CHAPTER II

EQUIVALENCE RELATIONS ON WORDS OVER FINITE FIELDS

This chapter consists of two sections. The first section presents the preliminary properties of words in $\mathcal{A}_r$ and results on the cardinalities of $\mathcal{A}_r$ and $\mathcal{C}_r$. In the last section, we study the equivalence relations $\sim_r, r \in k$, induced from the partition $\mathcal{A}_r$ and $\mathcal{C}_r$ of F_k and we give numerical examples to demonstrate our theorem.

2.1 Cardinalities of $\mathcal{A}_r$ and $\mathcal{C}_r$

For $w \in F_k$ with $\pi(w) = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(k)$, we note that

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

$$\Leftrightarrow \pi(w) = \begin{bmatrix} a & b \\ ar - b^{-1} & br \end{bmatrix} \text{ with } a \in k, b \in k^{\times}.$$

Therefore we have shown

Theorem 2.1.1. *For $r \in k$,*

$$\mathcal{A}_r = \left\{ w \in F_k : \pi(w) = \begin{bmatrix} a & b \\ ar - b^{-1} & br \end{bmatrix} \textit{ for some } a \in k, b \in k^{\times} \right\}.$$

The set $\mathcal{A}_0$ has been studied by Bacher in [2]. Our results are for the case $r \neq 0$. For $l \geq 0$, we write F_k^l for the set of words over k of length l, $\mathcal{A}_r^l = F_k^l \cap \mathcal{A}_r$ and $\mathcal{C}_r^l = F_k^l \cap \mathcal{C}_r$. Unless specified, we assume $r \in k^\times$ throughout this section. We begin with the right insertion.

Theorem 2.1.2. *Let $w \in F_k$. Then $w \in \mathcal{A}_r^l$ if and only if $w\alpha \in \mathcal{C}_r^{l+1}$ for all $\alpha \in k$. Moreover, if $w \in \mathcal{C}_r^l$, then there exists a unique $\alpha \in k$ such that $w\alpha \in \mathcal{A}_r^{l+1}$.*

Proof. Assume that $w \in \mathcal{A}_r^l$ and let $\alpha \in k$. Then $\pi(w) = \begin{bmatrix} a & b \\ ar - b^{-1} & br \end{bmatrix}$ for some $a \in k$ and $b \in k^\times$. Thus

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

If $ar - b^{-1} + \alpha br = (a + \alpha b)r$, then $-b^{-1} = 0$, a contradiction. Thus $w\alpha \in \mathcal{C}_r^{l+1}$. Conversely, suppose that $w \in \mathcal{C}_r^l$. Then $\pi(w) = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(k)$ and $d \neq br$. Note that for $\alpha \in k$, we have

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

Since $d \neq br$, we can choose a unique α, namely $\alpha = (ar - c)(d - br)^{-1} \in k$ such that $\pi(w\alpha) = \begin{bmatrix} -b & (d - br)^{-1} \\ -d & r(d - br)^{-1} \end{bmatrix}$ and hence $w\alpha \in \mathcal{A}_r^{l+1}$. □

For the left insertion, we obtain a slightly different property.

Theorem 2.1.3. *Let $w \in F_k$ with $\pi(w) = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(k)$.*

(i) *If $w \in \mathcal{C}_r^l$, then $d = 0$ if and only if $\alpha w \in \mathcal{C}_r^{l+1}$ for all $\alpha \in k$.*

(ii) *If $w \in \mathcal{A}_r^l$, then there exists a unique $\alpha \in k$ such that $\alpha w \in \mathcal{A}_r^{l+1}$.*

Proof. We first observe that for $\alpha \in k$,

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

(i) Assume that $w \in \mathcal{C}_r^l$. If $d = 0$, then $b \neq 0$, so $\pi(\alpha w) = \begin{bmatrix} c & 0 \\ -a + \alpha c & -b \end{bmatrix}$ and thus $\alpha w \in \mathcal{C}_r^{l+1}$. If $d \neq 0$, then there exists $\alpha = (b + dr)d^{-1}$ such that $\pi(\alpha w) = \begin{bmatrix} c & d \\ -d^{-1} + cr & dr \end{bmatrix}$ which implies $\alpha w \in \mathcal{A}_r^{l+1}$.

(ii) Assume that $w \in \mathcal{A}_r^l$. Then $d = br$. A simple calculation yields a unique $\alpha = r + r^{-1}$ such that $\pi(\alpha w) = \begin{bmatrix} c & br \\ -a + c(r + r^{-1}) & br^2 \end{bmatrix}$ which means $\alpha w \in \mathcal{A}_r^{l+1}$. □

Next we present results on left and right deletions of a word $w \in \mathcal{A}_r$.

Theorem 2.1.4. *Let $\alpha_1 \dots \alpha_l \in \mathcal{A}_r^l$. Then $\alpha_1 \dots \alpha_{l-1} \in \mathcal{C}_r^{l-1}$, and $\alpha_2 \dots \alpha_l \in \mathcal{A}_r^{l-1}$ if and only if $\alpha_1 = r + r^{-1}$.*

Proof. Assume that $\alpha_1 \dots \alpha_l \in \mathcal{A}_r^l$. Then $\pi(\alpha_1 \dots \alpha_l) = \begin{bmatrix} a & b \\ ar - b^{-1} & br \end{bmatrix}$ for some $a \in k$ and $b \in k^\times$. Thus

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

Since $b^{-1} \neq 0$, $b^{-1} - ar \neq -ar$ and so $\alpha_1 \dots \alpha_{l-1} \in \mathcal{C}_r^{l-1}$. Hence

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

Therefore $\alpha_2 \dots \alpha_l \in \mathcal{A}_r^{l-1} \Leftrightarrow b = (\alpha_1 b - br)r \Leftrightarrow \alpha_1 = r + r^{-1}$. □

Theorem 2.1.2 results in $|\mathcal{A}_r^{l+1}| \geq |\mathcal{C}_r^l|$ and Theorem 2.1.4 (i) gives rise to $|\mathcal{A}_r^{l+1}| \leq |\mathcal{C}_r^l|$. Thus $|\mathcal{A}_r^{l+1}| = |\mathcal{C}_r^l|$. Since $|\mathcal{A}_r^l| + |\mathcal{C}_r^l| = q^l$, we get the recurrence relation

$$|\mathcal{A}_r^{l+1}| + |\mathcal{A}_r^l| = q^l \text{ for } l \geq 0 \quad \text{and} \quad |\mathcal{A}_r^0| = 0.$$

Solving this relation, we obtain the cardinalities of $\mathcal{A}_r^l$ and $\mathcal{C}_r^l$ for all $l \geq 0$. It should be pointing out that Bacher had the same numbers for $r = 0$ in [2] Corollary 2.3. We record this result in

Corollary 2.1.5. *For a finite field k with q elements, $l \geq 0$ and $r \in k$, we have*

$$|\mathcal{A}_r^l| = \frac{q^l - (-1)^l}{q+1} \quad \textit{and} \quad |\mathcal{C}_r^l| = \frac{q^{l+1} + (-1)^l}{q+1}.$$

Other miscellaneous properties of words in $\mathcal{A}_r$ are given in the following theorem.

Theorem 2.1.6. *Let $\alpha_1\alpha_2 \dots \alpha_l \in \mathcal{A}_r^l$ so that $\pi(\alpha_1\alpha_2 \dots \alpha_l) = \begin{bmatrix} a & b \\ ar - b^{-1} & br \end{bmatrix}$ for some $a \in k, b \in k^\times$. Then*

(i) *$\alpha_l\alpha_{l-1} \dots \alpha_1 \in \mathcal{A}_r^l$ if and only if $a = (b^{-1} - b)r^{-1}$.*

(ii) *$(-\alpha_1) \dots (-\alpha_l) \in \mathcal{A}_r^l$ if and only if k is of characteristic two.*

Proof. Assume that $\alpha_1\alpha_2\dots\alpha_l \in \mathcal{A}_r^l$ with $\pi(\alpha_1\alpha_2\dots\alpha_l) = \begin{bmatrix} a & b \\ ar-b^{-1} & br \end{bmatrix}$ for some $a \in k, b \in k^\times$.

(i) Let $\sigma = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$. Since $\sigma \begin{bmatrix} w & x \\ y & z \end{bmatrix} \sigma = \begin{bmatrix} z & y \\ x & w \end{bmatrix}$ for all $w, x, y, z \in k$ and $\sigma = \sigma^{-1}$, we have

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

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

so $\pi(\alpha_l\dots\alpha_1) = \begin{bmatrix} a & -ar+b^{-1} \\ -b & br \end{bmatrix}$. Thus $\alpha_l\alpha_{l-1}\dots\alpha_1 \in \mathcal{A}_r^l \Leftrightarrow (b^{-1}-ar)r = br$ $\Leftrightarrow a = (b^{-1}-b)r^{-1}$.

(ii) Since

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

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

$$= (-1)^l\begin{bmatrix} a & ar-b^{-1} \\ b & br \end{bmatrix},$$

$\pi((-\alpha_1)\dots(-\alpha_l)) = (-1)^l\begin{bmatrix} a & -b \\ b^{-1}-ar & br \end{bmatrix}$ as we have shown in the proof of (i). Thus $(-\alpha_1)\dots(-\alpha_l) \in \mathcal{A}_r^l \Leftrightarrow 2br = 0 \Leftrightarrow k$ is of characteristic two as $b, r \in k^\times$. □

2.2 Induced Equivalence Relations

The partition $\mathcal{A}_r$ and $\mathcal{C}_r$ of F_k induces the equivalence relation $\sim_r$ on F_k. Its properties are studied in our next theorem.

Theorem 2.2.1. *Let $x \in F_k$ and $\beta \in k$. We have*
(i) *If $\alpha \in k$ and $\alpha \neq r$, then $\alpha\beta x \sim_r \gamma x$ where $\gamma = \dfrac{r^2 - (\alpha - \beta)r + 1 - \alpha\beta}{r - \alpha}$.*
(ii) *$r\beta x \in \mathcal{A}_r$ if and only if $x \in \mathcal{A}_0$.*

Proof. Let $\pi(x) = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(k)$ and $\beta \in k$.
(i) Assume that $\alpha \in k$ and $\alpha \neq r$. 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

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

Thus

$$\begin{aligned}
\alpha\beta x \in \mathcal{A}_r &\Leftrightarrow (-b + \beta d)r = -\alpha b - d + \alpha\beta d \\
&\Leftrightarrow -br + \beta dr = -\alpha b - d + \alpha\beta d \\
&\Leftrightarrow dr^2 - \alpha dr = -br + \alpha b + dr^2 - (\alpha - \beta)dr + (1 - \alpha\beta)d \\
&\Leftrightarrow dr = -b + \frac{(r^2 - (\alpha - \beta)r + 1 - \alpha\beta)}{r - \alpha}d,
\end{aligned}$$

so $\alpha\beta x \sim_r \gamma x$ where $\gamma = \dfrac{(r^2 - (\alpha - \beta)r + 1 - \alpha\beta)}{r - \alpha}$.
(ii) Since $\pi(r\beta x) = \begin{bmatrix} 0 & 1 \\ -1 & r \end{bmatrix} \begin{bmatrix} 0 & 1 \\ -1 & \beta \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} -a + \beta c & -b + \beta d \\ -c - ar + \beta rc & -d - br + \beta rd \end{bmatrix}$,
$r\beta x \in \mathcal{A}_r \Leftrightarrow (-b + \beta d)r = -d - br + \beta rd \Leftrightarrow d = 0 \Leftrightarrow x \in \mathcal{A}_0$. □

Remark. This result leads to an algorithm to distinguish words in F_k. It extends Bacher's work on $\sim_0$ in [2] Proposition 2.4 (ii) to $\sim_r, r \in k$. Note that $\alpha \sim_r \varepsilon \Leftrightarrow \alpha \neq r$. Combined with Theorem 2.2.1, we completely classify all words into the partition $\mathcal{A}_r$ and $\mathcal{C}_r$ of F_k.

We illustrate Theorem 2.2.1 and the above remark by the following numerical examples.

Example 2.2.2. Let $k = \mathbb{F}_3$. Consider $22102 \in F_k$.

$r = 0$. By Theorem 2.2.1 (i), $22102 \sim_0 (2 - 2^{-1})102 = 0102$. By Theorem 2.2.1 (ii), $0102 \sim_0 02 \sim_0 \varepsilon$. Then we have $22102 \in \mathcal{C}_0$.

$r = 1$. By Theorem 2.2.1 (i),

$$\begin{aligned} 22102 &\sim_1 \left[\frac{1^2 - (2-2)1 + 1 - 2 \cdot 2}{1-2}\right] 102 = 2102 \\ &\sim_1 \left[\frac{1^2 - (2-1)1 + 1 - 2 \cdot 1}{1-2}\right] 02 = 102. \end{aligned}$$

Since $2 \in \mathcal{C}_0$, $102 \in \mathcal{C}_1$ by Theorem 2.2.1 (ii). Then we have $22102 \in \mathcal{C}_1$.

$r = 2$. By Theorem 2.2.1 (ii), we first consider

$$102 \sim_0 (0 - 1^{-1})2 = 22 \sim_0 (2 - 2^{-1})\varepsilon = 0.$$

Then $102 \in \mathcal{A}_0$, so we have $22102 \in \mathcal{A}_2$.

Example 2.2.3. Let $k = \mathbb{F}_3$. The following tables display the sets $\mathcal{A}_r^l$ and $\mathcal{C}_r^l$ for $l \leq 3$ and $r = 0, 1, 2$, respectively.

$\mathcal{A}_0^0 = \{\}$	$\mathcal{C}_0^0 = \{\varepsilon\}$
$\mathcal{A}_0^1 = \{0\}$	$\mathcal{C}_0^1 = \{1, 2\}$
$\mathcal{A}_0^2 = \{11, 22\}$	$\mathcal{C}_0^2 = \{00, 01, 02, 10, 12, 20, 21\}$
$\mathcal{A}_0^3 = \{000, 010, 020, 102, 121, 201, 212\}$	$\mathcal{C}_0^3 = \{001, 002, 011, 012, 021, 022, 100, 101, 110, 111, 112, 120, 122, 200, 202, 210, 211, 220, 221, 222\}$

$\mathcal{A}_1^0 = \{\}$	$\mathcal{C}_1^0 = \{\varepsilon\}$
$\mathcal{A}_1^1 = \{1\}$	$\mathcal{C}_1^1 = \{0, 2\}$
$\mathcal{A}_1^2 = \{02, 21\}$	$\mathcal{C}_1^2 = \{00, 01, 10, 11, 12, 20, 22\}$
$\mathcal{A}_1^3 = \{001, 012, 100, 110, 120, 202, 221\}$	$\mathcal{C}_1^3 = \{000, 002, 010, 011, 020, 021, 022, 101, 102, 111, 112, 121, 122, 200, 201, 210, 211, 212, 220, 222\}$

$\mathcal{A}_2^0 = \{\}$	$\mathcal{C}_2^0 = \{\varepsilon\}$
$\mathcal{A}_2^1 = \{2\}$	$\mathcal{C}_2^1 = \{0, 1\}$
$\mathcal{A}_2^2 = \{01, 12\}$	$\mathcal{C}_2^2 = \{00, 02, 10, 11, 20, 21, 22\}$
$\mathcal{A}_2^3 = \{002, 021, 101, 112, 200, 210, 220\}$	$\mathcal{C}_2^3 = \{000, 001, 010, 011, 012, 020, 022, 100, 102, 110, 111, 120, 121, 122, 201, 202, 211, 212, 221, 222\}$