Zeitschrift: L'Enseignement Mathématique

Band: 33 (1987)

Heft: 1-2: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: ON THE GALOIS GROUPS OF THE EXPONENTIAL TAYLOR POLYNOMIALS

Kapitel: II. Application to the Exponential Taylor Polynomials

Autor: Coleman, Robert F.

DOI: https://doi.org/10.5169/seals-87891

where the degree of g_i *is* $x_i - x_{i-1}$ *and all the roots of* $g_i(x)$ *in* $\bar{\mathbf{Q}}_p$ *have valuation* $-\left(\dfrac{y_i - y_{i-1}}{x_i - x_{i-1}}\right)$.

We call the rational numbers, $\dfrac{y_i - y_{i-1}}{x_i - x_{i-1}}$, the slopes of g.

Example. The polynomial f_7 has three factors over $\mathbf{Q}_2$, of degrees 4, 2 and 1, respectively, which have slopes $-3/4$, $-1/2$ and 0.

COROLLARY. *Let* d *be a positive integer. Suppose that* d *divides the denominator of each slope (in lowest terms) of* g. *Then* d *divides the degree of each factor of* g *over* $\mathbf{Q}_p$.

Proof. It suffices to show that d divides the degree of each irreducible factor of g. Let h be such a factor. Let $\alpha \in \bar{\mathbf{Q}}_p$ be a root of h. Since d divides the denominator of the valuation of α (by Theorem NP), it follows that d divides the index of ramification of the extension $\mathbf{Q}_p(\alpha)/\mathbf{Q}_p$ which divides the degree of the extension which equals the degree of h.

II. APPLICATION TO THE EXPONENTIAL TAYLOR POLYNOMIALS

Fix a prime number p.

LEMMA. *Suppose* k *is a positive integer and*

$$k = a_0 + a_1 p + \dots a_s p^s$$

where $0 \leqslant a_i < p$. *Then*

$$\operatorname{ord}(k!) = \frac{k - (a_0 + a_1 + \dots + a_s)}{p - 1}.$$

This is easy and well known.

Now write

$$n = b_1 p^{n_1} + b_2 p^{n_2} + \dots + b_s p^{n_s}$$

where $n_1 > n_2 > \dots > n_s$ and $0 < b_i < p$. Let

$$x_i = b_1 p^{n_1} + \dots + b_i p^{n_i}.$$

LEMMA. *The vertices of the Newton polygon of* f_n *are*

$$(x_i, -\operatorname{ord}_p(x_i!)), \quad 1 < i < s.$$

This follows easily from the previous lemmas.

It follows that the slopes of f are

$$m = \frac{-\operatorname{ord}_p(x_i!) + \operatorname{ord}_p(x_{i-1}!)}{x_i - x_{i-1}} = \frac{-(p^{n_i}-1)}{p^{n_i}(p-1)}.$$

COROLLARY A. *Suppose that* p^m *divides* n. *Then* p^m *divides the degree of each factor of* f_n *over* $\mathbf{Q}_p$.

Proof. Since p^m divides n, $m \leqslant n_s < n_{s-1} < \dots$. Hence, it follows from (1) that p^m divides the denominator of each m. Therefore the corollary follows from the corollary to Theorem NP.

COROLLARY B. *Suppose that* $p^k \leqslant n$. *Then* p^k *divides the degree of the splitting field of* f_n *over* $\mathbf{Q}_p$.

Proof. The hypotheses imply that $k \leqslant n_1$. Hence p^k divides the denominator of m_1. As above this implies that p^k divides the degree of any extension of $\mathbf{Q}_p$ formed by adjoining a root of f_n with valuation $-m_1$. This yields the corollary.

III. GLOBAL CONCLUSIONS A AND B

A. f_n is irreducible.

Suppose

$$n = \prod_p p^{n_p}$$

is the prime factorization of n. Corollary A implies that, for each prime p, p^{n_p} divides the degree of each factor of f_n over $\mathbf{Q}$. The conclusion follows.

B. Suppose $n/2 < p \leqslant n$ is a prime number. Then G contains a p-cycle.

By Corollary B, p divides the degree of the splitting field of f_n over $\mathbf{Q}_p$ which divides the degree of the splitting field of f_n over $\mathbf{Q}$. Hence p divides the order of G_n. By Cauchy's Theorem G contains an element of order p. The conclusion follows since the only elements of order p in S_n are p-cycles if $p > n/2$.