ACTA ARITHMETICA
XXXII (1977)

Conspectus materiae tomi XXXII, fasciculi 1

La revue est consacrée à la Théorie des Nombres
The journal publishes papers on the Theory of Numbers
Die Zeitschrift veröffentlicht Arbeiten aus der Zahlentheorie
Журнал посвящен теории чисел

L'adresse de la Rédaction et de l'échange | Address of the Editorial Board and of the exchange | Die Adresse der Schriftleitung und des Austausches | Адрес редакции и книгообмена

ACTA ARITHMETICA
ul. Śniadeckich 8, 00-950 Warszawa

Les auteurs sont priés d'envoyer leurs manuscrits en deux exemplaires
The authors are requested to submit papers in two copies
Die Autoren sind gebeten um Zusendung von 2 Exemplaren jeder Arbeit
Рукописи статей редакция просит предлагать в двух экземплярах

PRINTED IN POLAND

WROCŁAWSKA DRUKARNIA NAUKOWA

Cyclic decomposition of polynomials

by

M. Bhaskaran (Girrawheen, W. Australia)

1. Introduction. In [1], Fried defined a polynomial $h(x) \in \boldsymbol{Q}[x]$ to be a *cyclic polynomial* if $h(x) = a(x-b)^n + c$ for some $a, b, c \in \boldsymbol{Q}$. The terminology is suggested by the fact that the Galois group of the splitting field of $h(x) - \lambda$ over $\boldsymbol{Q}(\lambda)$ (where λ is an indeterminate) is cyclic. He also defined that $h(x) = s_1\big(s_2\big(\ldots\big(s_l(x)\big)\big)\big)$ is a *prime decomposition* of $h(x)$ if each of the s_i's cannot be written as a composite of polynomials of strictly smaller degree. These definitions are equally applicable when the ground field is any algebraic number field k. Let us say that an irreducible polynomial $h(x) \in k[x]$ has a *cyclic decomposition of degree* r for $r > 1$ if $h(x) = g\big(s(x)\big)$ where $s(x)$ is a cyclic polynomial over k of degree r. If no such $r > 1$ exists, we say that $h(x)$ has no cyclic decomposition. If an irreducible polynomial has a cyclic decomposition of degree m and no other cyclic decomposition of degree a multiple of m, then the cyclic decomposition is said to be *maximal*.

Hereafter, b represents an element in k (not necessarily an integer) and c_q represents an element in k which may vary as q varies through k-primes. r is a natural number > 1. $[m_1, m_2]$ denotes the l.c.m. of m_1 and m_2.

The object of this note is to prove the following

THEOREM. *Let $h(x)$ be an irreducible polynomial over a number field k. Then if it has a cyclic decomposition, it has a unique maximal cyclic decomposition of the form $f\big((x-b)^m\big)$ for some polynomial $f(y)$ over k. $h(x) = g\big((x-b)^r\big)$ for some polynomial $g(y)$ over k if and only if $h(x)$ has irreducible cyclic factors of the form*

$$(x-b)^{p_j^{t_j}} + c_{q_{ji}} \bmod q_{ji},$$

where q_{ji} runs through an infinite number of k-primes for each j and $r = \prod_{j=1}^{l} p_j^{t_j}$, $p_1, p_2, \ldots, p_l$ distinct rational primes.

I thank the referee for some valuable criticisms in the preparation of this note.

2. Preliminaries. We prove the theorem for any monic irreducible polynomial in § 3. The proof for any irreducible polynomial over k is then got from the observations (a) and (b) below.

(a) Suppose

$$h(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0$$

be an irreducible polynomial over k. Then

$$H(x) = a_n^{n-1} h(x/a_n) = x^n + a_{n-1}x^{n-1} + \ldots + a_0 a_n^{n-1}$$

is a monic irreducible polynomial. If $h(x)$ has a cyclic factor $(x-b)^r + c_q \bmod q$ for a k-prime q with a sufficiently great norm, then it is easy to see that $H(x)$ has a cyclic factor $(x - a_n b)^r + a_n^r c \bmod q$. Hence, by Lemma 1 (stated below),

$$H(x) = g\left((x - a_n b)^r\right)$$

for some irreducible polynomial $g(y)$. Then

$$h(x) = g\left((a_n x - a_n b)^r\right)/a_n^{n-1} = G\left((x-b)^r\right)$$

for some irreducible polynomial $G(y)$ over k with a_n as the coefficient of the term in the highest degree.

(b) Conversely, if $h(x)$ has a cyclic decomposition of degree r, then $H(x)$ has a cyclic decomposition of degree r and this implies that $H(x)$ has cyclic factors of the form $(x - a_n b)^{p_j^{t_j}} + c'_{q_{ji}} \bmod q_{ji}$.

Now the proof of the non-trivial part of the theorem (second assertion) depends on the following two lemmas.

LEMMA 1. *Let $h(x) \in k[x]$ be a monic irreducible polynomial. Then $h(x) = g\left((x-b)^r\right)$ for some polynomial $g(y)$ over k if and only if $h(x)$ has cyclic (not necessarily irreducible) factors of the form $(x-b)^r + c_q \bmod q$ where q runs through an infinite number of k-primes.*

Proof. Put $x - b = X$. Let $h(x) = h_b(X)$ for some polynomial $h_b(y)$ over k. Let θ be a zero of $h_b(X)$ and let $\theta = \theta^{(1)}, \theta^{(2)}, \ldots, \theta^{(n)}$ (n being the degree of h) be the conjugates of θ over k. Then $h_b(X) = g(X^r)$ for some polynomial $g(y)$ over k if and only if there exist $\alpha_1, \alpha_2, \ldots, \alpha_r$ which are distinct natural numbers lying between 1 and n such that

$$\prod_{i=1}^{r} (X - \theta^{(\alpha_i)}) = X^r + a, \quad \text{where} \quad a = (-1)^r \theta^{(\alpha_1)} \theta^{(\alpha_2)} \ldots \theta^{(\alpha_r)}.$$

On the other hand, such a set of numbers $\alpha_1, \alpha_2, \ldots, \alpha_r$ exists if and only if for some choice of $\alpha_1, \alpha_2, \ldots, \alpha_r$ the first $r-1$ symmetric functions in $\theta^{(\alpha_1)}, \theta^{(\alpha_2)}, \ldots, \theta^{(\alpha_r)}$ are zero. And this happens if and only if $h(X) \bmod q$ has a factor (not necessarily irreducible) of form $X^r + c_q$ for infinitely many k-primes q by the following argument: There are infinite number of $k(\alpha)$-primes Q of degree 1 so that $\alpha \equiv$ a k-integer c_q modulo Q and consequently $h(X)$ has a factor $X^r + c_q \bmod q$ where q is the restriction of Q to k. Conversely, if $h(X)$ has a factor $X^r + c_q \bmod q$, then

$$X^r + c_q \equiv \prod_{i=1}^{r} (X - \theta^{(\alpha_i)}) \bmod q$$

for a suitable choice of natural numbers $\alpha_1, \alpha_2, \ldots, \alpha_r$ lying between 1 and n (q being considered as a $k(\theta^{(\alpha_1)}, \ldots, \theta^{(\alpha_r)})$ — ideal). Then the first $r-1$ symmetric functions in $\theta^{(\alpha_1)}, \theta^{(\alpha_2)}, \ldots, \theta^{(\alpha_r)}$ are divisible by q. If the norm of q is sufficiently large, this can happen only if each one of these symmetric functions is zero. Finally, substituting $x - b$ for X, we get the lemma.

LEMMA 2. *Let L be a finite normal extension of K (any number field) and let A^* be the set of all K-primes of degree 1 which split completely in L. Then A^* has the Dirichlet density $1/L:K$.*

This result, when A^* is replaced by the set A consisting of all K-primes (without the restriction about the degree) which split completely in L, is proved in [2] (p. 324, Cor. 4). The proof for the set A^* is substantially the same.

3. Proof of the theorem. (A) Suppose $h(x)$ of degree n has a cyclic decomposition $g\left((x-b)^r\right)$. We prove that b and g are unique in the above decomposition of degree r. If not, suppose $h(x) = g_1\left((x-b_1)^r\right)$. Then, considering the coefficients of x^{n-1} in the expansion of g and g_1, we get $b_1 = b$. Hence $g_1 = g$.

(B) Suppose $f_{m_1}\left((x-b_{m_1})^{m_1}\right)$ and $f_{m_2}\left((x-b_{m_2})^{m_2}\right)$ be two decompositions of $h(x)$ of degrees m_1 and m_2 respectively. Then we can prove that $b_{m_1} = b_{m_2} = b$ by considering the coefficients of x^{n-1} in these expressions. Hence, $h(x)$ is a polynomial in $(x-b)^{m_1}$, as well as in $(x-b)^{m_2}$, and thus a polynomial in $(x-b)^{[m_1,m_2]}$.

From (B), if follows that the degree of a maximal cyclic decomposition is unique and from (A), it follows that there is a unique maximal cyclic decomposition of the form $f\left((x-b)^m\right)$, thus proving the first assertion of the theorem.

The sufficiency condition of the second assertion follows from Lemma 1 and the fact that $h(x)$ is a polynomial in $(x-b)^{m_1}$, as well as in $(x-b)^{m_2}$, implies $h(x)$ is a polynomial in $(x-b)^{[m_1,m_2]}$. So, to conclude the proof of the theorem, it is enough to show that an irreducible polynomial with a cyclic decomposition of degree r has *irreducible* cyclic factors modulo q_{ji} of degree $p_j^{t_j}$ for each j, q_{ji} and $p_j^{t_j}$ being as stated in the theorem.

(C) First, we observe that a monic irreducible polynomial of the form $g(X^p)$ over k has irreducible cyclic factors of the form $X^p+c_q \bmod q$ for infinite number of primes q as follows. $g(X^p)$ has an irreducible factor $X^p+\alpha$ in $k(\alpha)$ where α is some algebraic number. Let ζ_p be a primitive pth root of unity. Taking $K=k(\alpha,\zeta_p)$ and $L=K$ and $K(\theta)$ successively in Lemma 2, we find that infinite number of K-primes of degree 1 do not split in $K(\theta)$. Then, it easily follows that infinite number of $k(\alpha)$-primes of degree 1 do not split in $k(\alpha,\theta)$. For any such $k(\alpha)$-prime Q (lying above a k-prime q with sufficiently great norm), $\alpha \equiv c_q \bmod Q$ for some k-integer c_q. Since Q does not split in $k(\alpha,\theta)$, $X^p+\alpha$ is irreducible modulo Q (by Kummer's theorem). As there are k-integral representatives for the residue classes modulo Q, this means that $-c_q$ is not a pth power residue of q. Thus X^p+c_q is irreducible modulo q and we get the desired result.

(D) If $h(x)$ has a cyclic decomposition of degree $p_j^{t_j}$, then

$$h(x) = g\left((x-b)^{p_j^{t_j}}\right)$$

for some monic irreducible polynomial g over k. Put $(x-b)^{p_j^{t_j-1}} = X$. Then $h(x)=g(X^{p_j})$. Now from (C), we get that $g(X^{p_j})$ has irreducible cyclic factors $X^{p_j}+c_{q_{ji}} \bmod q_{ji}$ for infinite number of q_{ji}. These $-c_{q_{ji}}$ are not p_jth powers modulo q_{ji}. From the well known result that an irreducible polynomial x^n+c over k splits modulo q (k—prime not dividing n) only if $-c$ is a dth power modulo q for some divisor d of n, it follows that $(x-b)^{p_j^{t_j}}+c_{q_{ji}}$ is irreducible modulo q_{ji} as $c_{q_{ji}}$ is not a p_jth power modulo q_{ji}. Putting $X=(x-b)^{p_j^{t_j-1}}$, we get that $h(x)$ has irreducible cyclic factors mod q_{ji} of the form $(x-b)^{p_j^{t_j}}+c_{q_{ji}}$. This completes the second assertion of the theorem.

4. Some comments. One may ask whether the necessary condition in the theorem could be strengthened as the existence of irreducible cyclic factors of the form $(x-b)^r+c_q \bmod q$ for infinite number of k-primes q. This seems to be a delicate problem to solve. Another question is whether the existence of irreducible cyclic factors of the form $(x-b_q)^r+c_q \bmod q$, where b_q also depend on q, $r>1$ and divides the degree of $h(x)$ and q runs through infinite number of k-primes, will guarantee cyclic decomposition for $h(x)$ in general. The answer is no as is illustrated by the following example (supplied to me by the referee):

We construct an irreducible monic polynomial $h(x)\in \boldsymbol{Z}[x]$ of degree 4 such that for infinitely many primes q, $h(x) \bmod q$ has a cyclic factor of degree 2, but $h(x)$ is indecomposable and not a cyclic polynomial.

Choose $h(x)$ of degree 4 such that the splitting field, K_h, of $h(x)$ over $\boldsymbol{Q}$ satisfies: $G(K_h/\boldsymbol{Q})$ (Galois group of K_h over $\boldsymbol{Q}$) is S_4 (the symmetric group on 4 letters). By Čebotarev density theorem, there exists an infinite set of primes q for which the Frobenius symbol of a prime of K_h over q is $(12)\,(34)\in S_4$. By Kummer's theorem, for these q, $h(x) \bmod q$ is a product of two irreducible factors of degree 2 (cyclic factors). On the other hand, let K_{h-y} be the splitting field of $h(x)-y$ over $\boldsymbol{Q}(y)$. Then $G\left(K_{h-y}/\boldsymbol{Q}(y)\right)$ is also S_4. Since S_4 is a doubly transitive group, there are no fields between $\boldsymbol{Q}(\bar{x})$ and $\boldsymbol{Q}(y)$, where $\bar{x}$ is a zero of $h(x)-y$. Therefore $h(x)$ is indecomposable.

References

[1] M. Fried, *Arithmetic properties of value sets of polynomials*, Acta Arith. 15 (1969), pp. 91–115.

[2] W. Narkiewicz, *Elementary and analytic theory of algebraic numbers*, Warszawa 1974.

Received on 12. 9. 1974
and in revised form on 11. 7. 1975 (618)