ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 33, Number 4, Winter 2003

SOLUTION OF A PROBLEM ABOUT SYMMETRIC FUNCTIONS

ROBERTO DVORNICICH AND UMBERTO ZANNIER

ABSTRACT. Let $a > b > c$ be positive integers with $(a, b, c) = 1$. Then the field $\mathbf{Q}(X^a + Y^a, X^b + Y^b, X^c + Y^c)$ is the field of all symmetric rational functions in X, Y over $\mathbf{Q}$. This solves a conjecture made by Mead and Stein.

Let X, Y be independent indeterminates and, for a positive integer m, let

$$N_m = N_m(X, Y) = X^m + Y^m$$

be the Newton symmetric power of order m. In the recent paper [**2**], the authors calculate the degree $[S : \mathbf{Q}(N_a, N_b)]$, where S is the field of all symmetric rational functions in X, Y with rational coefficients. They also raise a few conjectures on the fields $\mathbf{Q}(N_a, N_b, N_c)$. The purpose of the present paper is to prove their main Conjecture 1, which we state as the following.

Theorem 1. *If $a > b > c$ are distinct positive integers with $(a, b, c) = 1$, then the functions N_a, N_b, N_c generate S over $\mathbf{Q}$.*

In [**2**] the authors also state a conjecture (see Conjecture 4 of Section 3) about the minimal degree d of a polynomial relation satisfied by N_a, N_b, N_c where, by degree of a monomial $N_a^i N_b^j N_c^k$, they mean $ai + bj + ck$. At the end of the paper we shall show how our Theorem 1 implies a strong form of their conjecture, namely,

Theorem 2. *Assumptions being as in Theorem 1, we have $d = abc/2$ if abc is even and $d = (a - 1)bc/2$ otherwise.*

Proof of Theorem 1. To start with, we show that it is sufficient to prove the analogous statement with $\mathbf{Q}$ replaced by its algebraic closure

Received by the editors on October 2, 2000, and in revised form on March 21, 2001.

$\overline{\mathbf{Q}}$. In fact, note first that, as we shall show below, we have

$$[S : \mathbf{Q}(N_a, N_b)] = [\overline{\mathbf{Q}}S : \overline{\mathbf{Q}}(N_a, N_b)]. \tag{1}$$

Then, assuming $\overline{\mathbf{Q}}S = \overline{\mathbf{Q}}(N_a, N_b, N_c)$ and recalling the easy fact that $S/\mathbf{Q}(N_a, N_b)$ is finite, we find

$$\begin{aligned}[S : \mathbf{Q}(N_a, N_b)] &= [S : \mathbf{Q}(N_a, N_b, N_c)][\mathbf{Q}(N_a, N_b, N_c) : \mathbf{Q}(N_a, N_b)] \\ &\geq [S : \mathbf{Q}(N_a, N_b, N_c)][\overline{\mathbf{Q}}S : \overline{\mathbf{Q}}(N_a, N_b)] \\ &= [S : \mathbf{Q}(N_a, N_b, N_c)][S : \mathbf{Q}(N_a, N_b)],\end{aligned}$$

the last equality following from (1). Therefore, $[S : \mathbf{Q}(N_a, N_b, N_c)] = 1$, which is the desired conclusion.

To prove (1) we could appeal to the theory of regular extensions (see for instance [**5**]); however, it is perhaps easier to proceed directly. Let γ be a primitive element for S over $\mathbf{Q}(N_a, N_b)$ and let $f \in \overline{\mathbf{Q}}(N_a, N_b)[X]$ be its minimal equation over $\overline{\mathbf{Q}}(N_a, N_b)$. We may write $f = \alpha_1 f_1 + \cdots + \alpha_h f_h$, where $f_1 \cdots f_h \in \mathbf{Q}(N_a, N_b)[X]$ are nonzero and $\alpha_1, \dots, \alpha_h \in \overline{\mathbf{Q}}$ are linearly independent over $\mathbf{Q}$. Substituting γ in place of X we obtain a relation $0 = \alpha_1 f_1(\gamma) + \cdots + \alpha_h f_h(\gamma)$. Now $f_i(\gamma) \in S$ and $S = \mathbf{Q}(N_1, N_2)$ is purely transcendental over $\mathbf{Q}$. Hence we must have $f_i(\gamma) = 0$ for $i = 1, \dots, h$. Finally, $[S : \mathbf{Q}(N_a, N_b)] \leq \deg_X f_i \leq \deg_X f = [\overline{\mathbf{Q}}S : \overline{\mathbf{Q}}(N_a, N_b)]$. Since the opposite inequality is trivial, this concludes the argument.

We are left with the task of proving

$$\overline{\mathbf{Q}}S = \overline{\mathbf{Q}}(N_a, N_b, N_c). \tag{2}$$

Let $\mathcal{V}$ be the affine variety, over $\overline{\mathbf{Q}}$, determined by the generic point (N_a, N_b, N_c). Then the inclusion $\overline{\mathbf{Q}}(N_a, N_b, N_c) \subset \overline{\mathbf{Q}}S \subset \overline{\mathbf{Q}}(X, Y)$ corresponds to a dominant rational map $\varphi : \mathbf{A}^2 \to \mathcal{V}$. To prove (2) we have just to verify that $\deg \varphi = 2$. Assuming the contrary, for a point (x, y) in a nonempty Zariski open subset of $\mathbf{A}^2(\overline{\mathbf{Q}})$, there exists a point $(x', y') \in \mathbf{A}^2(\overline{\mathbf{Q}})$, with $\{x, y\} \neq \{x', y'\}$ and

$$N_m(x, y) = N_m(x', y'), \quad m = a, b, c.$$

Put, for $x \neq 0$, $z = y/x$, $u = x'/x$, $v = y'/x$. Then we have

$$N_m(1, z) = N_m(u, v), \quad m = a, b, c. \tag{3}$$

Moreover, since $\{x, y\} \neq \{x', y'\}$, we have that $\{1, z\} \neq \{u, v\}$. Also, as (x, y) runs through a nonempty Zariski open set in $\mathbf{A}^2(\overline{\mathbf{Q}})$, we have that z varies in a nonempty Zariski open set in $\mathbf{A}^1(\overline{\mathbf{Q}})$.

Eliminating v from the first two of the equations (3), we get

$$(1 + z^a - u^a)^b = (1 + z^b - u^b)^a.$$

Since $a > b$, this is a nontrivial algebraic equation for u over $\overline{\mathbf{Q}}(z)$. Clearly, similar equations are verified if we replace b with c and/or u with v. Since they hold for almost all $z \in \overline{\mathbf{Q}}$, we may assume that the equations

$$N_m(1, Z) = N_m(U, V), \quad m = a, b, c, \tag{4}$$

have a solution U, V in a finite extension L of $\overline{\mathbf{Q}}(Z)$ with $\{U, V\} \neq \{1, Z\}$. This amounts to a recurrence sequence of order four in a function field, having four distinct integral zeros (corresponding to $m = 0, a, b, c$). In general, such a sequence cannot have more than six zeros (see [**1**, Theorem 2]) and we have to improve on this in the present special case.

For future reference, we note that neither U nor V can be constant. In fact, assume for instance $V = \alpha \in \overline{\mathbf{Q}}$. If $\alpha = 1$ we would have $U^m = Z^m$ for $m = a, b, c$, whence $U = Z$ against our assumption. If, on the other hand, $\alpha \neq 1$, the equations $(1-\alpha^a+Z^a)^b = (1-\alpha^b+Z^b)^a$ and $(1 - \alpha^a + Z^a)^c = (1 - \alpha^b + Z^c)^a$ lead to a contradiction.

We extend to L the natural derivation of $\overline{\mathbf{Q}}(Z)$, denoting it with a prime. Differentiating (4), we obtain equations

$$Z^{m-1} - U^{m-1}U' - V^{m-1}V' = 0, \quad m = a, b, c.$$

In particular,

$$\det \begin{pmatrix} Z^a & U^a & V^a \\ Z^b & U^b & V^b \\ Z^c & U^c & V^c \end{pmatrix} = UVZ \cdot \det \begin{pmatrix} Z^{a-1} & U^{a-1} & V^{a-1} \\ Z^{b-1} & U^{b-1} & V^{b-1} \\ Z^{c-1} & U^{c-1} & V^{c-1} \end{pmatrix} = 0.$$

Adding the second column and subtracting the first one to the third and last column does not affect the value of the determinant. Therefore, taking (4) into account, we obtain

$$\det \begin{pmatrix} Z^a & U^a & 1 \\ Z^b & U^b & 1 \\ Z^c & U^c & 1 \end{pmatrix} = 0,$$

and clearly the same equation holds with V in place of U. Expanding the determinants and dividing by Z^cU^c, respectively Z^cV^c, we obtain, after a few calculations, the equalities

$$\frac{U^{a-c}-1}{U^{b-c}-1} = \frac{V^{a-c}-1}{V^{b-c}-1} = \frac{Z^{a-c}-1}{Z^{b-c}-1}. \tag{5}$$

We now put $a-c = Ad$, $b-c = Bd$, where $d = (a-c, b-c)$ and

$$R(T) = \frac{T^A - 1}{T^B - 1} = \frac{1+T+\cdots+T^{A-1}}{1+T+\cdots+T^{B-1}}.$$

Since $A > B$ and A, B are coprime, we have $\deg R = A-1$. Note that (5) may be rewritten as

$$R(U^d) = R(V^d) = R(Z^d). \tag{6}$$

In order to exploit (6), we introduce a new indeterminate λ and study the equation

$$R(T) = \lambda, \tag{7}$$

trying to determine its Galois group Γ over $\overline{\mathbf{Q}}(\lambda)$. (The final result already occurred in connection with an example in the recent paper [**1**], where no details were given. We supply here complete detail.)

We first calculate the ramification of the cover of the λ-sphere given by (7).

The points of the T-sphere above $\lambda = \infty$ are given by $T = \infty$ and $(T^B - 1)/(T-1) = 0$. Since this equation has no multiple roots, ramification may occur only for $T = \infty$, the corresponding ramification index being $A - B$.

The other branch points are given by the values $\lambda = R(t)$, where $R'(t) = 0$. This equation amounts to

$$At^{A-1}(t^B - 1) - Bt^{B-1}(t^A - 1) = 0, \quad t \neq 1, \tag{8}$$

where we may exclude the solution $t = 1$ because $R'(1) = (A/2B)(A - B) \neq 0$.

We now show that $R'(T)$ has no multiple roots except possibly $T = 0$. In fact, dividing the left side of (8) by t^{B-1} and differentiating, one gets

$$A(A-B)t^{A-B-1}(t^B - 1).$$

However, this polynomial has no common roots with the left side of (8), except possibly $t = 0, 1$.

If $B > 1$, $t = 0$ is a solution of (8). We have $R(0) = 1$, and the corresponding ramification index is just B. As to the remaining solutions, we show that, for any value of B, they give rise to distinct values for $R(t)$, except possibly for the value $R(t) = 1$. In fact, suppose that t_1, t_2 are two distinct nonzero solutions of (8), with $R(t_1) = R(t_2)$. Equation (8) can be written as

$$\frac{A}{B}\, t^{A-B} = R(t).$$

Therefore, we get $t_1^{A-B} = t_2^{A-B}$, i.e., $t_1^A t_2^B = t_2^A t_1^B$. On the other hand, $R(t_1) = R(t_2)$ leads to

$$t_1^A t_2^B - t_2^B - t_1^A + 1 = t_2^A t_1^B - t_1^B - t_2^A + 1.$$

From the last two equations, we get $(t_1^{A-B} - 1)t_1^B = (t_2^{A-B} - 1)t_2^B$. If $t_1^{A-B} = 1$, we get $t_1^A = t_1^B$ and $R(t_1) = 1$. Otherwise we get $t_1^B = t_2^B$ which, combined with $t_1^{A-B} = t_2^{A-B}$, gives $t_1 = t_2$.

In conclusion, the ramification indices above any of the branch points except $\lambda = 1, \infty$ are given by the sequence $2, 1, 1, \ldots, 1$, while the ramification sequence above $\lambda = \infty$ is given by $A - B, 1, 1, \ldots, 1$.

Also, if $B = 1$, we have $R(t) - 1 = t(1 + \cdots + t^{A-2})$, so there is no ramification above $\lambda = 1$.

Now recall that the Galois group Γ of (7), as a permutation group on $A - 1$ elements, can be generated by permutations whose cycle decompositions have the same type as the ramification sequences. One may pick precisely one permutation corresponding to each branch point, and in such a way their product is the identity. In particular, one may disregard any single such permutation and still generate Γ. (Such facts are implicit in the so-called Riemann existence theorem; see, e.g., [**4**, pp. 32–37, especially Remark 4.33].)

If $B = 1$, we disregard the permutation associated to ∞ and deduce that Γ is generated by transpositions. If $B \neq 1$, we instead disregard the permutation corresponding to 1, concluding that $\Gamma \subset \mathcal{S}_{A-1}$ is generated by transpositions and a cycle of length $A - B < A - 1$. Also, Γ is transitive, since $R(T) - \lambda$ is irreducible.

We have now the following presumably known lemma, whose proof we give for completeness. In view of what we have just proved, it implies that $\Gamma = \mathcal{S}_{A-1}$.

Lemma. *If a transitive subgroup Γ of $\mathcal{S}_n$ is generated by transpositions and a cycle of length $< n$, then $\Gamma = \mathcal{S}_n$.*

Proof of lemma. Because Γ is transitive, we may suppose after renumbering that the cycle is $\sigma = (1, 2, \dots, k)$, for a $k < n$ and that one of the transpositions is $\tau = (1, k + 1)$. Now observe the formulas $\tau\sigma^j\tau\sigma^{-j}\tau = (1, j + 1)$, for $j = 0, \dots, k - 1$. Since we have $\sigma = (1, k)(1, k - 1)\cdots(1, 2)$, we thus see that Γ is generated by transpositions. Now the results follows, e.g., from [**3**, Lemma 1, p. 139]. □

Coming back to the proof of Theorem 1, we remark that no two among U, V, Z can have a constant ratio. In fact, suppose for instance that $U = \mu V$, $\mu \in \overline{\mathbf{Q}}$. Using (4), we derive

$$(\mu^m + 1)V^m - 1 = Z^m, \quad m = a, b, c,$$

whence $((\mu^a + 1)V^a - 1)^b = ((\mu^b + 1)V^b - 1)^a$. Since V is nonconstant, this implies $\mu^a + 1 = 0$, which contradicts the previous equation for $m = a$. The other cases are dealt with similarly.

In particular, it follows that U^d, V^d, Z^d are distinct.

Denote by Ω the splitting field of $R(T) = \lambda$ over $\overline{\mathbf{Q}}(\lambda)$, where $\lambda = R(U^d)$. By (6), $U^d, V^d, Z^d \in \Omega$ and the Galois group $\mathrm{Gal}\,(\Omega/\overline{\mathbf{Q}}(\lambda))$ is $\Gamma \cong \mathcal{S}_{A-1}$.

To deal with U, V, Z rather than their dth powers, a little more work is needed. Observe that, since the ramification of $\overline{\mathbf{Q}}(U^d)$ over $\overline{\mathbf{Q}}(\lambda)$ above ∞ has indices given by $(A - B, 1, 1, \dots, 1)$, the extension $\Omega/\overline{\mathbf{Q}}(\lambda)$ is ramified above ∞ with indices all equal to $A - B$. Therefore, $\Omega/\overline{\mathbf{Q}}(U^d)$

is unramified above ∞. On the other hand, $\overline{\mathbf{Q}}(U)/\overline{\mathbf{Q}}(U^d)$ is totally ramified above ∞, whence U has degree d over Ω.

Since Γ is the full symmetric group, by (6) we may choose $\sigma \in \Gamma$ such that $\sigma(U^d) = U^d$, $\sigma(V^d) = Z^d$, $\sigma(Z^d) = V^d$.

Let ξ be an arbitrary dth root of 1. Since U has degree d over Ω, we can lift σ to an algebraic closure of $\overline{\mathbf{Q}}(\lambda)$ so that $\sigma(U) = \xi U$. Moreover, we must have $\sigma(V) = \alpha Z$, $\sigma(Z) = \beta V$, where α, β are suitable dth roots of unity. Applying σ to the equations (4), which we rewrite as

$$U^m + V^m - Z^m = 1, \quad m = a, b, c, \tag{9}$$

we get

$$\xi^m U^m + \alpha^m Z^m - \beta^m V^m = 1, \quad m = a, b, c. \tag{10}$$

Suppose first that, for all choices of ξ the equations (9) and (10) are identical for $m = a, b, c$, i.e., $\xi^m = 1$, $\alpha^m = \beta^m = -1$. Then $\xi = 1$, which implies $d = 1$. But in this case we have $\sigma(Z) = V$, $\sigma(V) = Z$, so $\alpha = \beta = 1$, a contradiction.

Therefore, we may assume that, for some choice of ξ and of $m \in \{a, b, c\}$ the equations (9) and (10) are not identical. Using (9) and (10) to eliminate one among U^m, V^m, Z^m, we obtain an equation of type

$$c_1 W_1^m + c_2 W_2^m = c_3,$$

where c_1, c_2, c_3 are constants, not all zero, and where $\{W_1, W_2, W_3\} = \{U, V, Z\}$. Say that $c_1 \neq 0$ and choose a $\sigma \in \Gamma$ with $\sigma(W_1^d) = W_3^d$ and $\sigma(W_2^d) = W_2^d$. As before, we may show that W_2 has degree d over Ω, so we may lift σ to have $\sigma(W_2) = W_2$. Applying σ to the last displayed equation, we get that the ratio W_1/W_3 is constant, a contradiction which concludes the proof of Theorem 1. □

Proof of Theorem 2. Let $F(N_a, N_b, N_c) = 0$ be a generating polynomial relation (see [**2**]) and let $\mathcal{V}$ be the hypersurface defined by $F(X, Y, Z) = 0$. It is part of the preceding proof (and also follows from Theorem 1) that the rational map $\varphi : (x, y) \mapsto (N_a(x, y), N_b(x, y), N_c(x, y))$, from the affine plane to $\mathcal{V}$, is dominant of degree 2. Define $\mathcal{W} \in \mathbf{A}^3$ by the equation $F(T^a, U^b, V^c) = 0$; it is easily seen that $F(T^a, U^b, V^c)$ is homogeneous, so $\mathcal{W}$ is a cone, whose degree d is the number we are seeking. We have an obvious rational map $\psi : (t, u, v) \mapsto (t^a, u^b, v^c)$ from $\mathcal{W}$ to $\mathcal{V}$. Plainly, $\deg \psi = abc$.

We consider a generic plane $\pi \in \mathbf{A}^3$ defined by an equation $\alpha T + \beta U + \gamma V = 0$. Then π will intersect $\mathcal{W}$ in d lines through the origin; in fact, $\mathcal{W}$ may be considered as a projective curve of degree d and, via this identification, π corresponds to a generic projective line. For any choice of a triple $\Theta = (\mu, \nu, \zeta)$ of roots of unity of order a, b, c, respectively, let π_Θ be the plane with equation $\alpha\mu T + \mathcal{B}\nu U + \gamma\zeta V = 0$. For generic α, β, γ no two such planes intersect in a line contained in $\mathcal{W}$. Hence the union of these planes will intersect $\mathcal{W}$ in $abcd$ lines and it will be defined by the equation $\prod_\Theta(\alpha\mu T + \beta\nu U + \gamma\zeta V) = 0$. We may plainly write the product on the left side as $G(T^a, U^b, V^c)$ for a suitable polynomial G. Consider the intersection of $\mathcal{V}$ with the hypersurface $G(X, Y, Z) = 0$. This intersection will decompose as a finite union of distinct irreducible curves. (Since π is a generic plane, we may assume that the intersection multiplicity is 1 along each curve.) Let h be the number of such curves. The inverse image of each curve under ψ will be a union of abc lines lying in the intersection of $\mathcal{W}$ with the union of planes π_Θ. Therefore, we get $d = h$ and we are left to compute h.

To this end, we use the map φ. The curves in question will correspond under our two-to-one map to the components of the curve $G(X^a + Y^a, X^b + Y^b, X^c + Y^c) = 0$ (which is a union of lines in $\mathbf{A}^2$), except that we have to disregard a possible component (with its multiplicity) given by $X + Y = 0$. In fact, (i) this line collapses to a point under the map φ in case a, b, c are all odd, and (ii) no other line can collapse, since the g.c.d. of N_a, N_b, N_c divides $X + Y$ in all cases. So, suppose first that abc is even. Then, since $G(N_a, N_b, N_c)$ has degree abc and, since φ has degree 2, we obtain $d = abc/2$. If a, b, c are all odd, we have a component $X + Y = 0$. To compute its multiplicity, we first observe that $(X + Y)^{i+j+k}$ divides exactly a term $N_a^i N_b^j N_c^k$. Further, observe that $G(X, Y, Z)$ is the sum of the term $\alpha^{abc} X^{bc}$ and of a linear combination of monomials $X^i Y^j Z^k$ for which $i + j + k > bc$, whence the required multiplicity is just bc. Therefore, we obtain $abc - bc$ as the number of suitable lines, and the conclusion again follows.

REFERENCES

1. E. Bombieri, J. Müller and U. Zannier, *Equations in one variable over function fields*, Acta Arith. **99** (2001), 27–39.

2. D.G. Mead and S.K. Stein, *Some algebra of Newton polynomials*, Rocky Mountain J. Math. **28** (1998), 303–309.

3. J-P. Serre, *Lectures on the Mordell-Weil theorem*, Vieweg, 1990.

4. H. Völklein, *Groups as Galois groups*, Cambridge Stud. Adv. Math. **93**, Cambridge Univ. Press, 1996.

5. A. Weil, *Foundations of algebraic geometry*, Amer. Math. Soc. Colloq. Publ., Amer. Math. Soc., Providence, RI, 1989.

Dipartimento di Matematica, Università di Pisa, Via Buonarroti 2, 56127 Pisa, Italy
E-mail address: `dvornic@dm.unipi.it`

1st Univ. Arch. - D.C.A, S. Croce 191, 30135 Venezia, Italy
E-mail address: `zannier@iuav.unive.it`