ON THE GALOIS GROUPS OF THE EXPONENTIAL TAYLOR POLYNOMIALS

Autor(en): **Coleman, Robert F.**

Objekttyp: **Article**

Zeitschrift: **L'Enseignement Mathématique**

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

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

Erstellt am: **Mar 26, 2014**

Persistenter Link: http://dx.doi.org/10.5169/seals-87891

L'Enseignement Mathématique, t. 33 (1987), p. 183-189

ON THE GALOIS GROUPS OF THE EXPONENTIAL TAYLOR POLYNOMIALS

by Robert F. COLEMAN

Let

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

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 $n \geqslant 8$. 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

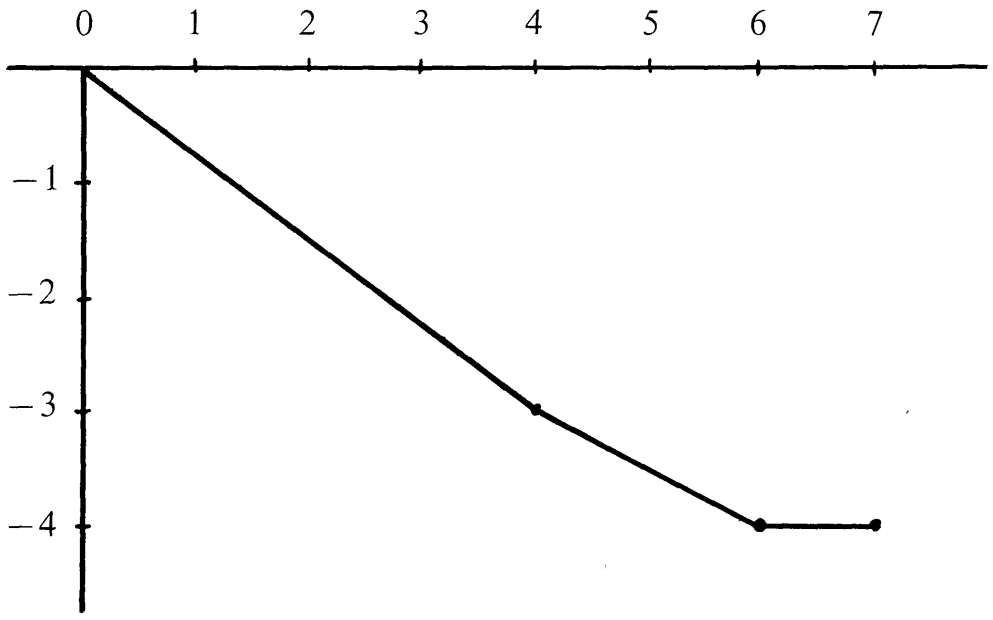
$$g(x) = a_0 + a_1 x + \ldots + a_k x^k$$

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

$$(i, \operatorname{ord}(a_i)), \quad 0 \leqslant i \leqslant k,$$

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

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

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

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*

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

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

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

This is easy and well known.

Now write

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

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

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

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

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

This follows easily from the previous lemmas.

It follows that the slopes of f are

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

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, $m \leqslant n_s < n_{s-1} < \ldots$. 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 $p > n/2$.

IV. Calculation of the discriminant

Let $f_n(x) = \frac{1}{n!}(x-\alpha_1)\dots(x-\alpha_n)$. Then

$$\begin{aligned} D_n &= \prod_{i\neq j}(\alpha_i-\alpha_j) = (-1)^{\binom{n}{2}}\prod_{i<j}(\alpha_i-\alpha_j) \\ &= (-1)^{\binom{n}{2}}\prod_{i=1}^{n}(n!\, f_n'(\alpha_i)) = (-1)^{\binom{n}{2}}\prod_{i=1}^{n} n!\, f_{n-1}(\alpha_i) \\ &= (-1)^{\binom{n}{2}}\prod_{i=1}^{n}(-\alpha_i^n) \qquad \left(\text{since } f_{n-1}(x) = f_n(x) - \frac{x^n}{n!}\right) \\ &= (-1)^{\binom{n}{2}+n}\left(\prod_{i=1}^{n}\alpha_i\right)^n = (-1)^{\binom{n}{2}+n}\left((-1)^n n!\, f_n(0)\right)^n \\ &= (-1)^{\binom{n}{2}}(n!)^n . \end{aligned}$$

V. End of Proof

Tschebyshev's Theorem (2 above) implies that for each $n > 1$ there is a prime number p such that

$$\operatorname{ord}_p(n!) = 1 .$$

Hence D_n is not a square if n is odd. If $n \equiv 2(4)$ then $D_n < 0$ so it is not a square in this case either. Finally if 4 divides n then we see that D_n is a square. This completes the proof for $n \geqslant 8$. The remaining cases can be handled individually using the above results and facts about S_n for small n. (See [S-2].)

VI. Final Remarks

1. Hilbert [H] proved that there exist extensions of $\mathbf{Q}$ with Galois group S_n. The splitting fields of the exponential polynomials provide explicit examples of such extensions. Moreover, they provide examples of such extensions ramified only at the primes dividing the order of the Galois group, a property not predictable by Hilbert's methods. (In fact, as can easily be checked using the results of II above, they are ramified at all primes dividing the order of the Galois group.) Schur also found A_n extensions of $\mathbf{Q}$ for n odd unramified outside $n!$ (see [S-2] and [S-3]). This raises the question, given a simple group G, does there exist a G extension of $\mathbf{Q}$ unramified outside the order of G?

2. The original proof of Schur utilized the following result:

THEOREM (Schur 1929 [S-1]). *Let* $1 \leqslant k \leqslant h$ *be integers. Then there exists a prime number* $p > k$ *which divides one of the following integers:*

$$h + 1,\ h + 2,\ ...,\ h + k\,.$$

The proof uses Tschebyshev's method. Schur needed this result to demonstrate the irreducibility of f_n, which we were able to obtain by elementary means. However, Schur obtained much more. He proved:

THEOREM (Schur, 1929, [S-1]). *Let* $a_0, a_1, ..., a_n$ *be integers such that* $(a_0, a_n, n!) = 1$. *Then*

$$a_0 + a_1 x + \frac{a_2 x^2}{2!} + ... + \frac{a_n x^n}{n!}$$

is irreducible.

3. *Exercises.*

(a) Calculate the Galois Groups of the Following polynomials:

(1) (Laguerre) $$L_n(x) = \sum_{k=0}^{n} \binom{n}{k} \frac{(-x)^k}{k!},$$

(2) $$J_n(x) = \frac{1}{x} \int_0^x L_n(t)dt = \frac{1}{n+1} \frac{dL_{n+1}(x)}{dx},$$

(3) (Hermite) $$H_m(x) = \sum_{k=0}^{[m/2]} \left(-\frac{1}{2}\right)^k \frac{m!}{(m-2k)!\,k!} x^{m-2k},$$

$$K_n^{(0)}(x^2) = H_{2n}(x), \qquad K_n^{(1)}(x^2) = \frac{1}{x} H_{2n+1}(x).$$

(b) Calculate the discriminants of polynomials:

$$\sum_{v=0}^{n} \binom{n+\alpha}{n-v} \frac{(-x)^v}{v!}, \qquad \text{for} \quad \alpha \in \mathbf{Q}.$$

(See [S-2] and [S-3].) Using either Schur's Criterion above or the methods of this note, determine the irreducibility of as many of these polynomials as you can.

(c) For each prime p, determine the inertia subgroups of G_n above p. (Note, we have only done this when n is a power of p.)

REFERENCES

[Ha] HALL, M. *Theory of Groups.* Macmillan. 1959.

[H] HILBERT, D. Über die Irreduzibilität ganzen rationalen Funktionen mit ganzzahligen Koeffizienten. *Jour. für Math. Bd. 110* (1892), 104-129.

[H-W] HARDY, G. H. and E. M. WRIGHT. An *Introduction to the Theory of Numbers*, fifth ed., Clavendon Press, Oxford, 1979.

[J-1] JORDAN, C. *Traité des Substitutions et des Equations Algébriques.* Gauthier-Villars, Paris (1870).

[J-2] —— Sur la limite de transivité des groupes non alternés. *Bul. Soc. Math. France 1* (1872-73), 40-71.

[S-1] SCHUR, I. Einige Sätze über Primzahlen mit Anwendungen auf Irreduzibilitätsfragen I (1929). *Gesammelte Abhandlungen*, Band III, No. 64, 140-151.

[S-2] —— Gleichungen ohne Affekt (1930). *Gesammelte Abhandlungen*, Band III, No. 67, 191-197.

[S-3] —— Affektlose Gleichungen in der Theorie der Laguerreschen und Hermiteschen Polynome (1931). *Gesammelte Abhandlungen*, Band III, Nr. 70, 227-233.

[T] TSCHEBYSHEV, P. I. Sur la totalité des nombres premiers inférieurs à une limite donnée. *J. de Math. 17* (1852), 341-365.

(Reçu le 22 août 1986)

Robert F. Coleman

University of California
Department of Mathematics
Berkeley, California 94720
USA

ADDED IN PROOF. For some interesting new results concerning the Galois theory of the polynomials mentioned above see: W. FEIT, *$\tilde{A}_5$ and $\tilde{A}_7$ are Galois groups over number fields.*