ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 42, Number 2, 2012

GENERATION OF THE SYMMETRIC FIELD BY NEWTON POLYNOMIALS IN PRIME CHARACTERISTIC

MAURIZIO MONGE

ABSTRACT. Let $N_m = x^m + y^m$ be the mth Newton polynomial in two variables, for $m \geq 1$. Dvornicich and Zannier proved that in characteristic zero three Newton polynomials N_a, N_b, N_c are always sufficient to generate the symmetric field in x and y, provided that a, b, c are distinct positive integers such that $(a, b, c) = 1$. In the present paper we prove that in the case of the prime characteristic p the result still holds, if we assume additionally that $a, b, c, a - b, a - c, b - c$ are prime with p. We also provide a counterexample in the case where one of the hypotheses is missing.

The result follows from the study of the factorization of a generalized Vandermonde determinant in three variables, which under general hypotheses factors as the product of a trivial Vandermonde factor and an irreducible factor. On the other side, the counterexample is connected to certain cases where Schur polynomials factor as a product of linear factors.

1. Introduction. Let $F = k(x, y)$ be the function field generated over a field k by the algebraically independent transcendentals x, y, and let S be the subfield of symmetric functions. Let N_m be the mth Newton polynomial (or power sum) in x and y

$$N_m = x^m + y^m, \quad \text{for } m \geq 1.$$

Note that if the characteristic is p, then $N_{p^k m} = N_m^{p^k}$, for each $k \in \mathbf{N}$.

We will also call $\mathcal{N}_{a,b}$ (respectively $\mathcal{N}_{a,b,c}$) the subfield of F generated by N_a, N_b (respectively N_a, N_b, N_c) over k, i.e.

$$\mathcal{N}_{a,b} = k(N_a, N_b), \qquad \mathcal{N}_{a,b,c} = k(N_a, N_b, N_c).$$

In [**5**] Mead and Stein calculated the degree of the extension $S/\mathcal{N}_{a,b}$ in characteristic zero and conjectured that $S = \mathcal{N}_{a,b,c}$ (i.e., N_a, N_b, N_c

Received by the editors on March 18, 2009, and in revised form on September 7, 2009.

DOI:10.1216/RMJ-2012-42-2-729

generate the whole symmetric field) whenever a, b, c are distinct integers such that $(a, b, c) = 1$, also providing evidence for their conjecture. This conjecture was finally settled in [**1**] by Dvornicich and Zannier, by computing the Galois group of a polynomial connected to a fundamental determinantal equation via the Riemann Existence theorem. The solution of the conjecture then followed after they proved that such a Galois group must be the full symmetric group, and considering the action of the Galois group on a system of equations connected to the problem.

These topological methods do not seem to admit an immediate generalization to the prime characteristic case. However, we will show that the same result also follows from the irreducibility of the main factor of the fundamental determinantal equation, and that in many cases such irreducibility can be proved by elementary methods.

It should also be noted that it is not possible to expect the conjecture to hold in prime characteristic without any additional hypothesis, since whenever a, b are distinct positive integers such that $(a, b) = 1$, then a, pa, b are coprime integers and $N_{pa} = N_a^p$, so $\mathcal{N}_{a,pa,b} = \mathcal{N}_{a,b}$ (that can be easily seen to be $\neq S$, in general). It is not enough just to request that a, b, c all be prime with p: in the last section to show that there exist triples of coprime integers a, b, c, all prime with p, such that $\mathcal{N}_{a,b,c}$ is strictly contained in S. The degree of such a non-trivial extension can be computed explicitly, and we will also exhibit a formula for this degree for a family of triples a, b, c such that the differences are not all prime with p.

2. Preliminary results. We will now prove that the solution of our problem only depends on the characteristic of the field of constants k. This allows us to replace k with any other field with the same characteristic, provided that x, y are still algebraically independent.

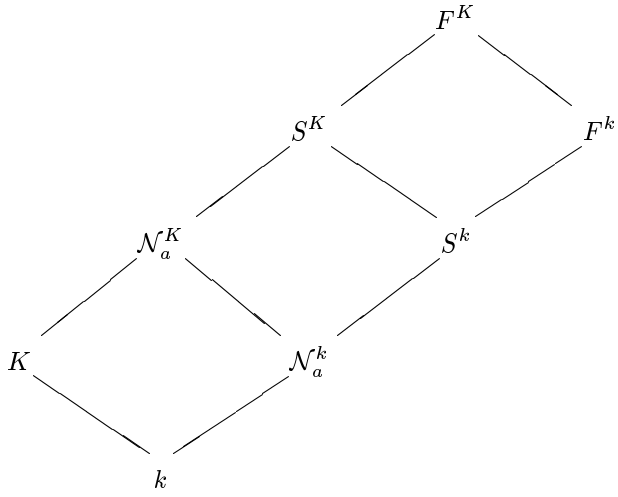
For any field L, let $\mathcal{N}_a^L$ be the field generated over L by a collection of Newton polynomials $N_{a_1}, \ldots, N_{a_s}$ (actually we will always be in the case of $s = 2, 3$). Similarly, let F^L (respectively S^L) be the field of functions (respectively symmetric functions) in x, y over L. Then we have:

Proposition 2.1. *Let K be a field such that x, y are algebraically independent over K, and let k be a subfield. Then*

$$[S^K : N_a^K] = [S^k : N_a^k],$$

intending that whenever one of the two degrees is finite, then the other one is finite too and the two degrees are equal.

Proof. In fact, we can consider the following diagram:



Since x, y are algebraically independent over K, it follows that K and F^k are linearly disjoint over k (see [**3**, Proposition 3.3, Chapter 8]). Consequently we have that $\mathcal{N}_a^K$ and S^k are linearly disjoint over $\mathcal{N}_a^k$ as well (see [**3**, Proposition 3.1, Chapter 8]), implying the equality whenever $S^k/\mathcal{N}_a^k$ or $S^K/\mathcal{N}_a^K$ is an algebraic extension of finite degree. □

Note that this proposition allows us to replace the field K with any other field L with the same characteristic, as they both contain the same prime field ($\mathbf{Q}$ or $\mathbf{F}_p$).

Another simple but crucial observation is that we just need to calculate the degree $[S : \mathcal{N}_a]$ when $\mathcal{N}_a$ is the field generated by a collection of Newton polynomials $N_{a_1}, \ldots, N_{a_s}$ satisfying $(a_1, \ldots, a_s) = 1$. In fact, if the $a_1, \ldots, a_s$ have a non-trivial gcd, g say, we obtain a field that is contained in the symmetric field in x^g, y^g. If we call $\mathcal{N}_{a/g}$ the field generated by $N_{a_1/g}, \ldots, N_{a_s/g}$, and call $S^{(g)}$ the symmetric field in x^g, y^g, we have that

$$[S : \mathcal{N}_a] = [S : S^{(g)}][S^{(g)} : \mathcal{N}_a] = g^2[S : \mathcal{N}_{a/g}].$$

Consequently, we can always assume $(a_1, \dots, a_s) = 1$ with no loss of generality.

2.2. Field generated by two polynomials. We now extend to the prime characteristic case the results obtained by Mead and Stein in [**5**]. We have the following

Proposition 2.3. *Let $a > b$ be coprime integers. If k has positive characteristic p, let's assume a, b prime with p. Then the extension $S/\mathcal{N}_{a,b}$ is a separable algebraic extension of degree*

$$[S : \mathcal{N}_{a,b}] = \begin{cases} ab/2 & \text{if } ab \text{ is even,} \\ [(a-1)b]/2 & \text{if } ab \text{ is odd.} \end{cases}$$

Proof. We can immediately see that the extension is a finite separable algebraic extension, because the Jacobian (see [**3**, Section 5, Chapter 8]) of the algebraic map $(x, y) \mapsto (x^a + y^a, x^b + y^b)$ is

$$\det \begin{pmatrix} ax^{a-1} & ay^{a-1} \\ bx^{b-1} & by^{b-1} \end{pmatrix} = ab(x^{a-1}y^{b-1} - x^{b-1}y^{a-1}),$$

that is, $\neq 0$ since we assumed a, b to be prime with the characteristic, or the characteristic to be zero. Note for future reference that we did not need to assume a, b to be coprime to achieve this.

To calculate the degree of the extension we will calculate the degree of $F/\mathcal{N}_{a,b}$; the degree of $S/\mathcal{N}_{a,b}$ will be precisely half of it. Observe that when we add x to the field $\mathcal{N}_{a,b}$ we get

$$y^a = N_a - x^a, \qquad y^b = N_b - x^b,$$

and consequently $y \in \mathcal{N}_{a,b}(x)$ since a, b is relatively prime. This proves that x is a primitive element for F, i.e., $F = \mathcal{N}_{a,b}(x)$, so we have to calculate the degree of x over $\mathcal{N}_{a,b}$.

But x is a solution of the polynomial

$$f(X) = (N_a - X^a)^b - (N_b - X^b)^a \in \mathcal{N}_{a,b}[X],$$

that is homogeneous of weight ab, if we assign weight 1 to X and a, b to N_a, N_b, respectively. Furthermore, N_a, N_b must be algebraically independent over k, since F has transcendence degree 2 over k, and $F/\mathcal{N}_{a,b}$ is algebraic.

The constant term of $f(X)$ is $N_a^b - N_b^a$, and it is irreducible. In fact it is homogeneous of weight ab, and a factor should have weight multiple of both a and b, and thus ab since a, b is relatively prime. Consequently $f(X)$ is irreducible as well as homogeneous, and its degree in X is ab when one of a, b is even (and in this case $p \neq 2$, since $(ab, p) = 1$), or $(a-1)b$ otherwise. □

3. Case with some of a, b, c divisible by p. In this section we will work in characteristic p, assuming the base field to be $\overline{\mathbf{F}} = \overline{\mathbf{F}}_p$ for convenience. We will see that we are not actually losing much assuming all of a, b, c to be prime with p. In fact, we have

Proposition 3.1. *Suppose that at least two of a, b, c are divisible by p. Then $\mathcal{N}_{a,b,c}$ cannot be S.*

Proof. Assume a, b to be divisible by p. Then $\mathcal{N}_{a,b,pc}$ is contained in $S^{(p)}$, the symmetric function field in x^p, y^p. But $\mathcal{N}_{a,b,c}$ has degree at most p over $\mathcal{N}_{a,b,pc}$, since it is generated by N_c, that satisfies $X^p - N_{pc}$. On the other hand, the degree $[S : S^{(p)}]$ is p^2, so $N_{a,b,c}$ cannot be equal to S. □

Conversely, the following proposition shows that the case with only one among a, b, c divisible by p can be reduced to the case where they are all prime with p.

Proposition 3.2. *Suppose a, b, c all prime with p. Then for all $k \geq 1$ we have $\mathcal{N}_{a,b,c} = \mathcal{N}_{a,b,p^k c}$.*

Proof. The extension $\mathcal{N}_{a,b,c}/\mathcal{N}_{a,b,p^k c}$ is purely inseparable, being generated by N_c that satisfies the purely inseparable equation

$$X^{p^k} - N_{p^k c} = 0.$$

But this extension is contained in the extension $S/\mathcal{N}_{a,b,p^k c}$ that is

separable (since, as we have seen in the proof of Proposition 3.1, $S/\mathcal{N}_{a,b}$ is separable). Thus, being both separable and purely inseparable, the extension $\mathcal{N}_{a,b,c}/\mathcal{N}_{a,b,p^kc}$ must be trivial. □

4. The main result. Most of this section is dedicated to proving the following

Proposition 4.1. *Let $a > b > c$ be relatively prime positive integers, and suppose that $a, b, c, a-c, a-b, b-c$ are prime to the characteristic p. Then we have that*

$$\mathcal{N}_{a,b,c} = S.$$

Proof. We will argue by contradiction, assuming the degree of $F/\mathcal{N}_{a,b,c}$ to be $\gneqq 2$. Let $\overline{F}^{\text{sep}}$ be a separable algebraic closure of the rational functions F, and suppose that there exist $z, w \in \overline{F}^{\text{sep}}$ different from x, y such that

$$x^m + y^m = z^m + w^m, \quad \text{for } m = a, b, c. \tag{1}$$

Since x, y are separable over $\mathcal{N}_{a,b,c}$ we can restrict our attention to the separable closure $\overline{F}^{\text{sep}}$.

It is easy to see that there cannot be two of x, y, z, w with a constant ratio: in fact x, y are algebraically independent, and the same must be true for z, w, since $k(z, w) \supseteq \mathcal{N}_{a,b,c}$, and $\mathcal{N}_{a,b,c}$ has transcendence degree 2. Now suppose that $z = \mu x$, with $\mu \in k$. Then replacing z with μx and eliminating w from (1), we have

$$\begin{aligned}\left((1-\mu^a)x^a + y^a\right)^b &= \left((1-\mu^b)x^b + y^b\right)^a,\\ \left((1-\mu^a)x^a + y^a\right)^c &= \left((1-\mu^c)x^c + y^c\right)^a,\end{aligned}$$

relations between x and y, which are assumed to be algebraically independent. Consequently they must be trivial, and considering the coefficients of x^b, x^c, x^a we deduce that this can happen if and only if $\mu^a = \mu^b = \mu^c = 1$, i.e., $\mu = 1$ since$(a, b, c) = 1$. But in this case $x = z$ and $y = w$, and x, y are not different from z, w.

To proceed let's extend to $\overline{F}^{\text{sep}}$ the standard derivation $\partial/\partial z$ on the field $\overline{\mathbf{F}}(z, w)$ (as we said before, z, w are algebraically independent),

that we will indicate with a prime. Taking the derivative of (1) we get the non trivial relations

$$x^{m-1}x' + y^{m-1}y' = z^{m-1}, \quad \text{for } m = a, b, c, \tag{2}$$

since we required a, b, c all to be prime with p. This system of equations can also be written as

$$\begin{pmatrix} x^{a-c} & y^{a-c} & z^{a-c} \\ x^{b-c} & y^{b-c} & z^{b-c} \\ 1 & 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} x' \cdot x^{c-1} \\ y' \cdot y^{c-1} \\ -z^{c-1} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}.$$

This last equation shows that x, y, z must be solutions of the determinantal polynomial $R(X, Y, Z)$ defined as

$$\begin{aligned} R(X, Y, Z) &= \det \begin{pmatrix} X^{a-c} & Y^{a-c} & Z^{a-c} \\ X^{b-c} & Y^{b-c} & Z^{b-c} \\ 1 & 1 & 1 \end{pmatrix} \\ &= Z^A(X^B - Y^B) - Z^B(X^A - Y^A) \\ &\quad + X^B Y^B (X^{A-B} - Y^{A-B}), \end{aligned} \tag{3}$$

where we have put $A = a - c$, $B = b - c$, and that we will see as a polynomial in Z with coefficients in $\overline{\mathbf{F}}[X, Y]$.

Let $V(X, Y, Z) = (X - Y)(Z - X)(Z - Y)$, the Vandermonde determinant in X, Y, Z. If we let $d = (A, B)$, then $R(X, Y, Z)$ is clearly divisible by $V(X^d, Y^d, Z^d)$, that is not zero on (x, y, z), since no two of x, y, z have constant ratio.

Thus, the quotient

$$T(X, Y, Z) = T_{A,B}(X, Y, Z) = \frac{R(X, Y, Z)}{V(X^d, Y^d, Z^d)},$$

that we are going to show to be irreducible, must vanish on (x, y, z). Let's observe that $T(X, Y, Z)$ is symmetric; it is also the Schur polynomial $s_\lambda(X^d, Y^d, Z^d)$ in X^d, Y^d, Z^d associated with the partition $\lambda = (A/d - 2, B/d - 1, 0)$ of the theory of symmetric functions, following the notation of [**4**].

To prove the irreducibility of $T(X, Y, Z)$ in $\overline{\mathbf{F}}[X, Y, Z]$, let's consider the polynomial

$$I(X, Y, Z) = \frac{R(X, Y, Z)}{(X^d - Y^d)},$$

that has an intermediate form between $R(X,Y,Z)$ and $T(X,Y,Z)$, and that we will use to extract information about $T(X,Y,Z)$. It can be written as

$$(4)\quad Z^A \prod_{\substack{\zeta^B=1\\ \zeta^d\neq 1}} (X-\zeta Y) - Z^B \prod_{\substack{\xi^A=1\\ \xi^d\neq 1}} (X-\xi Y) + X^B Y^B \prod_{\substack{\theta^{A-B}=1\\ \theta^d\neq 1}} (X-\theta Y).$$

The ζ, ξ, θ appearing in the (4) are respectively the Ath, the Bth and the $(A-B)$th roots of the unity, with the dth roots removed. They are all different, since p does not divide $A, B, A-B$, and the greatest common divisor of any two of $A, B, A-B$ is precisely d.

4.2. Irreducibility of $T(X,Y,Z)$. The strategy we are going to use to prove the irreducibility of $T(X,Y,Z)$ can be seen as a variation of Eisenstein's criterion, in a sense that will be specified below.

Let $f(U) = \sum_{i=0}^{s} f_i U^i \in R[U]$ be a polynomial in U over a commutative unitary ring R with degree $s \geq r$ for some $r \geq 1$, such that $f_r \notin P$ for some prime ideal $P \subset R$, $f_j \in P$ for $j < r$ and $f_0 \in P \setminus P^2$

$$f(U) = f_s U^s + \cdots + \underset{\not\in P}{f_r} U^r + \underset{\in P}{f_{r-1}} U^{r-1} + \cdots + \underset{\in P}{f_1} U + \underset{\in P\setminus P^2}{f_0}\ .$$

If it can be factored as $f(U) = g(U)h(U)$, we can easily deduce from the factorization modulo P that one of its factors, $g(U) = \sum g_i U^i$ say, must inherit this 'signature' and satisfy $g_r \notin P$, $g_j \in P$ for $j < r$ and $g_0 \in P \setminus P^2$, and in particular its degree is at least r. If r is equal to s, the degree of f, this forces $h(U)$ to have degree zero, and we recover precisely Eisenstein's irreducibility criterion. The polynomials that we are studying do not satisfy the requirements for Eisenstein's criterion, but this will be compensated by the fact that they are symmetric.

For convenience, this property of $f(U)$ will be called *signature of length r relative to the ideal P*, and since we can similarly have such a signature in the first r coefficients of the highest degree terms rather

than in the lowest degree terms

$$f(U) = \underset{P\setminus P^2}{f_s}\, U^s + \underset{P}{f_{s-1}} U^{s-1} + \cdots + \underset{P}{f_{s-r+1}} U^{s-r+1} + \underset{P}{f_{s-r}} U^{s-r} + \cdots + f_0,$$

we will respectively speak about *upper signatures* and *lower signatures*.

Note that $T(X,Y,Z)$ is primitive in Z (for instance because $I(X,Y,Z)$ is), so we will just have to show that it cannot split into factors with degree ≥ 1 in Z.

Arguing by contradiction, suppose that $T(X,Y,Z)$ can be factored into $k > 1$ irreducible factors with degree ≥ 1 in Z, $\prod_{i=1}^{k} G_i(X,Y,Z)$, say. Observing the form of

$$I(X,Y,Z) = T(X,Y,Z)(Z^d - X^d)(Z^d - Y^d)$$

that we wrote in (4), we can see that the terms of degree $< B$ in Z are divisible by $(X - \theta Y)$ for all $\theta^{A-B} = 1, \theta^d \neq 1$, that the coefficient of the constant term in Z is divisible only once, while the coefficient of Z^B is not divisible. Thus, this polynomial has a lower signature of length B relative to the ideal $P_\theta = \langle X - \theta Y \rangle$ for all $\theta^{A-B} = 1$, $\theta^d \neq 1$, and similarly it has an upper signature of length $A - B$ relative to the ideal $Q_\zeta = \langle X - \zeta Y \rangle$ for all $\zeta^B = 1, \zeta^d \neq 1$.

This polynomial has both an upper and a lower signature, unless either $d = B$, or $d = A - B$, and these cases will be considered separately.

4.3. Case 1 (with $B \neq d$ and $A - B \neq d$). The irreducible factors of $I(X,Y,Z)$ that inherit an upper (respectively lower) signature must have degree in Z at least B (respectively $A - B$), and they must be factors of $T(X,Y,Z)$. Since the degree in Z of $T(X,Y,Z)$ is precisely $A - 2d$, there must be one 'big' factor, $G_1(X,Y,Z)$ say, that inherits both an upper and a lower signature, or $T(X,Y,Z)$ would have degree $\geq A$ in Z. For the same reason, this big factor $G_1(X,Y,Z)$ must inherit *all* signatures of $I(X,Y,Z)$ relative to the P_θ and Q_ζ.

Thus, we have that any product of some of the remaining factors

$$\prod_{i\in I} G_i(X,Y,Z), \quad \text{with } I \subseteq \{2,3,\dots,k\}, \quad I \neq \varnothing,$$

must be monic in Z, have constant term of the form X^rY^s (for some $r,s \geq 0$), and in particular it cannot be symmetric. It follows that $T(X,Y,Z)$ cannot be factored as a non trivial product of symmetric polynomials, i.e., the action of the symmetric group S_3 as permutations of X,Y,Z on the irreducible factors is transitive.

Such an action does not preserve the degree in Z, but it preserves the total degree, and the $G_i(X,Y,Z)$ must have the same total degree. As we have seen, $G_1(X,Y,Z)$ has degree in Z at least $A-B$, and its leading coefficient is the product of precisely $B-d$ factors in X,Y of the form $(X-\zeta Y)$. Thus, its total degree is at least $A-d$.

On the other side the total degree of $T(X,Y,Z)$ is precisely $A+B-3d$. Were the number of factors ≥ 2, then the total degree should be at least

$$2(A-d) \gneqq A+B-3d,$$

since $A > B$ and $d > 0$. This contradiction proves that $G_1(X,Y,Z)$ must be the only factor, and that $T(X,Y,Z)$ is irreducible.

4.4. Case 2 (with $B=d$ or $A-B=d$). Let's show that the case with $A-B=d$ can be reduced to the case with $B=d$. Since

$$\frac{\det\begin{pmatrix} X^A & Y^A & Z^A \\ X^d & Y^d & Z^d \\ 1 & 1 & 1 \end{pmatrix}}{\det\begin{pmatrix} X^{2d} & Y^{2d} & Z^{2d} \\ X^d & Y^d & Z^d \\ 1 & 1 & 1 \end{pmatrix}} = \frac{(XYZ)^A \cdot \det\begin{pmatrix} 1 & 1 & 1 \\ X^{-A+d} & Y^{-A+d} & Z^{-A+d} \\ X^{-A} & Y^{-A} & Z^{-A} \end{pmatrix}}{(XYZ)^{2d} \cdot \det\begin{pmatrix} 1 & 1 & 1 \\ X^{-d} & Y^{-d} & Z^{-d} \\ X^{-2d} & Y^{-2d} & Z^{-2d} \end{pmatrix}},$$

we have that

$$T_{A,d}(X,Y,Z) = (XYZ)^{A-2d} \cdot T_{A,A-d}(X^{-1},Y^{-1},Z^{-1}).$$

Consequently, from a factorization of $T_{A,A-d}(X^{-1},Y^{-1},Z^{-1}) \in \overline{\mathbf{F}}[X^{-1}, Y^{-1},Z^{-1}]$ we can deduce a factorization of $T_{A,d}(X,Y,Z)$, distributing factors of $(XYZ)^{A-2d}$ on the factors of $T_{A,A-d}(X^{-1},Y^{-1},Z^{-1})$ to make all exponents positive. The only case where a non trivial

factorization can become a trivial factorization is when one of the factors of $T_{A,A-d}(X^{-1}, Y^{-1}, Z^{-1})$ is a non trivial monomial $X^{-r}Y^{-s}Z^{-t}$ for $r, s, t \geq 0$, but this cannot happen in view of the definition of $T_{A,A-d}(X, Y, Z)$.

To prove the irreducibility of $T_{A,d}(X, Y, Z)$, we will show that the variety defined in $\mathbf{P}^2(\overline{\mathbf{F}})$ is nonsingular. The irreducibility follows immediately, since two irreducible factors would define two projective varieties with non empty intersection (by the theorem of Bézout, see [**2**]), and on a point of this intersection all derivatives of the product would be zero.

Let's consider first the case with $d = 1$ and put for convenience $A = k$ for some integer $k \geq 2$, and $B = 1$. If $k = 2$, then $T_{k,1}(X, Y, Z) = 1$, so let's suppose $k > 2$. It's easy to see with a direct computation, or by considering the Jacobi-Trudi identity (see [**4**]), that $T_{k,1}(X, Y, Z)$ is the $(k-2)$th complete symmetric function, i.e., the sum of all monomials of degree $k-2$, denoted as $h_{k-2}(X, Y, Z)$ in the notation of [**4**].

We have that

$$\left(\frac{\partial}{\partial X} + \frac{\partial}{\partial Y} + \frac{\partial}{\partial Z}\right) T_{k,1}(X, Y, Z) = k \cdot T_{k-1,1}(X, Y, Z),$$

k times the sum of all monomials of degree $k-3$, since the contribution to the monomial $X^r Y^s Z^t$, for $r, s, t \geq 0$, $r + s + t = k - 3$, is given by

$$\frac{\partial}{\partial X} X^{r+1} Y^s Z^t + \frac{\partial}{\partial Y} X^r Y^{s+1} Z^t + \frac{\partial}{\partial Z} X^r Y^s Z^{t+1} = k \cdot X^r Y^s Z^t.$$

Suppose that there exists a point with homogeneous coordinates (x, y, z) satisfying the system of equations

$$\begin{cases} T_{k,1}(X, Y, Z) = 0, \\ (\partial/\partial X) T_{k,1}(X, Y, Z) = 0, \\ (\partial/\partial Y) T_{k,1}(X, Y, Z) = 0, \\ (\partial/\partial Z) T_{k,1}(X, Y, Z) = 0. \end{cases}$$

Since k is prime to characteristic p, the point (x, y, z) must also be a

solution of

$$T_{k,1}(X,Y,Z) - \frac{X}{k}\cdot\left(\frac{\partial}{\partial X}+\frac{\partial}{\partial Y}+\frac{\partial}{\partial Z}\right)T_{k,1}(X,Y,Z) = \sum_{i=0}^{k-2} Y^i Z^{k-2-i} = \prod_{\substack{\phi^{k-1}=1\\ \phi\neq 1}} (Y-\phi Z).$$

Since we also supposed $k-1$ to be prime to characteristic p, the coordinates of this point must satisfy $y=\phi z$ for some $\phi^{k-1}=1, \phi\neq 1$. Repeating the computation with other variables we have that any two of x,y,z differ by a $(k-1)$th root of the unity different from 1.

Consequently, this point is of the form $(\phi t, \psi t, t) \in \mathbf{P}^2\overline{\mathbf{F}}$, with $\phi^{k-1}=\psi^{k-1}=1$ and $\phi,\psi,1$ all different, and $t\neq 0$. But we have that

$$\begin{aligned}\frac{\partial}{\partial Z}T_{k,1}(X,Y,Z) &= \frac{\partial}{\partial Z}\frac{R(X,Y,Z)}{V(X,Y,Z)}\\ &= \frac{kZ^{k-1}(X-Y)-(X^k-Y^k)}{V(X,Y,Z)}\\ &\quad - R(X,Y,Z)\frac{(\partial/\partial Z)V(X,Y,Z)}{V(X,Y,Z)^2},\end{aligned}$$

where as usual we called $V(X,Y,Z)$ the Vandermonde determinant and $R(X,Y,Z)$ the determinantal polynomial defined in (3) for $A=k$, $B=1$. Evaluating at $(\phi t,\psi t,t)$, and taking into account that $R(\phi t,\psi t,t)=0$, we deduce that

$$\left.\frac{\partial}{\partial Z}T_{k,1}(X,Y,Z)\right|_{(\phi t,\psi t,t)} = (k-1)\frac{t^{k-3}}{(1-\phi)(1-\psi)} \neq 0.$$

Let's now take care of the case with $d\geq 1$, and write $A=kd, B=d$. To prove the irreducibility of $T_{kd,d}(X,Y,Z)=T_{k,1}(X^d,Y^d,Z^d)$, we will show that it defines a nonsingular variety as well. So, let's consider the system of equations

$$\begin{cases} T_{k,1}(X^d,Y^d,Z^d)=0,\\ dX^{d-1}\cdot(\partial/\partial X)T_{k,1}(X^d,Y^d,Z^d)=0,\\ dY^{d-1}\cdot(\partial/\partial Y)T_{k,1}(X^d,Y^d,Z^d)=0,\\ dZ^{d-1}\cdot(\partial/\partial Z)T_{k,1}(X^d,Y^d,Z^d)=0.\end{cases}$$

Clearly any point (x, y, z) such that x, y, z are all $\neq 0$ cannot satisfy this system, because this would imply that (x^d, y^d, z^d) would be a singular point for $T(X, Y, Z)$, and this cannot happen as we have just seen.

So let's suppose that the above equations are satisfied in a point (x, y, z) with $y = 0$, say. Such a point must be a solution of

$$T_{k,1}(X^d, 0, Z^d) = \prod_{\substack{\phi^{k-1}=1 \\ \phi \neq 1}} (X^d - \phi Z^d),$$

implying that x^d and z^d differ by a factor that is a $(k-1)$th root of unity different from 1. Consequently, (x^d, y^d, z^d) must be of the form $(\phi t, 0, t)$ for $\phi^{k-1} = 1, \phi \neq 1$ and $t \neq 0$, and all we have to show is that

$$\frac{\partial}{\partial Z} T_{k,1}(X, Y, Z)\Big|_{(\phi t, 0, t)} = (k-1)\frac{t^{k-3}}{1-\phi} \neq 0.$$

4.5. Conclusion. We just proved that $T(X, Y, Z)$ is irreducible as a polynomial in Z with coefficients in $\overline{\mathbf{F}}[X, Y, Z]$, and consequently it will also be irreducible in $\overline{\mathbf{F}}(X, Y)[Z]$ thanks to Gauss's lemma, since the ring $\overline{\mathbf{F}}[X, Y]$ is factorial.

Recall that the following equations

$$x^m + y^m - z^m = w^m, \quad \text{for } m = a, b, c \tag{5}$$

are assumed to be satisfied for some w, z different from x, y, and that $T(X, Y, Z)$ is a relation satisfied by x, y, z.

Note that z must be transcendental over $\overline{\mathbf{F}}(x)$. In fact, suppose that this is not the case: y is a root of the polynomial $R(x, U, z)$, considered as a polynomial in U over $\overline{\mathbf{F}}(x, z)$, and consequently of $T(x, U, z)$ since no two of x, y, z have constant ratio. Furthermore, $T(x, U, z)$ cannot vanish identically, since its constant term is a homogeneous polynomial in x, z, i.e., of the form $\prod(x - \theta_i z)$, and x, z do not have a constant ratio.

This implies the existence of a non trivial algebraic relation of y over $\overline{\mathbf{F}}(x, z)$, and consequently that y is algebraic over $\overline{\mathbf{F}}(x)$, but this is impossible since we assumed x, y to be algebraically independent. Let's

also note for future reference that w must be transcendental over $\overline{\mathbf{F}}(x)$ as well.

The algebraic independence of x, z allows us to define an isomorphism $\varepsilon : \overline{\mathbf{F}}(x,y) \to \overline{\mathbf{F}}(x,z)$ that fixes the constants and such that

$$x \longmapsto x, \qquad y \longmapsto z.$$

Since z is a root of the polynomial $T(x,y,U)$ in U, we can extend ε to $\overline{\mathbf{F}}(x,y,z)$ defining the image of z to be any root of

$$\varepsilon T(x,y,U) = T(\varepsilon x, \varepsilon y, U) = T(x,z,U) = T(x,U,z),$$

since $T(X,Y,Z)$ is a symmetric polynomial. In particular, we can put $\varepsilon(z) = y$.

Let's now extend ε to the algebraic closure of $\overline{\mathbf{F}}(x,y,z)$, and let $u = \varepsilon(w)$ (actually we have $w \in \overline{\mathbf{F}}(x,y,z)$, but we will not have to use this fact). Applying ε to (5) we get

$$x^m + z^m - y^m = u^m, \quad \text{for } m = a,b,c. \tag{6}$$

Adding together (5) and (6) we get

$$2x^m = w^m + u^m, \quad \text{for } m = a,b,c \tag{7}$$

(recall that the hypotheses rule out the case of characteristic 2). Eliminating u from (7) for $m = a, b$ we have

$$(2x^a - w^a)^b - (2x^b - w^b)^a = 0. \tag{8}$$

This is a non trivial algebraic relation of w over $\overline{\mathbf{F}}(x)$, that had been proved to be transcendental over $\overline{\mathbf{F}}(x)$. This contradiction concludes the proof. □

A comment on the hypotheses we required at the beginning of the theorem is needed. Let's restrict to the case of a, b, c coprime and all prime to p, as we are allowed to do thanks to Proposition 3.2. Computer experiments show that in many cases where p divides the differences $a-c, a-b, b-c$ the Newton polynomials N_a, N_b, N_c still generate the full symmetric field.

A careful analysis of the proof shows that in Case 1 of the proof of the irreducibility of $T(X,Y,Z)$ we did not actually use the fact that $A = a - c$ is prime to p (in Case 2 this hypothesis is important and necessary, as we will show with some examples below). We have omitted this small weakening of the hypothesis to avoid complicating the statement too much.

Furthermore, the conclusive step works flawlessly without $T(X,Y,Z)$ being irreducible, provided that we know its factors to be *all symmetric polynomials*. It is possible to show examples where precisely this happens (such as $T_{7,3}(X,Y,Z)$ in characteristic 2), but it seems difficult to show this for some classes of polynomials.

On the other hand, if we do not require $a-c, a-b, b-c$ to be prime to p, there are cases where N_a, N_b, N_c do not generate the full symmetric field. A family of cases where this happens is related to the factorization of $T_{p^r,1}(X,Y,Z)$, for $r \geq 1$. In fact, we have

$$T_{p^r,1}(X,Y,Z) = \prod_{\substack{\alpha \in \mathbf{F}_{p^r} \\ \alpha \neq 0,1}} (Z - \alpha X + (\alpha - 1)Y),$$

as we will show below together with a few other factorizations of the polynomials $T_{A,B}(X,Y,Z)$, for $A, B, A-B$ not all prime to p.

5. A family of counterexamples. Let p be a prime $\neq 2$, and for each $\eta \in \mathbf{F}_p$, let's consider the polynomial

$$P_\eta(X) = X^2 - 2\eta X + \eta. \tag{9}$$

Note that a root of $P_\eta(X)$ cannot be root of $P_\kappa(X)$ for $\eta \neq \kappa$, because the equation

$$X^2 - 2\eta X + \eta = 0,$$

considered as an equation in η for a given X determines univocally η, unless $X = 1/2$, which is never a solution because $P_\eta(1/2) = 1/4 \neq 0$ for each $\eta \in \mathbf{F}_p$.

Furthermore, each $P_\eta(X)$ has distinct roots unless its discriminant $4(\eta^2 - \eta)$ vanishes, and this can only happen for $\eta = 0, 1$.

Thus, as η varies in $\mathbf{F}_p$ the polynomials $P_\eta(X)$ have $2p-2$ different roots overall, and note that $2p-2 > p$ for $p \geq 3$. Consequently, since in

$\mathbf{F}_p$ there are only p elements, one of these roots will belong to $\mathbf{F}_{p^2} \setminus \mathbf{F}_p$, and this implies that at least one of the $P_\eta(X)$ is irreducible in $\mathbf{F}_p[X]$ for some $\eta \in \mathbf{F}_p$.

Let $P_\eta(X)$ be irreducible, and let $\alpha, \beta \in \mathbf{F}_{p^2} \setminus \mathbf{F}_p$ be its roots. These roots are interchanged by the Frobenius automorphism $\mathscr{F}$

$$\mathscr{F} : \overline{\mathbf{F}} \longrightarrow \overline{\mathbf{F}}, \qquad \tau \longmapsto \tau^p.$$

In particular, they are interchanged applying $\mathscr{F}$ any odd number of times, i.e.,

$$\alpha^{p^{2k+1}} = \beta, \qquad \beta^{p^{2k+1}} = \alpha$$

for any integer k.

Note also that, by construction, we have

$$2\alpha\beta = 2\eta = \alpha + \beta.$$

If we now define

$$z = \alpha x + (1-\alpha)y, \qquad w = (1-\alpha)x + \alpha y, \tag{10}$$

we have that, for any integer k,

$$\begin{aligned}
z^{p^{2k+1}+1} + w^{p^{2k+1}+1} &= z^{p^{2k+1}} \cdot z + w^{p^{2k+1}} \cdot w \\
&= (\alpha x + (1-\alpha)y)^{p^{2k+1}} (\alpha x + (1-\alpha)y) \\
&\quad + ((1-\alpha)x + \alpha y)^{p^{2k+1}} ((1-\alpha)x + \alpha y) \\
&= (\beta x^{p^{2k+1}} + (1-\beta)y^{p^{2k+1}})(\alpha x + (1-\alpha)y) \\
&\quad + ((1-\beta)x^{p^{2k+1}} + \beta y^{p^{2k+1}})((1-\alpha)x + \alpha y) \\
&= (2\alpha\beta - \alpha - \beta + 1)(x^{p^{2k+1}+1} + y^{p^{2k+1}+1}) \\
&\quad + (\beta + \alpha - 2\beta\alpha)(x^{p^{2k+1}} y + x y^{p^{2k+1}}) \\
&= x^{p^{2k+1}+1} + y^{p^{2k+1}+1}.
\end{aligned}$$

Thus, if we take a, b, c equal to $p^{2k+1}+1, p^{2\ell+1}+1, 1$ for $k > \ell \geq 0$, we have found an 'alternative' pair z, w in (10) that satisfies equation (1), and consequently N_a, N_b, N_c cannot generate the full symmetric field.

We can also calculate the degree of the symmetric field over the field generated by $N_{p^r+1}, N_{p^s+1}, N_1$ for $r > s \geq 0$, because all we have to do is count the number of z that together with some w satisfy (1). In particular those different from x, y can be found among the roots of $T_{p^{r-s},1}(x, y, U)^{p^s}$ considered as a polynomial in U, and given the factorization of $T_{p^{r-s},1}(x, y, U)$ in linear factors we know that they must be of the form $z = \alpha x + (1-\alpha)y$ for $\alpha \in \mathbf{F}_{p^{r-s}}$, $\alpha \neq 1, 0$.

Furthermore, w is uniquely determined as $w = (1-\alpha)x + \alpha y$, and if we put $\beta = \alpha^{p^r}$, then α, β must satisfy the condition $2\alpha\beta = \alpha + \beta$, and are the roots of a polynomial $P_\eta(X)$ for some $\eta \in \overline{\mathbf{F}}_p$. If $\alpha = \beta$, then $\alpha = 0, 1$, and we get $z = y$ or $z = x$ respectively, so let's consider the case $\alpha \neq \beta$. Now, if we put $\gamma = \alpha^{p^s}$, the condition $2\alpha\gamma = \alpha + \gamma$ must be satisfied as well, and consequently $\beta = \gamma = \alpha^{p^s}$.

We have that $\mathscr{F}^s$ (i.e., $\mathscr{F}$ applied s times) maps α to β, and applied to the coefficients of $P_\eta(X)$ we get another polynomial of the same form, $P_\kappa(X)$ say. Since $P_\eta(\beta) = P_\kappa(\beta) = 0$, this implies that $\eta = \kappa$, and it follows that symmetrically $\mathscr{F}^s$ maps β to α, and leaves η fixed. Since the same is true for $\mathscr{F}^r$, we have that η is fixed by $\mathscr{F}^m$ for $m = (r, s)$, i.e., that $\eta \in \mathbf{F}_{p^m}$, while α has degree precisely 2 over $\mathbf{F}_{p^m}$, in other words that $\alpha \in \mathbf{F}_{p^{2m}} \setminus \mathbf{F}_{p^m}$.

We can now distinguish two cases: when $2m \nmid (r-s)$, we have that $\mathbf{F}_{p^{2m}} \cap \mathbf{F}_{p^{r-s}} = \mathbf{F}_{p^m}$, and the only α allowed are $0, 1$, and $N_{p^r+1}, N_{p^s+1}, N_1$ consequently generate the full symmetric field.

On the other hand, when $2m \mid (r-s)$ we have that $\mathbf{F}_{p^{2m}} \subset \mathbf{F}_{p^{r-s}}$, and all we have to do is count the number of solutions of

$$X^2 - 2\eta X + \eta = 0, \qquad X \in \mathbf{F}_{p^{2m}} \setminus \mathbf{F}_{p^m}$$

while η varies in $\mathbf{F}_{p^m}$. Repeating the same computation we did at the beginning of this section, we deduce that the total number of solutions in $\mathbf{F}_{p^{2m}}$ is precisely $2p^m - 2$, and that each $X \in \mathbf{F}_{p^m}$ is a solution for some η except for $X = 1/2$, and the number of these bad solutions in $\mathbf{F}_{p^m}$ is precisely $p^m - 1$. Adding the trivial solutions $\alpha = 0, 1$ and dividing by two we obtain the degree.

In conclusion, for any $r > s \geq 1$ and $m = (r, s)$, the degree of the symmetric field S over the field generated by $N_{p^r+1}, N_{p^s+1}, N_1$ is

$$[S : \mathcal{N}_{p^r+1, p^s+1, 1}] = \begin{cases} 1 & \text{if } 2m \nmid (r-s) \\ (p^m+1)/2 & \text{if } 2m \mid (r-s). \end{cases}$$

We can easily see that in characteristic 2 we can construct an analogous family of counterexamples considering the pair

$$z = \alpha x + (1-\alpha)y, \qquad w = (1-\alpha)x + \alpha y,$$

where $\alpha \in \mathbf{F}_{2^2} \setminus \mathbf{F}_2$ is a third root of the unity, but in this case the indices a, b, c must be chosen of the form $2^{2l}+1, 2^{2k}+1, 1$, where *even* powers of 2 appear.

In fact, in characteristic 2 the condition $2\alpha\beta = \alpha + \beta$ is equivalent to $\alpha = \beta$ (and this in characteristic $\neq 2$ can never happen, unless $\alpha = 0, 1$).

To calculate the degree of S over $N_{2^r+1}, N_{2^s+1}, N_1$ let's observe that all we have to do is count the number of elements $\alpha \in \mathbf{F}_{2^{r-s}}$ that are left fixed by $\mathscr{F}^s$ and $\mathscr{F}^r$, and they are precisely the elements of $\mathbf{F}_{2^m}$, for $m = (r, s)$. Dividing by two we get the degree of the extension

$$[S : \mathcal{N}_{2^r+1, 2^s+1, 1}] = 2^{m-1}.$$

5.1. Factorization of certain families of $T(X, Y, Z)$. We will now show that

$$T_{p^r,1}(X, Y, Z) = \prod_{\substack{\alpha \in \mathbf{F}_{p^r} \\ \alpha \neq 0,1}} (Z - \alpha X + (\alpha - 1)Y). \tag{11}$$

To check the equality, calling as usual $V(X, Y, Z)$ the Vandermonde determinant, it is enough to observe that we have

$$T_{p^r,1}(X, Y, Z) \cdot V(X, Y, Z) = \det \begin{pmatrix} X^{p^r} & Y^{p^r} & Z^{p^r} \\ X & Y & Z \\ 1 & 1 & 1 \end{pmatrix},$$

and the determinant vanishes if we put $Z = \alpha X - (\alpha - 1)Y$ for each $\alpha \in \mathbf{F}_{p^r}$. We have to exclude the factors $(Z - \alpha X + (\alpha - 1)Y)$ for $\alpha = 0, 1$, because they are precisely the factors dividing $V(X, Y, Z)$, but the remaining $p^r - 2$ factors are factors of $T_{p^r,1}(X, Y, Z)$, which has degree precisely $p^r - 2$ in Z. To conclude we have just to verify that the constant factor by which they may differ is 1, but this is obvious

considering that the two expressions appearing in (11) are both monic in Z.

Another factorization of the same flavor is the following:

$$T_{p^{2r}-1,p^r-1}(X,Y,Z) = \prod_{\substack{\alpha,\beta\in\mathbf{F}_{p^r}\\ \alpha,\beta\neq 0}} (Z-\alpha X-\beta Y). \tag{12}$$

In fact, when we replace $Z=\alpha X+\beta Y$, we have that for each $\alpha,\beta\in\mathbf{F}_{p^r}$ this substitution makes

$$T_{p^{2r}-1,p^r-1}(X,Y,Z)\cdot V(X^{p^r-1},Y^{p^r-1},Z^{p^r-1})\cdot XYZ = \det\begin{pmatrix} X^{p^{2r}} & Y^{p^{2r}} & Z^{p^{2r}} \\ X^{p^r} & Y^{p^r} & Z^{p^r} \\ X & Y & Z \end{pmatrix}$$

vanish, and discarding as before the factors $(Z-\alpha X+\beta Y)$ where $\alpha=0$ or $\beta=0$, we are left with $p^{2r}-2p^r+1$ linear factors, and this is precisely the degree of $T_{p^{2r}-1,p^r-1}(X,Y,Z)$. To prove the equality, we must again observe that both factors are monic in Z.

It can also be interesting to observe that all these substitutions $Z=\alpha X+\beta Y$, for $\alpha,\beta\in\mathbf{F}_{p^r}$, also make the determinant

$$\det\begin{pmatrix} X^{p^s} & Y^{p^s} & Z^{p^s} \\ X^{p^t} & Y^{p^t} & Z^{p^t} \\ X & Y & Z \end{pmatrix}$$

vanish for each $s>t\geq 1$ that are both divisible by r.

This determinant is also a multiple of $T_{p^s-1,p^t-1}(X,Y,Z)$, and differs from it for a factor $V(X^{p^m-1},Y^{p^m-1},Z^{p^m-1})\cdot XYZ$, that can vanish after the substitution only if we put either α or β equal to 0.

Consequently for all $s>t\geq 1$, both divisible by r, we have that

$$T_{p^{2r}-1,p^r-1}(X,Y,Z) \;\Big|\; T_{p^s-1,p^t-1}(X,Y,Z).$$

Since actually both of these polynomials are polynomials in X^{p^r-1}, Y^{p^r-1}, Z^{p^r-1}, we must also have the following divisibility rule:

$$T_{p^r+1,1}(X,Y,Z) \;\Big|\; T_{(p^s-1/p^r-1),(p^t-1/p^r-1)}(X,Y,Z).$$

6. Irreducibility of $T_{p^r+1,1}(X,Y,Z)$. We will now show that $T_{p^r+1,1}(X,Y,Z)$, for $r \geq 1$, that we just showed to be a factor of a class of $T(X,Y,Z)$, is irreducible. Note that such polynomials do not belong to the family of polynomials that we have shown to be irreducible in Case 2 of Proposition 4.1 proving that the projective variety that they define is nonsingular, and in fact the point with homogeneous coordinates (t,t,t) for $t \neq 0$ is a singular point for $T_{p^r+1,1}(X,Y,Z)$.

We will use the following strategy: let

$$f(Z) = f_k Z^k + \cdots + f_1 Z + f_0 \in k[X_1, \ldots, X_n, Z]$$

be a homogeneous polynomial in $X_1, \ldots, X_n, Z$, considered as a polynomial in Z with coefficients in $k[X_1, \ldots, X_n]$. Let's suppose that there exists a $P \in k[X_1, \ldots, X_n]$ such that f_0 is a power of P, and that $P \nmid f_1$. Then $f(Z)$ is irreducible in $k[X_1, \ldots, X_n, Z]$.

Suppose in fact that $f(Z) = a(Z)b(Z)$, with $a(Z) = \sum_i a_i Z^i$, $b(Z) = \sum_i b_i Z^i$, both of degree ≥ 1 in Z. Then we have that

$$f_0 = a_0 b_0, \qquad f_1 = a_1 b_0 + a_0 b_1.$$

Since the factorization is not trivial, and the factors are homogeneous, a_0 and b_0 have to be non trivial powers of P, but this is absurd since it would imply that $P \mid f_1$. Consequently, $f(Z)$ cannot factored in factors with degree ≥ 1 in Z, and to deduce the irreducibility in $k[X_1, \ldots, X_n, Z]$ it suffices to show that it is primitive as a polynomial in Z, but this is obvious considering that $P \nmid f_1$.

To apply this strategy to $T_{p^r+1,1}(X,Y,Z)$, consider that it is the sum of all monomials of degree $p^r - 1$, and if viewed as polynomials in Z its constant term is

$$\sum_{i=0}^{p^r-1} X^i Y^{p^r-1-i} = \frac{X^{p^r} - Y^{p^r}}{X - Y} = (X-Y)^{p^r-1}.$$

On the other hand, the coefficient of the term of degree one in Z is

$$\sum_{i=0}^{p^r-2} X^i Y^{p^r-2-i} = \frac{X^{p^r-1} - Y^{p^r-1}}{X - Y} = \prod_{\substack{\zeta^{p^r-1}=1 \\ \zeta \neq 1}} (X - \zeta Y).$$

Thus, we have verified that the constant term is a power of $X-Y$, and this is a factor that does not appear in the coefficient of Z.

Consequently, the irreducibility follows, applying the above strategy. Knowing the irreducibility of this family of polynomials provides us one more case where Proposition 4.1 is true, in particular when a, b, c are coprime integers, prime to the characteristic p, and such that $a-b=p^r$ for some $r \geq 1$ and $b-c=1$.

Acknowledgments. We wish to thank Roberto Dvornicich for reading the first draft of this paper and for offering kind support and advice during our work.

REFERENCES

1. R. Dvornicich and U. Zannier, *Solution of a problem about symmetric functions*, Rocky Mountain J. Math. **33** (2003), 1279–1288.

2. R. Hartshorne, *Algebraic geometry*, Grad. Texts Math. **52**, Springer, New York, 1977.

3. S. Lang, *Algebra*, Springer, New York, 2002.

4. I.G. Macdonald, *Symmetric functions and Hall polynomials* (2nd edition), Oxford University Press, New York, 1995.

5. D.G. Mead and S.K. Stein, *Some algebra of Newton polynomials*, Rocky Mountain J. Math. **28** (1998), 303–310.

Scuola Normale Superiore di Pisa, Piazza dei Cavalieri, 7–56126 Pisa, Italy
Email address: maurizio.monge@gmail.com