SL_2 and a subset of $\{\mathbf{Z}/p\mathbf{Z}\}^*$

Roland BACHER

Prépublication de l'Institut Fourier n° 501 (2000)
http://www-fourier.ujf-grenoble.fr/prepublications.html

Abstract: [1] This paper defines a subset of $\{\mathbf{Z}/p\mathbf{Z}\}^*$ (finite words with letters in the finite field $\mathbf{Z}/p\mathbf{Z}$ of prime characteristic p) which has some nice arithmetic and combinatorial properties. The case $p = 2$ has been treated in **[B2]**. The link with SL_2 (together with more motivation coming from geometry) originates in **[B1]**.

1 Introduction and main results

Let us consider the oriented affine plane $\mathbf{R}^2$ together with two ordered triangles (Δ, Δ') which have the same area and share a common oriented edge starting at a vertex $A \in \Delta \cap \Delta'$ and ending at $B \in \Delta \cap \Delta'$. The orbits (under affine transformations) of such pairs (Δ, Δ') are indexed by $\mathbf{R}$ since we have in affine coordinates

$$C' = A + B - C + \alpha(B - A)$$
$$C = A + B - C' + \alpha(B - A)$$

(with α a suitable real number) for the remaining vertices $C \in \Delta$ and $C' \in \Delta'$.

A sequence of triangles $(\Delta_0, \ldots, \Delta_k)$ of equal area, having a common vertex O such that Δ_i and Δ_{i+1} always intersect along a common edge (such a sequence of triangles has a starlike looking) yields hence a sequence $(\alpha_1, \ldots, \alpha_k)$ of real numbers and any finite sequence of real numbers can arise in this way (of course, some triangles may be overlapping).

Although there is no notion of angle in affine geometry, some of these starlike sequences may close up modulo a homothetie (which may be of negative ratio) and in this case there is a well defined integral multiple k of π which we may call the angle of such a sequence.

[1] Math. class.: 05C38, 20G15, 68R15. Keywords: SL_2, equivalence relation

All this (except for the integer k which is generally no longer defined) carries over to arbitrary fields (or suitable rings, cf. **[B1]** for the case of integers) and this paper deals with the case of finite primary (or more generally finite) fields.

We will hence study the set of finite sequences $\alpha_1, \ldots, \alpha_k$ over finite fields which give rise by the above geometrical construction to sequences (defined up to affine transformations) of triangles $(\Delta_0, \ldots, \Delta_k)$ which close up modulo a homothetie.

Let p denote a prime number. We consider the free monoid $\mathcal{M}_p = \{0, 1, \ldots, p-1\}^*$ of all finite words with letters in the field $\mathbf{Z}/p\mathbf{Z}$ (which we identify with the finite set $\{0, \ldots, p-1\}$ in the obvious way). Given an element $w = \alpha_1 \ldots \alpha_l,\ \alpha_i \in \mathbf{Z}/p\mathbf{Z}$ of $\mathcal{M}_p$ we consider the matrix

$$M(w) = \begin{pmatrix} 0 & -1 \\ 1 & 1-\alpha_1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 1-\alpha_2 \end{pmatrix} \cdots \begin{pmatrix} 0 & -1 \\ 1 & 1-\alpha_l \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z}/p\mathbf{Z}) \quad .$$

Set

$$\mathcal{S} = \{w \in \mathcal{M}_p \mid M(w) \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \text{is upper triangular}\}$$

i.e. $\mathcal{S}$ is the set of all words w such that

$$M(w) = \begin{pmatrix} a & b \\ -b^{-1} & 0 \end{pmatrix}$$

for suitable $a \in \mathbf{Z}/p\mathbf{Z}$ and $b \in (\mathbf{Z}/p\mathbf{Z})^*$.

Remarks 1.1. (i) It is an exercice to check that

$$\{M(w) \mid w \in \mathcal{M}_p\} = \mathrm{SL}_2(\mathbf{Z}/p\mathbf{Z})$$

(use for instance the fact that the matrices

$$S = M(1) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},\ T = M(1110) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad ,$$

defined over the integers, generate $\mathrm{SL}_2(\mathbf{Z})$, see **[S]**, Chapter VII, Theorem 2).

(ii) Most results of this paper remain valid when replacing the finite primary field $\mathbf{Z}/p\mathbf{Z}$ by an arbitrary field.

Let $\mathcal{C} = \mathcal{M}_p \setminus \mathcal{S}$ denote the complement of $\mathcal{S}$ in $\mathcal{M}_p$. Denote by $\mathcal{M}_p^l$ the subset of all words of length exactly l in $\mathcal{M}_p$. We set $\mathcal{S}^l = \mathcal{S} \cap \mathcal{M}_p^l$ and $\mathcal{C}^l = \mathcal{C} \cap \mathcal{M}_p^l$.

Theorem 1.2. *(i) $w \in \mathcal{S}^l$ if and only if $\alpha w \in \mathcal{C}^{l+1}$ and $w\alpha \in \mathcal{C}^{l+1}$ for every $\alpha \in \mathbf{Z}/p\mathbf{Z}$.*

(ii) For any $w \in \mathcal{C}^l$ there exist unique values $\alpha,\ \beta \in \mathbf{Z}/p\mathbf{Z}$ such that $\alpha w,\ w\beta \in \mathcal{S}^{l+1}$.

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

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

(v) $\alpha_1 \dots \alpha_l \in \mathcal{S}^l$ if and only if $(2-\alpha_1) \dots (2-\alpha_l) \in \mathcal{S}^l$.

Corollary 1.3. *We have for all $l = 0, 1, 2, \dots$*

$$\sharp(\mathcal{S}^l) = \frac{p^l - (-1)^l}{p+1}\ , \quad \sharp(\mathcal{C}^l) = \frac{p^{l+1} + (-1)^l}{p+1} \quad .$$

Consider the equivalence relation $\sim$ on $\mathcal{M}_p$ with classes $\mathcal{S}$ and $\mathcal{C}$. Denote by ϵ the empty word (of length 0) in $\mathcal{M}_p$. Extend the applications $x \longmapsto x+1,\ x \longmapsto x-1$ of the field $\mathbf{Z}/p\mathbf{Z}$ to applications of the set $\mathbf{Z}/p\mathbf{Z} \cup \{\epsilon\}$ into itself by setting $(\epsilon \pm 1) = \epsilon$.

Proposition 1.4. One has

$$\begin{aligned} &x11y \sim xy\ , \\ &x\alpha 0\beta y \sim x(\alpha+1)(\beta+1)y\ , \\ &x\alpha 2\beta y \sim x(\alpha-1)(\beta-1)y \end{aligned}$$

where $x, y \in \mathcal{M}_p,\ \alpha, \beta \in \mathbf{Z}/p\mathbf{Z} \cup \{\epsilon\}$ with $\alpha = \epsilon \Longrightarrow x = \epsilon$ and $\beta = \epsilon \Longrightarrow y = \epsilon$ (i.e. α is the last letter of word $x\alpha$ if $x\alpha$ is non-empty and β is the first letter of the word βy if βy is non-empty).

Remark 1.5. If $p = 2$ or 3 then the previous proposition characterizes the sets $\mathcal{S}$ and $\mathcal{C}$ completely: it yields substitutions which replace every word except $1 \in \mathcal{S}$ and $\epsilon \in \mathcal{C}$ by an equivalent word which is strictly shorter.

Set

$$\mathcal{P}^l = \{\alpha_1 \dots \alpha_l \in \mathcal{S}^l \mid \alpha_1\alpha_2 \dots \alpha_k \in \mathcal{C}^k \quad \text{for } k = 1, \dots, l-1\}$$

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

Theorem 1.6. *(i) ("Unique factorization") We have $w \in \mathcal{S}$ if and only if w can be written as*

$$w = p_1\delta_1 p_2\delta_2 \dots p_k\delta_k p_{k+1}$$

for some $k \geq 0$ with $p_1, \dots p_{k+1} \in \mathcal{P}$ and $\delta_1, \dots, \delta_k \in \mathbf{Z}/p\mathbf{Z}$. Moreover, such a factorization of $w \in \mathcal{S}$ is unique.

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

$$\sharp(\mathcal{P}^l) = (p-1)^{l-1} \quad .$$

Remarks 1.7. (i) Theorem 1.6 shows that the vector space (over an arbitrary field) with basis the set

$$\{\epsilon\} \cup \{w\alpha \mid w \in \mathcal{S},\ \alpha \in \mathbf{Z}/p\mathbf{Z}\}$$

can be turned into a graded algebra $\mathcal{A}$ (the product is given by extending linearly the concatenation of words in $\mathcal{M}_p$ and the grading is induced by the length of words in $\mathcal{M}_p$). It has in fact a simple structure: the algebra $\mathcal{A}$ is a free algebra on $p(p-1)^{l-2}$ generators of degree $l = 2, 3, 4, \ldots$.

(ii) Counting elements in $\mathcal{S}^{l+1}$ using Theorem 1.6 and equating with the result given by Corollary 1.3 one gets a proof of the identities

$$\sum_{k=0}^{[l/2]} \binom{l-k}{k} p^k (p-1)^{l-2k} = \frac{p^{l+1} + (-1)^l}{p+1}$$

which hold for any $p \in \mathbf{C}$ (equality holds for p any prime and extends over $\mathbf{C}$ since both sides are polynomial in p) and $l \in \mathbf{N}$.

Given two words $w, w' \in \mathcal{M}_p^l$ of the form

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

(with $\alpha_i \in \mathbf{Z}/p\mathbf{Z}$) we call w' an *immediate successor* of w and w an *immediate predecessor* of w'.

Theorem 1.8. *Each element $w \in \mathcal{S}^l$ has a unique immediate successor and a unique immediate predecessor in $\mathcal{S}^l$.*

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

$$w_0,\ w_1,\ w_2,\ w_3, \ldots \in \mathcal{S}^l$$

with w_{i+1} an immediate successor of w_i. Since $\mathcal{S}^l$ is finite there exists a smallest integer k such that $w_k = w_i$ for some $i < k$. The existence of unique immediate predecessors in $\mathcal{S}^l$ implies $i = 0$.

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

$$\tilde{W} = \ldots \alpha_{-1}\alpha_0\alpha_1\alpha_2 \ldots \in (\mathbf{Z}/p\mathbf{Z})^{\mathbf{Z}}$$

such that $\alpha_1\alpha_2 \ldots \alpha_l = w$ and all factors of length l (subwords formed by l consecutive letters) of $\tilde{W}$ are elements of $\mathcal{S}^l$.

Theorem 1.9. *Let $\tilde{W} = \ldots \alpha_{q-1}\alpha_0\alpha_1 \ldots \alpha_{q-1}\alpha_0\alpha_1 \in \{\mathbf{Z}/p\mathbf{Z}\}^{\mathbf{Z}}$ be an infinite $q-$periodic word. Then there exists a smallest integer $k \leq p^2 - 1$ (in fact, k is either p or a divisor of (p^2-1)) such that all factors of length $kq-1$ in $\tilde{W}$ belong to $\mathcal{S}$.*

Remark 1.10. It follows (cf. assertion (i) of Lemma 2.1) that all factors of length $lkq-1$ ($l \geq 1$) of $\tilde{W}$ belong also to $\mathcal{S}$. One can moreover show that if m is an integer with the property that all factors of length m in $\tilde{W}$ belong to $\mathcal{S}^m$, then $m = lkq-1$ for a suitable integer $l \geq 1$ (here q denotes the minimal period length of the infinite periodic word $\tilde{W}$).

Definition 1.11. Given an integer $N \geq 2$, a *mock parity check set* (MPCS for short) of length d is a subset $\mathcal{P} \subset \{\mathbf{Z}/N\mathbf{Z}\}^d$ (words of length d with letters in the set $\{\mathbf{Z}/N\mathbf{Z}\}$) such that

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

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

Denote by $\mathrm{Perm}_{\mathbf{Z}/N\mathbf{Z}}$ the group of permutations of the finite set $\mathbf{Z}/N\mathbf{Z}$ and let $\varphi : \{\mathbf{Z}/N\mathbf{Z}\}^{d-2} \longrightarrow \mathrm{Perm}_{\mathbf{Z}/N\mathbf{Z}}$ be an application which associates to each element $z \in \{\mathbf{Z}/N\mathbf{Z}\}^{d-2}$ a permutation $\varphi_z : \mathbf{Z}/N\mathbf{Z} \longrightarrow \mathbf{Z}/N\mathbf{Z}$.

Proposition 1.12. *The set*

$$\mathcal{P} = \{\alpha_1\alpha_2 \ldots \alpha_{d-1}\alpha_d \mid \varphi_{\alpha_2\alpha_3\ldots\alpha_{d-1}}(\alpha_1) = \alpha_d\}$$

is a MPCS and every MPCS is of this form.

Remarks 1.13. (i) This proposition shows that the set of all MPCS can be endowed with a group structure (the set $(\mathrm{Perm}_{\mathbf{Z}/N\mathbf{Z}})^{N^{d-2}}$ has an obvious group structure).

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

Theorem 1.14. *The set*

$$\mathcal{P}^l = \mathcal{S}^l \cup \{\alpha_1 \ldots \alpha_l \in \mathcal{C}^l \mid \alpha_1 \ldots \alpha_{l-1} \in \mathcal{S}^{l-1} \quad \text{and} \quad \alpha_2 \ldots \alpha_l \in \mathcal{S}^{l-1}\}$$

is a MPCS in $(\mathbf{Z}/p\mathbf{Z})^l$.

2 Proofs

Proof of Theorem 1.2. 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 $w\alpha \notin \mathcal{S}$ if $w \in \mathcal{S}$ (since then $M(w) = \begin{pmatrix} a & b \\ -b^{-1} & 0 \end{pmatrix}$). On the other hand, if $w \in \mathcal{C}$ then $M(w) = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with $d \neq 0$ and the above

computation implies the existence of a unique β such that $w\beta \in \mathcal{S}$. 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

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

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

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

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

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

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

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

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

Transposing $M(\alpha_1 \dots \alpha_l)$ and multiplying by $(-1)^l$ shows that $(2-\alpha_l) \dots (2-\alpha_1) \in \mathcal{S}$. Assertion (iv) implies now (v).

Proof of Corollary 1.3. Assertion (ii) of Theorem 1.2 shows that $\sharp(\mathcal{S}^{l+1}) \geq \sharp(\mathcal{C}^l)$ and assertion (iii) implies $\sharp(\mathcal{S}^{l+1}) \leq \sharp(\mathcal{C}^l)$ hence establishing $\sharp(\mathcal{S}^{l+1}) = \sharp(\mathcal{C}^l)$. Induction on l (using the obvious identity $\sharp(\mathcal{S}^l) + \sharp(\mathcal{C}^l) = p^l$) yields now the result.

Proof of Proposition 1.4. The first line 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 α and β are both non-empty. The last two lines of the proposition follow from the identities

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

and

$$\begin{pmatrix} 0 & -1 \\ 1 & 1-\alpha \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 1-\beta \end{pmatrix} = \begin{pmatrix} 1 & 2-\beta \\ -2+\alpha & -3+2\alpha+2\beta-\alpha\beta \end{pmatrix}$$

$$= -\begin{pmatrix} 0 & -1 \\ 1 & 2-\alpha \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 2-\beta \end{pmatrix}$$

(in fact, the last line of Proposition 1.4 is easily deduced from the second one by using assertion (v) of Theorem 1.2). We leave the remaining cases (with $\epsilon \in \{\alpha, \beta\}$) to the reader (they follow in fact easily from Theorem 1.6).

Lemma 2.1. (i) If $w, w' \in \mathcal{S}$ then $ww' \in \mathcal{C}$ and $w\alpha w' \in \mathcal{S}$ for any $\alpha \in \mathbf{Z}/p\mathbf{Z}$.

(ii) If exactly one of w, w' is an element of $\mathcal{S}$ then $w\alpha w' \in \mathcal{C}$ for any $\alpha \in \mathbf{Z}/p\mathbf{Z}$.

Proof of Lemma 2.1. The computation

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

shows (i).

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

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

which shows $w\alpha w' \in \mathcal{C}$. The case $w \in \mathcal{C},\ w' \in \mathcal{S}$ follows now using assertion (iv) of Theorem 1.2.

Proof of Theorem 1.6. Assertion (i) follows easily from the previous lemma and the definition of $\mathcal{P}$.

Assertion (ii) follows from assertion (ii) of Theorem 1.2.

Proof of Theorem 1.8. Follows from assertions (iii) and (ii) in Theorem 1.2.

Proof of Theorem 1.9. The elements

$$M_{\alpha_0\alpha_1\ldots\alpha_{q-1}}, M_{\alpha_1\ldots\alpha_{q-1}\alpha_0}, \ldots, M_{\alpha_{q-1}\alpha_0\ldots\alpha_{q-2}} \in \mathrm{SL}_2(\mathbf{Z}/p\mathbf{Z})$$

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

The easy proof of Proposition 1.12 is left to the reader.

Proof of Theorem 1.13. This result follows readily from Theorem 1.8, assertion (i) of Theorem 1.2 and Corollary 1.3.

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

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* $\{0,1\}^*$, to appear in Europ. Journal of Combinatorics.

[S] J-P. Serre, *Cours d'Arithmétique*, Presses Universitaires de France.

Roland BACHER
INSTITUT FOURIER
Laboratoire de Mathématiques
UMR5582 (UJF-CNRS)
BP 74
38402 St MARTIN D'HÈRES Cedex (France)