

I. Review of the Newton Polygon

Objektyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **33 (1987)**

Heft 1-2: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **19.09.2024**

Nutzungsbedingungen

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern. Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden. Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

Haftungsausschluss

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

ON THE GALOIS GROUPS OF THE EXPONENTIAL TAYLOR POLYNOMIALS

by Robert F. COLEMAN

Let

$$f_n(x) = 1 + x + \frac{x^2}{2!} + \dots + \frac{x^n}{n!}$$

denote the n^{th} Taylor polynomial of the Exponential Function.

In 1930, [S-2], Schur proved the following theorem about $f_n(x)$:

THEOREM (Schur). *The Galois group, G_n , of f_n is A_n , the alternating group on n letters, if 4 divides n and is S_n , the symmetric group on n letters, otherwise.*

In this note we shall give a proof different from Schur's. Our ulterior motive is to demonstrate the utility of Newton polygons.

We must:

- A. Show that f_n is irreducible.
- B. Show that G_n contains a p -cycle for any prime number p between $n/2$ and $n-2$.
- C. Calculate the discriminant, D_n , of f_n and determine when it is a square.

We need the following:

1. The main theorem about p -adic Newton polygons (see below).
2. Bertrand's Postulate [B], proven by Tschebyshev [T], which asserts that for each integer n , at least 8, there exists a prime number strictly between $n/2$ and $n-2$. (See also [H-W] Chapter 22.)
3. The theorem of Jordan which asserts that if G is a transitive subgroup of S_n which contains a p -cycle for some prime p strictly between $n/2$ and $n-2$ then G contains A_n . (See [J-1], Note C and [J-2], Theorem 1 or [Ha], Theorems 5.6.2 and 5.7.2.)
4. The fact that the Galois group of a polynomial of degree n is contained in A_n iff its discriminant is a square.

We shall use 1 for A and B . This will imply G_n is transitive and together with 2 and 3 will imply G_n contains A_n for $n \geq 8$. We shall use the differential equation satisfied by the exponential function and 2 again to perform C . Finally, we shall use 4 to complete the proof. (We shall also require liberal doses of Galois theory.)

I. REVIEW OF THE NEWTON POLYGON

Let

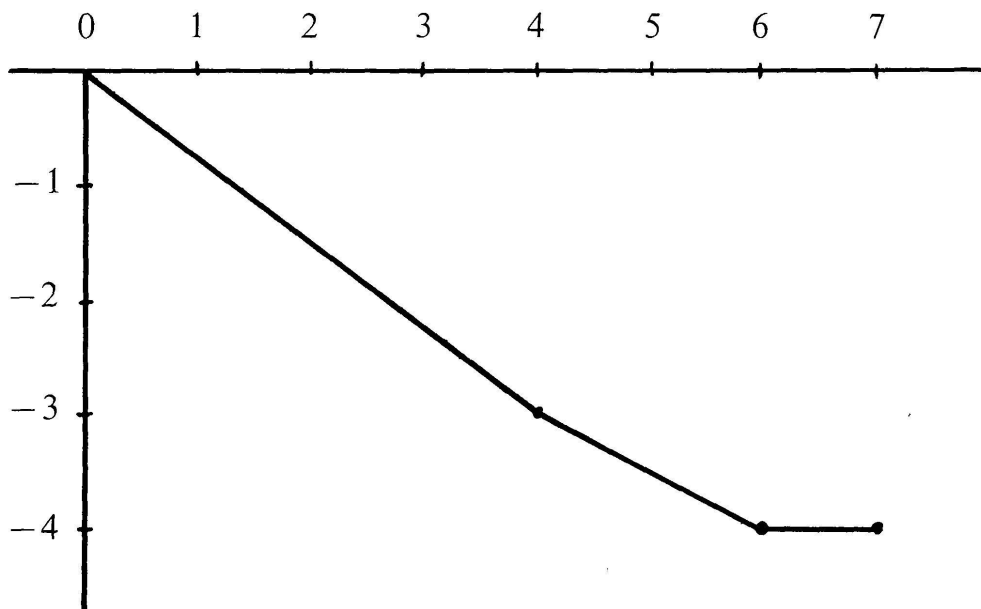
$$g(x) = a_0 + a_1x + \dots + a_kx^k$$

be a polynomial over \mathbf{Q}_p . Consider the points:

$$(i, \text{ord}(a_i)), \quad 0 \leq i \leq k,$$

in the Cartesian plane. The Newton polygon of g is defined to be the lower convex hull of these points.

Example. The Newton Polygon of $f_7(x)$ considered over \mathbf{Q}_2 , is



The main theorem about these polygons is:

THEOREM NP. Let $(x_0, y_0), (x_1, y_1), \dots, (x_p, y_p)$ denote the successive vertices of this polygon. Then over \mathbf{Q}_p , g factors as follows:

$$g(x) = g_1(x)g_2(x) \dots g_r(x)$$

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 $-\left(\frac{y_i - y_{i-1}}{x_i - x_{i-1}}\right)$.

We call the rational numbers, $\frac{y_i - y_{i-1}}{x_i - x_{i-1}}$, 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

$$k = a_0 + a_1p + \dots + a_s p^s$$

where $0 \leq a_i < p$. Then

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

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

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