COLLOQUIUM MATHEMATICUM

XVIII DÉDIÉ À M. TADEUSZ WAŻEWSKI 1967

REDUCIBILITY OF POLYNOMIALS OF THE FORM $f(x)-g(y)$

BY

A. SCHINZEL (WARSZAWA)

I have proposed in [3] the following problem: do there exist non-constant polynomials $f(x)$ and $g(y)$ such that $f(x)-g(y)$ is reducible over the complex field and is neither of the form

$$a\big(b(x)\big)-a\big(c(y)\big), \tag{1}$$

nor of the form

$$AT_4\big(b(x)\big)+AT_4\big(c(y)\big),$$

where a, b, c are polynomials, the degree of a is greater than 1, A is a constant and

$$T_4(z) = \cos(4\arccos z) = 8z^4-8z^2+1$$

(for earlier results on this topic see [1])?

Recently B. J. Birch, J. W. S. Cassels and M. Guy have solved this problem in the affirmative by finding the following example:

$$\begin{aligned} f(x)-g(y) = {} & x^7-7\lambda tx^5+(4-\lambda)tx^4+(14\lambda-35)t^2x^3- \\ & -(8\lambda+10)t^2x^2+\big((3-\lambda)t^2+7(3\lambda+2)t^3\big)x- \\ & -y^7+7\mu ty^5+(4-\mu)ty^4-(14\mu-35)t^2y^3- \\ & -(8\mu+10)t^2y^2-\big((3-\mu)t^2+7(3\mu+2)t^3\big)y-7t^3 \\ = {} & [x^3+\lambda x^3y-\mu xy^2-y^3-(3\lambda+2)tx+(3\mu+2)ty+t]\times \\ & \times[x^4-\lambda x^3y-x^2y^2-\mu xy^3+y^4+2(\mu-\lambda)tx^2-7txy+ \\ & +2(\lambda-\mu)ty^2+(3-\lambda)tx-(3-\mu)ty-7t^2]. \end{aligned}$$

In this example, t is a parameter, $\lambda = (1+\sqrt{-7})/2$, $\mu = (1-\sqrt{-7})/2$. Since λ/μ is irrational, the coefficients of f and g are not all rational except for $t=0$, when $f(x)-g(y) = x^7-y^7$ is of the form (1). The aim of the present note is to show that this is necessarily the case if at least one of the degrees of f and g is a prime. More exactly, we prove the

THEOREM. *Let f and g be non-constant polynomials with rational coefficients and let the degree of f be a prime, say p. Then $f(x)-g(y)$ is reducible over the complex field if and only if $g(y)=f(c(y))$ and either c has rational coefficients or*

$$f(x)-g(y) = A(x+a)^p - Bd(y)^p, \tag{2}$$

where d has rational coefficients and A, B and a are rationals.

COROLLARY. *Under the assumptions of the theorem, the case (2) being excepted, $f(x)-g(y)$ is reducible over the complex field only if it is reducible over the rational field.*

In the sequel, we shall denote by C the complex field, by Q the rational field, and, for any given field K, by $|K|$ its degree and by $K[x]$ the ring of polynomials in x over K. By ζ_p is meant the primitive p-th root of unity. We have

LEMMA 1. *Let $a \in Q$, $a \neq 0$ and $\sqrt[p]{a}$ be a rational root of the equation $x^p - a = 0$ if there are such roots or any root otherwise. Then $(x^p-a)/(x-\sqrt[p]{a})$ is irreducible over $Q(\sqrt[p]{a})$.*

Proof. Setting $K = Q(\sqrt[p]{a})$ we have

$$\left(|K|, |Q(\zeta_p)|\right) = \begin{cases} (1, p-1) & \text{if } \sqrt[p]{a} \text{ is rational,} \\ (p, p-1) & \text{if } \sqrt[p]{a} \text{ is irrational.} \end{cases}$$

Thus in any case $\left(|K|, |Q(\zeta_p)|\right) = 1$. Hence

$$|KQ(\zeta_p)| = |K|\,|Q(\zeta_p)| = (p-1)|K|$$

and

$$|K(\zeta_p\sqrt[p]{a})| = |K(\zeta_p)| = |KQ(\zeta_p)| = (p-1)|K|.$$

Since $\zeta_p\sqrt[p]{a}$ is a zero of the polynomial $(x^p-a)/(x-\sqrt[p]{a})$ and $(p-1)$ is its degree over K, the polynomial is irreducible over K, q.e.d.

LEMMA 2. *If polynomials f and g satisfy the conditions of the Theorem and $g(y) = f(c(y))$, where $c(y) \in C[y]$, then either $c(y) \in Q[y]$ or (2) holds.*

Proof. Let

$$f(x) = \sum_{i=0}^{p} a_i x^{p-i}, \quad g(x) = \sum_{i=0}^{q} b_i x^{q-i}, \quad c(x) = \sum_{j=0}^{r} c_j x^{r-j}.$$

It follows from the identity

$$g(x) = \sum_{i=0}^{q} b_i x^{q-i} = \sum_{i=0}^{p} a_i \Big(\sum_{j=0}^{r} c_j x^{r-j}\Big)^{p-i} \tag{3}$$

that

$$b_0 = a_0 c_0^p \tag{4}$$

and that for each positive $j < r$ the polynomial

$$D_j(x) = \frac{g(x)}{pb_0} - \frac{1}{p}\Big(\sum_{i=0}^{j-1} \frac{c_i}{c_0} x^{r-i}\Big)^p$$

has the leading coefficient c_j/c_0. The induction with respect to j shows that

$$\frac{c_j}{c_0} \in Q \qquad (0 \leqslant j < r). \tag{5}$$

Thus the leading coefficient of the polynomial $D_r(x)$ equal to ϱ, say, is rational. On the other hand, it follows from (3) that

$$\varrho = \frac{c_r}{c_0} + \frac{a_1}{pa_0c_0}, \qquad c_r = \varrho c_0 - \frac{a_1}{pa_0}. \tag{6}$$

Suppose now that (2) does not hold; thus the polynomial

$$f\left(x - \frac{a_1}{a_0 p}\right) - a_0 x^p$$

is non-constant. Let $d_0 x^s$ be its leading term ($0 < s < p$, d_0 rational). The polynomial

$$f\big(c(x)\big) - a_0\left(c(x) + \frac{a_1}{a_0 p}\right)^p = g(x) - b_0\left(\sum_{j=0}^{r-1} \frac{c_j}{c_0} x^{r-j} + \varrho\right)^p$$

has rational coefficients and the leading coefficient $d_0 c_0^s$. Thus $c_0^s \in Q$ and since, by (4), $c_0^p \in Q$, we get $c_0^{(s,p)} = c_0 \in Q$. It follows by (5) and (6) that $c(x) \in Q[x]$. The proof is complete.

Remark. The method used in the above proof gives the following more general statement.

Let K be a field of characteristic χ and L an arbitrary extension of K. If $f(x), g(x) \in K[x]$, $c(x) \in L[x]$, $g(x) = f\big(c(x)\big)$ and χ does not divide the degree of f, then there exist a positive integer q and $\varkappa$, $\lambda \in L$, $d(x)$, $h(x) \in K[x]$ such that

$$\lambda^q \in K, \qquad c(x) = \lambda d(x) - \varkappa, \qquad f(x) = h\big((x+\varkappa)^q\big).$$

The condition

$$\text{degree of } f \not\equiv 0 \pmod{\chi}$$

is necessary as is shown by the example:

$$\chi = 2, \qquad K = GF[2], \qquad L = GF[4] = K(\omega),$$
$$f(x) = x^2 + x, \qquad g(x) = x^2 + 1, \qquad c(x) = x + \omega.$$

Proof of the theorem. The sufficiency of the conditions given in the theorem follows immediately from the factorization

$$f(x)-f(c(y)) = (x-c(y))\sum_{n=1}^{p}\frac{f^{(n)}(x)}{n!}(c(y)-x)^{n-1}.$$

In order to prove the necessity of the conditions we assume without loss of generality that the leading coefficient of f is 1 and that of g is, say, a. Let

$$f(x)-g(y) = h_1(x,y)h_2(x,y)\dots h_r(x,y) \qquad (r>1) \tag{7}$$

be the decomposition of $f(x)-g(y)$ into factors irreducible over C with the coefficient of the highest power of x in each $h_i(x,y)$ equal to 1. Since $f(x)-g(y)$ is reducible, it follows from a theorem of Ehrenfeucht [2] that the degree of g is divisible by p and equals, say, kp, where k is an integer. Give x the weight k and y the weight 1 and denote the highest isobaric part of $h_i(x,y)$ by $H_i(x,y)$ $(1\leqslant i\leqslant r)$. It follows from (7) that

$$x^p-ay^{kp} = H_1(x,y)H_2(x,y)\dots H_r(x,y). \tag{8}$$

Let $\sqrt[p]{a}$ be defined as in Lemma 1. Since $x-\sqrt[p]{a}y^k \mid x^p-ay^{kp}$ and $x-\sqrt[p]{a}y^k$ is irreducible over C we may assume without loss of generality that

$$x-\sqrt[p]{a}y^k \mid H_1(x,y). \tag{9}$$

Suppose that $H_1(x,y)\neq x-\sqrt[p]{a}y^k$. In view of the normalization of $h_i(x,y)$, $H_1(x,1)/(x-\sqrt[p]{a})$ is not a constant. On the other hand, by (8) we get

$$\frac{x^p-a}{x-\sqrt[p]{a}} = \frac{H_1(x,1)}{x-\sqrt[p]{a}}H_2(x,1)\dots H_r(x,1). \tag{10}$$

It follows from Lemma 1 that $H_1(x,1)\notin K[x]$, where $K=Q(\sqrt[p]{a})$, and, a fortiori, $h_1(x,y)\notin K[x,y]$. The field of coefficients of h_1 is algebraic over K, thus there is a polynomial $h_1'(x,y)$ with coefficients algebraically conjugate over K to those of h_1 such that

$$h_1'(x,y)\neq h_1(x,y).$$

In view of the normalization of h_1, the coefficient of the highest power of x in $h_1'(x,y)$ equals 1, and since $h_1'(x,y)$ is irreducible over C it must occur in the factorization (7) as, say, h_2. We get

$$H_1'(x,y) = H_2(x,y),$$

where the coefficients of $H_1'(x, y)$ are algebraically conjugate over K to those of $H_1(x, y)$. By (9) we have

$$x-\sqrt[p]{a}y^k | H_2(x, y),$$

and by (10)

$$x-\sqrt[p]{a} \,\Big|\, \frac{x^p - a}{x-\sqrt[p]{a}},$$

which is impossible, since $x^p - a$ has no multiple zeros. Therefore

$$H_1(x, y) = x-\sqrt[p]{a}y^k,$$

and, by the definition of H_1,

$$h_1(x, y) = x - c(y).$$

We obtain now from (7) that $g(y) = f(c(y))$ and the theorem follows from Lemma 2.

Note added in proof. The following new non-trivial example of reducibility of $f(x) - g(y)$ has been found by Birch, Cassels and Guy:

$$\begin{aligned} & x^{11}+11\big(\lambda, -2, -3\mu\tau, -16\lambda, 3\mu^2(\lambda-4), 30\mu\tau, -63\mu, \\ & \qquad\qquad -20\mu^4, 3\mu^4\tau^2, -9\theta\big)(x, 1)^9 - \\ & -y^{11}-11\big(\mu, -2, -3\lambda\sigma, -16\mu, 3\lambda^2(\mu-4), 30\lambda\sigma, -63\lambda, \\ & \qquad\qquad -20\lambda^4, 3\lambda^4\sigma^2, 9\theta\big)(y, 1)^9 \\ & = [(1, -\lambda, -1, 1, \mu, -1)(x, y)^5 + \theta(2, -\lambda, -\mu, 2)(x, y)^3 - \\ & \qquad -2\theta(\mu, -3, \lambda)(x, y)^2 + \theta(\mu^3, \lambda^3)(x, y) - 6\theta] \times \\ & \times [(1, \lambda, \sigma, 2, \tau, \mu, 1)(x, y)^6 + \theta(\mu\tau, -\lambda^3, -2\theta, \mu^3, -\lambda\sigma)(x, y)^4 + \\ & +2\theta(\lambda, \lambda^2, -\mu^2, -\mu)(x, y)^3 - \theta\big(\mu(2\theta+3), 3\theta, \lambda(2\theta-3)\big)(x, y)^2 + \\ & \qquad +4\theta(-\mu^3, \lambda^3)(x, y) + 33], \end{aligned}$$

where

$$\theta^2 = -11, \quad \lambda = \frac{-1+\theta}{2}, \quad \mu = \frac{-1-\theta}{2},$$

$$\sigma = \mu - 1, \quad \tau = \lambda - 1.$$

REFERENCES

[1] H. Davenport, D. J. Lewis and A. Schinzel, *Equations of the form $f(x) = g(y)$*, Quarterly Journal of Mathematics 12 (1961), p. 304-312.

[2] A. Ehrenfeucht, *Kryterium absolutnej nieprzywiedlności wielomianów*, Prace Matematyczne 2 (1958), p. 167-169.

[3] A. Schinzel, *Some unsolved problems on polynomials*, Matematicka Biblioteka 25 (1963), p. 63-70.

Reçu par la Rédaction le 27. 12. 1965