in I$, g.c.d. $(i(1), \ldots, i(u)) = 1$, and the characteristic of the field is suitably restricted, it consists of (possibly) two coordinate hyperplanes and a large irreducible component. It follows easily that the decomposition group for $X(I)$ is a primitive group containing a 2-cycle; thus it is S_n. Cohen [1] has shown that this last result holds even for a sublocus X' of $X(I)$ defined as follows (subject to restrictions on the characteristic): for $J \subset I \cup \{0\}$ with $|I \cup \{0\} - J| \geqslant 2$, X' is the subset of $X(I)$, $x(i) = a(i)$ for $i \in J$ with $a(i)$ a nonzero constant. In Section 4 we present evidence that the irreducible components of the intersection of $X(I)$ and the discriminant locus remain irreducible upon intersection with these Cohen loci.

For a polynomial $f(y) = x(0)' \cdot y^n + \sum_{i=1}^{n} x(i)' \cdot y^{n-i} \in F[y]$ the discriminant of f, $D(f)$ is traditionally defined as ([4], p. 86–87):

$$D(f) = (x(0)')^{2\cdot n-2} \cdot \prod_{i \neq j} (y(i)' - y(j)') \tag{1.1}$$

where $y(1)', \ldots, y(n)'$ are the zeros of f.

Consider the *universal polynomial of degree n*:

$$\sum_{i=0}^{n} x(i) \cdot y^{n-i} \cdot z^i = 0. \tag{1.2}$$

Denote it by $z^n \cdot f(y/z; \boldsymbol{x})$. Then $D(f(y/z; \boldsymbol{x}))$ is D_n. Also:

$$\begin{aligned} D(f(z/y; \boldsymbol{x})) &= x(n)^{2\cdot n-2} \cdot \prod_{i \neq j} \big((z/y(i)) - (z/y(j))\big) \\ &= x(n)^{2\cdot n-2} \cdot \Big(\prod_{i \neq j} (y(j)/z) - (y(i)/z)\Big) \cdot \Big(\prod_{i \neq j} (y(i)/z) \cdot (y(j)/z)\Big)^{-1} \\ &= x(n)^{2\cdot n-2} \cdot (x(n)/x(0))^{-2\cdot(n-1)} \cdot \Big(\prod_{i \neq j} \big((y(j)/z) - (y(i)/z)\big)\Big) \\ &= D(f(y/z; \boldsymbol{x})). \end{aligned}$$

Finally, consider the trinomial $x(0) \cdot y^n + x(j) \cdot y^{n-j} \cdot z^j + x(n) \cdot z^n = z^n \cdot f(y/z; I)$ with $I = \{j, n\}$. Then

$$D(f(y/z; I)) = (x(0)^{j-1}) \cdot (x(n)^{n-j-1}) \cdot E(I) \tag{1.3}$$

with $E(I) = n^n \cdot x(0)^{n-j} \cdot x(n)^j + (-1)^{n-1} \cdot (j)^j \cdot (n-j)^{n-j} \cdot x(j)^n$. If $(\mathrm{char}(F), j)$ $= (\mathrm{char}(F), n-j) = (\mathrm{char}(F), n) = (n, j) = 1$, then $E(I)$ is irreducible since the specialization of $x(0)$ to 1 gives an irreducible polynomial.

2. Basic lemmas on the resultant. As in expression (1.2) consider the polynomial

$$z^n \cdot f(y/z; \boldsymbol{x}) = \sum x(i) \cdot y^{n-i} \cdot z^i$$

and its discriminant $D(f(y/z; \boldsymbol{x}))$. Throughout this section $I = \{i(1), \ldots, i(u)\}$ denotes a subset of $\{1, 2, \ldots, n\}$ with these properties:

(2.1) (a) $i(1) < i(2) < \ldots < i(u) = n$; and

(b) $(i(1), i(2), \ldots, i(u)) = 1$.

For simplicity denote $x(0) \cdot y^n + \sum_{j=1}^{u} x(i(j)) \cdot y^{n-i(j)} \cdot z^{i(j)}$ by $z^n \cdot f(y/z; I)$. It is valuable to let $\bar{i}(j) = n - i(j)$ whenever it is clear that $i(u) = n$.

The *fundamental theorem on discriminants* ([4], p. 87):

$$x(0) \cdot D(f(y/z; x)) = R\left(f(y; x), \frac{\partial}{\partial y}(f(y; x))\right)$$

(often abbreviated $R(f, f')$) where $R(f, f')$ is the determinant of the matrix $M(\boldsymbol{x})$:

$$(2.2) \qquad \begin{matrix} \\ n-1 \\ \\ \\ \\ n \\ \\ \\ \end{matrix} \begin{bmatrix} x(0) & x(1) & \ldots & x(n) & 0 & \ldots & 0 \\ 0 & x(0) & \ldots & x(n-1) & x(n) & \ldots & 0 \\ \vdots & & & & & & \vdots \\ 0 & \ldots & \ldots & \ldots & \ldots & \ldots & x(n) \\ n \cdot x(0) & (n-1) \cdot x(1) & \ldots & & & & 0 \\ 0 & n \cdot x(0) & \ldots & & & & \\ \vdots & & & & & & \\ 0 & & & & \ldots & 2 \cdot x(n-2) & x(n-1) \end{bmatrix}$$

In the specialization of $z^n \cdot f(y/z; \boldsymbol{x})$ to $z^n \cdot f(y/z; I)$ the resulting specialization of $M(\boldsymbol{x})$ is denoted $M(I)$. Clearly, $D(f(y/z; \boldsymbol{x}))$ is a homogeneous polynomial of degree $2 \cdot n - 2$.

DEFINITION 2.1. A monomial $\prod_{i=0}^{n} x(i)^{r(i)}$ is defined to have *weight* equal to $\sum_{i=0}^{n} i \cdot r(i)$, and a polynomial is said to be *weight homogeneous* if all terms have the same weight. Denote the weight of a weight homogeneous polynomial $h \in F[x(0), \ldots, x(n)]$ by $\mathrm{wt}(h)$.

LEMMA 2.2. *The polynomial $D(f(y/z; \mathbf{x}))$ is weight homogeneous of weight $n\cdot(n-1)$. The polynomial $D(f(y/z; I))$ is equal to*

$$(x(0)^{i(1)-1})\cdot(x(n)^{n-i(u-1)-1})\cdot E(I)$$

where

$$\deg(E(I)) = n-i(1)+i(u-1) \quad \text{and} \quad \mathrm{wt}(E(I)) = n\cdot i(u-1).$$

Proof. The statement that $D(f(y/z; \mathbf{x}))$ is weight homogeneous is equivalent to the statement that $D(f(y/z; \bar{\mathbf{x}}))$ is homogeneous (of degree $n\cdot(n-1)$) in $x(0), \ldots, x(n)$ where $\bar{\mathbf{x}} = (1, x(1), x(2)^2, \ldots, x(n)^n)$.

For α an indeterminate, consider the effect of changing $(x(0), \ldots, x(n))$ to $(\alpha\cdot x(0), \ldots, \alpha\cdot x(n))$: $z^n\cdot f(y/z; \bar{\mathbf{x}})$ becomes

$$\sum \alpha^i\cdot x(i)^i\cdot y^{n-i}\cdot z^i = \sum x(i)^i\cdot y^{n-i}\cdot(\alpha\cdot z)^i.$$

From expression (1.2) the effect on $D(f(y/z; \bar{\mathbf{x}}))$ is this: If $\bar{y}(1), \ldots, \bar{y}(n)$ are the zeros of $f(y; \bar{\mathbf{x}})$, then $\prod_{i\neq j}(\bar{y}(i)-\bar{y}(j))$ becomes $\prod_{i\neq j}(\alpha\cdot\bar{y}(i)-\alpha\cdot\bar{y}(j))$ or $\alpha^{n\cdot(n-1)}\cdot D(f(y/z; \bar{\mathbf{x}}))$.

Now consider the second statement of the lemma. The first $i(1)$ columns of $M(I)$ are divisible by $x(0)$, and the last $n-i(u-1)-1$ columns of $M(I)$ are divisible by $x(n)$. The remainder of the lemma follows easily. ∎

The proof, in Section 3, that $E(I)$ is irreducible, depends on considering the effect on $E(I)$ of setting $x(i(j)) = 0$ (write $E(I) \bmod (x(i(j)))$; it is the same as $E(I-\{i(j)\})$). These next lemmas simplify calculations.

LEMMA 2.3. *Let $I' = \{i'(1), \ldots, i'(u')\}$ be a subset of $\{1, 2, \ldots, n\}$ satisfying* (2.1) (a) *but not necessarily* (2.1) (b): $(i'(1), \ldots, i'(u')) = d$. *Rename the $u'+1$-tuple of variables $(x(0), x(i'(1)), \ldots, x(i'(u')))$ to be*

$$(x'(0), x'(i'(1)/d), \ldots, x'(i'(u')/d)).$$

For

$$I''(\mathbf{x}') = \{i'(1)/d, \ldots, i'(u')/d\}$$

(a subset of $\{1, 2, \ldots, n/d\}$) allow a slight misuse of notation and write $f(y/z; I') = f((y/z)^d; I''(\mathbf{x}'))$. Then

$$D(f(y/z; I')) = (-1)^{n-(n/d)}\cdot x(0)^{d-1}\cdot x(n)^{d-1}\cdot d^n\cdot D(z^{n/d}\cdot f(y/z; I''(\mathbf{x}')))^d.$$

Consequently, $E(I') = (-1)^{n-(n/d)}\cdot d^n\cdot(E(I''(\mathbf{x}')))^d$ (where $E(I''(\mathbf{x}'))$ is computed from $f(y/z; I''(\mathbf{x}'))$).

Proof. Factor out d from each of the last n rows of $M(I')$. Then rearrange the rows so that the new rows, in order, are the old 1st, $(d+1)$th, $(2\cdot d+1)$th, ...; 2nd, $(d+2)$nd, ...; ... rows. Then do the same for the columns. The result is a block diagonal matrix with d blocks: the first $d-1$ blocks are the same and equal to

$$M' = \begin{matrix} \\ n/d \\ n/d \end{matrix}\overbrace{\qquad\qquad}^{n/d}\ \begin{matrix} \\ \overbrace{\qquad}^{\bar{i}'(1)/d} \end{matrix}$$

$$\begin{bmatrix} x(0) & 0\ldots & x(i'(1)) & \ldots & x(n) & 0 & \ldots 0 \\ & \ddots & & & & & \\ & & x(0) & \ldots\ldots\ldots & & & x(n) \\ (n/d)\cdot x(0) & 0 & \ldots & (\bar{i}'(1)/d)\cdot x(i'(1)) & \ldots & 0 & \\ & \ddots & & & & & \end{bmatrix};$$

and the last block, M'', is obtained from M' by removing the (n/d)th row and the last column. Expand the determinant of M' along the last column to obtain $\det(M') = (-1)^{(n/d)}\cdot x(n)\cdot\det(M'')$. The lemma follows easily from the observation that $\det(M'')$ is the resultant of $f(y; I''(\mathbf{x}'))$ and $\frac{\partial}{\partial y}f(y; I''(\mathbf{x}'))$ and so equals $x(0)\cdot D(f(y; I''(\mathbf{x}')))$. ∎

LEMMA 2.4. *Let $I' = \{i'(1), \ldots, i'(u')\}$, as in Lemma 2.3, be a subset of $\{1, 2, \ldots, n\}$ satisfying* (2.1) (a) (*i.e.*, $i'(u') = n$). *Let $I'' = \{i'(1), \ldots, i'(u'-1)\}$ regarded as a subset of $\{1, 2, \ldots, i'(u'-1)\}$, and, allowing a slight misuse of notation, write*

(2.3) (a) $\quad f(y/z; I') = (y/z)^{\bar{i}'(u'-1)}\cdot f(y/z; I'') + x(n).$

Then $D(f(y/z; I'))/x(n)^{\bar{i}'(u'-1)-1} \bmod (x(n))$ equals

(2.3) (b) $\quad (-1)^{n'}\cdot\bar{i}'(u'-1)^{\bar{i}'(u'-1)}\cdot x(i'(u'-1))^{\bar{i}'(u'-1)+1}\cdot D(f(y/z; I''))$

with $n' = (n-1)\cdot\bar{i}'(u'-1)$.

Proof. Factor $x(n)$ out of each of the last $\bar{i}'(u'-1)-1$ columns of $M(I')$ to obtain the matrix $\bar{M}'$ whose determinant is

$$x(0)\cdot D(f(y/z; I'))/x(n)^{\bar{i}'(u'-1)-1}.$$

Consider the matrix

$$\bar{M}'' = \begin{matrix} i'(u'-1) \\ n-1 \\ \bar{i}'(u'-1) \end{matrix}\left\{\begin{matrix} \\ \\ \\ \end{matrix}\right.\begin{bmatrix} x(0) & \ldots & x(i'(u'-1)) & 0 & \ldots & & \overbrace{\qquad}^{\bar{i}'(u'-1)} \\ & \ddots & & & & \overbrace{\quad}^{\bar{i}'(u'-1)-1} & 0 \\ 0 & & x(0) & & x(i'(u'-1)) & 0\ldots & x(n) \\ \hline n\cdot x(0) & \ldots & \bar{i}'(u'-1)\cdot x(i'(u'-1)) & 0 & \ldots & & 0 \\ 0 & \ddots & & \ddots & & & \\ & n\cdot x(0) & & \bar{i}'(u'-1)\cdot x(i'(u'-1)) & & & \\ \hline & & & & & \bar{i}'(u'-1)\cdot x(i'(u'-1)) & 0 \\ & & & & & 0 & \ddots \\ & & & & & & 1 \end{bmatrix}$$

The last $\bar{i}'(u'-1)$ rows of $\bar{M}''$ are, in order, the $(i'(u'-1)+1)$th, ..., $(n-1)$th rows of $\bar{M}'$, while the $(i'(u'-1)+1)$th to the $(i'(u'-1)+n)$th rows of $\bar{M}''$ are, in order, the nth to the $(2\cdot n-1)$th rows of $\bar{M}'$.

Thus, $\det(\bar{M}'') \bmod (x(n))$ is the product of

$$\left(\bar{i}'(u'-1)\cdot x\left(i'(u'-1)\right)\right)^{\bar{i}'(u'-1)}$$

and the determinant of the following matrix:

$$\bar{M}''' = \begin{matrix} \\ i'(u'-1) \\ \\ \\ i'(u'-1) \end{matrix}\left\{\begin{matrix} \left[\begin{matrix} x(0) & \dots & x(i'(u'-1)) \\ & \ddots & \\ x(0) & \dots & x(i'(u'-1)) \end{matrix}\right. \\ \hline \left.\begin{matrix} n\cdot x(0) & \dots & \bar{i}'(u'-1)\cdot x(i'(u'-1)) \\ & \ddots & \\ n\cdot x(0) & \dots & \bar{i}'(u'-1)\cdot x(i'(u'-1)) \end{matrix}\right] \end{matrix}\right.$$

Subtract $\bar{i}'(u'-1)$ times each of the first $i'(u'-1)$ rows from the corresponding one of the last $i'(u'-1)$ rows, and then expand the determinant of the resulting matrix about the $2\cdot i'(u'-1)$th column (which has only one nonzero entry, $x(i'(u'-1))$, in the $i'(u'-1)$th row). The result is

$$(-1)^{3\cdot i'(u'-1)}\cdot x\left(i'(u'-1)\right)\cdot R\left(f(y;I''), \frac{\partial}{\partial y}\left(f(y;I'')\right)\right),$$

and from this the conclusion of the lemma follows easily. ∎

COROLLARY 2.5. *Let* $I' = \{i'(1), \dots, i'(u')\}$ *be a subset of* $\{1, 2, \dots, n\}$ *satisfying* (2.1) (a). *Rename the* u'*-tuple of variables* $\left(x(i'(1)), \dots, x(i'(u'))\right)$ *to be* $\left(x'(0), x'(i'(2)-i'(1)), \dots, x'(n-i'(1))\right)$. *Let* $I''' = \{i'(2)-i'(1), \dots, n-i'(1)\}$ *regarded as a subset of* $\{1, 2, \dots, n-i'(1)\}$ *and write*

$$z^{n-i'(1)}\cdot f(y/z; I'''(x')) = \sum_{j=1}^{u'} x'\left(i'(j)-i'(1)\right)\cdot y^{n-i'(j)}\cdot z^{i'(j)-i'(1)}.$$

Then $D\left(f(y/z;I')\right)/x(0)^{i'(1)-1} \bmod (x(0))$ *equals*

$$(2.4)\qquad (-1)^{(n-1)\cdot i'(1)}\cdot i'(1)^{i'(1)}\cdot x\left(i'(1)\right)^{i'(1)+1}\cdot D\left(f(y/z; I'''(x'))\right).$$

Assume that $u' \geqslant 3$. *Then*

(2.5) (a)

$$E(I') \bmod (x(n)) \equiv (-1)^{(n-1)\cdot\bar{i}'(u'-1)}\cdot\bar{i}'(u'-1)^{\bar{i}'(u'-1)}\cdot x\left(i'(u'-1)\right)^{\bar{i}'(u'-2)}\cdot E(I'')$$

where I'', *regarded as a subset of* $\{1, 2, \dots, i'(u'-1)\}$ *is given in the statement of Lemma* 2.4; *and*

$$(2.5)\ (b)\qquad E(I') \bmod (x(0)) \equiv (-1)^{(n-1)\cdot i'(1)}\cdot i'(1)^{i'(1)}\cdot x\left(i'(1)\right)^{i'(2)}\cdot E\left(I'''(x')\right).$$

Proof. From Section 1, $D\left(f(y/z;I')\right) = D\left(f(z/y;I')\right)$ where $y^n\cdot f(z/y;I')$ equals

$$x(0)\cdot z^n + \sum_{j=1}^{u'} x\left(i'(j)\right)\cdot y^{i'(j)}\cdot z^{n-i'(j)}.$$

Apply Lemma 2.4 to $D\left(f(z/y;I')\right)$ by changing $x(n)$ to $x(0)$ (the coefficient of z^n), by changing $x\left(i'(u'-1)\right)$ to $x\left(i'(1)\right)$ after noting that the power of y that appears in the corresponding terms changes from $\bar{i}'(u'-1)$ to $i'(1)$, and finally by noting, again from Section 1, that $D\left(f(y/z; I'''(x'))\right) = D\left(f(z/y; I'''(x'))\right)$.

Formula (2.5) (a) follows, now, immediately from Lemma 2.2 by checking the power of $x\left(i'(u'-1)\right)$ that appears on both sides of the equation. Similarly for (2.5) (b). ∎

Finally, the next lists summarize the application of Corollary 2.5 and Lemma 2.3 to simplify the expressions $E(I) \bmod (x(k))$ for $k = 0, i(1), \dots$ $\dots, i(u) = n$. Consider the greatest common divisors of the following sets: for $\{\bar{i}(u-1), \dots, \bar{i}(1), n\} - \{\bar{i}(j)\}$ let this be $d(j)$, $j = 1, \dots, u-1$; for $\{i(u-1)-$ $-i(u-2), \dots, i(u-1)-i(1), i(u-1)\}$ let this be $d(u)$; and for $\{\bar{i}(u-1), \dots, \bar{i}(1)\}$ let this be $d(0)$. Denote by $I(j)$ the set

$$\{i(1)/d(j), \dots, i(j-1)/d(j), i(j+1)/d(j), \dots, i(u)/d(j)\},$$

regarded as a subset of $\{1, 2, \dots, i(u)/d(j)\}$ if $j \neq u$; let $I(u)$ be the set

$$\{i(1)/d(u), \dots, i(u-1)/d(u)\}$$

regarded as a subset of $\{1, 2, \dots, i(u-1)/d(u)\}$; and let $I(0)$ be the set

$$\{(i(2)-i(1))/d(0), \dots, (n-i(1))/d(0)\}.$$

Compatible with notation of the previous results of this subsection define $f(y/z; I(j))$ by the following formulae:

$$(2.6)\ (a)\qquad f(y/z;I) = f\left((y/z)^{d(j)}; I(j)\right) + x\left(i(j)\right)\cdot(y/z)^{n-i(j)},$$

$j = 0, 1, \dots, u-1$ where $i(0) = 0$; and

$$(b)\qquad f(y/z;I) = (y/z)^{\bar{i}(u-1)}\cdot f\left(y/z; I(u)\right) + x(n).$$

Then, for $E\left(I(j)\right)$ computed from $f\left(y/z; I(j)\right)$ as above:

$$(2.7)\ (a)\qquad E(I) \equiv (-1)^{n-(n/d(j))}\cdot d(j)^n\cdot\left(E\left(I(j)\right)\right)^{d(j)} \bmod \left(x\left(i(j)\right)\right)$$

for $j \neq 0, 1, u-1, u$;

$$(b)\qquad E(I) \equiv (-1)^{n'}\cdot x\left(i(u-1)\right)^{\bar{i}(u-2)}\cdot\bar{i}(u-1)^{\bar{i}(u-1)}\cdot d(u)^{i(u-1)}\times$$

$$\times E\left(I(u)\right)^{d(u)} \bmod (x(n)),$$

with $n' = n\cdot\left(\bar{i}(u-1)+1\right) - \left(i(u-1)/d(u)\right)$;

$$(c)\qquad E(I) \equiv (-1)^{n''}\cdot x\left(i(1)\right)^{i(2)}\cdot i(1)^{i(1)}\cdot d(0)^{\bar{i}(1)}\cdot E\left(I(0)\right)^{d(0)} \bmod (x(0)),$$

with $n'' = n\cdot\left(i(1)+1\right) - \left(\bar{i}(1)/d(0)\right)$;

(d) $E(I) \equiv (-1)^{n-(n/d(1))} \cdot x(0)^{i(2)-i(1)} \cdot d(1)^n \cdot E(I(1))^{d(1)} \bmod (x(i(1)))$; and

(e) $E(I) \equiv (-1)^{n-(n/d(u-1))} \cdot x(n)^{i(u-1)-i(u-2)} \cdot d(u-1)^n \times$
$\times E(I(u-1))^{d(u-1)} \bmod (x(i(u-1)))$.

This subsection concludes with an example to accustom the reader with these formulae and to display the comparative case with which we may now show that, for I satisfying expression (2.1), $E(I)$ is reduced.

EXAMPLE 2.6. Let $n = 15$, $I = \{5, 6, 15\}$ so $f(y/z; I)$ is a *quadrinomial*. We simplify the formulae (2.7) by totally disregarding the power of -1 appearing in the initial term of the products. In addition we use expression (1.3) to compute $E(I)$ in the case that $f(y/z; I)$ is a *trinomial*. Compute:

(2.8) (a) $E(I) \equiv 9^9 \cdot x(6)^{10} \cdot (6^6 \cdot x(0) \cdot x(6)^5 - 5^5 \cdot x(5)^6) \bmod (x(15))$;

(b) $E(I) \equiv 5^5 \cdot x(5)^6 \cdot (10^{10} \cdot x(5)^9 \cdot x(15) - 9^9 \cdot x(6)^{10}) \bmod (x(0))$;

(c) $E(I) \equiv 3^{15} \cdot x(0) \cdot (5^5 \cdot x(0)^3 \cdot x(15)^2 + 2^2 \cdot 3^3 \cdot x(6)^5)^3 \bmod (x(5))$; and

(d) $E(I) \equiv 5^{15} \cdot x(15) \cdot (3^3 \cdot x(0)^2 \cdot x(15) + 2^2 \cdot x(5)^3)^5 \bmod (x(6))$.

All expressions are of weight 90 and degree 16. If $E(I)$ is irreducible, then it is reduced; assume that $E(I) = F \cdot G$. Let F be the factor of largest weight. From (2.8) (b) and (c), F has weight 60 or 90. If F has weight 60, then $\deg(F) = 10$ and $\deg(G) = 6$ which implies, from (2.8) (c), that $G \bmod (x(5))$ is a constant times $x(0) \cdot (5^5 \cdot x(0)^3 \cdot x(15)^2 + 2^2 \cdot 3^3 \cdot x(6)^5)$ which is reduced if $\mathrm{char}(F)$ does not divide $2 \cdot 3 \cdot 5$. Clearly, with this supposition $E(I)$ is reduced. ∎

3. The irreducibility of $E(I)$. This section consists of the proof, divided into parts, of the following:

THEOREM 3.1. *For*

$$z^n \cdot f(y/z; I) = x(0) \cdot y^n + \sum_{j=1}^{u} x(i(j)) \cdot y^{n-i(j)} \cdot z^{i(j)}$$

where expression (2.1) *holds* (*i.e.*, $(i(1), \ldots, i(u)) = 1$, $i(u) = n$) *consider* $E(I)$, *defined by the formula*

$$D(f(y/z; I)) = x(0)^{i(1)-1} \cdot x(n)^{i(u-1)-1} \cdot E(I)$$

(*as in Lemma* 2.2). *Then, there exists an explicitly computable integer* $N(i(1), \ldots, i(u))$ *such that* $E(I)$ *is irreducible if* $(\mathrm{char}(F), N(i(1), \ldots, i(u))) = 1$.

We go through the proof on the assumption that $\mathrm{char}(F) = 0$, and, at the conclusion, collect observations on the integer $N(i(1), \ldots, i(u))$. When $f(y/z; I)$ is a trinomial the result is known: expression (1.3).

Part 1. *Reduction to the case when* $f(y/z; I)$ *is a quadrinomial.* Induct on the cardinality of I assuming that the result is true in the case that $|I| = 3$ (or

2). For this argument let c_j denote a constant of no serious consequence to the computations. Suppose $E(I) = F \cdot G$. Conclude from expression (2.7) that

(3.1) (a) $F \equiv c_1 \cdot x(0)^{r(1)} \cdot (E(I(1)))^{s(1)} \bmod (x(i(1)))$ with
$s(1) \leqslant d(1)$ and $r(1) \leqslant i(2) - i(1)$; and

(b) $F \equiv c_2 \cdot (E(I(2)))^{s(2)} \bmod (x(i(2)))$ with $s(2) \leqslant d(2)$.

Thus, from Lemma 2.2, $\mathrm{wt}(F) = s(1) \cdot \mathrm{wt}(E(I(1))) = s(1) \cdot n \cdot i(u-1)/(d(1))$ $= s(2) \cdot \mathrm{wt}(E(I(2))) = s(2) \cdot n \cdot i(u-1)/(d(2))$. Note that the weight, in these cases, involves the coefficients of $f(y/z; I)$ although they appear in terms of lower degree in y/z in $f(y/z; I(j))$. From this equation $d(1) \cdot s(2) = d(2) \cdot s(1)$, and since $(d(1), d(2)) = 1$, this implies that either $s(1) = d(1)$ and $s(2) = d(2)$, or $s(i) = 0$ for some $i = 1, 2$. In either case, one of F or G is a constant, and this concludes the argument under the induction assumption.

Part 2. *The basic equations when* $f(y/z; I)$ *is a quadrinomial.* Let $I = \{i(1), i(2), i(3)\}$ and start the analysis as in Part 1 by an application of (2.7) and (1.3) to a factor F of $E(I)$ to conclude:

(3.2) (a) $F \equiv c_0 \cdot x(i(1))^{r(0)} \cdot (E(I(0)))^{s(0)} \bmod (x(0))$
$\equiv c_0 \cdot x(i(1))^{r(0)} \cdot (A(0) + (-1)^{(\bar{i}(1)/d(0))-1} \cdot B(0))^{s(0)}$
with
$s(0) \leqslant d(0)$, $r(0) \leqslant i(2)$, $i'(2, 1) = (i(2) - i(1))/d(0)$,
$A(0) = (\bar{i}(1)/d(0))^{\bar{i}(1)/d(0)} \cdot x(i(1))^{\bar{i}(2)/d(0)} \cdot x(i(3))^{i'(2,1)}$, and
$B(0) = i'(2, 1)^{i'(2,1)} \cdot (\bar{i}(2)/d(0))^{\bar{i}(2)/d(0)} \cdot x(i(2))^{\bar{i}(1)/d(0)}$;

(b) $F \equiv c_3 \cdot x(i(2))^{r(3)} \cdot (E(I(3)))^{s(3)} \bmod (x(i(3)))$
$\equiv c_3 \cdot x(i(2))^{r(3)} \cdot (A(3) + (-1)^{(i(2)/d(3))-1} \cdot B(3))^{s(3)}$
with
$s(3) \leqslant d(3)$, $r(3) \leqslant \bar{i}(1)$, $i''(2, 1) = (i(2) - i(1))/d(3)$,
$A(3) = (i(2)/d(3))^{i(2)/d(3)} \cdot x(0)^{i''(2,1)} \cdot x(i(2))^{i(1)/d(3)}$, and
$B(3) = (i(1)/d(3))^{i(1)/d(3)} \cdot i''(2, 1)^{i''(2,1)} \cdot x(i(1))^{i(2)/d(3)}$;

(c) $F \equiv c_1 \cdot x(0)^{r(1)} \cdot E(I(1))^{s(1)} \bmod (x(i(1)))$
$\equiv c_1 \cdot x(0)^{r(1)} \cdot (A(1) + (-1)^{(i(3)/d(1))-1} \cdot B(1))^{s(1)}$
with
$s(1) \leqslant d(1)$, $r(1) \leqslant i(2) - i(1)$,
$A(1) = (n/d(1))^{n/d(1)} \cdot x(0)^{\bar{i}(2)/d(1)} \cdot x(i(3))^{i(2)/d(1)}$, and
$B(1) = (i(2)/d(1))^{i(2)/d(1)} \cdot (\bar{i}(2)/d(1))^{\bar{i}(2)/d(1)} \cdot x(i(2))^{n/d(1)}$;

(d) $F \equiv c_2 \cdot x(i(3))^{r(2)} \cdot E(I(2))^{s(2)} \bmod (x(i(2)))$
$\equiv c_2 \cdot x(i(3))^{r(2)} \cdot (A(2) + (-1)^{(i(3)/d(2))-1} \cdot B(2))^{s(2)}$

with

$$s(2) \leqslant d(2),\ r(2) \leqslant i(2)-i(1),$$

$$A(2) = \left(n/d(2)\right)^{n/d(2)} \cdot x(0)^{\bar{i}(1)/d(2)} \cdot x\left(i(3)\right)^{i(1)/d(2)}, \text{ and}$$

$$B(2) = \left(i(1)/d(2)\right)^{i(1)/d(2)} \cdot \left(\bar{i}(1)/d(2)\right)^{\bar{i}(1)/d(2)} \cdot x\left(i(1)\right)^{n/d(2)}.$$

Part 3. *Two variable monomial equalities.* The powers a and b to which the variables $x\left(i(j)\right)$ and $x\left(i(k)\right)$ appear in the monomial $x\left(i(j)\right)^a \cdot x\left(i(k)\right)^b$ in F may be checked through the appearance of this monomial in the formulae of (3.2): monomials involving only $x(0)$ and $x\left(i(3)\right)$ in (3.2) (c) and (d) give the formulae

$$r(1)+s(1)\cdot\left(\bar{i}(2)/d(1)\right) = s(2)\cdot\left(\bar{i}(1)/d(2)\right)$$

and

$$s(1)\cdot\left(i(2)/d(1)\right) = r(2)+s(2)\cdot\left(i(1)/d(2)\right);$$

monomials involving only $x(0)$ and $x\left(i(2)\right)$ in (3.2) (b) and (c) give the formulae

$$s(3)\cdot i''(2,\ 1) = r(1) \quad \text{and} \quad r(3)+s(3)\cdot\left(i(1)/d(3)\right) = s(1)\cdot n/d(1);$$

monomials involving only $x\left(i(1)\right)$ and $x\left(i(3)\right)$ in (3.2) (a) and (d) give the formulae

$$r(0)+s(0)\cdot\left(\bar{i}(2)/d(0)\right) = s(2)\cdot\left(n/d(2)\right) \quad \text{and} \quad s(0)\cdot i'(2,\ 1) = r(2);$$

and monomials involving only $x\left(i(1)\right)$ and $x\left(i(2)\right)$ in (3.2) (a) and (b) give the formulae

$$r(0) = s(3)\cdot\left(i(2)/d(3)\right) \quad \text{and} \quad s(0)\cdot\left(\bar{i}(1)/d(0)\right) = r(3).$$

Eliminate $r(0)$, $r(1)$, $r(2)$ and $r(3)$ from these equations to obtain equations relating the quantities $s(i)/d(i) = s'(i)$, $i = 0,\ 1,\ 2,\ 3$:

(3.3) (a) $s'(3)\cdot\left(\bar{i}(1)-\bar{i}(2)\right) = s'(2)\cdot\bar{i}(1)-s'(1)\cdot\bar{i}(2)$;

(b) $s'(1)\cdot n = s'(0)\cdot\bar{i}(1)+s'(3)\cdot i(1)$;

(c) $s'(3)\cdot i(2) = s'(2)\cdot n-s'(0)\cdot\bar{i}(2)$; and

(d) $s'(0)\cdot\left(i(2)-i(1)\right) = s'(1)\cdot i(2)-s'(2)\cdot i(1)$.

Note: $i(2)-i(1) = \bar{i}(1)-\bar{i}(2)$, and given any two of these equations the other two are linearly dependent upon these.

Finally we record the coefficients, up to sign, of the monomials of F involving only two variables: coefficients of monomials involving only $x(0)$ and $x\left(i(3)\right)$ in (3.2) (c) and (d)

(3.4) (a) $c_1\cdot\left(n/d(1)\right)^{n\cdot s'(1)}$ and $c_2\cdot\left(n/d(2)\right)^{n\cdot s'(2)}$ where c_1 divides $d(1)^n$ and c_2 divides $d(2)^n$;

coefficients of monomials involving only $x(0)$ and $x\left(i(2)\right)$ in (3.2) (b) and (c)

(b) $c_3\cdot\left(i(2)/d(3)\right)^{i(2)\cdot s'(3)}$ and
$c_1\cdot\left(i(2)/d(1)\right)^{i(2)\cdot s'(1)}\cdot\left(\bar{i}(2)/d(1)\right)^{\bar{i}(2)\cdot s'(1)}$ where
c_3 divides $\bar{i}(2)^{\bar{i}(2)}\cdot d(3)^{i(2)}$;

coefficients of monomials involving only $x\left(i(1)\right)$ and $x\left(i(3)\right)$ in (3.2) (a) and (d)

(c) $c_0\cdot\left(\bar{i}(1)/d(0)\right)^{\bar{i}(1)\cdot s'(0)}$ and
$c_2\cdot\left(i(1)/d(2)\right)^{i(1)\cdot s'(2)}\cdot\left(\bar{i}(1)/d(2)\right)^{\bar{i}(1)\cdot s'(2)}$ where
c_0 divides $i(1)^{i(1)}\cdot d(0)^{\bar{i}(1)}$; and

coefficients of monomials involving only $x\left(i(1)\right)$ and $x\left(i(2)\right)$ in (3.2) (a) and (b)

(d) $c_0\cdot\left(\left(i(2)-i(1)\right)/d(0)\right)^{(i(2)-i(1))\cdot s'(0)}\cdot\left(\bar{i}(2)/d(0)\right)^{\bar{i}(2)\cdot s'(0)}$ and
$c_3\cdot\left(i(1)/d(3)\right)^{i(1)\cdot s'(3)}\cdot\left(\left(i(2)-i(1)\right)/d(3)\right)^{(i(2)-i(1))\cdot s'(3)}$.

Part 4. *The divisibility relation for a sequence.* Recall, for a prime p, that the notation $p^i \| r$ means that the ith power of p is the highest power of p that divides r. A sequence of integers $\bar{a}(1)$, $\bar{a}(2)$, $\bar{a}(3)$ satisfies the *divisibility relation* if the following holds: $\left(\bar{a}(1),\ \bar{a}(2),\ \bar{a}(3)\right) = 1$; and, for each prime p, if $p^i \| \bar{a}(2)$, then either $p^i \| \bar{a}(1)$ or $p^i \| \bar{a}(3)$. Clearly, if $\bar{a}(1)$, $\bar{a}(2)$, $\bar{a}(3)$ satisfy the divisibility relation then $\bar{a}(2) = \left(\bar{a}(2),\ \bar{a}(1)\right)\cdot\left(\bar{a}(2),\ \bar{a}(3)\right)$.

Consider the following sequences:

(3.5) (a) $i(2)-i(1),\ \bar{i}(2),\ n$;

(b) $i(1),\ i(2)-i(1),\ \bar{i}(2)$;

(c) $n,\ i(1),\ i(2)-i(1)$;

(d) $n,\ \bar{i}(1),\ i(2)-i(1)$; and

(e) $i(2)-i(1),\ i(2),\ n$.

From $\left(i(1),\ i(2),\ n\right) = 1$ each sequence is a relatively prime triple. Suppose that each satisfies the divisibility relation. Then, from the expression $i(2) = i(1)+\left(i(2)-i(1)\right)$ (3.5) (b), (c) and (e) yield

$$\left(i(2),\ i(2)-i(1)\right)\cdot\left(i(2),\ n\right)$$
$$= \left(i(1),\ n\right)\cdot\left(i(1),\ i(2)-i(1)\right)+\left(i(2)-i(1),\ i(1)\right)\cdot\left(i(2)-i(1),\ \bar{i}(2)\right).$$

Divide this by $\left(i(1),\ i(2)-i(1)\right)$ to obtain

$$\left(i(2),\ n\right) = \left(i(1),\ n\right)+\left(i(2)-i(1),\ \bar{i}(2)\right) \quad \text{or} \quad \left(i(2),\ n\right) > \left(i(1),\ n\right).$$

Similarly, from the expression $\bar{i}(1) = \bar{i}(2)+\bar{i}(1)-\bar{i}(2)$ (3.5) (a), (b) and (d) yield

$$\left(\bar{i}(1),\ n\right)\cdot\left(\bar{i}(1),\ \bar{i}(1)-\bar{i}(2)\right)$$
$$= \left(\bar{i}(2),\ \bar{i}(1)-\bar{i}(2)\right)\cdot\left(\bar{i}(2),\ n\right)+\left(\bar{i}(1)-\bar{i}(2),\ i(1)\right)\cdot\left(\bar{i}(1)-\bar{i}(2),\ \bar{i}(2)\right).$$

Divide this by $(\bar{i}(1), \bar{i}(1)-\bar{i}(2)) = (\bar{i}(2), \bar{i}(1)-\bar{i}(2))$ to obtain

$$(\bar{i}(1), n) = (\bar{i}(2), n)+(\bar{i}(1)-\bar{i}(2), i(1))$$

or

$$(\bar{i}(1), n) = (i(1), n) > (\bar{i}(2), n) = (i(2), n).$$

This contradiction shows that *it is not possible for all of the sequences of expression* (3.5) *to satisfy the divisibility relation.*

Part 5. Conclusion that there exists $i \neq j$ for which $s'(i) = s'(j)$. From the argument of Part 1, $E(I)$ is irreducible in the quadrinomial case if there exists $i \neq j$ for which $s'(i) = s'(j)$, and this concludes the proof of the theorem. The remainder of this part consists of computations to show that *either $s'(l) = s'(k)$ for some $l \neq k$ or all of the sequences of expression* (3.13) *satisfy the divisibility relation*: from the conclusion of Part 4 this proves the theorem.

The treatments of each of the sequences of expression (3.5) are approximately the same; tedious, mostly, once one has been inspected. Therefore we consider only (3.5) (b) which is, perhaps, the most involved since it has $i(2)-i(1)$ as the middle term. Suppose $p^e \| i(2)-i(1)$ with $e > 0$. We must show that if $p \nmid i(1)$ (resp., $p \nmid \bar{i}(2)$) then either $p^e \| \bar{i}(2)$ (resp., $p^e \| i(1)$) or $s'(l) = s'(k)$ for some $l \neq k$.

Assume $p \nmid i(1)$ and $p^f \| \bar{i}(2)$ with $e \neq f$. Let a_l be the power of p in c_l, $i = 0, 1, 2, 3$. There are two subcases: start with the case $f > e$. Then $p^e \| \bar{i}(1)$. Also, $p \nmid n$, so $p \nmid d(1)$, $d(2)$ or $d(3)$, and $p^e \| d(0)$. By equating the powers of p that appear in the pairs of coefficients of expression (3.4), we obtain (in order) four equations: $0 = 0$; $a_3 = f \cdot \bar{i}(2) \cdot s'(1)$; $a_0 = e \cdot \bar{i}(1) \cdot s'(2)$; and $a_0 + (f-e) \cdot \bar{i}(2) \cdot s'(0) = a_3 + e \cdot (i(2)-i(1)) \cdot s'(3)$.

Eliminate a_0 and a_3 to get

$$e \cdot \bar{i}(1) \cdot s'(2) + (f-e) \cdot \bar{i}(2) \cdot s'(0) = f \cdot \bar{i}(2) \cdot s'(1) + e \cdot (i(2)-i(1)) \cdot s'(3).$$

Now use the equations of (3.3) (a) and (d) to eliminate $s'(0)$ and $s'(3)$; the result is $s'(1) = s'(2)$.

Now consider the subcase $e > f$, so $p^f \| \bar{i}(1)$. Again, from the pairs of coefficients of expression (3.4): $0 = 0$; $a_3 = f \cdot \bar{i}(1) \cdot s'(1)$; $a_0 = f \cdot \bar{i}(1) \cdot s'(2)$; and

$$a_0 + (e-f) \cdot (i(2)-i(1)) \cdot s'(0) = a_3 + e \cdot (i(2)-i(1)) \cdot s'(3).$$

Thus,

$$f \cdot \bar{i}(1) \cdot s'(2) + (e-f) \cdot (i(2)-i(1)) \cdot s'(0) = f \cdot \bar{i}(2) \cdot s'(1) + e \cdot (i(2)-i(1)) \cdot s'(3).$$

Eliminating $s'(0)$ and $s'(3)$ as above, one concludes $s'(1) = s'(2)$.

Part 6. Comments on the divisors of $N(i(1), \ldots, i(u))$. The proof above has established that $E(I)$ is irreducible (as a polynomial in $\boldsymbol{Z}[x(0), \ldots, x(n)]$). It is clear from the proof that, in extending the result from $\boldsymbol{Q}$ to F of arbitrary characteristic, the characteristics of difficulty must include the divisors of $i(1), \ldots, i(u)$, and $i(j)-i(k)$ for $j \neq k$, $j = 1, \ldots, u$; $k = 1, \ldots, u$. It is reasonable to guess that these are the only bad primes and that $N(i(1), \ldots, i(u))$ may be taken to be the product of just these primes. There is, however, a fair objection to this. The argument of Parts 4 and 5 depends on divisibility properties of differences of coefficients in the list of expression (3.4), and such an argument cannot work directly over a field of positive characteristic.

Thus, appropriately, as an ending to our argument, we appeal to a well known lemma of Noether: Since $E(I)$ (as a polynomial in $\boldsymbol{Z}[x(0), \ldots, x(n)]$) is irreducible, there is an explicitly computable integer $N(i(1), \ldots, i(u))$ such that, for p a prime not dividing $N(i(1), \ldots, i(u))$, $E(I) \bmod (p)$ is irreducible in $\boldsymbol{Z}/(p)[x(0), \ldots, x(n)]$ (e.g., [2]; Lemma 3.1 on p. 219). This is the integer whose existence is asserted in the statement of the theorem.

4. The intersection of $E(I)$ with a Cohen locus. A Cohen sublocus of $X(I)$ derives from a subset J of $I \cup \{0\}$ with $|I \cup \{0\} - J| \geqslant 2$ and nonzero values $a(i) \in F$ for $i \in J$.

Denote the result of specialization of $x(i)$ to $a(i)$ in $E(I)$, $i \in J$, by $E(I, \boldsymbol{a})$.

In the next theorem we consider only the case $I = \{m, m+1, n\}$ and $J = \{0, n\}$ (i.e., set $x(0) = a(0)$ and $x(n) = a(n)$).

THEOREM 4.1. *If the characteristic is suitably large (dependent only on m and n), then $E(I, \boldsymbol{a})$ is irreducible where I and J are given above.*

Proof. Since the result is so special we show the method of proof only in the case $m = 5$, $n = 15$ (i.e., Example 2.6) to avoid tedious calculation. With no loss assume that $F = \bar{F}$ is algebraically closed. Denote $E(I, \boldsymbol{a})$ by E and note that (2.8) (c) and (d) are valid for E and (2.8) (a) and (b) can be used to identify the terms of E which do not contain both $x(0)$ and $x(n)$.

Write $E = R(16)+R(15)+ \ldots +R(0)$ where $R(k)$ consists of all terms of total degree k in $x(5)$ and $x(6)$. From (3.8) (up to change of the sign of E):

$$R(16) = -5^5 \cdot 9^9 \cdot x(5)^6 \cdot x(6)^{10};$$

$$R(15) = 3^{15} \cdot 2^6 \cdot 3^9 \cdot a(0) \cdot x(6)^{15} + 5^{15} \cdot 2^{10} \cdot a(15) \cdot x(5)^{15}.$$

Suppose $E = F \cdot G$. Display the terms of F and G by their total degrees:

$$F = P(i)+P(i-1)+ \ldots +P(0),$$

$$G = Q(j)+Q(j-1)+ \ldots +Q(0), \quad i+j = 16.$$

Since $P(i) \cdot Q(j) = R(16)$ both $P(i)$ and $Q(j)$ are monomials. Moreover $P(i) \cdot Q(j-1)+P(i-1) \cdot Q(j) = R(15)$ contains both $x(6)^{15}$ and $x(5)^{15}$. This is impossible if either $P(i)$ or $Q(j)$ is divisible by $x(5) \cdot x(6)$. So each of $P(i)$ and $Q(j)$ is a power of a single variable, say $P(i) = c(10) \cdot x(6)^{10}$ and $Q(j) = d(6) \cdot x(5)^6$ for some $c(10)$, $d(6)$ in $\bar{F}$.

Since $c(10)\cdot d(6) = -5^5\cdot 9^9$ we may assume $c(10) = -9^9$, $d(6) = 5^5$. Hence $R(15) = -3^{18}\cdot x(6)^{10}\cdot Q(5)+5^5\cdot x(5)^6\cdot P(9)$. All monomials in the first term are divisible by at least 10 powers of $x(6)$ and those in the second by at most 9, so there is no cancellation of terms. Hence

$$Q(5) = -6^6\cdot a(0)\cdot x(6)^5, \qquad P(9) = 10^{10}\cdot a(15)\cdot x(5)^9,$$

$$F = -9^9\cdot x(6)^{10}+10^{10}\cdot a(15)\cdot x(5)^9+P(8)+\ \dots\ +P(0).$$

Note that $E \bmod (x(5))$ is $3^{15}\cdot a(0)$ times a product of fifteen terms of the form $2^{2/5}\cdot 3^{3/5}\cdot x(6)+\varepsilon_i\cdot 5\cdot a(0)^{3/5}\cdot a(15)^{2/5}$ where the ε_i are various fifth roots of 1. Since $F \bmod (x(5))$ starts with $3^{18}\cdot x(6)^{10}$ it must contain a product, π, of ten of the above factors:

$$\pi = 2^4\cdot 3^6\cdot x(6)^{10}+\ \dots\ +\varepsilon\cdot 5^{10}\cdot a(0)^6\cdot a(15)^4 \quad \text{with} \quad \varepsilon^5 = 1$$

and

$$F \equiv -3^{18}\cdot x(6)^{10}+\ \dots\ \equiv -3^{12}\cdot 2^{-4}\cdot \pi \bmod (x(5)).$$

Hence the constant term, $P(0)$, of F is $-3^{12}\cdot 2^{-4}\cdot 5^{10}\cdot a(0)^6\cdot a(15)^4\cdot\varepsilon$. A similar argument gives

$$F \equiv 10^{10}\cdot a(15)\cdot x(5)^9+\ \dots\ \equiv 10^{10}\cdot 2^{-6}\cdot a(15)\cdot \pi' \bmod (x(6)),$$

where π' is a product of 9 factors of the form

$$2^{2/3}\cdot x(5)+\eta_j\cdot 3\cdot a(0)^{2/3}\cdot a(15)^{1/3} \quad \text{with} \quad \eta_j^3 = 1.$$

Hence $P(0) = 5^{10}\cdot 2^4\cdot 3^9\cdot a(0)^6\cdot a(15)^4\cdot\eta$. If the characteristic of $\bar{F}$ is not 2, 3 or 5, comparison of these two expressions for $P(0)$ gives $\eta\cdot 2^8 = -\varepsilon\cdot 3^3$. Put both sides to the 15th power to get a contradiction if $(\mathrm{Char}(\bar{F}),\ 2^{120}+3^{45}) = 1$. ∎

References

[1] S. Cohen, *The Galois group of a polynomial with two indeterminate coefficients*, Pacific J. Math. 90 (1980), pp. 63–76. Also, corrections: ibid. 97 (1981), pp. 482–486.

[2] M. Fried and G. Sacerdote, *Solving diophantine problems over all residue class fields of a number field and all finite fields*, Ann. of Math. 104 (1976), pp. 203–233.

[3] D. Mumford, *Introduction to algebraic geometry*, University of Harvard Notes, 1966.

[4] B. L. van der Waerden, *Modern Algebra*, Vol. 1, Springer-Verlag, Berlin 1937; rev. English translation, Unger, New York 1953.

Added in proof:

[5] J. H. Smith, *General trinomials having symmetric Galois group*, Proc. Amer. Math. Soc. 63 (1977), pp. 208–217.

[6] — *Erratum to "General trinomials having symmetric Galois group"*, ibid. 77 (1979), p. 298.

Received on 9.9.1982
and in revised form on 16.2.1983 (1319)

ACTA ARITHMETICA
XLIV (1984)

On sums of sequences of integers, I

by

A. Balog and A. Sárközy (Budapest)

1. Throughout this paper, we use the following notation: c_1, c_2, ..., M_0, M_1, ... denote positive absolute constants. θ_1, θ_2, ... are real numbers such that $|\theta_i| \leqslant 1$ for all i. We write $e^x = \exp(x)$ and $e^{2\pi i x} = e(\alpha)$. The distance from α to the nearest integer is denoted by $\|\alpha\|$ so that $\|\alpha\| = \min(\alpha-[\alpha], [\alpha]+1-\alpha)$. We put $\min(A, 1/0) = A$. We denote the least prime factor of n by $p(n)$, while the greatest prime factor of n is denoted by $P(n)$. $\nu(n)$ denotes the number of all the prime factors of n:

$$\nu(n) = \sum_{p^\alpha \mid n,\, p^{\alpha+1}\nmid n} \alpha.$$

2. In this series, we study the arithmetic nature of the numbers of the form $a+b$ where a, b are taken from "dense" sequences of integers. (See [2] for some related results.) In fact, this paper is devoted to the proof of the following theorem:

THEOREM. *Let* $M > M_0$, $\mathscr{A} \subset \{1, 2, \dots, M\}$ *and* $\mathscr{B} \subset \{1, 2, \dots, M\}$. *Put*

$$A(n) = \sum_{\substack{a\leqslant n\\ a\in\mathscr{A}}} 1, \qquad B(n) = \sum_{\substack{b\leqslant n\\ b\in\mathscr{B}}} 1,$$

$$A = A(M), \qquad B = B(M).$$

If

$$AB > M^{5/3}(\log M)^{13}, \tag{1}$$

then there exist integers a, b *such that* $a\in\mathscr{A}$, $b\in\mathscr{B}$ *and*

$$P(a+b) \leqslant y \tag{2}$$

where

$$y \overset{\text{def}}{=} \begin{cases} \exp\{4(\log M\log\log M)^{1/2}\} & \text{for } AB > M^2\exp\{-2(\log M\log\log M)^{1/2}\},\\ \dfrac{M^2}{AB}\exp\left(4\dfrac{\log M}{\log(M^2/AB)}\log\log M\right) & \text{for } AB \leqslant M^2\exp\{-2(\log M\log\log M)^{1/2}\}. \end{cases} \tag{3}$$