CAHIERS DE TOPOLOGIE ET GEOMETRIE DIFFERENTIELLE CATEGORIQUES *Vol. LIV-1 (2013)*

LINEAR GROUPS AND PRIMITIVE POLYNOMIALS OVER $\mathbf{F}_p$

by Jean-Yves DEGOS

Résumé. En nous inspirant du groupe de Klein $\mathrm{GL}_3(\mathbb{F}_2)$ (voir l'introduction), nous introduisons les nouvelles notions de groupes n-cyclables et de groupes n-brunniens de type I et II (voir section 1). Nous montrons ensuite que les groupes $\mathrm{SL}_n(\mathbb{F}_p)$ et $\mathrm{GL}_n(\mathbb{F}_p)$ jouissent d'une structure de groupes n-brunniens de type I pour p premier et $n \geq 3$ (voir section 2). Dans la section 3, nous énonçons deux conjectures, à savoir les conjectures $A(n,p,P)$ et $B(n,p,P)$ concernant les polynômes primitifs sur $\mathbb{F}_p$, et nous donnons des résultats partiels dans la section 4.

Abstract. Motivated by the case of Klein's group $\mathrm{GL}_3(\mathbb{F}_2)$ (see the introduction), we introduce the new notions of n-cyclable groups and n-brunnian groups of type I and II (see section 1). We then prove that the groups $\mathrm{SL}_n(\mathbb{F}_p)$ and $\mathrm{GL}_n(\mathbb{F}_p)$ enjoy a structure of n-brunnian groups of type I for p prime and $n \geq 3$ (see section 2). In section 3, we state two conjectures, namely the conjectures $A(n,p,P)$ and $B(n,p,P)$ about primitive polynomials over $\mathbb{F}_p$, and we give some evidence in section 4.

Keywords. borromean groups, brunnian groups, primitive polynomials, linear groups, finite fields.

Mathematics Subject Classification (2010). 12Y05, 20H30.

Introduction

The group $\mathrm{GL}_3(\mathbb{F}_2) \simeq \mathrm{PGL}_3(\mathbb{F}_2)$ is known to be the automorphism group of Klein's quartic ([6]):

$$X(7) = \{[x:y:z] \in \mathbb{P}^2(\mathbb{C})\,,\; x^3y + y^3z + z^3x = 0\}\,.$$

According to the literature, this group is generated by a generator of order 2, a generator of order 3, and a generator of order 7 (see [1]). But, in 2005, Guitart showed that it could be generated by the following three matrices

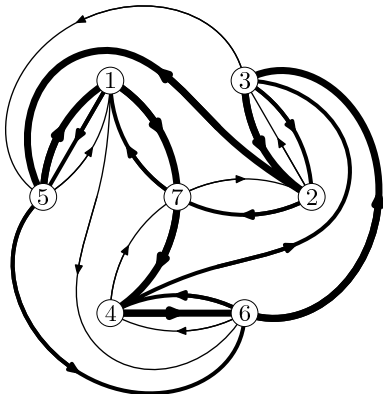

Figure 1: Action of $\mathrm{GL}_3(\mathbb{F}_2)$ on $\{1,2,3,4,5,6,7\}$

([4] and [5], **5**):

$$r = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}, s = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix}, \text{ and } i = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix};$$

and that it could be viewed as a subgroup of the symmetric group $\mathfrak{S}_7$, which acts on $\{1,2,3,4,5,6,7\}$ as the permutations $r = (1746325)$, $s = (5164723)$, and $i = (1564327)$ do ([5], Proposition 10), like in Figure 1.

The group $\mathrm{GL}_3(\mathbb{F}_2)$ is thus called a borromean group.

In front of this situation, we can ask the following questions:

(i) How could we make this threefold geometrical symmetry visible in the algebraic description of $\mathrm{GL}_3(\mathbb{F}_2)$ as a matrix group?

(ii) Could we generalize the notion of a borromean group to dimension n?

In the following, we are going to give partial answers to these questions.

1. A few definitions and generalizations

In knot theory, the borromean rings consist of three topological circles which are linked and form a brunnian link, i.e., removing any ring results in two unlinked rings. A brunnian link is a nontrivial link that becomes trivial if any

component is removed. In other words, cutting any loop frees all the other loops (so that no two loops can be directly linked).

Imitating these notions, we can define the notions of brunnian groups in two ways.

1.1 The notion of an n-cyclable group

Definition 1.1. *Let $n \geq 1$ be an integer. A group G is n-cyclable if it can be generated by n elements $g_1, g_2, \ldots, g_n$ satisfying the following axiom: if $M(g_1, g_2, \ldots, g_n) = 1$ (with M a word in $g_1, g_2, \ldots, g_n$), then*

$$M(g_{\gamma^k(1)}, g_{\gamma^k(2)}, \ldots, g_{\gamma^k(n)}) = 1\,,$$

where γ is the n-cycle $(1, 2, \ldots, n)$, and $1 \leq k \leq n-1$.

1.2 The notion of an n-brunnian group of type I

Definition 1.2. *A group G is n-brunnian of type I if:*

(i) it is n-cyclable;

(ii) for all $1 \leq i \leq n$, if we set $g_i = 1$, the group generated by $g_1, g_2, \ldots, g_n$ is trivial.

1.3 The notion of an n-brunnian group of type II

Definition 1.3. *A group G is n-brunnian of type II if:*

(i) it is n-cyclable;

(ii) for all $1 \leq i \leq n$, the group generated by $g_1, g_2, \ldots, g_n$ except g_i does not generate G.

2. The groups $\mathrm{SL}_n(\mathbb{F}_p)$ and $\mathrm{GL}_n(\mathbb{F}_p)$ as brunnian groups

To state the theorems, we need two definitions.

Definition 2.1. *Let $n \geq 2$ an integer. For $1 \leq i, j \leq n$ and $i \neq j$, we denote by $T_{i,j}$ the transvection matrix $(t_{k,l})$ with $t_{k,k} = 1$ for $1 \leq k \leq n$, $t_{i,j} = 1$*

and $t_{k,l} = 0$ *if* $k \neq l$ *and* $(k,l) \neq (i,j)$*, namely:*

$$T_{i,j} = \begin{bmatrix} 1 & 0 & \dots & & & 0 \\ 0 & 1 & \dots & & & \vdots \\ \vdots & \vdots & \ddots & 1_{i,j} & & \\ & & & \ddots & & \vdots \\ & & & & \ddots & 0 \\ 0 & \dots & & \dots & 0 & 1 \end{bmatrix}.$$

Definition 2.2. *If* $n \geq 2$ *is an integer,* p *is a prime, and*

$$f(X) = X^n + a_{n-1}X^{n-1} + \cdots a_1 X + a_0 \in \mathbb{F}_p[X]$$

then we denote by $\mathrm{Comp}\,(f(X))$ *the matrix:*

$$\mathrm{Comp}\,(f(X)) = \begin{bmatrix} 0 & 0 & \dots & 0 & -a_0 \\ 1 & 0 & \dots & 0 & -a_1 \\ 0 & 1 & \dots & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & -a_{n-1} \end{bmatrix}.$$

Theorem 2.3. *Let* $n \geq 3$ *be an integer and* p *be a prime number.*
We set $G_1 = T_{1,2}$*,* $G = \mathrm{Comp}\,(X^n - 1)$*, and*
$G_{i+1} = GG_iG^{-1}$ *for* $1 \leq i \leq n-1$*. Then*

$$SL_n(\mathbb{F}_p) = \langle G_1, G_2, \dots, G_n \rangle .$$

The group $SL_n(\mathbb{F}_p)$ *is therefore* n*-cyclable, and* n*-brunnian of type I with respect to these generators. It is also* n*-brunnian of type II.*

Proof. The fact that $\mathrm{SL}_n(\mathbb{F}_p)$ is n-cyclable (and n-brunnian of type I) is an easy consequence of the main lemma, which is proved in section 4.

Therefore, we just have to show that $\mathrm{SL}_n(\mathbb{F}_p)$ is n-brunnian of type II. However, it can be shown that the group generated by $G_1, G_2, \dots, G_{n-1}$ is the group of all matrices of the following form:

$$\begin{bmatrix} 1 & \times & \cdots & \times \\ 0 & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \times \\ 0 & \cdots & 0 & 1 \end{bmatrix},$$

where the $\times$ symbols stand for any element of $\mathbb{F}_p$. This group is a Sylow subgroup of $\mathrm{SL}_n(\mathbb{F}_p)$ and has order

$$p^{\frac{n(n-1)}{2}},$$

and is therefore not equal to $\mathrm{SL}_n(\mathbb{F}_p)$. □

Corollary 2.4. *With the notations of Theorem* 2.3*, let* $s : \mathrm{SL}_n(\mathbb{F}_p) \to \mathrm{PSL}_n(\mathbb{F}_p)$ *be the canomial map,* $H_i = s(G_i)$ *for* $1 \leq i \leq n$*, and*

$$\begin{array}{ccc} \theta : \mathrm{PSL}_n(\mathbb{F}_p) & \to & \mathrm{PSL}_n(\mathbb{F}_p) \\ s(M) & \mapsto & s(G)s(M)s(G)^{-1} \end{array}.$$

Then:

(i) $H_{i+1} = \theta(H_i)$ *for* $1 \leq i \leq n-1$*;*

(ii) $\mathrm{PSL}_n(\mathbb{F}_p) = \langle H_1, H_2, \ldots, H_n \rangle$.

The group $\mathrm{PSL}_n(\mathbb{F}_p)$ *is therefore an* n*-cyclable, and* n*-brunnian of type I, with respect to these generators.*

Proof. The proof is the same as that of Corollary 2.6 below. □

Theorem 2.5. *Let* $n \geq 3$ *be an integer,* p *be a prime number and* d *be a generator of* $\mathbb{F}_p^\times$.

We denote by $G_1 = (g_{i,j})$ *the matrix defined by* $g_{i,i} = 1$ *for* $1 \leq i \leq n$ *and* $i \neq 3$*,* $g_{3,3} = d$*,* $g_{1,2} = 1$ *and* $g_{i,j} = 0$ *if* $i \neq j$ *and* $(i,j) \neq (1,2)$*. We set* $G = \mathrm{Comp}\,(X^n - 1)$.

We set $G_{i+1} = GG_iG^{-1}$ *for* $1 \leq i \leq n-1$*. Then*

$$\mathrm{GL}_n(\mathbb{F}_p) = \langle G_1, G_2, \ldots, G_n \rangle .$$

The group $\mathrm{GL}_n(\mathbb{F}_p)$ *is therefore an* n*-cyclable and* n*-brunnian group of type I with respect to these generators. It is also and* n*-brunnian group of type II.*

Proof. The fact that $\mathrm{GL}_n(\mathbb{F}_p)$ is n-cyclable (and n-brunnian of type I) is an easy consequence of the main lemma, which is proved in section 4.

Therefore, we just have to show that $\mathrm{GL}_n(\mathbb{F}_p)$ is n-brunnian of type II. However, it can be shown that the group generated by $G_1, G_2, \ldots, G_{n-1}$ is the group of all matrices which are upper triangular, with a 1 in position $(n-1, n-1)$. This group has order

$$p^{\frac{n(n-1)}{2}}(p-1)^{n-1},$$

and is therefore not equal to $\mathrm{GL}_n(\mathbb{F}_p)$. □

Corollary 2.6. *With the notations of Theorem* 2.5*, let* $s : \mathrm{GL}_n(\mathbb{F}_p) \to \mathrm{PGL}_n(\mathbb{F}_p)$ *be the canomial map,* $H_i = s(G_i)$ *for* $1 \leq i \leq n$*, and*

$$\begin{array}{rccc} \theta : \mathrm{PGL}_n(\mathbb{F}_p) & \to & \mathrm{PGL}_n(\mathbb{F}_p) \\ s(M) & \mapsto & s(G)s(M)s(G)^{-1} \end{array} .$$

Then:

(i) $H_{i+1} = \theta(H_i)$ *for* $1 \leq i \leq n-1$*;*

(ii) $\mathrm{PGL}_n(\mathbb{F}_p) = \langle H_1, H_2, \ldots, H_n \rangle$.

The group $\mathrm{PGL}_n(\mathbb{F}_p)$ *is therefore an* n*-cyclable, and* n*-brunnian of type I, with respect to these generators.*

Proof. First, the points (i) and (ii) are obvious. We only have to check that the automorphism θ has order n. Let k be the order of θ in $\mathrm{PGL}_n(\mathbb{F}_p)$. Then k divides n, because G has order n in $\mathrm{GL}_n(\mathbb{F}_p)$. Then, we have:

$$\begin{array}{rcl} \theta^k = 1_{\mathrm{PGL}_n(\mathbb{F}_p)} & \Rightarrow & \forall M \in \mathrm{GL}_n(\mathbb{F}_p), \theta^k(s(M)) = s(M) \\ & \Rightarrow & \forall M \in \mathrm{GL}_n(\mathbb{F}_p), s(G)^k s(M) s(G)^{-k} = s(M) \\ & \Rightarrow & \forall M \in \mathrm{GL}_n(\mathbb{F}_p), \exists \lambda \in \mathbb{F}_p^\times, G^k M G^{-k} = \lambda M. \end{array}$$

But if $k \neq n$, this last property is false for $M = \mathrm{Comp}(Q(X))$ for any irreducible polynomial $Q(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0$. We now are going to prove that.

Indeed, the eigenvalues of $G^k M G^{-k}$ are the eigenvalues of M, namely the elements of the set:

$$\Lambda := \left\{ \alpha^{p^i} \text{ for } 0 \leq i \leq n-1 \right\},$$

α being a root of $Q(X)$.

The equality $G^k M G^{-k} = \lambda M$ implies that $x \mapsto \lambda x$ is a bijection of Λ. If it is not the identity map, there are two integers i and j with $i \neq j$ and $\lambda \alpha^{p^i} = \alpha^{p^j}$, and we deduce from this fact that $\lambda \notin \mathbb{F}_p^\times$. Consequently, this bijection is the identity map, and $\lambda = 1$. Thus, $G^k M G^{-k} = M$. However, this is impossible, as we prove it below. Indeed, we have:

$$G^k M G^{-k} = (m_{\gamma^{-k}(i), \gamma^{-k}(j)})_{i,j} \text{ where } M = (m_{i,j})_{i,j} .$$

Hence, for all $1 \leq i, j \leq n$, $m_{\gamma^{-k}(i), \gamma^{-k}(j)} = m_{i,j}$. Using this with $i = 1$ and $j = n$, we obtain:

$$-a_0 = 1 \text{ and } -a_{i-1} = 0 \text{ for } 2 \leq i \leq n .$$

Therefore $Q(X) = X^n - 1$, which is a contradiction, because $Q(X)$ is irreducible.

We conclude that $k = n$. □

3. Two conjectures on primitive polynomials

Definition 3.1. *Let $n \geq 1$ an integer, $p \geq 2$ a prime number, and $P(X) \in \mathbb{F}_p[X]$ with $\deg P = n$. The polynomial $P(X)$ is said to be primitive if it is the minimal polynomial of a primitive element of $\mathbb{F}_{p^n}$.*

Example 3.2. If $n = 2$ and $p = 2$, $P(X) = X^2 + X + 1$ is the only primitive polynomial of degree n over $\mathbb{F}_p[X]$.

Example 3.3. If $n = 8$ and $p = 2$, $P(X) = X^8 + X^4 + X^3 + X + 1$ is an irreducible polynomial of degree n over $\mathbb{F}_p[X]$, but it is not a primitive one.

Conjecture 3.4 (A(n,p,P))**.** *Let p be a prime number, $n \geq 2$ be an integer, and $P(X) \in \mathbb{F}_p[X]$ be a primitive polynomial of degree n. Let $G = \mathrm{Comp}(X^n - 1)$ and $C = \mathrm{Comp}(P(X))$. Then*

$$GL_n(\mathbb{F}_p) = \langle G, C \rangle .$$

Remark 3.5. Conjecture $A(n, p, P)$ results from Conjecture $B(n, p, P)$ that follows.

Conjecture 3.6 (B(n,p,P))**.** *Let p be a prime number and $n \geq 2$ be an integer. Let $P(X) \in \mathbb{F}_p[X]$ be a primitive polynomial of degree n.*
Let $G = \mathrm{Comp}(X^n - 1)$, $C = \mathrm{Comp}(P(X))$ and let us define $(G_i)_{1 \leq i \leq n}$ by

$$\left\{ \begin{array}{rcl} G_1 & = & C\,, \\ G_{i+1} & = & GG_iG^{-1} \text{ for } 1 \leq i \leq n-1\,. \end{array} \right.$$

Then $GL_n(\mathbb{F}_p) = \langle G_1, G_2, \ldots, G_n \rangle$. So the group $GL_n(\mathbb{F}_p)$ is n-cyclable and n-brunnian of type I with respect to these generators.

4. Some evidence

4.1 Three theorems

Theorem 4.1. *Given $P(X) = X^2 + a_1X + a_0$ a primitive polynomial of degree 2 over $\mathbb{F}_p$ with $p \in \{2, 3\}$, we have the following results:*
(i) $B(2, 3, P)$ is true; therefore $A(2, 3, P)$ is true;
(ii) $A(2, 2, P)$ is true, but $B(2, 2, P)$ is false.

The proof of Theorem 4.1 uses elementary operations.

Proof. (i) $p = 3$.

As a_0 generates $\mathbb{F}_p^\times$, we only have to show that the following matrices:

$$T := \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, T' := \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \text{ and } M := \begin{bmatrix} 1 & 0 \\ 0 & a_0 \end{bmatrix}$$

are in $\langle G_1, G_2 \rangle$.

We start from

$$H := G_2 {a_0}^{p-2} G_1 = \begin{bmatrix} \frac{1}{a_0} & a_1 - \frac{a_1}{a_0} \\ 0 & a_0 \end{bmatrix}.$$

As $p = 3$, we have ${a_0}^2 = 1$, so $a_0 = -1$ and

$$H^2 = \begin{bmatrix} 1 & -a_1 \\ 0 & 1 \end{bmatrix}.$$

As $-a_1 \neq 0$, there is an integer k such that $H^{2k} = T$. Then $T \in \langle G_1, G_2 \rangle$.

Starting from ${a_0}^{p-1} G_1 G_2$, we could show that $T' \in \langle G_1, G_2 \rangle$.

Then $\langle G_1, G_2 \rangle$ contains all the tranvections, and so contains $\mathrm{SL}_2(\mathbb{F}_p)$.

The matrices M and G_1 have the same determinant: a_0. Then, they are equivalent modulo $\mathrm{SL}_2(\mathbb{F}_p)$.

We can conclude that $M \in \langle G_1, G_2 \rangle$ and $\langle G_1, G_2 \rangle = \mathrm{GL}_2(\mathbb{F}_p)$.

(ii) $p = 2$. Then we have:

$$GC = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \text{ and } CG = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix},$$

so $\langle G, C\rangle = \mathrm{SL}_2(\mathbb{F}_2) = \mathrm{GL}_2(\mathbb{F}_2)$.

But:

$$G_1 = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \text{ and } G_2 = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} = {G_1}^2 ,$$

then $\langle G_1, G_2\rangle = \langle G_1\rangle \neq \mathrm{GL}_2(\mathbb{F}_2)$. □

The following lemma is the heart of this paper, and will be useful to prove Theorem 4.3 and Theorem 4.4.

Lemma 4.2 (Main lemma)**.** *Let $n \geq 3$ be an integer, p be a prime number, and $H \subset GL_n(\mathbb{F}_p)$ a subgroup satisfying the following properties:*

(i) for every $h \in H$, then $GhG^{-1} \in H$, where $G = \mathrm{Comp}\,(X^n - 1)$;

(ii) the group H contains a matrix D the determinant of which is d and generates $\mathbb{F}_p^{\times}$;

(iii) the group H contains a tranvection matrix $T_{i,j}$ with $j = \gamma(i)$ or $i = \gamma(j)$.

Then $H = GL_n(\mathbb{F}_p)$.

Proof. Let g be the isomorphism of $GL_n(\mathbb{F}_p)$ defined by $g(M) = GMG^{-1}$. Set $T_1 := T_{i,j}$ and $T_k := g^{-1}(T_{k-1})$ for $2 \leq k \leq n$. Then T_k is a transvection matrix, and $T_k \in H$, because it is a conjugate of T_1 by $G^{-(k-1)}$. More precisely, for $1 \leq k \leq n$, we have:

$$T_k = T_{\gamma^{-(k-1)}(i),\gamma^{-(k-1)}(j)} .$$

Then, as $j = \gamma(i)$ or $i = \gamma(j)$, there is an n-cycle $(j_1, j_2, \ldots j_n)$ such that the set

$$\{T_k \,|\, 1 \leq k \leq n\}$$

can be rewritten as the set:

$$T_{j_1,j_2},\, T_{j_2,j_3},\, \ldots,\, T_{j_n,j_1} .$$

As $n \geq 3$, we can use the well-known formula ([7], proof of Theorem 9.2, XIII, 9, page 541), and deduce that:

$$T_{k_1,k_2} T_{k_2,k_3} {T_{k_1,k_2}}^{p-1} {T_{k_2,k_3}}^{p-1} = T_{k_1,k_3} \text{ for } k_2 \notin \{k_1, k_3\}$$

to show that H contains all the matrices $T_{k,l}$ with $1 \leq k, l \leq n$ and $k \neq l$. We conclude that $SL_n(\mathbb{F}_p) \subset H$.

Now, as H contains a matrix of determinant d, which is equivalent modulo $SL_n(\mathbb{F}_p)$ (therefore modulo H) to a dilatation matrix of determinant d, and as H is stable by conjugation by G and d generates $\mathbb{F}_p^\times$, then H contains all the dilatations matrices.

Therefore $H = GL_n(\mathbb{F}_p)$. □

Theorem 4.3. *Let us suppose that $p = 2$, n is* odd*, and there is an i in $\{1, n-1\}$ such that $P(X) = X^n + X^i + 1$ is primitive.*
Then $B(n, p, P)$ is true, therefore $A(n, p, P)$ is true.

Proof. To prove Theorem 4.3, we just have to check that the subgroup

$$H = \langle G_1, \ldots, G_n \rangle$$

satisfies the three points (i), (ii), (iii) of the main lemma.

(i) : the group H is stable by conjugation by G;

(ii) : the group H contains $G_1 = \mathrm{Comp}(P(X))$, the determinant of which is 1, and generates $\mathbb{F}_2^\times$;

(iii) : we have $G^{-1}C = G^{-1}G_1 = T_{i,n}$, which is a transvection matrix of order 2, with $\gamma(i) = n$ or $\gamma(n) = i$. Moreover, we have $G^2 = G_2G_1 \in H$. As n and 2 are coprime, there are integers u and v such that $2u + nv = 1$. Therefore, $G = (G^2)^u \in H$, and $T_{i,n} \in H$. □

Theorem 4.4. *Let us suppose that $p = 2$, n is* even*, and there is an i in $\{1, n-1\}$ such that $P(X) = X^n + X^i + 1$ is primitive.*
Then $A(n, p, P)$ is true.

Proof. To prove Theorem 4.4, we just have to check that the subgroup

$$H = \langle G, C \rangle$$

satisfies the three points (i), (ii), (iii) of the main lemma.

(i) : the group H is stable by conjugation by G;

(ii) : the group H contains $G_1 = \mathrm{Comp}(P(X))$, the determinant of which is 1, and generates $\mathbb{F}_2^\times$;

(iii) : we have $G^{-1}C = G^{-1}G_1 = T_{i,n}$, which is a transvection matrix of order 2, with $\gamma(i) = n$ or $\gamma(n) = i$. Moreover, $T_{i,n} \in H$. □

We can find in [2] the irreducible polynomials of the form $x^n + x + 1$ over $\mathbb{F}_2$, up to $n = 30000$. There are only 33.

4.2 The centers of $\langle G, C\rangle$ and $\langle G_1, G_2, \ldots, G_n\rangle$

According to Conjecture $A(n,p,P)$, we should have $\mathrm{GL}_n(\mathbb{F}_p) = \langle G, C\rangle$, with the notations of Conjecture 3.4. Thus, we should have also the equality between the centers of these groups. This is the case.

According to Conjecture $B(n,p,P)$, the group $\langle G_1, G_2, \ldots, G_n\rangle$ equals the group $\mathrm{GL}_n(\mathbb{F}_p)$, with the notations of Conjecture 3.6. Thus, we should have also the equality between the centers of these groups. This is the case, provided $G \in \langle G_1, G_2, \ldots, G_n\rangle$.

To prove these results, we need a lemma.

Lemma 4.5. *We have:*

$$ {G_1}^{1+p+\cdots+p^{n-1}} = \begin{bmatrix} (-1)^n a_0 & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & (-1)^n a_0 \end{bmatrix}, $$

therefore $\langle G, C\rangle$ and $\langle G_1, G_2, \ldots, G_n\rangle$ both contain all the homotheties.

Proof. If $\sigma : x \mapsto x^p$ is the Frobenius automorphism, there is a matrix Q with coefficients in $\mathbb{F}_p(\alpha)$ (where α is a root of $P(X)$) such that $Q^{-1}CQ = D$, with

$$ D = \begin{bmatrix} \sigma^0(\alpha) & 0 & \ldots & 0 \\ 0 & \sigma^1(\alpha) & \vdots & \vdots \\ \vdots & \vdots & \ddots & 0 \\ 0 & \ldots & 0 & \sigma^{n-1} \end{bmatrix}, $$

therefore: ${G_1}^{1+p+\cdots+p^{n-1}} = QD^{1+p+\cdots+p^{n-1}}Q^{-1} = (-1)^n a_0 Id$. But as $P(X)$ is a primitive polynomial, $(-1)^n a_0$ generates $\mathbb{F}_p^\times$, QED. □

Theorem 4.6. *We have the following results (the notation $Z(\Gamma)$ stands for the center of the group Γ):*

(i) $Z(\langle G, C\rangle) = \{xId, x \in \mathbb{F}_p^\times\}$;

(ii) if $G \in \langle G_1, G_2, \ldots, G_n\rangle$, $Z(\langle G_1, G_2, \ldots, G_n\rangle) = \{xId, x \in \mathbb{F}_p^\times\}$;

Proof. We know from the previous lemma that all the homotheties are contained in $\langle G, C\rangle$ and $\langle G_1, G_2, \ldots, G_n\rangle$. Now, if a matrix M is in the center

of $\langle G_1, G_2, \ldots, G_n \rangle$, it commutes with G^{-1} and G_1. As it commutes with G^{-1}, it has the following form:

$$\begin{bmatrix} \alpha_1 & \alpha_2 & \ldots & \alpha_n \\ \alpha_n & \alpha_1 & \ldots & \alpha_{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_2 & \alpha_3 & \ldots & \alpha_1 \end{bmatrix},$$

and as it commutes with G_1, the following equations hold:

$$-a_0\alpha_i = \alpha_i \text{ for } 2 \leq i \leq n$$

and

$$-a_i\alpha_j = 0 \text{ for } 1 \leq i \leq n-2 \text{ and } 2 \leq j \leq n.$$

Consequently, for a given $2 \leq j \leq n$, if $\alpha_j \neq 0$, we have:

$$a_1 = a_2 = \cdots = a_{n-1} = 0 \text{ and } a_0 = -1$$

hence $P(X) = X^n - 1$. This is a contradiction, because $P(X)$ is supposed to be primitive, hence irreducible. Thus, we have $\alpha_j = 0$ for $2 \leq j \leq n$. Therefore, the matrix M is that of an homothety. □

4.3 Experimental checkings

We used a Sage worksheet to do computations to check the conjectures on Langevin's table of primitive polynomials (see [8]). In the next subsubsections, we give the functions of our worksheet, and we give the results we obtained.

4.3.1 The Sage functions

We used the following Sage functions.

```
def Comp(n,p,f):
    A=GL(n,p)
    Fp=GF(p)
```

```
    FpX.<x>=PolynomialRing(Fp,'x')
    M=Matrix(n,n,range(n*n))
    for i in range(1,n+1):
        for j in range (1,n+1):
            M[i-1,j-1]=0
        M[i-1,n-1]=-FpX(f)[i-1]
    for i in range (1,n):
        M[i,i-1]=1
    return M

def G(n,p):
    return Comp(n,p,x^n-1)

def C(n,p,P):
    return Comp(n,p,P)

def Gi(k,n,p,P):
    if k==1:
       return C(n,p,P)
    else:
       return G(n,p)*Gi(k-1,n,p,P)*G(n,p)^(-1)

def ConjA(n,p,P):
    print n,p,P
    gens_A=[GL(n,p)(C(n,p,P)),GL(n,p)(G(n,p))]
    H_A=MatrixGroup(gens_A)
    return GL(n,p).order()==H_A.order()

def ConjB(n,p,P):
    print n,p,P
    gens_B=[GL(n,p)(Gi(k,n,p,P)) for k in range(1,n+1)]
    print n,p,P
    H_B=MatrixGroup(gens_B)
    return GL(n,p).order()==H_B.order()
```

4.3.2 The results

The results we obtained are given below. We have tested each primitive polynomial of Langevin's table (see [8]) of degree n over $\mathbb{F}_p$ for which $p^n \leq 50000$ with our personnal MacBook.

Primitive polynomials over $\mathbb{F}_2$

n	p	$P(x)$	$A(n,p,P)$	$B(n,p,P)$
2	2	x^2+x+1	True	False
3	2	x^3+x+1	True	True
4	2	x^4+x+1	True	True
5	2	x^5+x^2+1	True	True
6	2	x^6+x+1	True	True
7	2	x^7+x+1	True	True
8	2	$x^8+x^7+x^2+x+1$	True	True
9	2	x^9+x^4+1	True	True
10	2	$x^{10}+x^3+1$	True	True
11	2	$x^{11}+x^2+1$	True	True
12	2	$x^{12}+x^8+x^2+x+1$	True	True
13	2	$x^{13}+x^5+x^2+x+1$	True	True
14	2	$x^{14}+x^{12}+x^2+x+1$	True	True
15	2	$x^{15}+x+1$	True	True
16	2	$x^{16}+x^5+x^3+x^2+1$	?	?

Primitive polynomials over $\mathbb{F}_3$

n	p	$P(x)$	$A(n,p,P)$	$B(n,p,P)$
2	3	x^2+x+2	True	True
3	3	x^3+2x^2+1	True	True
4	3	x^4+x^3+2	True	True
5	3	$x^5+x^4+x^2+1$	True	True
6	3	x^6+x^5+2	True	True
7	3	$x^7+x^6+x^4+1$	True	True
8	3	x^8+x^5+2	True	True
9	3	$x^9+x^7+x^5+1$	True	True
10	3	$x^{10}+x^9+x^7+2$	?	?

Primitive polynomials over $\mathbb{F}_5$

n	p	$P(x)$	$A(n,p,P)$	$B(n,p,P)$
2	5	x^2+x+2	True	True
3	5	x^3+x^2+2	True	True
4	5	x^4+x^3+x+3	True	True
5	5	x^5+x^2+2	True	True
6	5	x^6+x^5+2	True	True
7	5	x^7+x^6+2	?	?

Primitive polynomials over $\mathbb{F}_7$

n	p	$P(x)$	$A(n,p,P)$	$B(n,p,P)$
2	7	x^2+x+3	True	True
3	7	x^3+x^2+x+2	True	True
4	7	$x^4+x^3+x^2+3$	True	True
5	7	x^5+x^4+4	True	True
6	7	$x^6+x^5+x^4+3$	?	?

Primitive polynomials over $\mathbb{F}_{11}$

n	p	$P(x)$	$A(n,p,P)$	$B(n,p,P)$
2	11	x^2+x+7	True	True
3	11	x^3+x^2+3	True	True
4	11	x^4+x^3+8	True	True
5	11	$x^5+x^4+x^3+3$	?	?

Primitive polynomials over $\mathbb{F}_{13}$

n	p	$P(x)$	$A(n,p,P)$	$B(n,p,P)$
2	13	x^2+x+2	True	True
3	13	x^3+x^2+2	True	True
4	13	$x^4+x^3+x^2+6$	True	True
5	13	$x^5+x^4+x^3+6$	?	?

Primitive polynomials over $\mathbb{F}_{17}$

n	p	$P(x)$	$A(n,p,P)$	$B(n,p,P)$
2	17	x^2+x+3	True	True
3	17	x^3+x^2+7	True	True
4	17	x^4+x^3+5	?	?

Primitive polynomials over $\mathbb{F}_{19}$

n	p	$P(x)$	$A(n,p,P)$	$B(n,p,P)$
2	19	x^2+x+2	True	True
3	19	x^3+x^2+6	True	True
4	19	x^4+x^3+2	?	?

Primitive polynomials over $\mathbb{F}_{23}$

n	p	$P(x)$	$A(n,p,P)$	$B(n,p,P)$
2	23	x^2+x+7	True	True
3	23	x^3+x^2+6	True	True
4	23	x^4+x^3+20	?	?

Primitive polynomials over $\mathbb{F}_{29}$

n	p	$P(x)$	$A(n,p,P)$	$B(n,p,P)$
2	29	x^2+x+3	True	True
3	29	x^3+x^2+3	True	True
4	29	x^4+x^3+2	?	?

Primitive polynomials over $\mathbb{F}_{31}$

n	p	$P(x)$	$A(n,p,P)$	$B(n,p,P)$
2	31	x^2+x+12	True	True
3	31	x^3+x^2+9	True	True
4	31	x^4+x^3+13	?	?

Primitive polynomials over $\mathbb{F}_{37}$

n	p	$P(x)$	$A(n,p,P)$	$B(n,p,P)$
2	37	x^2+x+5	True	True
3	37	x^3+x^2+17	?	?

Primitive polynomials over $\mathbb{F}_{41}$

n	p	$P(x)$	$A(n,p,P)$	$B(n,p,P)$
2	41	x^2+x+12	True	True
3	41	x^3+x^2+11	?	?

Primitive polynomials over $\mathbb{F}_{43}$

n	p	$P(x)$	$A(n,p,P)$	$B(n,p,P)$
2	43	x^2+x+3	True	True
3	43	x^3+x^2+9	?	?

Primitive polynomials over $\mathbb{F}_{47}$

n	p	$P(x)$	$A(n,p,P)$	$B(n,p,P)$
2	47	x^2+x+13	True	True
3	47	x^3+x^2+2	?	?

Primitive polynomials over $\mathbb{F}_{53}$

n	p	$P(x)$	$A(n,p,P)$	$B(n,p,P)$
2	53	x^2+x+5	True	True
3	53	x^3+x^2+2	?	?

Primitive polynomials over $\mathbb{F}_{59}$

n	p	$P(x)$	$A(n,p,P)$	$B(n,p,P)$
2	59	x^2+x+2	True	True
3	59	x^3+x^2+9	?	?

Primitive polynomials over $\mathbb{F}_{61}$

n	p	$P(x)$	$A(n,p,P)$	$B(n,p,P)$
2	61	x^2+x+2	True	True
3	61	x^3+x^2+6	?	?

Primitive polynomials over $\mathbb{F}_{67}$

n	p	$P(x)$	$A(n,p,P)$	$B(n,p,P)$
2	67	x^2+x+12	True	True
3	67	x^3+x^2+6	?	?

Primitive polynomials over $\mathbb{F}_{71}$

n	p	$P(x)$	$A(n,p,P)$	$B(n,p,P)$
2	71	x^2+x+11	True	True
3	71	x^3+x^2+8	?	?

Primitive polynomials over $\mathbb{F}_{73}$

n	p	$P(x)$	$A(n,p,P)$	$B(n,p,P)$
2	73	x^2+x+11	True	True
3	73	x^3+x^2+5	?	?

Primitive polynomials over $\mathbb{F}_{79}$

n	p	$P(x)$	$A(n,p,P)$	$B(n,p,P)$
2	79	x^2+x+3	True	True
3	79	x^3+x^2+2	?	?

Primitive polynomials over $\mathbb{F}_{83}$

n	p	$P(x)$	$A(n,p,P)$	$B(n,p,P)$
2	83	x^2+x+2	True	True
3	83	x^3+x^2+11	?	?

Primitive polynomials over $\mathbb{F}_{89}$

n	p	$P(x)$	$A(n,p,P)$	$B(n,p,P)$
2	89	x^2+x+6	True	True
3	89	x^3+x^2+6	?	?

Primitive polynomials over $\mathbb{F}_{97}$

n	p	$P(x)$	$A(n,p,P)$	$B(n,p,P)$
2	97	x^2+x+5	True	True
3	97	x^3+x^2+5	?	?

Conclusion

In this paper, we introduced the new notions of n-cyclable groups and n-brunnian groups of type I and II (see section 1). We then proved that the groups $\mathrm{SL}_n(\mathbb{F}_p)$, $\mathrm{PSL}_n(\mathbb{F}_p)$, $\mathrm{GL}_n(\mathbb{F}_p)$, and $\mathrm{PGL}_n(\mathbb{F}_p)$ enjoy a structure of n-brunnian groups of type I for p prime and $n \geq 3$ (see section 2). In section 3, we state two conjectures, namely the conjectures $A(n,p,P)$ and $B(n,p,P)$ about primitive polynomials over $\mathbb{F}_p$, and we give some evidence in section 4.

Unfortunately, the conjectures $A(n,p,P)$ and $B(n,p,P)$ do not characterize primitive polynomials, because, they are both true for the polynomial of Example 3.3.

It is altogether interesting to find some significant counterexamples, or to find a conceptual proof of them.

References

[1] [Bavard C.] La surface de Klein, *Le journal de maths des élèves*, Volume 1 (1993), No. 1,
http://www.umpa.ens-lyon.fr/JME/Vol1Num1/artCBavard/artCBavard.pdf.

[2] [Brillhart J., Zierler N.] – On $x^n + x + 1$ over $GF(2)$, *Information and control* **16** (5) (1970) 502–505.

[3] [Degos J.-Y.] – A Sage Worksheet for studying Conjecture A and Conjecture B, 2011,
http://jeanyves.degos.free.fr/ConjAandB.sws.

[4] [Guitart R.] – Moving logic, from Boole to Galois, *Colloque International "Charles Ehresmann : 100 ans"*, 7-9 octobre 2005, Amiens, *Cah. Top. Géo. Diff. Cat.* **XLVI-3** (2005) 196–198.

[5] [Guitart R.] – Klein's group as a borromean object, *Cah. Top. Géo. Diff. Cat.*, **L-2**, (2009) 144–155.

[6] [Klein F.] – Uber die Transformationen siebenter Ordnung der elliptischen Funktionen, *Math. Ann.* **14** (1879), 428–471.

[7] [Lang S.] – Algebra, *Addison Wesley*, Third edition, New-York, Paris, 1993.

[8] [Langevin P.] – Quelques polynômes primitifs,
http://langevin.univ-tln.fr/CDE/primitif.data.

[9] [Lidl R., Niederreiter H.] – Finite fields, Encyclopedia of Mathematics and its Applications **20**, *Cambridge University Press*, 2008.

Jean-Yves Degos
Rés. Les Lotus, appt 19
22, avenue de Chiquet
33600 Pessac (France)
jydegos@gmail.com