

# $SL_2(k)$ and a subset of words over $k$

Roland Bacher

March 14, 2007

*Abstract:*<sup>1</sup> Given a field  $k$ , this paper defines a subset of the free semi-group  $F_k$  (whose elements are all finite words with letters in  $k$ ) which has some interesting arithmetic and combinatorial properties. The case  $p = 2$  has been treated in [B2] with slightly different notations. The link with  $SL_2$  and motivation for studying this subset originates in [B1].

## 1 Introduction

Given a group or semi-group  $\Gamma$  generated (in the sense of semi-groups) by some subset  $S \subset \Gamma$ , the *Cayley graph* of  $\Gamma$  with respect to  $S$  is the oriented graph having vertices  $\gamma \in \Gamma$  and oriented edges  $(\gamma, \gamma s)_{s \in S}$ . In this paper, we consider generating sets  $S$  which are not necessarily finite thus yielding oriented Cayley graphs which are perhaps not locally finite.

The above situation gives rise to a homomorphism of semi-groups

$$\pi : F_S \longrightarrow \Gamma$$

where  $F_S$  denotes the free semi-group on the set  $S$  consisting of all finite words  $s_1 \dots s_l$  with letters in the alphabet  $S$ . The set  $F_S$  is also called the *free monoid* on  $S$  and is often denoted by  $S^*$ . We will stick to the notation  $F_S$  since our set  $S$  will be identified with a field  $k$  and the notation  $k^*$  would be misleading in this case.

This paper deals with the group  $\Gamma = SL_2(k)$  over an arbitrary field  $k$  generated by the set of matrices

$$S = \left\{ \begin{pmatrix} 0 & -1 \\ 1 & \alpha \end{pmatrix} \mid \alpha \in k \right\}.$$

We will study the preimage  $\mathcal{A} \subset F_S$  of all finite words with letters in  $S$  (whose elements are indexed by the elements of the field  $k$ ) such that

$$\pi(\mathcal{A}) = \left\{ \begin{pmatrix} a & -b \\ b^{-1} & 0 \end{pmatrix} \mid a \in k, b \in k^* \right\}.$$

---

<sup>1</sup>Math. class.: 05C38, 20G15, 68R15. Keywords:  $SL_2$ ,  $PSL_2$ , equivalence relation, de Bruijn sequence

The set  $\mathcal{A}$  can also be described as follows: Recall that the projective line  $\mathbf{P}^1(k)$  consists of all 1-dimensional subspaces in  $k^2$ . We denote by  $L(x)$  the subspace (line) spanned by  $\begin{pmatrix} 1 \\ x \end{pmatrix}$  and by  $L(\infty)$  the subspace spanned by  $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$  (hence  $L(x)$  denotes the unique line in  $k^2$  which has slope  $x$  and runs through the origin). The group  $\mathrm{SL}_2(k)$  acts on  $\mathbf{P}^1(k)$  (this action goes in fact down to the projective group  $\mathrm{PSL}_2(k)$  which is the quotient of  $\mathrm{SL}_2(k)$  by  $\pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ ). The subset  $\mathcal{A}$  considered above can now be defined as the set of all words  $w \in F_S$  such that  $\pi(w)L(\infty) = L(0)$ .

The aim of this paper is the description of some properties of the set  $\mathcal{A} \subset F_k$  and of its complement  $\mathcal{C} = F_S \setminus \mathcal{A} \subset F_S$ . All results will be stated in the next section. Proofs will be given in section 3.

## 2 Definitions and main results

Consider a field  $k$  and the set

$$S = \left\{ \begin{pmatrix} 0 & -1 \\ 1 & \alpha \end{pmatrix} \mid \alpha \in k \right\} \subset \mathrm{SL}_2(k) \quad .$$

**Lemma 2.1.** *The set  $S$  generates  $\mathrm{SL}_2(k)$  as a semigroup.*

This lemma shows that every element of  $\mathrm{SL}_2(k)$  can be written in at least one way as a finite word with letters in  $S$ . Since the elements of  $S$  are obviously indexed by  $k$  we will only write  $\alpha$  instead of  $\begin{pmatrix} 0 & -1 \\ 1 & \alpha \end{pmatrix}$ . We identify hence the free monoid  $F_S$  on  $S$  with the free monoid  $F_k$  on  $k$  consisting of the set of all finite words with letters in the field  $k$ . We recall that we are interested in the subset  $\mathcal{A} \subset F_k$  defined by

$$\mathcal{A} = \{w = \alpha_1 \dots \alpha_l \in F_k \mid \pi(w)L(\infty) = L(0)\}$$

(where  $L(\infty) = k \begin{pmatrix} 0 \\ 1 \end{pmatrix}$  and  $L(0) = k \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ ) and in its complement  $\mathcal{C} = F_k \setminus \mathcal{A}$ . We denote by  $F_k^l$  the subset of all words of length exactly  $l$  in  $F_k$ . We set  $\mathcal{A}^l = \mathcal{A} \cap F_k^l$  and  $\mathcal{C}^l = \mathcal{C} \cap F_k^l$ .

**Theorem 2.2.** (i)  $w \in \mathcal{A}^l$  if and only if  $\alpha w \in \mathcal{C}^{l+1}$  and  $w\alpha \in \mathcal{C}^{l+1}$  for every  $\alpha \in k$ .

(ii) For any  $w \in \mathcal{C}^l$  there exist unique values  $\alpha, \beta \in k$  such that  $\alpha w, w\beta \in \mathcal{A}^{l+1}$ .

(iii) if  $\alpha_1 \dots \alpha_l \in \mathcal{A}^l$  then  $\alpha_2 \alpha_3 \dots \alpha_l$  and  $\alpha_1 \alpha_2 \dots \alpha_{l-1} \in \mathcal{C}^{l-1}$ .

(iv)  $\alpha_1 \alpha_2 \dots \alpha_{l-1} \alpha_l \in \mathcal{A}^l$  if and only if  $\alpha_l \alpha_{l-1} \dots \alpha_2 \alpha_1 \in \mathcal{A}^l$ .

(v)  $\alpha_1 \dots \alpha_l \in \mathcal{A}^l$  if and only if  $(-\alpha_1) \dots (-\alpha_l) \in \mathcal{A}^l$ .

**Corollary 2.3.** For  $k$  the finite field on  $q = p^d$  elements (with  $p$  the finite prime characteristic of  $k$ ) and for  $l = 0, 1, 2, \dots$  we have

$$\#(\mathcal{A}^l) = \frac{q^l - (-1)^l}{q + 1}, \quad \#(\mathcal{C}^l) = \frac{q^{l+1} + (-1)^l}{q + 1}.$$

Consider the equivalence relation  $\sim$  on  $F_k$  with classes  $\mathcal{A}$  and  $\mathcal{C}$ . Denote by  $\epsilon$  the empty word (of length 0) in  $F_k$ . Extend the applications  $x \mapsto x + 1$ ,  $x \mapsto x - 1$  of the field  $k$  to applications of the set  $k \cup \{\epsilon\}$  into itself by setting  $(\epsilon \pm 1) = \epsilon$ .

**Proposition 2.4.** (i) One has

$$\begin{aligned} x0y &\sim xy, \\ x\alpha 1\beta y &\sim x(\alpha - 1)(\beta - 1)y, \\ x\alpha(-1)\beta y &\sim x(\alpha + 1)(\beta + 1)y \end{aligned}$$

where  $x, y \in F_k$ ,  $\alpha, \beta \in k \cup \{\epsilon\}$  with  $\alpha = \epsilon \implies x = \epsilon$  and  $\beta = \epsilon \implies y = \epsilon$  (i.e.  $\alpha$  is the last letter of word  $x\alpha$  if  $x\alpha$  is non-empty and  $\beta$  is the first letter of the word  $\beta y$  if  $\beta y$  is non-empty).

(ii) One has

$$\begin{aligned} \alpha\beta x &\sim (\beta - \alpha^{-1})x && \text{if } 0 \neq \alpha \in k, \beta \in k, x \in F_k, \\ 0\beta x &\sim x && \text{if } \beta \in k, x \in F_k. \end{aligned}$$

**Remarks 2.5.** (i) If  $k$  is the field on 2 or 3 elements, then assertion (i) of previous proposition characterizes the sets  $\mathcal{A}$  and  $\mathcal{C}$  completely: it yields substitutions which replace every word except  $0 \in \mathcal{A}$  and  $\epsilon \in \mathcal{C}$  by an equivalent word which is strictly shorter.

(ii) Over any field  $k$ , assertion (ii) above and the trivial observation  $\alpha \sim \epsilon \iff \alpha \neq 0$  for  $\alpha \in k$  determine the sets  $\mathcal{A}$  and  $\mathcal{C}$ .

Set

$$\mathcal{P}^l = \{\alpha_1 \dots \alpha_l \in \mathcal{A}^l \mid \alpha_1 \alpha_2 \dots \alpha_h \in \mathcal{C}^h \text{ for } h = 1, \dots, l - 1\}$$

and  $\mathcal{P} = \cup \mathcal{P}^l$ .

**Theorem 2.6.** (i) (“Unique factorization in  $\mathcal{A}$ ”) We have  $w \in \mathcal{A}$  if and only if  $w$  can be written as

$$w = p_1 \delta_1 p_2 \delta_2 \dots p_n \delta_n p_{n+1}$$

for some  $n \geq 0$  with  $p_1, \dots, p_{n+1} \in \mathcal{P}$  and  $\delta_1, \dots, \delta_n \in k$ . Moreover, such a factorization of  $w \in \mathcal{A}$  is unique.

(ii) We have for  $l \geq 1$

$$\#(\mathcal{P}^l) = (q - 1)^{l-1}$$

if  $k$  is the finite field on  $q = p^d$  elements.

**Corollary 2.7.** *One has for any natural integer  $l$  the identity*

$$(x+1) \sum_{k=0}^{\lfloor l/2 \rfloor} \binom{l-k}{k} x^k (x-1)^{l-2k} = x^{l+1} + (-1)^l$$

which is equivalent to the identities

$$\sum_{s=0}^k \binom{l-s}{s} \binom{l-2s}{k-s} (-1)^s = 1$$

for  $k = 0, 1, \dots, l$ .

**Remark 2.8.** Theorem 2.6 shows that the vector space (over an arbitrary field) with basis the set

$$\{\epsilon\} \cup \{w\alpha \mid w \in \mathcal{A}, \alpha \in k\}$$

can be turned into a graded algebra  $\mathbf{A}$  (the product is given by extending linearly the concatenation of words in  $F_k$  and the grading is induced by the length of words in  $F_k$ ). It has in fact a very simple structure: the algebra  $\mathbf{A}$  is a free non-commutative algebra (on  $q(q-1)^{l-2}$  generators of degree  $l = 2, 3, 4, \dots$  if  $k$  is the finite field on  $q = p^d$  elements).

Given two words  $w, w' \in F_k^l$  of the form

$$w = \alpha_0 \alpha_1 \dots \alpha_{l-1}, \quad w' = \alpha_1 \dots \alpha_{l-1} \alpha_l$$

we call  $w'$  an *immediate successor* of  $w$  and  $w$  an *immediate predecessor* of  $w'$ .

**Theorem 2.9.** *Each element  $w \in \mathcal{A}^l$  has a unique immediate successor and a unique immediate predecessor in  $\mathcal{A}^l$ .*

Given an element  $w_0 \in \mathcal{A}^l$ , the previous theorem yields a sequence

$$w_0, w_1, w_2, w_3, \dots \in \mathcal{A}^l$$

with  $w_{i+1}$  an immediate successor of  $w_i$ .

Otherwise stated: For each  $w \in \mathcal{A}^l$  there exists an infinite word

$$\tilde{W} = \dots \alpha_{-1} \alpha_0 \alpha_1 \alpha_2 \alpha_3 \dots$$

such that  $\alpha_1 \alpha_2 \dots \alpha_l = w$  and all factors  $w_i w_{i+1} \dots w_{i+l-1}$  of length  $l$  (subwords formed by  $l$  consecutive letters) of  $\tilde{W}$  are elements of  $\mathcal{A}^l$ .

Until the end of this section we assume that  $k$  is the finite field with  $q = p^d$  elements. In this case  $\mathcal{A}^l$  is finite. Given  $w \in \mathcal{A}^l$  there exists hence a smallest integer  $r$  such that the infinite word  $\tilde{W}$  associated to  $w$  is  $r$ -periodic.

**Theorem 2.10.** Let  $\tilde{W} = \dots \alpha_{r-1} \alpha_0 \alpha_1 \dots \alpha_{r-1} \alpha_0 \alpha_1 \dots$  be an infinite  $r$ -periodic word with letters in a finite field  $k$ . Then there exists a smallest integer  $t \leq q^2 - 1$  (in fact,  $t$  is either  $q$  or a divisor of  $(q^2 - 1)$ ) such that all factors of length  $tr - 1$  in  $\tilde{W}$  belong to  $\mathcal{A}$ .

**Remark 2.11.** It follows (cf. assertion (i) in Lemma 3.1 of section 3) that all factors of length  $ltr - 1$  ( $l \geq 1$ ) of  $\tilde{W}$  belong also to  $\mathcal{A}$ . One can moreover show that if  $m$  is an integer with the property that all factors of length  $m$  in  $\tilde{W}$  belong to  $\mathcal{A}^m$ , then  $m = ltr - 1$  for a suitable integer  $l \geq 1$  (here  $r$  denotes the minimal period length of the infinite periodic word  $\tilde{W}$ ).

**Definition 2.12.** Given a finite set  $E$  having  $N \geq 2$  elements, a *mock parity check set* (MPCS for short) of length  $d$  is a subset  $\mathcal{M} \subset E^d$  (words of length  $d$  with letters in  $E$ ) such that

(i) each element  $w \in \mathcal{M}$  has a unique immediate successor and a unique immediate predecessor in  $\mathcal{M}$ .

(ii)  $\mathcal{M}$  consists of exactly  $N^{d-1}$  elements.

Denote by  $\text{Perm}_E$  the group of permutations of the finite set  $E$  and let  $\varphi : E^{d-2} \rightarrow \text{Perm}_E$  be an application which associates to each element  $z \in E^{d-2}$  a permutation  $\varphi_z : E \rightarrow E$ .

**Proposition 2.13.** The set

$$\mathcal{M} = \{\alpha_1 \alpha_2 \dots \alpha_{d-1} \alpha_d \in E^d \mid \varphi_{\alpha_2 \alpha_3 \dots \alpha_{d-1}}(\alpha_1) = \alpha_d\}$$

is a MPCS and every MPCS is of this form.

**Remarks 2.14.** (i) This proposition shows that the set of all MPCS can be endowed with a group structure (the set of functions on  $E^{N^{d-2}}$  with values in  $\text{Perm}_E$  has an obvious group structure given by  $(\varphi\psi)_z = \varphi_z \circ \psi_z$ ).

(ii) A MPCS  $\mathcal{M} \subset E^d$  yields a permutation of its elements: send each  $w \in \mathcal{M}$  to its (unique) successor in  $\mathcal{M}$ . Call a MPCS a (generalized) *de Bruijn sequence* if the associated permutation consists of a unique cycle. One can show that (generalized) de Bruijn sequences exist for all integers  $N \geq 2$  and  $d \geq 1$ .

**Theorem 2.15.** Given a finite field  $k$ , the set

$$\mathcal{M}^l = \mathcal{A}^l \cup \{\alpha_1 \dots \alpha_l \in \mathcal{C}^l \mid \alpha_1 \dots \alpha_{l-1} \in \mathcal{A}^{l-1} \text{ and } \alpha_2 \dots \alpha_l \in \mathcal{A}^{l-1}\}$$

is a MPCS of  $k^l$ .

### 3 Proofs

**Proof of Lemma 2.1.** Take  $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}_2(k)$ . If  $a \neq 0$  we have necessarily  $d = \frac{1+bc}{a}$  and the computation

$$\begin{pmatrix} 0 & -1 \\ 1 & \frac{-c-1}{a} \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & -a \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & \frac{b-1}{a} \end{pmatrix} = \begin{pmatrix} a & b \\ c & \frac{1+bc}{a} \end{pmatrix}$$

yields the result.

The case  $a = 0$  is reduced to precedent case by multiplying first with  $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$  and by remarking that this matrix has order 4 (or 2 if the ground field  $k$  is of characteristic 2). QED

**Proof of Theorem 2.2.** One has

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & x \end{pmatrix} = \begin{pmatrix} b & -a + bx \\ d & -c + dx \end{pmatrix}$$

which shows that  $w\alpha \notin \mathcal{A}$  if  $w \in \mathcal{A}$  (since then  $\pi(w) = \begin{pmatrix} a & -b \\ b^{-1} & 0 \end{pmatrix}$ ). On the other hand, if  $w \in \mathcal{C}$  then  $\pi(w) = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$  with  $d \neq 0$  and the above computation implies the existence of a unique  $\beta$  such that  $w\beta \in \mathcal{A}$ . This proves half of (i) and (ii). The proof of the remaining half is similar (it is also implied by assertion (iv)).

In order to prove (iii) one considers

$$\begin{aligned} \pi(\alpha_2 \dots \alpha_l) &= \pi(\alpha_1)^{-1} \pi(\alpha_1 \dots \alpha_l) = \begin{pmatrix} \alpha_1 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} a & -b \\ b^{-1} & 0 \end{pmatrix} \\ &= \begin{pmatrix} \alpha_1 a + b^{-1} & -\alpha_1 b \\ -a & b \end{pmatrix} \end{aligned}$$

which shows that  $\alpha_2 \dots \alpha_l \in \mathcal{C}^{l-1}$ . A similar computation yields  $\alpha_1 \dots \alpha_{l-1} \in \mathcal{C}^{l-1}$ .

Since

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & \alpha \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} \alpha & 1 \\ -1 & 0 \end{pmatrix}$$

we get by conjugating  $\pi(\alpha_1 \dots \alpha_l) = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$  with  $\sigma = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

$$\sigma \pi(\alpha_1 \dots \alpha_l) \sigma = \begin{pmatrix} \alpha_1 & 1 \\ -1 & 0 \end{pmatrix} \dots \begin{pmatrix} \alpha_l & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} d & c \\ b & a \end{pmatrix}$$

If  $\pi(\alpha_1 \dots \alpha_l) = \begin{pmatrix} a & -b \\ b^{-1} & 0 \end{pmatrix}$  we get by taking the inverse of  $\sigma \pi(\alpha_1 \dots \alpha_l) \sigma$

$$\pi(\alpha_l \dots \alpha_1) = \begin{pmatrix} 0 & -1 \\ 1 & \alpha_l \end{pmatrix} \dots \begin{pmatrix} 0 & -1 \\ 1 & \alpha_1 \end{pmatrix} = \begin{pmatrix} 0 & b^{-1} \\ -b & a \end{pmatrix}^{-1} = \begin{pmatrix} a & -b^{-1} \\ b & 0 \end{pmatrix}$$

which shows that  $\alpha_l \dots \alpha_1 \in \mathcal{A}$  and proves (iv).

Transposing  $\pi(\alpha_1 \dots \alpha_l)$  and multiplying by  $(-1)^l$  shows that  $(-\alpha_l) \dots (-\alpha_1) \in \mathcal{A}$ . Assertion (iv) implies now (v).

**Remark 3.1.** The properties of the action of  $\mathrm{SL}_2(k)$  (or  $\mathrm{PSL}_2(k)$ ) on the projective line  $\mathbf{P}^1(k)$  can be used to get a more conceptual proof of most assertions in Theorem 2.2.

**Proof of Corollary 2.3.** Assertion (ii) of Theorem 2.2 shows that  $\#(\mathcal{A}^{l+1}) \geq \#(\mathcal{C}^l)$  and assertion (iii) implies  $\#(\mathcal{A}^{l+1}) \leq \#(\mathcal{C}^l)$  hence establishing  $\#(\mathcal{A}^{l+1}) = \#(\mathcal{C}^l)$ . Induction on  $l$  (using the obvious identity  $\#(\mathcal{A}^l) + \#(\mathcal{C}^l) = q^l$ ) yields now the result.

**Proof of Proposition 2.4.** The first line of assertion (i) follows from the identity

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}.$$

If  $\alpha$  and  $\beta$  are both non-empty, the last two lines of the proposition follow from the identities

$$\begin{aligned} & \begin{pmatrix} 0 & -1 \\ 1 & \alpha \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & \beta \end{pmatrix} \\ &= \begin{pmatrix} -1 & 1-\beta \\ \alpha-1 & \alpha\beta-\alpha-\beta \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & \alpha-1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & \beta-1 \end{pmatrix} \end{aligned}$$

and

$$\begin{aligned} & \begin{pmatrix} 0 & -1 \\ 1 & \alpha \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & \beta \end{pmatrix} = \begin{pmatrix} 1 & 1+\beta \\ -1-\alpha & -\alpha-\beta-\alpha\beta \end{pmatrix} \\ &= - \begin{pmatrix} 0 & -1 \\ 1 & \alpha+1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & \beta+1 \end{pmatrix} \end{aligned}$$

(in fact, the last line of Proposition 2.4 is easily deduced from the second one by using assertion (v) of Theorem 2.2). We leave the remaining cases of assertion (i) (with  $\epsilon \in \{\alpha, \beta\}$ ) to the reader (they follow also easily from Theorem 2.6).

Assertion (ii) follows from the computations

$$\begin{pmatrix} 0 & -1 \\ 1 & \alpha \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & \beta \end{pmatrix} \begin{pmatrix} \alpha\beta a + \beta c - a & \alpha\beta b + \beta d - b \\ -\alpha a - c & -\alpha b - d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

and

$$\begin{aligned} & \begin{pmatrix} 0 & -1 \\ 1 & \gamma \end{pmatrix} \begin{pmatrix} \alpha\beta a + \beta c - a & \alpha\beta b + \beta d - b \\ -\alpha a - c & -\alpha b - d \end{pmatrix} \\ &= \begin{pmatrix} \alpha a + c & \alpha b + d \\ \alpha\beta a + \beta c - a - \alpha\gamma a - \gamma c & \alpha\beta b + \beta d - b - \alpha\gamma b - \gamma d \end{pmatrix}. \end{aligned}$$

**Lemma 3.2.** (i) If  $w, w' \in \mathcal{A}$  then  $ww' \in \mathcal{C}$  and  $w\alpha w' \in \mathcal{A}$  for any  $\alpha \in k$ .

(ii) If exactly one of  $w, w'$  is an element of  $\mathcal{A}$  then  $w\alpha w' \in \mathcal{C}$  for any  $\alpha \in k$ .

**Proof of Lemma 3.2.** The computation

$$\begin{pmatrix} a & -b \\ b^{-1} & 0 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & \alpha \end{pmatrix} \begin{pmatrix} a' & -b' \\ b'^{-1} & 0 \end{pmatrix} = \begin{pmatrix} -ba' - ab'^{-1} - \alpha bb'^{-1} & bb' \\ -(bb')^{-1} & 0 \end{pmatrix}$$

shows (i).

Let us now suppose that  $w \in \mathcal{A}$ ,  $w' \in \mathcal{C}$ . This implies  $\pi(w\alpha) = \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix}$  and  $\pi(w') = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$  with  $d' \neq 0$ . We get hence

$$\pi(w\alpha w') = \begin{pmatrix} aa' + bc' & ab' + bd' \\ a^{-1}c' & a^{-1}d' \end{pmatrix}$$

which shows  $w\alpha w' \in \mathcal{C}$ . The case  $w \in \mathcal{C}$ ,  $w' \in \mathcal{A}$  follows using assertion (iv) of Theorem 2.2.

**Remark 3.3.** One can also use the more conceptual computation

$$\pi(w\alpha w')L(\infty) = \pi(w)\pi(\alpha)\pi(w')L(\infty) = \pi(w)\pi(\alpha)L(0) = \pi(w)L(\infty) = L(0)$$

(for  $w, w' \in \mathcal{A}$ ) in order to prove assertion (i) of Lemma 3.2.

Similarly, the case  $w \in \mathcal{C}$ ,  $w' \in \mathcal{A}$  is dealt by

$$\pi(w\alpha w')L(\infty) = \pi(w)\pi(\alpha)\pi(w')L(\infty) = \pi(w)\pi(\alpha)L(0) = \pi(w)L(\infty) \neq L(0)$$

and assertion (iv) of Theorem 2.2 completes the proof of assertion (ii) in Lemma 3.2.

**Proof of Theorem 2.6.** Assertion (i) follows easily from the previous lemma and the definition of  $\mathcal{P}$ .

Assertion (ii) follows from assertion (ii) of Theorem 2.2.

**Proof of Corollary 2.7.** Let  $k$  be the finite field with  $q = p^d$  elements. An exercise using Theorem 2.6 shows that we have

$$\#(\mathcal{A}^{l+1}) = \sum_{k=0}^{\lfloor l/2 \rfloor} \binom{l-k}{k} q^k (q-1)^{l-2k}.$$

Corollary 2.3 establishes then the result if  $x$  is a power of a prime number. The proof follows now from the fact that both sides are polynomials in  $x$ .

**Proof of Theorem 2.9.** Follows from assertions (iii) and (ii) in Theorem 2.2.

**Proof of Theorem 2.10.** The elements

$$\pi(\alpha_0\alpha_1\dots\alpha_{q-1}), \pi(\alpha_1\dots\alpha_{q-1}\alpha_0), \dots, \pi(\alpha_{q-1}\alpha_0\dots\alpha_{q-2}) \in \mathrm{SL}_2(k)$$

are all conjugate and have hence a common order  $t$  which obviously works.

The easy proof of Proposition 2.13 is left to the reader.

**Proof of Theorem 2.15.** This result follows readily from Theorem 2.9, assertion (i) of Theorem 2.2 and Corollary 2.3.

I thank J.P. Allouche, P. de la Harpe and J. Helmstetter for useful comments.

I thank also an anonymous referee for the remark that the paper deals in fact with the projective group  $\mathrm{PSL}_2(k)$  and for suggesting Remarks 3.1 and 3.3.

### Bibliography

[B1] R. Bacher, *Curvature flow of maximal integral triangulations*, Ann. Inst. Fourier [49], 4 (1999), 1115-1128.

[B2] R. Bacher, *An equivalence relation on  $\{0,1\}^*$* , Europ. Journal of Combinatorics 21 (2000), 853-864.

Roland Bacher  
INSTITUT FOURIER  
Laboratoire de Mathématiques  
UMR 5582 (UJF-CNRS)  
BP 74  
38402 St MARTIN D'HÈRES Cedex (France)  
e-mail: Roland.Bacher@ujf-grenoble.fr