MATH. SCAND. 3 (1955), 28–30

A PROBLEM IN FACTORIZATION OF POLYNOMIALS

L. CARLITZ and F. R. OLSON

If $f(x)$ is a cubic polynomial with rational coefficients and k is a constant,

$$f\big(x+kf(x)\big) = f(x)\,\varphi(x)\,,$$

we seek conditions that $\varphi(x)$ factor into two cubics.

Let $f(x)$ be a polynomial of degree n with coefficients in the rational field R and irreducible over R. It is easily seen that if k is an arbitrary rational number different from zero then

$$f\big(x+kf(x)\big) = f(x)\,\varphi(x)\,, \tag{1}$$

where $\varphi(x)$ is a polynomial with rational coefficients. We note that the factorization property of (1) is not altered if x is replaced by $x+c$. Further, if $\varphi(x)$ has the factorization

$$\varphi(x) = \varphi_1(x)\,\varphi_2(x)\ldots\varphi_t(x) \qquad \big(\text{degree } \varphi_i(x) = n_i\big) \tag{2}$$

then $n|n_i$. For if $\varphi_i(\varrho)=0$ then $f\big(\varrho+kf(\varrho)\big)=0$. Hence a root r of $f(x)$ may be expressed as a polynomial function of a root of $\varphi_i(x)$ and we see that the field $R(r)\subseteqq R(\varrho)$. This implies $n|n_i$.

We have the Taylor expansion

$$f\big(x+kf(x)\big) = f(x) + f'(x)kf(x) + f''(x)k^2f(x)^2/2! + \ldots$$

so that

$$\varphi(x) = 1 + kf'(x) + f''(x)k^2f(x)^2/2! + \ldots\,. \tag{3}$$

It follows that if $\varphi(x)$ should have a root in common with $f(x)$, this would also be a root of the equation

$$1 + f'(x)k = 0\,,$$

but this is impossible because all the irreducible factors of (1) are of degree $\geqq n$.

If $f(x)$ is quadratic, (1) factors into two irreducible quadratics for all

Received September 20, 1954.

$k \neq 0$. We next consider the cubic case and find conditions that $\varphi(x)$ factor into two cubics.

There is no loss of generality in considering the irreducible cubic

$$f(x) = x^3 + px + q \tag{4}$$

and assuming

$$f\big(x + kf(x)\big) = f(x)\,\varphi_1(x)\,\varphi_2(x)\,. \tag{5}$$

Let r, r_1, and r_2 be the roots of $f(x)$ and ϱ a root of $\varphi_1(x)$, say. Hence we may write

$$\varrho + k(\varrho - r)(\varrho - r_1)(\varrho - r_2) = r$$

which implies, since $r \neq \varrho$,

$$1 + k(\varrho - r_1)(\varrho - r_2) = 0\,. \tag{6}$$

Then

$$\varrho = \tfrac{1}{2}(r_1 + r_2 \pm D^{\frac{1}{2}}) \tag{7}$$

where

$$D = (r_1 + r_2)^2 - 4r_1r_2 - 4/k = -3r^2 - 4p - 4/k = -3r^2 - K\,.$$

Since ϱ is to satisfy a cubic equation, it is necessary that D be a square in the field $R(r)$, that is

$$-3r^2 - K = (a_0 + a_1 r + a_2 r^2)^2\,, \tag{8}$$

where a_0, a_1 and a_2 are rational. Comparison of coefficients in (8) yields

$$\begin{aligned} {a_1}^2 - {a_2}^2 p + 2a_0a_2 + 3 &= 0\,, \\ -{a_2}^2 q + 2a_0a_1 - 2a_1a_2p &= 0\,, \\ {a_0}^2 - 2a_1a_2q + K &= 0\,. \end{aligned} \tag{9}$$

Elimination of a_0 from the first two equations in (9) and division by ${a_1}^3$ gives

$$1 + p(a_2/a_1)^2 + q(a_2/a_1)^3 = -3(1/a_1)^2\,. \tag{10}$$

Hence K and in turn k is determined by the solutions of a Diophantine equation equivalent to

$$y^2 = x^3 - ax - b\,. \tag{11}$$

For a discussion of (11) see [1, pp. 255–260].

For $p = 0$ equation (10) may be written as

$$(a_1 + 1)^3 + (a_1 - 1)^3 = -2q{a_2}^3\,. \tag{12}$$

Thus if $q = \pm 4t^3$, (12) is a Fermat equation with the choice of a_1 limited

to ± 1. Hence we find from (9) that for $q=-4$ the only value for k is $k=-1/3$. Thus for $f(x)=x^3-4$ we have the factorization

$$-27f\big(x-\tfrac{1}{3}f(x)\big) = (x^3-4)(x^3+3x^2+3x-1)(x^3-3x^2-3x+11),$$

as can be verified without much trouble.

For $q=-2$ equation (12) has no solution [1, p. 269, ex. 144] and (1) with $f(x)=x^3-2$ becomes

$$f\big(x+kf(x)\big) = f(x)\,(k^3x^6+3k^2x^4-4k^3x^3+3kx^2-6k^2x+4k^3+1),$$

where the sextic is irreducible for all k. On the other hand for $q=-9/2$ equation (12) has an infinity of solutions [1, p. 246] and hence $f(x)=x^3-9/2$ permits the desired factorization for infinitely many k.

Thus it is seen that for a given cubic the number of choices for k may be zero, finite or infinite.

REFERENCE

1. Trygve Nagell, *Introduction to number theory*, New York, 1951.

DUKE UNIVERSITY, DURHAM, N. C., U.S.A.