CHAPTER III

SUBSETS OF WORDS OVER $\mathbb{Z}/N\mathbb{Z}$

In this chapter, we work on words over $\mathbb{Z}/N\mathbb{Z}$ defined parallel to Bacher's. We investigate their arithmetic properties in the first section. More on $\bar{\mathcal{A}}$ is presented in the second section.

3.1 Words over $\mathbb{Z}/N\mathbb{Z}$

Let

$$S' = \left\{ \begin{bmatrix} 0 & 1 \\ -1 & \alpha \end{bmatrix} : \alpha \in \mathbb{Z}/N\mathbb{Z} \right\}.$$

We begin by giving the proof of the following lemma.

Lemma 3.1.1. *The set S' generates $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ as a semigroup.*

Proof. Recall Theorem 2 in Chapter VII of Serre's book [3] that the set of matrices $\left\{ \begin{bmatrix} -1 & -1 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \right\}$ generates $\mathrm{SL}_2(\mathbb{Z})$ as a group. Since the map $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ obtained by reducing the matrix entries modulo N is a surjective group homomorphism. Then $\left\{ \begin{bmatrix} -1 & -1 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \right\}$ mod N also generates $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ as a group.

Consider $\langle S' \rangle$, a semigroup generated by S'. Since $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ is finite, $\langle S' \rangle$ is a finite closed subset of $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$, so it is a subgroup. Note that $\langle S' \rangle$ con-

tains both generators $\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$ and $\begin{bmatrix} -1 & -1 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$ of $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. Hence $\langle S' \rangle = \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. □

This lemma shows that every element of $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ can be written in at least one way as a finite word with letters in S'.

Next, we establish a way to determine if words are in $\bar{\mathcal{A}}$. For $w \in F_N$ with $\pi(w) = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$, we note that

$$w \in \bar{\mathcal{A}} \Leftrightarrow \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} b \\ d \end{bmatrix} \Leftrightarrow d = 0$$

$$\Leftrightarrow \pi(w) = \begin{bmatrix} a & b \\ -b^{-1} & 0 \end{bmatrix} \text{ with } a \in \mathbb{Z}/N\mathbb{Z}, b \in (\mathbb{Z}/N\mathbb{Z})^\times.$$

Hence we have shown

Theorem 3.1.2. *Let N be a positive integer. Then*

$$\bar{\mathcal{A}} = \left\{ w \in F_N : \pi(w) = \begin{bmatrix} a & b \\ -b^{-1} & 0 \end{bmatrix} \text{ for some } a \in \mathbb{Z}/N\mathbb{Z}, b \in (\mathbb{Z}/N\mathbb{Z})^\times \right\}.$$

For $l \geq 0$, we write F_N^l for the set of words over $\mathbb{Z}/N\mathbb{Z}$ of length l, $\bar{\mathcal{A}}^l = F_N^l \cap \bar{\mathcal{A}}$ and $\bar{\mathcal{C}}^l = F_N^l \cap \bar{\mathcal{C}}$. We first study the insertion and deletion in $\bar{\mathcal{A}}$.

Theorem 3.1.3. *If $w \in \bar{\mathcal{A}}^l$, then $\alpha w \in \bar{\mathcal{C}}^{l+1}$ and $w\alpha \in \bar{\mathcal{C}}^{l+1}$ for every $\alpha \in \mathbb{Z}/N\mathbb{Z}$.*

Proof. Assume that $w \in \bar{\mathcal{A}}^l$ and let $\alpha \in \mathbb{Z}/N\mathbb{Z}$. Then $\pi(w) = \begin{bmatrix} a & b \\ -b^{-1} & 0 \end{bmatrix}$ where $a \in \mathbb{Z}/N\mathbb{Z}$ and $b \in (\mathbb{Z}/N\mathbb{Z})^\times$. Thus

$$\pi(\alpha w) = \pi(\alpha)\pi(w) = \begin{bmatrix} 0 & 1 \\ -1 & \alpha \end{bmatrix} \begin{bmatrix} a & b \\ -b^{-1} & 0 \end{bmatrix} = \begin{bmatrix} -b^{-1} & 0 \\ -a - \alpha b^{-1} & -b \end{bmatrix}$$

and

$$\pi(w\alpha) = \pi(w)\pi(\alpha) = \begin{bmatrix} a & b \\ -b^{-1} & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ -1 & \alpha \end{bmatrix} = \begin{bmatrix} -b & a+\alpha b \\ 0 & -b^{-1} \end{bmatrix}.$$

Since $b \neq 0$, $\alpha w \in \bar{\mathcal{C}}^{l+1}$ and $w\alpha \in \bar{\mathcal{C}}^{l+1}$. □

Theorem 3.1.4. *Let* $w \in \bar{\mathcal{C}}^l$ *with* $\pi(w) = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$.

(i) *If* $\gcd(d, N) = 1$, *i.e.,* $d \in (\mathbb{Z}/N\mathbb{Z})^\times$, *then there exist unique* $\alpha, \beta \in \mathbb{Z}/N\mathbb{Z}$ *such that* $\alpha w \in \bar{\mathcal{A}}^{l+1}$ *and* $w\beta \in \bar{\mathcal{A}}^{l+1}$.

(ii) *If* $\gcd(d, N) > 1$, *then* $\alpha w \in \bar{\mathcal{C}}^{l+1}$ *and* $w\beta \in \bar{\mathcal{C}}^{l+1}$ *for all* $\alpha, \beta \in \mathbb{Z}/N\mathbb{Z}$.

Proof. We first note that for $\alpha \in \mathbb{Z}/N\mathbb{Z}$,

$$\pi(\alpha w) = \pi(\alpha)\pi(w) = \begin{bmatrix} 0 & 1 \\ -1 & \alpha \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} c & d \\ -a+\alpha c & -b+\alpha d \end{bmatrix}.$$

Then $\alpha w \in \bar{\mathcal{A}}^{l+1} \Leftrightarrow -b + \alpha d \equiv 0 \mod N$. This congruence equation has a solution $\Leftrightarrow \gcd(d, N) | b$. We claim that $\gcd(d, N) | b$ is equivalent to $\gcd(d, N) = 1$ and the theorem can easily be deduced. It is obvious that $\gcd(d, N) = 1$ implies $\gcd(d, N) | b$. If $\gcd(d, N) | b$, then $\gcd(d, N)$ is a common divisor of d and b. Since $ad - bc = 1$, $\gcd(d, N) \leq \gcd(d, b) = 1$, so $\gcd(d, N) = 1$. Hence we have the claim. □

Theorem 3.1.5. *If* $\alpha_1 \dots \alpha_l \in \bar{\mathcal{A}}^l$, *then* $\alpha_2 \dots \alpha_l$ *and* $\alpha_1 \dots \alpha_{l-1} \in \bar{\mathcal{C}}^{l-1}$.

Proof. Assume that $\alpha_1 \dots \alpha_l \in \bar{\mathcal{A}}^l$. Then $\pi(\alpha_1 \dots \alpha_l) = \begin{bmatrix} a & b \\ -b^{-1} & 0 \end{bmatrix}$ for some $a \in \mathbb{Z}/N\mathbb{Z}$ and $b \in (\mathbb{Z}/N\mathbb{Z})^\times$. Thus

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

and

$$\pi(\alpha_1 \dots \alpha_{l-1}) = \pi(\alpha_1 \dots \alpha_l)\pi(\alpha_l)^{-1} = \begin{bmatrix} a & b \\ -b^{-1} & 0 \end{bmatrix} \begin{bmatrix} \alpha_l & -1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} \alpha_l a + b & -a \\ -\alpha_l b^{-1} & b^{-1} \end{bmatrix}.$$

Since $b \neq 0$, $\alpha_2 \dots \alpha_l$ and $\alpha_1 \dots \alpha_{l-1} \in \bar{C}^{l-1}$. □

Other properties of words in $\bar{A}$ are given in the following theorems. Some result will be used in the next section.

Theorem 3.1.6. *$\alpha_1\alpha_2 \dots \alpha_l \in \bar{A}^l$ if and only if $\alpha_l\alpha_{l-1} \dots \alpha_1 \in \bar{A}^l$.*

Proof. Consider $\sigma = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ and $\alpha_1 \dots \alpha_l \in F_N$ with $\pi(\alpha_1 \dots \alpha_l) = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ in $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. Since $\sigma \begin{bmatrix} w & x \\ y & z \end{bmatrix} \sigma = \begin{bmatrix} z & y \\ x & w \end{bmatrix}$ for all $w, x, y, z \in \mathbb{Z}/N\mathbb{Z}$ and $\sigma = \sigma^{-1}$, we have

$$\begin{aligned} \begin{bmatrix} d & c \\ b & a \end{bmatrix} &= \sigma\pi(\alpha_1\alpha_2 \dots \alpha_l)\sigma = (\sigma\pi(\alpha_1)\sigma)(\sigma\pi(\alpha_2)\sigma) \dots (\sigma\pi(\alpha_l)\sigma) \\ &= \begin{bmatrix} \alpha_1 & -1 \\ 1 & 0 \end{bmatrix} \dots \begin{bmatrix} \alpha_l & -1 \\ 1 & 0 \end{bmatrix} = \left(\begin{bmatrix} 0 & 1 \\ -1 & \alpha_l \end{bmatrix} \dots \begin{bmatrix} 0 & 1 \\ -1 & \alpha_1 \end{bmatrix} \right)^{-1} \\ &= \pi(\alpha_l \dots \alpha_1)^{-1}, \end{aligned}$$

so $\pi(\alpha_l \dots \alpha_1) = \begin{bmatrix} a & -c \\ -b & d \end{bmatrix}$. Thus $\alpha_1\alpha_2 \dots \alpha_l \in \bar{A}^l \Leftrightarrow d = 0 \Leftrightarrow \alpha_l\alpha_{l-1} \dots \alpha_1 \in \bar{A}^l$.

□

Theorem 3.1.7. *$\alpha_1 \dots \alpha_l \in \bar{\mathcal{A}}^l$ if and only if $(-\alpha_1) \dots (-\alpha_l) \in \bar{\mathcal{A}}^l$.*

Proof. Let $\alpha_1 \dots \alpha_l \in F_N$ with $\pi(\alpha_1 \dots \alpha_l) = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. Note that

$$\pi((-\alpha_l)\dots(-\alpha_1)) = \begin{bmatrix} 0 & 1 \\ -1 & -\alpha_l \end{bmatrix} \dots \begin{bmatrix} 0 & 1 \\ -1 & -\alpha_1 \end{bmatrix} = (-1)^l \begin{bmatrix} 0 & -1 \\ 1 & \alpha_l \end{bmatrix} \dots \begin{bmatrix} 0 & -1 \\ 1 & \alpha_1 \end{bmatrix}$$

$$= (-1)^l \left(\begin{bmatrix} 0 & 1 \\ -1 & \alpha_1 \end{bmatrix} \dots \begin{bmatrix} 0 & 1 \\ -1 & \alpha_l \end{bmatrix} \right)^T = (-1)^l \pi(\alpha_1 \dots \alpha_l)^T = (-1)^l \begin{bmatrix} a & c \\ b & d \end{bmatrix}.$$

Then $\pi((-\alpha_1)\dots(-\alpha_l)) = (-1)^l \begin{bmatrix} a & -b \\ -c & d \end{bmatrix}$ as we have shown in the proof of Theorem 3.1.6. Hence $\alpha_1 \dots \alpha_l \in \bar{\mathcal{A}}^l \Leftrightarrow d = 0 \Leftrightarrow (-\alpha_1)\dots(-\alpha_l) \in \bar{\mathcal{A}}^l$. □

The partition $\bar{\mathcal{A}}$ and $\bar{\mathcal{C}}$ of F_k also induces the equivalence relation $\sim$ on F_k. We record some relationships between two words in the next theorem.

Theorem 3.1.8. *Let $x \in F_N$ and $\beta \in \mathbb{Z}/N\mathbb{Z}$. We have*

(i) *If $\alpha \in (\mathbb{Z}/N\mathbb{Z})^\times$, then $\alpha\beta x \sim (\beta - \alpha^{-1})x$.*

(ii) *$0\beta x \sim x$.*

Proof. Let $\pi(x) = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ and $\beta \in \mathbb{Z}/N\mathbb{Z}$.

(i) Assume that $\alpha \in (\mathbb{Z}/N\mathbb{Z})^\times$. Then

$$\pi(\alpha\beta x) = \begin{bmatrix} 0 & 1 \\ -1 & \alpha \end{bmatrix} \begin{bmatrix} 0 & 1 \\ -1 & \beta \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} -a + \beta c & -b + \beta d \\ -\alpha a - c + \alpha\beta c & -\alpha b - d + \alpha\beta d \end{bmatrix}$$

and

$$\pi((\beta - \alpha^{-1})x) = \begin{bmatrix} 0 & 1 \\ -1 & \beta - \alpha^{-1} \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} c & d \\ -a + (\beta - \alpha^{-1})c & -b + (\beta - \alpha^{-1})d \end{bmatrix}.$$

Thus

$$\begin{aligned}\alpha\beta x \in \bar{\mathcal{A}} &\Leftrightarrow -\alpha b - d + \alpha\beta d = 0 \\ &\Leftrightarrow -b + (\beta - \alpha^{-1})d = 0 \\ &\Leftrightarrow (\beta - \alpha^{-1})x \in \bar{\mathcal{A}},\end{aligned}$$

so $\alpha\beta x \sim (\beta - \alpha^{-1})x$.

(ii) Since $\pi(0\beta x) = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ -1 & \beta \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} -a+\beta c & -b+\beta d \\ -c & -d \end{bmatrix}$, $0\beta x \in \bar{\mathcal{A}}$ $\Leftrightarrow d = 0 \Leftrightarrow x \in \bar{\mathcal{A}}$, so $0\beta x \sim x$. □

Remark. The above theorem yields partial answers for determination of words into classes $\bar{\mathcal{A}}$ and $\bar{\mathcal{C}}$. However, a good mathematical software such as Maple™ can easily compute the product of 2×2 matrices modulo positive integer N. This allows us to directly distinguish words in F_N.

Some numerical examples are given in

Example 3.1.9. The following boxes display the sets $\bar{\mathcal{A}}^l$ for $l \leq 3$ of words over

1. $\mathbb{Z}/4\mathbb{Z}$.

$$\begin{aligned}&\bar{\mathcal{A}}^0 = \{\} \\ &\bar{\mathcal{A}}^1 = \{0\} \\ &\bar{\mathcal{A}}^2 = \{11, 33\} \\ &\bar{\mathcal{A}}^3 = \{000, 010, 020, 030, 103, 121, 202, 212, 222, 232, 301, 323\}\end{aligned}$$

2. $\mathbb{Z}/6\mathbb{Z}$.

$$\begin{aligned}
&\bar{\mathcal{A}}^0 = \{\} \\
&\bar{\mathcal{A}}^1 = \{0\} \\
&\bar{\mathcal{A}}^2 = \{11, 55\} \\
&\bar{\mathcal{A}}^3 = \{000, 010, 020, 030, 040, 050, 105, 121, 204, 212, 234, \\
&\qquad 242, 303, 323, 343, 402, 424, 432, 454, 501, 545\}
\end{aligned}$$

3.2 More on $\bar{\mathcal{A}}$

We concentrate more on $\bar{\mathcal{A}}$ and record its further properties in this last section. This work includes unique factorization, predecessors, successors and periodic words. We also conclude this chapter by numerical examples.

In order to prove the fact about unique factorization on $\bar{\mathcal{A}}$, we start with the following lemma.

Lemma 3.2.1. (i) *If $w, w' \in \bar{\mathcal{A}}$ then $ww' \in \bar{\mathcal{C}}$ and $w\alpha w' \in \bar{\mathcal{A}}$ for any $\alpha \in \mathbb{Z}/N\mathbb{Z}$.* (ii) *If exactly one of w, w' is an element of $\bar{\mathcal{A}}$ then $w\alpha w' \in \bar{\mathcal{C}}$ for any $\alpha \in \mathbb{Z}/N\mathbb{Z}$.*

Proof. To prove (i), let $\pi(w) = \begin{bmatrix} a & b \\ -b^{-1} & 0 \end{bmatrix}$ and $\pi(w') = \begin{bmatrix} a' & b' \\ -b'^{-1} & 0 \end{bmatrix}$ for some $a, a' \in \mathbb{Z}/N\mathbb{Z}$, $b, b' \in (\mathbb{Z}/N\mathbb{Z})^\times$, and let $\alpha \in \mathbb{Z}/N\mathbb{Z}$. Then

$$\pi(ww') = \begin{bmatrix} a & b \\ -b^{-1} & 0 \end{bmatrix} \begin{bmatrix} a' & b' \\ -b'^{-1} & 0 \end{bmatrix} = \begin{bmatrix} aa' - bb'^{-1} & ab' \\ -a'b^{-1} & -b^{-1}b' \end{bmatrix},$$

and

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

Thus $w\alpha w' \in \bar{\mathcal{A}}$ for any $\alpha \in \mathbb{Z}/N\mathbb{Z}$. Since $b, b' \in (\mathbb{Z}/N\mathbb{Z})^\times$, $ww' \in \bar{\mathcal{C}}$.

To prove (ii), suppose that $w \in \bar{\mathcal{A}}$ and $w' \in \bar{\mathcal{C}}$ and let $\alpha \in \mathbb{Z}/N\mathbb{Z}$. Then $\pi(w) = \begin{bmatrix} a & b \\ -b^{-1} & 0 \end{bmatrix}$ for some $a \in \mathbb{Z}/N\mathbb{Z}$ and $b \in (\mathbb{Z}/N\mathbb{Z})^\times$, and $\pi(w') = \begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix}$ in $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ with $d' \neq 0$. Thus

$$\pi(w\alpha w') = \begin{bmatrix} a & b \\ -b^{-1} & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ -1 & \alpha \end{bmatrix} \begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix} = \begin{bmatrix} -ba' + ac' + \alpha bc' & -bb' + ad' + \alpha bd' \\ -b^{-1}c' & -b^{-1}d' \end{bmatrix}.$$

Since $b \in (\mathbb{Z}/N\mathbb{Z})^\times$ and $d' \neq 0$, $w\alpha w' \in \bar{\mathcal{C}}$. For another case, let $w = \beta_1 \dots \beta_m \in \bar{\mathcal{C}}$ and $w' = \beta_1' \dots \beta_n' \in \bar{\mathcal{A}}$ for some positive integers m and n. By Theorem 3.1.6, we have $\beta_n' \dots \beta_1' \in \bar{\mathcal{A}}$ and $\beta_m \dots \beta_1 \in \bar{\mathcal{C}}$. The previous proof shows that

$$\beta_n' \dots \beta_1' \alpha \beta_m \dots \beta_1 \in \bar{\mathcal{C}}.$$

Thus we get $w\alpha w' = \beta_1 \dots \beta_m \alpha \beta_1' \dots \beta_n' \in \bar{\mathcal{C}}$ by Theorem 3.1.6. □

Let $\mathcal{P}^l = \{\alpha_1\alpha_2 \dots \alpha_l \in \bar{\mathcal{A}}^l : \alpha_1 \dots \alpha_h \in \bar{\mathcal{C}}^h \text{ for } h = 1, \dots, l-1\}$ and $\mathcal{P} = \bigcup \mathcal{P}^l$.

Theorem 3.2.2. [Unique Factorization in $\bar{\mathcal{A}}$] *Let $w \in F_N$. Then $w \in \bar{\mathcal{A}}$ 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 $\delta_1, \dots, \delta_n \in \mathbb{Z}/N\mathbb{Z}$. Moreover, such a factorization of $w \in \bar{\mathcal{A}}$ is unique.

Proof. Suppose that w can be written as in this form. By Lemma 3.2.1, it is easy to see that $w \in \bar{\mathcal{A}}$. Conversely, assume that $w = \alpha_1\alpha_2 \dots \alpha_l \in \bar{\mathcal{A}}^l$. Then there is the smallest positive integer s such that $\alpha_1 \dots \alpha_s \in \bar{\mathcal{A}}$. Setting $p_1 = \alpha_1 \dots \alpha_s \in \mathcal{P}$ and $\delta_1 = \alpha_{s+1}$. Thus $\alpha_{s+2}\alpha_{s+3} \dots \alpha_l$ must be in $\bar{\mathcal{A}}^{l-(s+1)}$ by Lemma 3.2.1. Repeating this process we get the sets $\{\delta_1, \dots, \delta_n\} \subset \mathbb{Z}/N\mathbb{Z}$ and $\{p_1, \dots, p_{n+1}\} \subset \mathcal{P}$ so that

$w = p_1\delta_1 p_2\delta_2 \dots p_n\delta_n p_{n+1}$ for some $n \geq 0$. The smallest length of p_i for each i implies the uniqueness of this factorization. □

Given two words $w, w' \in F_N$ of the form

$$w = \alpha_0\alpha_1 \dots \alpha_{l-1} \quad \text{and} \quad w' = \alpha_1\alpha_2 \dots \alpha_l,$$

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

Theorem 3.2.3. *Each element $w \in \bar{\mathcal{A}}^l$ has a unique immediate successor and a unique immediate predecessor in $\bar{\mathcal{A}}^l$.*

Proof. Assume that $\alpha_0\alpha_1 \dots \alpha_{l-1} \in \bar{\mathcal{A}}^l$. Then $\pi(\alpha_0\alpha_1 \dots \alpha_{l-1}) = \begin{bmatrix} a & b \\ -b^{-1} & 0 \end{bmatrix}$ for some $a \in \mathbb{Z}/N\mathbb{Z}$ and $b \in (\mathbb{Z}/N\mathbb{Z})^\times$. Thus

$$\begin{aligned} \pi(\alpha_1\alpha_2 \dots \alpha_{l-1}) &= \pi(\alpha_0)^{-1}\pi(\alpha_0\alpha_1 \dots \alpha_{l-1}) \\ &= \begin{bmatrix} \alpha_0 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} a & b \\ -b^{-1} & 0 \end{bmatrix} = \begin{bmatrix} \alpha_0 a + b^{-1} & \alpha_0 b \\ a & b \end{bmatrix}, \end{aligned}$$

so

$$\begin{aligned} \pi(\alpha_1\alpha_2 \dots \alpha_l) &= \pi(\alpha_1\alpha_2 \dots \alpha_{l-1})\pi(\alpha_l) \\ &= \begin{bmatrix} \alpha_0 a + b^{-1} & \alpha_0 b \\ a & b \end{bmatrix} \begin{bmatrix} 0 & 1 \\ -1 & \alpha_l \end{bmatrix} = \begin{bmatrix} -\alpha_0 b & \alpha_0 a + b^{-1} + \alpha_0\alpha_l b \\ -b & a + \alpha_l b \end{bmatrix}. \end{aligned}$$

Since $b \in (\mathbb{Z}/N\mathbb{Z})^\times$, $\alpha_1\alpha_2 \dots \alpha_l \in \bar{\mathcal{A}}^l \Leftrightarrow \alpha_l = -ab^{-1}$. Hence w has a unique immediate successor in $\bar{\mathcal{A}}^l$. Similarly, we can show that w also has a unique immediate predecessor in $\bar{\mathcal{A}}^l$. □

For $w = \alpha_1\alpha_2 \dots \alpha_l \in \bar{\mathcal{A}}^l$, by Theorem 3.2.3 there exists an infinite word

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

such that $\alpha_{i+1} \dots \alpha_{i+l}$ is the immediate successor in $\bar{\mathcal{A}}^l$ of $\alpha_i \dots \alpha_{i+l-1}$ for all integer i. That is, all subwords formed by l consecutive letters of W are elements in $\bar{\mathcal{A}}^l$. Since $\bar{\mathcal{A}}^l$ is finite, the infinite word W associated to w is periodic. Hence for every $w \in \bar{\mathcal{A}}^l$, there exists the smallest positive integer s such that the infinite word W associated to w is s-periodic.

Example 3.2.4. Some infinite periodic words over $\mathbb{Z}/6\mathbb{Z}$.

1. The infinite periodic word corresponding to both 0 and 000 is a 1-periodic word $\dots 000 \dots$.

2. The infinite periodic words corresponding to 11 and 55 are 1-periodic words $\dots 111 \dots$ and $\dots 555 \dots$, respectively.

3. The infinite periodic word corresponding to both 121 and 212 is a 2-periodic word $\dots 1212 \dots$.

4. The infinite periodic word corresponding to $234, 343$ and 432 is a 4-periodic word $\dots 23432343 \dots$.

Theorem 3.2.5. *Let $W = \dots \alpha_{s-1}\alpha_0\alpha_1 \dots \alpha_{s-1}\alpha_0\alpha_1 \dots$ be an infinite s-periodic word with letters in $\mathbb{Z}/N\mathbb{Z}$. Then there exists a smallest positive integer t such that all subwords of length $ts-1$ in W belong to $\bar{\mathcal{A}}$. Moreover, all subwords of length $lts-1$ $(l \geq 1)$ of W belong to $\bar{\mathcal{A}}$.*

Proof. We observe that the elements

$$\pi(\alpha_0\alpha_1 \dots \alpha_{s-1}), \pi(\alpha_1 \dots \alpha_{s-1}\alpha_0), \dots, \pi(\alpha_{s-1}\alpha_0 \dots \alpha_{s-2}) \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$$

are all conjugate. Then they have a common order $t' \geq 1$, we claim that t' has the desired property. Let w be a subword of length $t's$ in W. Thus $w = \underbrace{w'w' \dots w'}_{t' \text{ copies}}$

where w' is a subword of length s in W, so

$$\pi(w) = \pi(\underbrace{w'w'\dots w'}_{t' \text{ copies}}) = (\pi(w'))^{t'} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Assume that $w = \beta_1 \dots \beta_{t's}$. The subword of length $t's - 1$ associated with w is in $\bar{\mathcal{A}}$ as a result of $\pi(\beta_1 \dots \beta_{t's-1}) = \pi(w)\pi(\beta_{t's})^{-1} = \begin{bmatrix} \beta_{t's} & -1 \\ 1 & 0 \end{bmatrix}$. Hence $t \leq t'$ exists by the well-ordering principle. □

Remark. In the above proof, sometimes $t < t'$. For example, consider the infinite 1-periodic word, $\dots 000 \dots$. The order of $\pi(0) = 4$ but we can choose $t = 2$ since $0 \in \bar{\mathcal{A}}$. Moreover, since t' divides $|\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})|$, we know that $t \leq |\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})|$.

Example 3.2.6. In $\mathbb{Z}/6\mathbb{Z}$, consider the 4-periodic word $W = \dots 23432343 \dots$.

1. We have $t = 1$ so that all subwords of length $4(1) - 1 = 3$ in W belong to $\bar{\mathcal{A}}$.
   $(234, 343, 432, 323)$

2. For $l = 2$, all subwords of length $4(2) - 1 = 7$ in W belong to $\bar{\mathcal{A}}$.
   $(2343234, 3432343, 4323432, 3234323)$

3. For $l = 3$, all subwords of length $4(3) - 1 = 11$ in W belong to $\bar{\mathcal{A}}$.
   $(23432343234, 34323432343, 43234323432, 32343234323)$