RT-MAT 2002-26

The Galois group of $x^n - x^{n-1} - \ldots - x - 1$

Paulo A. Martin

Outubro 2002

The Galois group of $x^n - x^{n-1} - \cdots - x - 1$.

Paulo A. Martin
Instituto de Matemática e Estatística da Univeridade de São Paulo,
Caixa Postal 66281, CEP 05315-970, São Paulo, SP, Brazil
email: agozzini@ime.usp.br

Running head: Galois group of $x^n - x^{n-1} - \cdots - x - 1$.

Abstract

In this paper we prove that if n is an even integer or a prime number, then the Galois group of of $x^n - x^{n-1} - \cdots - x - 1$ is the symmetric group S_n. This polynomial family arises quite naturally from a kind of generalized Fibonnaci sequence. In order to prove our result for $n = p$ prime, we had to prove that $x^p - x^{p-1} - \cdots - x - 1$ is irreducible in $\mathbf{F}_p[x]$, which seems to be a result of independent interest.

Keywords: Galois groups, polynomials with group S_n, generalized Fibonacci sequences, irreducibility criteria.

Introduction

In general it is difficult to construct extensions of the rational number field with a given Galois group G. Hilbert's irreducibility result provides the *existence* of Galois extensions of $\mathbb{Q}$ with the symmetric group in n symbols S_n as Galois group. I. Schur, [1], considered the family of polynomials

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

and proved that the Galois group G_n of f_n is S_n if $n \not\equiv 0 \mod 4$ and A_n (the alternating group) otherwise.

In a later paper Schur,[2], considered also the Laguerre and Hermite polynomials

$$L_n = \frac{e^x}{n!}\frac{d^n(x^n e^{-x})}{dx^n} = \sum_{\nu=0}^{\infty}\binom{n}{\nu}\frac{(-x)^\nu}{\nu!},$$

$$H_m(x) = \sum_{\mu=0}^{[m/2]}(-1)^\mu\binom{m}{2\mu}1\cdot 3\cdot 5\cdots(2\mu-1)x^{m-2\mu}.$$

R. Coleman,[4], has given a different proof of some of Schur's result, using Newton polygons. H. Osada, [5], proved that the Galois group of $x^n - x - 1$ is S_n for all $n \geq 2$.

We have found another such a simple family while playing with a kind of generalized Fibonacci sequence (see section 1). In the study of the sucessive quotients of this sequence there appears the equation

$$f_n(x) = x^n - x^{n-1} - \cdots - x - 1 = 0,$$

whose unique positive root is a Pisot number (when $n = 2$ this root is the golden number). We were able to prove that the Galois Group of the above equation is S_n for every even or prime n. We believe that the result is true for every value of n. In the last section we proved this for n up to 30.

1 A remarkable family of polynomials

It is well known that if we consider the Fibonacci sequence $\{a_n\}$ and put $b_n = a_{n+1}/a_n$, then $\{b_n\}$ converges to the golden ratio

$$\phi_2 = \frac{1+\sqrt{5}}{2} = 1.6180339\ldots.$$

The recurrence $a_{n+2} = a_{n+1} + a_n$ implies that

$$b_{n+1}b_n = b_n + 1.$$

Since $\{b_n\}$ is a convergent sequence, its limit ϕ_2 must be the positive root of

$$x^2 = x + 1.$$

Consider now a slightly more general Fibonacci sequence $\{a_n\}$: 1, 1, 1, 3, 5, 9, ..., which obeys the recurrence $a_{n+3} = a_{n+2} + a_{n+1} + a_n$. Putting as

above $b_n = a_{n+1}/a_n$ we see that if $\{b_n\}$ is convergent, its limit ϕ_3 must be a positive root of

$$x^3 = x^2 + x + 1.$$

It is not difiecult to see that the only positive root of the above polynomial is

$$\phi_3 = \frac{1 + \sqrt[3]{19 - 3\sqrt{33}} + \sqrt[3]{19 + 3\sqrt{33}}}{3} = 1.83929\ldots$$

and that the sequence $\{b_n\}$ is in fact convergent.

In general we consider the k-Fibonacci sequence $\{a_n\}$:

$$1, \ldots, 1, k, k + (k-1), k + (k-1) + (k-2), \ldots$$

which begins with k 1's, and obeys the recurrence

$$a_{n+k} = a_{n+k-1} + a_{n+k-2} + \cdots + a_n.$$

The corresponding $b_n = a_{n+1}/a_n$, if convergent, must converge to a positive root of

$$x^k = x^{k-1} + \cdots + x + 1,$$

and this is the family of polynomials we will consider in this paper:

$$f_n(x) = x^n - x^{n-1} - x^{n-2} - \cdots - x - 1.$$

If we multiply $f_n(x)$ by $(x-1)$ the family becomes

$$g_n(x) = x^{n+1} - 2x^n + 1. \tag{1}$$

It is clear that except for $x = 1$, g_n and f_n have the same roots. We will see that each $f_n(x)$ has only one positive zero ϕ_n, which converges to 2. Here are some values of these roots:

$\phi_2 = 1.6180339...$	$\phi_4 = 1.92756...$
$\phi_3 = 1.8392867...$	$\phi_5 = 1.96595...$

Table 1: Some values of the positive roots.

2 Algebraic properties of this family

Since $f_n(1) < 0$ and $f_n(2) = g_n(2) = 1$, there is a real root ϕ_n of $f_n(x)$ with $1 < \phi_n < 2$. By Descarte's rule of signs this is the unique positive root of $f_n(x)$. The same rule applied to $g_n(x)$ shows that if n is even $f_n(x)$ has exactly one negative root $-1 < r_n < 0$ (indeed, for n even $f_n(-1) = 1$ and $f_n(0) = -1$); if n is odd ϕ_n is the ony real root of $f_n(x)$.

Theorem 2.1 (Miles, [6], and Miller,[7]) *Every root $z \neq \phi_n$ of $f_n(x)$ verifies:*

$$|z| < 1.$$

Corollary 2.2 *The polynomial $f_n(x)$ is an irreducible polynomial over $\mathbb{Q}$.*

Proof: In fact, since $f_n(x)$ does not have rational roots, if we can factor (in $\mathbb{Z}[x]$ by Gauss lemma)

$$f_n(x) = \varphi(x)\psi(x),$$

it is clear that the degrees of φ and ψ are ≥ 2 (clearly we can suppose $n \geq 4$). Let ϕ_n be the unique positive root of $f_n(x)$ and suppose that $\psi(\phi_n) = 0$. Then by theorem 2.1 and the observations at the beginning of this section all the roots z of $\varphi(x)$ verify: $|z| < 1$. But this is not possible since the constant term of φ is an integer. □

Lemma 2.3 *The discriminant D_n of $g_n(x)$ is*

$$D_n = (-1)^{\binom{n+1}{2}}[(n+1)^{n+1} - 2^{n+1}n^n]$$

Proof: Let $\alpha_1, \alpha_2, \ldots, \alpha_{n+1}$ be the roots of $g_n(x)$ in the complex field $\mathbb{C}$. Since

$$\begin{aligned} D_n = \prod_{i<j}(\alpha_i - \alpha_j)^2 &= (-1)^{\binom{n+1}{2}} \prod_{i=1}^{n+1} \prod_{j \neq i} (\alpha_i - \alpha_j) \\ &= (-1)^{\binom{n+1}{2}} \prod_{i=1}^{n+1} g_n'(\alpha_i) \end{aligned} \tag{2}$$

and $g_n'(x) = x^{n-1}[(n+1)x - 2n]$ we can write

$$\prod_{i=1}^{n+1} g_n'(\alpha_i) = \prod_{i=1}^{n+1} \alpha_i^{n-1}[(n+1)\alpha_i - 2n].$$

But since $\alpha_1\alpha_2\cdots\alpha_{n+1} = (-1)^{n+1}$ we have

$$\begin{aligned}\prod_{i=1}^{n+1} g_n'(\alpha_i) &= (-1)^{(n+1)(n-1)}(n+1)^{n+1}\prod_{i=1}^{n+1}[\alpha_i - \frac{2n}{n+1}] \\ &= (-1)^{(n+1)(n-1)}(-1)^{n+1}(n+1)^{n+1}\prod_{i=1}^{n+1}[\frac{2n}{n+1} - \alpha_i] \qquad (3) \\ &= (-1)^{n^2+n}(n+1)^{n+1}g_n(\frac{2n}{n+1}).\end{aligned}$$

Now we calculate:

$$\begin{aligned}g_n(\frac{2n}{n+1}) &= (\frac{2n}{n+1})^{n+1} - 2(\frac{2n}{n+1})^n + 1 \\ &= \frac{2^{n+1}n^{n+1}}{(n+1)^{n+1}} - \frac{2^{n+1}n^n}{(n+1)^n} + 1 \qquad (4)\end{aligned}$$

Substituting (4) into (3) we have:

$$\begin{aligned}\prod_{i=1}^{n+1} g_n'(\alpha_i) &= (-1)^{n^2+n}(n+1)^{n+1}\left[\frac{2^{n+1}n^{n+1}}{(n+1)^{n+1}} - \frac{2^{n+1}n^n}{(n+1)^n} + 1\right] \\ &= (-1)^{n^2+n}\left[2^{n+1}n^{n+1} - 2^{n+1}n^n(n+1) + (n+1)^{n+1}\right] \qquad (5) \\ &= (-1)^{n^2+n}[(n+1)^{n+1} - 2^{n+1}n^n] \\ &= [(n+1)^{n+1} - 2^{n+1}n^n],\end{aligned}$$

because $n^2 + n$ is even for every n. This finishes the proof. □

Lemma 2.4 *The discriminant d_n of $f_n(x)$ is*

$$d_n = \frac{(-1)^{\binom{n+1}{2}}[(n+1)^{n+1} - 2^{n+1}n^n]}{(n-1)^2}.$$

Proof: The roots of $g_n(x)$ are $1, \alpha_2, \ldots, \alpha_{n+1}$. Then

$$d_n = \frac{D_n}{\prod_{k=2}^{n+1}(1-\alpha_k)^2}.$$

But since $\alpha_2, \ldots, \alpha_{n+1}$ are the roots of $f_n(x)$ we simply have

$$\prod_{k=2}^{n+1}(1-\alpha_k) = f_n(1) = -(n-1),$$

which gives the lemma. □

Remark 2.5 *In fact, R. Swan has proved, [8], that the discriminant D of $x^n + ax^k + b$ is*

$$D = (-1)^{\binom{n}{2}} b^{k-1} \left[n^{n_1} b^{n_1-k_1} + (-1)^{n_1+1}(n-k)^{n_1-k_1} k^{k_1} a^{n_1}\right]^d,$$

where $n > k > 0$, $d = (n,k)$ and $n = n_1 d$, $k = k_1 d$.

Table 2 gives some initial values of D_n and d_n:

n	2	3	4	5	6	7	8
D_n	5	-176	-5067	153344	5148425	-194049792	-8202514103
d_n	5	-44	-563	9584	205937	-5390272	-167398247

Table 2: Some initial values of D_n and d_n

Lemma 2.6 *The discriminant D_n of $g_n(x)$ is never a perfect square. And so the discriminant d_n of f_n is also never a perfect square*

Proof: Notice first that

$$\binom{n+1}{2} \equiv 0 \mod 2 \Longleftrightarrow n \equiv 0,3 \mod 4,$$

and since $(n+1)^{n+1} - 2^{n+1}n^n < 0$ for every $n \geq 2$, $D_n < 0$ for $n \equiv 0,3 \mod 4$. Therefore, if $n \equiv 0,3 \mod 4$, $D_n < 0$, and so D_n cannot be a square. For $n \equiv 1,2 \mod 4$ we can write the discriminant D_n as

$$D_n = 2^{n+1}n^n - (n+1)^{n+1}.$$

Suppose $n \equiv 1 \mod 4$. If also $n \equiv 0 \mod 3$ then

$$D_n \equiv -1 \mod 3$$

and so D_n cannot be a square. If $n \equiv 2 \mod 3$,

$$D_n \equiv (-1)^{n+1}(-1)^n \equiv -1 \mod 3$$

and D_n cannot be a square. Let $n \equiv 1 \mod 3$. Then $n = 1 + 12k$ and we can write D_n as

$$D_n = 2^{2+12k}\left[(1+12k)^{1+12k} - (1+6k)^{2+12k}\right].$$

It is enough to prove that $D_n/2^{2+12k}$ is not a perfect square. For this consider the following cases

(1) $k \equiv 1 \mod 7$. Then, since $\{0, 1, 4, 2\}$ are the only squares $\mod 7$ and

$$D_n \equiv 5^{1+12k} \equiv 5 \mod 7,$$

(because $5^{12} \equiv 1 \mod 7$), D_n cannot be a perfect square.

(2) $k \equiv 2 \mod 7$. Then

$$D_n \equiv 4^{1+12k} - (-1)^{2+12k} \equiv 4 - 1 \equiv 3 \mod 7,$$

because $4^{12} \equiv 1 \mod 7$, and so D_n cannot be a perfect square.

(3) $k \equiv 3 \mod 7$. Then

$$D_n \equiv 2^{1+12k} - (5)^{2+12k} \equiv 2 - 4 \equiv 5 \mod 7,$$

because $5^2 \equiv 4 \mod 7$ and $2^{12} \equiv 1 \mod 7$. So D_n cannot be a perfect square.

(4) $k \equiv 4 \mod 7$. Then

$$D_n \equiv -(4)^{2+12k} \equiv -2 \mod 7,$$

and so D_n cannot be a perfect square.

(5) $k \equiv 5 \mod 7$. Then

$$D_n \equiv 5^{1+12k} - (3)^{2+12k} \equiv 5 - 2 \equiv 3 \mod 7,$$

and so D_n cannot be a perfect square.

(5) $k \equiv 6 \mod 7$. Then

$$D_n \equiv 3^{1+12k} - (2)^{2+12k} \equiv 3 - 4 \equiv 6 \mod 7,$$

and so D_n cannot be a perfect square.

(6) Let $k \equiv 0 \mod 7$ then $k = 7m$ and

$$d_n = 2^{2+12k}\frac{(1+12k)^{1+12k} - (1+6k)^{2+12k}}{(12k)^2}$$

and so it is enough to prove that

$$\frac{(1+12k)^{1+12k} - (1+6k)^{2+12k}}{(3k)^2}$$

is not a perect square. In terms of the parameter m we must prove that

$$\frac{(1+12\cdot 7\cdot m)^{1+12\cdot 7\cdot m} - (1+6\cdot 7\cdot m)^{2+12\cdot 7\cdot m}}{9\cdot 49\cdot m^2}$$

is not a perfect square. In fact we will see that for every value of m we have

$$\frac{(1+12\cdot 7\cdot m)^{1+12\cdot 7\cdot m} - (1+6\cdot 7\cdot m)^{2+12\cdot 7\cdot m}}{9\cdot 49\cdot m^2} \equiv 39 \mod 43, \qquad (6)$$

and since 39 is not a square mod 43 we are done. Since we are working the finite field $\mathbb{F}_{43}$ there is only a finite number of possible values for the left hand side of (6). An easy, but tedious, case by case computation yields (6).

Now suppose $n \equiv 2 \mod 4$. Then $n = 2 + 4k$ and we will prove that

$$\frac{2^{3+4k}(2+4k)^{2+4k} - (3+4k)^{3+4k}}{(1+4k)^2} \equiv 2 \mod 3$$

for every value of k. This implies that d_n (and hence D_n) is not a perfect square. Again we work in a finite field $\mathbb{F}_3$ and there is only a finite number of possible values. A simple computation implies the result. Since

$$D_n = (n-1)^2 d_n,$$

and D_n is never a perfect square, it is clear that d_n cannot be a perfect square. This finishes the proof of the lemma. □

It is also interesting to note (see table 3) that the factorization of $|d_n|$ is rather peculiar; it seems that for n even d_n is a square free integer, and for n odd d_n is 2^{n-1} times a square free integer. From this and from theorem 6 of [5] it would follow that the Galois group of f_n is S_n for n even. But we were not able to prove that d_n behaves this way and we had to follow a different path.

n	$\lvert d_n \rvert$
2	5
3	$2^2 \cdot 11$
4	563
5	$2^4 \cdot 599$
6	205937
7	$2^6 \cdot 84223$
8	$1319 \cdot 126913$
9	$2^8 \cdot 17 \cdot 487 \cdot 2851$
10	$7 \cdot 35616734267$
11	$2^{10} \cdot 19 \cdot 131 \cdot 4550179$
12	$10607 \cdot 211723 \cdot 267679$
13	$2^{12} \cdot 6317 \cdot 1328851967$
14	$112589 \cdot 219361 \cdot 87132013$
15	$2^{14} \cdot 241 \cdot 2347 \cdot 2879 \cdot 5484307$
16	$131 \cdot 1103237 \cdot 74329019184449$
17	$2^{16} \cdot 83 \cdot 2376011291 \cdot 655308793$
18	$12479 \cdot 3119618081 \cdot 1833387643403$
19	$2^{18} \cdot 1439 \cdot 4097227 \cdot 4142481973103$
20	$167 \cdot 1840593902677 \cdot 1981694167788721$

Table 3: Factorization of $|d_n|$.

Theorem 2.7 *Let G_n be the Galois group of $f_n(x)$ over $\mathbb{Q}$. Then G_n contains a transposition.*

Proof: We begin by defining a new polynomial $h_n(x)$:

$$h_n(x) = (n+1)g_n(x) - xg_n'(x) = -2x^n + (n+1).$$

Denoting by $\bar{g}_n$ and $\bar{g}_n'$ the reductions of g_n and g_n' module a prime p, we conclude that if $\bar{g}_n$ and $\bar{g}_n'$ have a common root (in an algebraic closure of $\mathbb{F}_p$), then the common roots of $\bar{g}_n$ and $\bar{g}_n'$ are the n-th roots of

$$\frac{\bar{n}+\bar{1}}{\bar{2}}.$$

Let $p > 2$ be a prime that divides the disciminant d_n – it is easy to see that there are always such primes – (and so p also divides D_n). Let us suppose

also that p is a prime that ramifies. Consider $\bar{f}_n(x) \in \mathbb{F}_p[x]$ the reduction of $f_n(x)$. The discriminant of $\bar{f}_n$ is zero in $\mathbb{F}_p$ and so $\bar{f}_n$ has a multiple root $\bar{\alpha}$. Let us prove that there is only one multiple root. By the above the multiple root α verifies:

$$\bar{\alpha}^n = \frac{\bar{n}+\bar{1}}{\bar{2}},$$

and from $\bar{g}_n'(\bar{\alpha}) = 0$ it comes

$$(n+1)\bar{\alpha}^n - \bar{2}\bar{n}\bar{\alpha}^{n-1} = 0,$$

and so (we can clearly suppose $\bar{\alpha} \neq 0$, because $\bar{\alpha}$ is a root of $\bar{g}_n(x)$ and $\bar{g}_n(0) = \bar{1}$)

$$(\bar{n}+\bar{1})\bar{\alpha}^{n+1} = \bar{2}\bar{n}\bar{\alpha}^n$$

from this we conclude some important things:

$$\bar{\alpha} = \frac{\bar{2}\bar{n}}{\bar{n}+\bar{1}},$$

and so $\bar{\alpha} \in \mathbb{F}_p$, $\bar{n} \not\equiv 0 \mod p$ and $\bar{\alpha}$ is the unique multiple root of $\bar{g}_n$ (and so, of $\bar{f}_n$).

Now we show that $\bar{\alpha}$ is a double root of $\bar{g}_n$.

$$\bar{h}_n'(x) = -\bar{2}\bar{n}x^{n-1},$$

and so, since $\bar{n} \neq 0$, $\bar{h}_n$ has only simple roots. Hence, $\bar{g}_n$ cannot have triple roots. Since $g_n(x) = (x-1)f_n(x)$, $f_n(1) = -(n-1)$ and $(n-1) \not\equiv 0 \mod p$, we conclude that $\bar{f}_n(x)$ cannot have a triple root.

We concluded that in $\mathbb{F}_p[x]$ we must have the factorization:

$$\bar{g}_n = \bar{f}_1 \cdot \ldots \cdot \bar{f}_m, \tag{7}$$

with

$$\bar{f}_1(x) = (x-\bar{\alpha})^2,$$

and $\bar{f}_2, \ldots, \bar{f}_m$, monic irreducible.

By Hensel's lemma, ([3], Theorem 5.3, pg. 192) considering $f_n(x)$ and $g_n(x)$ as polynomials in $\mathbb{Z}_p[x]$, where $\mathbb{Z}_p$ is the ring of p-adic integers, we can lift the factorization (7) to $\mathbb{Q}_p$, (in fact to $\mathbb{Z}_p[x]$):

$$g_n(x) = f_1 \cdot \ldots \cdot f_m,$$

with $f_1(x) = x^2+ax+b$, (necessarily irreducible), $f_2, \ldots, f_m$ monic irreducible with the same respective degrees as $\bar{f}_2, \ldots, \bar{f}_m$

Let us show that the extensions over $\mathbb{Q}_p$ generated by the roots of the f_i $(i \geq 2)$ are unramified. Fix f_i and let θ be one root of f_i. Then we can put

$$[\mathbb{Q}_p(\theta) : \mathbb{Q}_p] = ef,$$

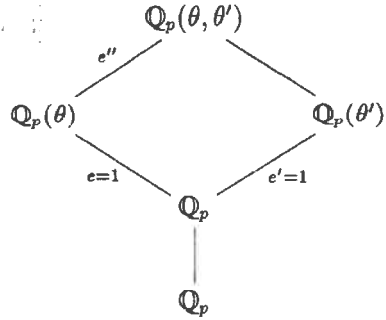
where e is the ramification index and f is the residue degree:

$$f = \partial(f_i) = \partial(\bar{f}_i) = [\overline{\mathbb{Q}}_p(\theta) : \overline{\mathbb{Q}}_p],$$

But then, since $e \geq 1$ and

$$[\mathbb{Q}_p(\theta) : \mathbb{Q}_p] = [\overline{\mathbb{Q}}_p(\theta) : \overline{\mathbb{Q}}_p]$$

we must have $e = 1$. If θ' is another root of f_i then we have, by the same arguments that the ramification index $e' = 1$. But this imples that the ramification index e'' of $\mathbb{Q}_p(\theta, \theta')$ over $\mathbb{Q}_p(\theta)$ is also 1, because it is obtained from the compositum of two unramified extensions:



This proves that the extension E_p generated over $\mathbb{Q}_p$ by all the roots of all the f_i $(i \geq 2)$ is unramified. By hypothesis, p ramifies in the splitting field of $f_n(x)$ over $\mathbb{Q}_p$ which is E_p. If α' is a root of $f_1(x) = x^2 + ax + b$ in E_p then $[\mathbb{Q}_p(\alpha') : \mathbb{Q}_p] = 2$ and so, the relation $[\mathbb{Q}_p(\alpha') : \mathbb{Q}_p] = ef$ and the fact that $e \geq 2$ implies $e = 2$.

Let $E_n/\mathbb{Q}$ be the splitting field of $f_n(x)$ over $\mathbb{Q}$ and choose a prime $\mathfrak{P}$ in E_n over p. Then $D_{\mathfrak{P}} = Gal((E_n)_{\mathfrak{P}}/\mathbb{Q}_p)$ is the decomposition group of $\mathfrak{P}$. If $\mathcal{O}_{n,\mathfrak{P}}$ is the valuation ring of the completion $(E_n)_{\mathfrak{P}}$ and P is its maximal ideal we have the inertia subgroup

$$I_{\mathfrak{P}} = \{\sigma \in D_{\mathfrak{P}} \ : \ \sigma(x) \equiv x \mod P\},$$

and the inertia subfield $T_{\mathfrak{P}}$. By local Hilbert theory $T_{\mathfrak{P}}$ is the maximal unramified extension of $\mathbb{Q}_p$ contained in $(E_n)_{\mathfrak{P}}$ and

$$[(E_n)_{\mathfrak{P}} : T_{\mathfrak{P}}] = e = 2.$$

Since the roots of f_i for $i \geq 2$ generate unramified extensions, the subgroup $I_{\mathfrak{P}}$ fixes all these roots. But if β and α' are roots of the quadratic polynomial $f_1(x)$ over $\mathbb{Q}_p$ then there is an element τ in $I_{\mathfrak{P}}$ such that

$$\tau(\beta) = \alpha', \qquad \tau(\alpha') = \beta,$$

and τ fixes all other roots. Then $D_{\mathfrak{P}} \subset Gal(E_n/\mathbb{Q})$ contains a transposition. This finishes the proof of the theorem. □

Remark 2.8 *In fact we have proved that for a ramified $p > 2$ and $\mathfrak{p}$ a prime ideal of the splitting field E of $f_n(x)$ over $\mathbb{Q}$, $\mathfrak{p}|p$, the inertia group of $\mathfrak{p}$ over $\mathbb{Q}$ is generated by a transposition. See also Lemma 1 of [5]. This means that for every prime $p > 2$ the inertia group of $\mathfrak{p}$ dividind p is trivial or generated by a transposition. If n is even, d_n is clearly odd, and so we have proved that for every prime p the inertia group of $\mathfrak{p}|p$ is trivial or generated by a transposition.*

Theorem 2.9 *Let n be an even integer. The Galois group of $f_n(x)$ is the symmetric group on n symbols S_n and if $E/\mathbb{Q}$ is the splitting field of $f_n(x)$ over $\mathbb{Q}$, the extension $E/\mathbb{Q}(\sqrt{d_n})$ is unramified.*

Proof: Corollary 2.2 implies that $Gal(f_n)$ is a transitive subgroup of S_n. But lemma 5 of Osada's article [5] says that a transitive subgroup of S_n generated by transpositions must be all S_n. By theorem 2.7 and remark 2.8 above, this is the case for $Gal(f_n)$, when n is even. For the last part it is enough to say that the intersection of the alternating group A_n with any inertia group must be trivial. This proves the theorem. □

Remark 2.10 *For the prime $p = 2$ in the case of odd n, although theorem 2.7 continues to hold, (and even it is still true that for every prime $p > 2$ inertia groups above p are trivial or generated by a transposition), the polynomial $\bar{h}_n(x)$ is identically zero and so we cannot deduce the behaviour of the factorization in $\mathbb{F}_2$ of $\bar{f}_n(x)$.*

3 The case of prime degree

Let p be a prime number and $\bar{f}_p(x) = x^p - x^{p-1} - \cdots - x - 1$ the reduction mod p of $f_p(x)$. We will prove that $\bar{f}_p(x)$ is irreducible in $\mathbb{F}_p[x]$. In order to do this we prove first a kind of reciprocity:

Lemma 3.1 *If p is a prime number we have the reciprocity formula in $\mathbb{F}_p[x]$*

$$x^p \bar{f}_p(2 - \frac{1}{x}) = \bar{f}_p(x).$$

Proof: We can write $\bar{f}_p(x) = x^p - (x-1)^{p-1}$ because in $\mathbb{F}_p[x]$

$$\bar{f}_p(x) = x^p - \frac{x^p - 1}{x - 1} = x^p - \frac{(x-1)^p}{x-1} = x^p - (x-1)^{p-1}$$

and so

$$\begin{aligned} x^p \bar{f}_p(2 - \frac{1}{x}) &= x^p \left((2 - \frac{1}{x})^p - (1 - \frac{1}{x})^{p-1} \right) \\ &= x^p (2 - \frac{1}{x^p}) - x(x-1)^{p-1} \\ &= 2x^p - 1 - x(x-1)^{p-1}. \end{aligned} \tag{8}$$

Since $g_p(x) = (x-1) f_p(x) = x^{p+1} - 2x^p + 1$ we have

$$2x^p - 1 = x^{p+1} - (x-1)\bar{f}_p(x)$$

and so

$$\begin{aligned} x^p \bar{f}_p(2 - \frac{1}{x}) &= x^{p+1} - (x-1)\bar{f}_p(x) - x(x-1)^{p-1} \\ &= x\left[x^p - (x-1)^{p-1}\right] - (x-1)\bar{f}_p(x) \\ &= \bar{f}_p(x). \end{aligned} \tag{9}$$

This finishes the proof of the lemma. □

Lemma 3.2 *In the quotient ring $R = \mathbb{F}_p[x]/(f_p(x))$ we have that $\xi^p = x$, where*

$$\xi = -x^{p-1} + x^{p-2} + \cdots + x + 3.$$

Besides, x is invertible in R and $\xi = 2 - 1/x$. (We are writing simply x for its class in R).

Proof: Since in R we have $x^{p+1} - 2x^p + 1 = 0$ (because $g_p(x) = (x-1)f_p(x)$ and $x \neq 1$) we can write

$$x[x^p - 2x^{p-1}] = -1,$$

and this proves that x is invertible and that

$$\frac{-1}{x} = x^p - 2x^{p-1}. \tag{10}$$

Besides, from $x^{p+1} - 2x^p + 1 = 0$ it follows that

$$x - 2 + \frac{1}{x^p} = 0,$$

that is:

$$x = 2 - \frac{1}{x^p} = \left(2 - \frac{1}{x}\right)^p.$$

Now, by (10) we write

$$\left(2 - \frac{1}{x}\right) = 2 - \frac{-\frac{1}{x} + 1}{(1-x)} = 2 + \frac{x^p - 2x^{p-1} + 1}{1-x} =$$

$$= 2 + \frac{-x^{p-1} + x^p + 1 - x^{p-1}}{1-x} = 2 + \frac{-x^{p-1}(1-x) + 1 - x^{p-1}}{1-x} =$$

$$= -x^{p-1} + \frac{1 - x^{p-1}}{1-x} + 2 = -x^{p-1} + x^{p-2} + \cdots + x + 1 + 2,$$

and this proves tha lemma. □

Theorem 3.3 *The polynomial $\bar{f}_p(x) = x^p - x^{p-1} - \cdots - x - 1$ is irreducible in $\mathbb{F}_p[x]$ for every prime number p.*

Proof: It is easy to see that $\bar{f}_p(x)$ is irreducible in $\mathbb{F}_p[x]$ if and only if

(1) $(\bar{f}_p(x), x^p - x) = 1$,
(2) $\bar{f}_p(x) | (x^{p^p} - x)$.

To prove the first condition is equivalent to prove that $\bar{f}_p(x)$ has no root in $\mathbb{F}_p$. To prove the second condition it is enough to prove that each root of $\bar{f}_p$ is a root of $x^{p^p} - x$. Now, we have already noticed that

$$\bar{f}_p(x) = x^p - (x-1)^{p-1},$$

and so, since,

$$(x^p - x, f_p(x)) = 1 \Longleftrightarrow f_p(m) \neq 0, \quad \forall m \in \mathbb{F}_p,$$

and since $y^{p-1} = 1$ for every $y \in \mathbb{F}_p^*$ we have, for $m \neq 1$,

$$\bar{f}_p(m) = (m)^p - (m-1)^{p-1} = m - 1 \neq 0.$$

But $\bar{f}_p(1) = 1$ and so we are done. This proves the first claim. For the second: let us suppose that in $\mathbb{F}_p[x]$ we have a factorization

$$\bar{f}_p(x) = f_1(x) \cdot \cdots \cdot f_k(x),$$

where each $f_j(x)$ is irreducible with degree n_j. Let

$$A_j = \{\alpha_j, \alpha_j^p, \cdots, \alpha_j^{p^{n_j-1}}\}$$

be the set of roots of $f_j(x)$ in an algebraic closure of $\mathbb{F}_p$ (notice that $\alpha_j^{p^{n_j}} = \alpha_j$). By lemma 3.1 the map $\alpha \mapsto 2 - 1/\alpha$ gives a bijection of the set of all roots of $\bar{f}_p(x)$ onto itself, and so the set

$$\{2 - \frac{1}{\alpha_j}, 2 - \frac{1}{\alpha_j^p}, \ldots, 2 - \frac{1}{\alpha_j^{p^{n_j-1}}}\}$$

is also a subset of the roots of $\bar{f}_p(x)$. But this set is clearly an orbit under the action of the Frobenius automorphism $u \mapsto u^p$, and this means that it must be some A_k. But lemma 3.2 says that

$$\left(2 - \frac{1}{\alpha_j^p}\right) = \left(2 - \frac{1}{\alpha_j}\right)^p = \alpha_j,$$

and so $A_k = A_j$, and this means that $\alpha \mapsto 2 - 1/\alpha$ gives a permutation of A_j. Let

$$\phi\colon A_j \longrightarrow A_j, \qquad \phi(\beta) = 2 - 1/\beta.$$

It is easy to see that ϕ is a cyclic permutation (an n_j-cycle). A simple induction argument shows that

$$\phi^k(\beta) = \frac{k - (k-1)\beta}{(k-1) - k\beta},$$

where $\phi^k = \phi \circ \phi \circ \cdots \circ \phi$ (the composition of ϕ with itself k times). Then

$$\phi^{n_j}(\alpha_j) = \alpha_j$$

that is:

$$\frac{n_j - (n_j+1)\alpha_j}{(n_j-1) - n_j\alpha_j} = \alpha_j,$$

and hence

$$n_j\alpha_j^2 - 2n_j\alpha_j + n_j = 0.$$

If $n_j \not\equiv 0 \mod p$ we have

$$\alpha_j^2 - 2\alpha_j + 1 = 0,$$

But this is impossible because dividing this last expression by α_j we obtain

$$\alpha_j - 2 + \frac{1}{\alpha_j} = 0,$$

and so

$$\alpha_j = 2 - \frac{1}{\alpha_j}.$$

But this in turn implies (again by lemma 3.2)

$$\alpha_j^p = \left(2 - \frac{1}{\alpha_j}\right)^p = \alpha_j$$

which would gives us that $\alpha_j \in \mathbb{F}_p$. This is impossible by the first claim. This finishes the proof of the theorem. □

We are now ready to prove the main theorem of this section:

Theorem 3.4 *Let p be a prime number. Then de Galois group of $f_p(x)$ is the symmetric group S_p in p symbols.*

Proof: It is well known that a transitive subgroup of S_p containing a transposition and a p-cycle is S_p. From our previous theorem 2.1 and theorem 2.7 it is enough to prove that $Gal(f_p)$ has a p-cycle. Since

$$D_p = (-1)^{\binom{n+1}{2}}[(p+1)^{p+1} - 2^{p+1}p^p]$$

it is clear that p docs not divide D_p (and *a fortiori* does not divide d_p). This means that p does not ramify. By theorem 3.3 $f_p(x)$ is irreducible in $\mathbb{F}_p[x]$. From these two facts (and Hensel's lemma) it folows that considering f_p over the p-adic field $\mathbb{Q}_p$ we have that its Galois group is cyclic and contains a p-cycle. This proves the theorem. □

4 Final remarks

It is well known that a transitive permutation subgroup of S_n that contains a transposition and an $n-1$ cycle must be S_n. In the table bellow the first line gives the degree of f_n and the second line gives the smallest prime p such that the the decomposition of f_n in $\mathbb{F}_p$ has exactly one factor of degree 1 and other irreducible factor of degree $n-1$. By Dedekind's theorem there is a $(n-1)$-cycle in the Galois group of f_n over $\mathbb{Q}$.

n	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
p	7	3	19	17	3	13	7	61	71	29	79	19	199	59	167

n	18	19	20	21	22	23	24	25	26	27	28	29	30
p	7	3	23	7	349	19	641	149	83	641	137	127	197

Table 4: Degree of f_n and smallest prime p giving an $n-1$ cycle.

These calculations suggest that it is likely that the Galois group of $f_n(x)$ is S_n for every n.

References

[1] I. Schur, *Gleichungen ohne Affect.* Gesammelte Abhandlungen, Band III, No. 67, 191-197

[2] I. Schur, *Affectlose Gleichungen in der Theorie der Laguerreschen und Hermiteschen Polynome.* Gesammelte Abhandlungen, Band III, No. 70, 227-233.

[3] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers.* PWN - Polish Scientific Publishers, Warszawa 1974.

[4] R. F. Coleman, *On the Galois Groups of the exponential Taylor Polynomials.* L'Enseignement Mathematique, t. 33 (1987), 183-189

[5] H. Osada, *The Galois Groups of the Polynomials* $X^n + aX^l + b$. Journal of Number Theory **25**, 230-238 (1987)

[6] E. P. Miles, Jr. *Generalized Fibonacci Numbers and Associated Matrices.* Amer. Math. Monthly **67**, (1960): 745-752

[7] M. D. Miller, *On Generalized Fibonacci Numbers.* Amer. Math. Monthly **78**, (1971) 1108-1109

[8] R. Swan, *Factorization of Polynomials Over Finite Fields,* Pacific J. of Math, **12**(2), (1962), 1099-1106

TRABALHOS DO DEPARTAMENTO DE MATEMÁTICA

TÍTULOS PUBLICADOS

2001-01 KOSZMIDER, P. Universal Matrices and Strongly Unbounded Functions. 18p.

2001-02 JUNQUEIRA, L. and KOSZMIDER, P. On Families of Lindelöf and Related Subspaces of 2^{ω_1}.30p.

2001-03 KOSZMIDER, P. and TALL, F. D. A Lindelöf Space with no Lindelöf Subspace of Size $\aleph_1$. 11p.

2001-04 COELHO, F. U. and VARGAS, R. R. S. Mesh Algebras. 20p.

2001-05 FERNANDEZ, R. The equation $\frac{\partial u}{\partial t}+H\left(t,x_1,...,x_n,u,\frac{\partial u}{\partial x_1},...,\frac{\partial u}{\partial x_n}\right)=0$ and the method of characteristics in the framework of generalized functions. 24p.

2001-06 COSTA, R. and MURAKAMI, L.S.I. Some Properties of the Automorphisms of a Bernstein Algebra. 6p.

2001-07 BEKKERT, V., MARCOS, E.N. and MERKLEN, H. A. Indecomposables in derived categories of skewed-gentle algebras. 35p.

2001-08.0 GORODSKI, C. A class of complete embedded minimal submanifolds in noncompact symmetric spaces. 6p.

2001-08 MARCOS, E.N., MERKLEN, H.A., SÁENZ, C. Standardly Stratified Split and Lower Triangular Algebras. 11p.

2001-09 FURTA, S. and PICCIONE, P. Global Existence of Periodic Travelling Waves of an Infinite Non-Linearly Supported Beam I. Continuous Model. 14p.

2001-10 BARONE-NETTO, A. and FURTA, S. Stability of Trivial Equilibrium Position of two Non-Linearly Coupled Oscillators. 36p.

2001-11 BORSARI, L.D. and GONÇALVES, D.L. Obstruction theory and minimal number of coincidences for maps from a complex into a manifold. 17p.

2001-12 DOKUCHAEV, M.A. and GONÇALVES, J.Z. Identities on Units of Algebraic Algebras. 9p.

2001-13 GALVÃO, M.E.E.L. and GÓES, C.C. Constant Mean Curvature Surfaces in Half Space Models. 26p.

2002-01 COELHO, F. U. and LANZILOTA, M. A. On non-semiregular components containing paths from injective to projective modules. 13p.

2002-02 COELHO, F. U., LANZILOTTA, M. A. and SAVIOLI, A. M. P. D. On the Hochschild cohomology of algebras with small homological dimensions. 11p.

2002-03 COELHO, F. U., HAPPEL, D. and UNGER, L. Tilting up algebras of small homological dimensions. 20p.

2002-04 SHESTAKOV, I.P. and UMIRBAEV. U.U. Possion brackets and two-generated subalgebras of rings of polynomials. 19p.

2002-05 SHESTAKOV, I.P. and UMIRBAEV. U.U. The tame and the wild automorphisms of polynomial rings in three variables. 34p.

2002-06 ALENCAR, R. and LOURENÇO, M.L. On the Gelbaum-de Lamadrid's result. 16p.

2002-07 GRISHKOV, A. Lie algebras with triality. 28p.

2002-08 GRISHKOV, A. N. and GUERREIRO, M. Simple classical Lie algebras in characteristic 2 and their gradations, I. 21p.

2002-09 MELO, S. T., NEST, R. and SCHROHE, E. K-Theory of Boutet de Monvel's algebra. 8p.

2002-10 POJIDAEV, A. P. Enveloping algebras of Filippov algebras. 17p.

2002-11 GORODSKI, C. and THORBERGSSON, G. The classification of taut irreducible representations. 47p.

2002-12 BORRELLI, V. and GORODSKI, C. Minimal Legendrian submanifolds of S^{2n+1} and absolutely area-minimizing cones. 13p.

2002-13 CHALOM, G. and TREPODE, S. Representation type of one point extensions of quasitilted algebras. 16p.

2002-14 GORODSKI, C. and THORBERGSSON, G. Variationally complete actions on compact symmetric spaces. 8p.

2002-15 GRISHKOV, A .N. and GUERREIRO, M. Simple classical Lie algebras in characteristic 2 and their gradations, II. 15p.

2002-16 PEREIRA, Antônio Luiz and PEREIRA, Marcone Corrêa. A Generic Property for the Eigenfunctions of the Laplacian. 28p.

2002-17 GALINDO, P., LOURENÇO, M. L. and MORAES, L. A. Polynomials generated by linear operators. 10p.

2002-18 GRISHKOV, A. and SIDKI, S. Representing idempotents as a sum of two nilpotents of degree four. 9p.

2002-19 ASSEM, I. and COELHO, F. U. Two-sided gluings of tilted algebras. 27p.

2002-20 ASSEM, I. and COELHO, F. U. Endomorphism rings of projectives over Laura algebras. 10p.

2002-21 CONDORI, L. O. and LOURENÇO, M. L. Continuous homomorphisms between topological algebras of holomorphic germs. 11p.

2002-22 MONTES, R. R. and VERDERESI, J. A. A new characterization of the Clifford torus. 5p.

2002-23 COELHO, F. U., DE LA PEÑA, J. A. and TREPODE, S. On minimal non-tilted algebras. 27p.

2002-24 GRISHKOV, A. N. and ZAVARNITSINE, A. V. Lagrange's theorem for Moufang Loops. 21p

2002-25 GORODSKI, C., OLMOS, C. and TOJEIRO, R. Copolarity of isometric actions. 23p.

2002-26 MARTIN, Paulo A. The Galois group of $x^n - x^{n-1} - \ldots - x - 1$. 18p.

Nota: Os títulos publicados nos Relatórios Técnicos dos anos de 1980 a 2000 estão à disposição no Departamento de Matemática do IME-USP.

Cidade Universitária "Armando de Salles Oliveira"
Rua do Matão, 1010 - Cidade Universitária
Caixa Postal 66281 - CEP 05315-970