A Note on Presentation of General Linear Groups over a Finite Field

Swati Maheshwari and R. K. Sharma
Department of Mathematics, Indian Institute of Technology Delhi, New Delhi, India
Email: swatimahesh88@gmail.com; rksharmaiitd@gmail.com

Received 22 September 2016
Accepted 20 June 2018

Communicated by J.M.P. Balmaceda

AMS Mathematics Subject Classification (2000): 20F05, 16U60, 20H25

Abstract. In this article we have given Lie regular generators of linear group $GL(2, \mathbb{F}_q)$, where $\mathbb{F}_q$ is a finite field with $q = p^n$ elements. Using these generators we have obtained presentations of the linear groups $GL(2, \mathbb{F}_{2^n})$ and $GL(2, \mathbb{F}_{p^n})$ for each positive integer $n$.

Keywords: Lie regular units; General linear group; Presentation of a group; Finite field.

1. Introduction

Suppose $\mathbb{F}$ is a finite field and $GL(n, \mathbb{F})$ is the general linear the group of $n \times n$ invertible matrices and $SL(n, \mathbb{F})$ is special linear group of $n \times n$ matrices with determinant 1. We know that $GL(n, \mathbb{F})$ can be written as a semidirect product, $GL(n, \mathbb{F}) = SL(n, \mathbb{F}) \rtimes \mathbb{F}^*$, where $\mathbb{F}^*$ denotes the multiplicative group of $\mathbb{F}$. Let $H$ and $K$ be two groups having presentations $H = \langle X \mid R \rangle$ and $K = \langle Y \mid S \rangle$, then a presentation of semidirect product of $H$ and $K$ is given by,

$$H \rtimes_{\eta} K = \langle X, Y \mid R, S, xyx^{-1} = \eta(y)(x) \, \forall x \in X, y \in Y \rangle,$$

where $\eta : K \to Aut(H)$ is a group homomorphism. Now we summarize some literature survey related to the presentation of groups. In 1977, S.M. Green established a presentation of $SL(n, \mathbb{F})$ for, $n \geq 3$ (see [3]) and in 1994, T.A. Fransis has found a presentation of $GL(n, \mathbb{F})$, where $\mathbb{F}$ is a division ring (see [2]). In case $\mathbb{F}$ is a field, T.A. Fransis has also provided a presentation of $SL(n, \mathbb{F})$.
Generators for the semigroup has been provided by J. Konieczny (see [5]). A presentation of $SL(n, \mathbb{F})$ has also been given by G. Chiaselotti (see [1]). We have seen that a presentation of $SL(n, \mathbb{F})$ has been found, so we can always find one presentation of $GL(n, \mathbb{F})$ using semidirect product. In that case, cardinality of the generating set of $GL(n, \mathbb{F})$ is dependent on $\mathbb{F}$. It motivates us to find a presentation of $GL(n, \mathbb{F})$ with fix number of generators. In this article, we establish a presentation of $GL(2, \mathbb{F}_q)$ with fix number of generators, where generators are Lie regular units. These elements have been first introduced by R. K. Sharma et al. in 2012 (see [8, 4]). A generating set for $GL(4, \mathbb{Z}_n)$ has been found by S. Maheshwari and R. K. Sharma in 2016 (see [7]).

Throughout this paper, $\phi$ denotes the Euler’s totient function and $U(R)$ denotes the unit group of the ring $R$. Suppose $G$ be a group then $o(G)$ denotes the order of the group $G$.

2. Preliminaries

Here we record some well known results and basic definitions, which we shall use frequently in this note.

Lemma 2.1. The order of the special linear group $SL(2, \mathbb{F}_q)$ is $\frac{o(GL(2, \mathbb{F}_q))}{q-1}$.

Definition 2.2. An element ‘$a$’ of a ring $R$ is said to be Lie regular if $a = [e, u] = eu - ue$, where $e$ is an idempotent of $R$ and $u$ is a unit of $R$. Further, a unit in $R$ is said to be Lie regular unit if it is Lie regular as an element of $R$.

In the following lemma $e_{ij}(r)$ for $1 \leq i, j \leq n$ and $r \in \mathbb{F}_q$ denotes elementary matrix of the form $e_{ij} = I + re_{ij}$, where $e_{ij}$ denotes the matrix with 1 on the $(i,j)$-th position and 0 elsewhere and $I$ is the $n \times n$ identity matrix.

Lemma 2.3. [2, p. 944] Suppose $\mathbb{F}_q$ is a finite field. Then $SL(n, \mathbb{F}_q)$ has a presentation with generators $e_{ij}(r)$ and relations:

\( (i) \) $e_{ij}(r)e_{ij}(s) = e_{ij}(r + s)$,

\( (ii) \) $[e_{ij}(r), e_{kl}(s)] = 1$ if $i \neq l, j \neq k$,

\( (iii) \) $[e_{ij}(r), e_{jk}(s)] = e_{ik}(rs)$ if $i, j$ and $k$ are distinct, and

\( (iv) \) $ee_{ji}(r)e^{-1} = e_{ij}(-trt)$ for $e = e_{ij}(t)e_{ji}(-t^{-1})e_{ij}(t), t \in \mathbb{F}_q^*$.  

Let $\alpha$ be a primitive element of $\mathbb{F}_q$, where $q = p^n$ and $1 \leq i, j \leq q - 1$. For convenience, we rewrite the above presentation in new symbols as follows:
Corollary 2.4. Let
\[ a_i = \begin{pmatrix} 1 & \alpha^i \\ 0 & 1 \end{pmatrix}, \quad b_j = \begin{pmatrix} 1 & 0 \\ \alpha^j & 1 \end{pmatrix}. \]

Then SL(2, \(\mathbb{F}_{p^n}\)) is generated by \(a_i\) and \(b_j\) with these relations:

(i) \(a_i^p = 1\) and \(b_j^p = 1\),

(ii) for \(i \neq j\), we have \(a_i a_j = a_k\), \(b_i b_j = b_k\), where \(k\) is such that \(\alpha^i + \alpha^j = \alpha^k\), and \(1 \leq k \leq q - 1\),

(iii) \((a_i b_{q-1-i}^{-1} a_i)(b_j b_{q-1-j}^{-1} a_i)^{-1} = a_{2i+j}^{-1}\),

(iv) \((b_i a_{q-1-i}^{-1} b_i)(a_j a_{q-1-j}^{-1} b_i)^{-1} = b_{2i+j}^{-1}\).

Theorem 2.5. [6, Theorem 1.1] Two groups having same presentation are isomorphic.

3. Lie Regular Generators of General Linear Groups

Observe that the element
\[ a = \begin{pmatrix} 1 & 0 \\ -1 & -1 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix} \]
is a Lie regular unit in \(M_2(\mathbb{F}_q)\) and \(b = \begin{pmatrix} 0 & k \\ 1 & 0 \end{pmatrix}\), where \(k\) is invertible in \(\mathbb{F}_q\), is also a Lie regular unit in \(M_2(\mathbb{F}_q)\) (see [8, Proposition 2.14]).

Theorem 3.1. Suppose \(\mathbb{F}_{2^n}\) is a finite field and \(\alpha \in \mathbb{F}_{2^n}^*\) is a primitive element i.e. \(o(\alpha) = 2^n - 1\). Then the linear group GL(2, \(\mathbb{F}_{2^n}\)) is generated by Lie regular units \(a, b\) and \(c\), where
\[ a = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \quad b = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad c = \begin{pmatrix} 0 & \alpha \\ 1 & 0 \end{pmatrix}. \]

Proof. Let \(G\) be a subgroup of GL(2, \(\mathbb{F}_{2^n}\)) generated by \(a, b\) and \(c\). Set
\[ a_i = (bc)^{-i}(bab)(bc)^i = \begin{pmatrix} 1 & \alpha^i \\ 0 & 1 \end{pmatrix}, \quad b_j = (bc)^j a(bc)^{-j} = \begin{pmatrix} 1 & 0 \\ \alpha^j & 1 \end{pmatrix}, \]
where \(1 \leq i, j \leq 2^n - 1\). By using Corollary 2.4, \(a_i\) and \(b_j\) generate SL(2, \(\mathbb{F}_q\)).

Let \(x = bc = \begin{pmatrix} 1 & 0 \\ 0 & \alpha \end{pmatrix}\), then order of \(x\) is \(2^n - 1\). Consider a subgroup of \(G\),
\[ H = \langle x \mid x^{2^n-1} \rangle. \]

We see that \(H \cap SL(2, \mathbb{F}_{2^n}) = \{I_2\}\), thus
\[ o(HSL(2, \mathbb{F}_{2^n})) = (2^n - 1) o(SL(2, \mathbb{F}_{2^n})). \]

Since \( HSL(2, \mathbb{F}_{2^n}) \subseteq G \leq GL(2, \mathbb{F}_{2^n}) \) and by lemma 2.1, \( o(GL(2, \mathbb{F}_{2^n})) = (2^n - 1) o(SL(2, \mathbb{F}_{2^n})) \), as a consequence, we have \( HSL(2, \mathbb{F}_{2^n}) = GL(2, \mathbb{F}_{2^n}) \).

**Theorem 3.2.** Suppose \( F_q \) is a finite field with \( q = p^n \), where \( p \) is an odd prime and \( \alpha \in F_q^* \) is a primitive element i.e. \( o(\alpha) = q - 1 \). Then the linear group \( GL(2, F_q) \) is generated by Lie regular units \( a, b \) and \( c \), where
\[
a = \begin{pmatrix} 1 & 0 \\ -1 & -1 \end{pmatrix}, \quad b = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad c = \begin{pmatrix} 0 & \alpha \\ 1 & 0 \end{pmatrix}.
\]

**Proof.** Let \( G \) be a subgroup of \( GL(2, F_q) \) generated by \( a, b \) and \( c \). Set
\[
a_i = (bc)^{-i}(bc) \frac{\alpha^i}{(2^n - 1)} ab(ab)^i = \begin{pmatrix} 1 & \alpha^i \\ 0 & 1 \end{pmatrix},
\]
\[
b_j = (bc)^j((bc) \frac{\alpha^j}{(2^n - 1)} a(ab)^{-j} = \begin{pmatrix} 1 & 0 \\ \alpha^j & 1 \end{pmatrix},
\]
where \( 1 \leq i, j \leq q - 1 \). By using Corollary 2.4, \( a_i \) and \( b_j \) generate \( SL(2, F_q) \). Remaining proof is same as proof of Theorem .

**4. Presentation of \( GL(2, \mathbb{F}_{2^n}) \)**

In the following theorem we assume that \( 1 \leq i, j \leq 2^n - 1 \) and \( n > 1 \).

**Theorem 4.1.** Let
\[
a = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \quad b = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad c = \begin{pmatrix} 0 & \alpha \\ 1 & 0 \end{pmatrix},
\]
where \( \alpha \) is a primitive element of \( \mathbb{F}_{2^n} \). Then a presentation of \( GL(2, \mathbb{F}_{2^n}) \) is
\[
\langle a, b, c \mid a^2, b^2, c^{2(2^n - 1)}, c^2 \in \text{center}, (ab)^3, (bc)^{2^n - 1}, \quad aa_ia = (bab)b_i(ab), a_1a_2 = a_{k_0} \rangle,
\]
where \( k_0 \in \mathbb{N} \) is such that \( \alpha + \alpha^2 = \alpha^{k_0} \) and
\[
a_i = (bc)^{-i}(bab)(bc)^i = \begin{pmatrix} 1 & \alpha^i \\ 0 & 1 \end{pmatrix}, \quad b_j = (bc)^ja(bc)^{-j} = \begin{pmatrix} 1 & 0 \\ \alpha^j & 1 \end{pmatrix}.
\]

**Proof.** \( \alpha + \alpha^2 \) is non-zero element in \( \mathbb{F}_{2^n} \) for \( n > 1 \). So there exist \( k_0 \) such that \( \alpha + \alpha^2 = \alpha^{k_0} \). Let \( G \) be a group generated by \( a, b, c \) and having presentation,
\[
\langle a, b, c \mid a^2, b^2, c^{2(2^n - 1)}, c^2 \in \text{center}, (ab)^3, (bc)^{2^n - 1}, \quad aa_ia = (bab)b_i(ab), a_1a_2 = a_{k_0} \rangle.
\]
First, we shall show that \( G \) is finite. Consider a group \( H \) having the following presentation

\[
H = \langle a_i, b_j \mid a_i^2, b_j^2, a_i a_j = a_k, b_i b_j = b_k, a_i b_{2^n-1-i} b_j (a_i b_{2^n-1-i} a_i)^{-1} = a_{2i+j}, \\
(b_i a_{q-1-i} b_j) (a_j (b_i a_{q-1-i} b_j)^{-1} = b_k^{-1}) \rangle,
\]

where \( k \in \mathbb{N} \) is such that \( \alpha^i + \alpha^j = \alpha^k \). We have some observations,

(i) If \( a_1 a_2 = a_{k_0} \), then \( a_1 a_{k+1} = a_{k_0 + (k-1)} \) for \( 1 \leq k, k_0 \leq 2^n - 1 \) and \( k_0 \) is such that \( \alpha + \alpha^2 = \alpha^{k_0} \). We shall show this by induction, for \( k = 1 \) it holds. Assume for \( k = m \), \( a_m a_{m+1} = a_{k_0 + (m-1)} \), from here we get

\[
bab(bc)^{-1} = (bc)^{1-k_0} bab(bc)^{k_0-2} bab. \tag{4.1}
\]

Let \( k = m + 1 \). Then

\[
a_{m+1} a_{m+2} = (bc)^{-1-m} bab(bc)^{-1} bab(bc)^{m+2} = (bc)^{-m-k_0} bab(bc)^{m+k_0} \text{ using (4.1)} = a_{k_0 + m}.
\]

(ii) \( b_i b_j = b_i \).

(iii) \( (ab)_i^2 = 1 \).

The statement holds by using the relation \( a_1 a_i = (bab)b_i(bab) \) and the observation (1).

(iv) \( c a_i c^{-1} = b_{i-1} \).

As relations in the group \( H \) can be obtained by using above observations and relations in the group \( G \). Which implies that the group \( H \) is a subgroup of \( G \), infact it is a normal subgroup of the group \( G \). Corollary 2.4 and Theorem 2.5, give that the group \( H \) is isomorphic to \( SL(2, \mathbb{F}_{2^n}) \). Now consider the quotient group \( G/H \), we see that

\[
G/H = \langle c \mid c^{2^n-1} \rangle.
\]

and \( o(G) = o(GL(2, \mathbb{F}_{2^n})) \). This proves that \( G \cong GL(2, \mathbb{F}_{2^n}) \). \( \blacksquare \)

In \( \mathbb{F}_2 \), we see that \( \alpha = 1 \), so the element \( b \) is same as the element \( c \). Hence we have a remark for presentation of \( GL(2, \mathbb{F}_2) \).

**Remark 4.2.** A representation of \( GL(2, \mathbb{F}_2) \) is

\[
\langle a, b \mid a^2, b^2, (ab)^3 \rangle.
\]

In the following corollary we are giving a presentation of \( GL(2, \mathbb{F}_{2^n}) \), where \( 2 \leq n \leq 7, n \neq 5 \). In this case, we have a primitive polynomial, \( 1 + x + x^n \) (see [9]) and hence \( \alpha + \alpha^2 = \alpha^{n+1} \).
Corollary 4.3. A presentation of $GL(2, \mathbb{F}_{2^n})$ is
\[ \langle a, b, c \mid a^2, b^2, c^{2(q-1)}, c^2 \in \text{center}, (ab)^3, (bc)^{2^n-1}, aa, a = (bab)b_i(bab), a_1a_2 = a_{n+1} \rangle. \]

5. Presentation of $GL(2, \mathbb{F}_q)$

Theorem 5.1. Let $p$ be an odd prime, $q = p^n$ for $n \geq 1$ and $\alpha$ is a primitive element of $\mathbb{F}_q$. Let
\[ a = \begin{pmatrix} 1 & 0 \\ -1 & -1 \end{pmatrix}, b = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, c = \begin{pmatrix} 0 & \alpha \\ 1 & 0 \end{pmatrix} \]
and $a_i = (bc)^{i} \frac{q}{q-1} ab(b)^i, b_i = (bc)^i ((bc) \frac{q}{q-1} a)(bc)^{-i}$ for $1 \leq i, j \leq q-1$. Then a presentation of $GL(2, \mathbb{F}_q)$ is
\[ \langle a, b, c \mid a^2, b^2, c^{2(q-1)}, c^2 \in \text{center}, (ab)^3, ((bc) \frac{q}{q-1} a)(bc)^q \rangle, \]
\[ a_1a_2 = a_2a_1 = a_{k_0}, a'_i = a_{k'_v}, b_{q-1}b_i = b_i b_{q-1}, \]
\[ a_{q-1}^i b_{q-1}^{-1} a_{q-1}^{-1} = b(b)^{\frac{q}{q-1}}, aa_i a = a_{q-1}^{-1} b_i a_{q-1}^{-1}, \]
\[ (a_{q-1} b_{q-1}^{-1} a_{q-1}) b_m (a_{q-1} b_{q-1}^{-1} a_{q-1})^{-1} = a_m^{-1}) \]
where $k_0$ and $k'_v$ are such that $\alpha + \alpha^2 = \alpha^k_0$, $i' \alpha = \alpha^{k'_v}$ and $1 \leq k_0, k'_v, m \leq q-1$.

Proof. Let $\alpha + \alpha^2$ be not an invertible element in $\mathbb{F}_q$. Then $\alpha + \alpha^2 = 0$, it provides that $\alpha = -1$. This is the possible case when $q = 3$. We will discuss this case separately. Hence $\alpha + \alpha^2$ is invertible in $\mathbb{F}_q$, $q \neq 3$, so there exist $k_0$ such that $\alpha + \alpha^2 = \alpha^k_0$. Since $i'$ and $\alpha$ are non-zero elements of $\mathbb{F}_q$. Hence there exist $k'_v$ such that $i' \alpha = \alpha^{k'_v}$ as $i' \alpha$ is a non-zero element. Suppose $G$ is a subgroup of $GL(2, \mathbb{F}_q)$ generated by $a, b, c$ and having presentation
\[ \langle a, b, c \mid a^2, b^2, c^{2(q-1)}, c^2 \in \text{center}, (ab)^3, ((bc) \frac{q}{q-1} a)(bc)^q \rangle, \]
\[ a_1a_2 = a_2a_1 = a_{k_0}, a'_i = a_{k'_v}, b_{q-1}b_i = b_i b_{q-1}, \]
\[ a_{q-1}^i b_{q-1}^{-1} a_{q-1}^{-1} = b(b)^{\frac{q}{q-1}}, aa_i a = a_{q-1}^{-1} b_i a_{q-1}^{-1}, \]
\[ (a_{q-1} b_{q-1}^{-1} a_{q-1}) b_m (a_{q-1} b_{q-1}^{-1} a_{q-1})^{-1} = a_m^{-1}) \]
First we shall show that group $G$ is finite. Consider a subgroup $H$ of $G$ which is given by
\[ H = \langle a_i, b_j \mid a_i^2, b_j^2, a_i a_j = a_{k_i}, b_i b_j = b_{k_j}, (a_i b_{q-1}^{-1} a_j) b_j (a_i b_{q-1}^{-1} a_j)^{-1} = a_{2i+j}, (b_i a_{q-1}^{-1} b_k) a_j (b_i a_{q-1}^{-1} b_k)^{-1} = b_{2i+j} \rangle, \]
where $k \in \mathbb{N}$ is such that $\alpha^i + \alpha^j = \alpha^k, 1 \leq k \leq q-1$. We have some observations,
(i) $ba, b = b_i$.
The statement holds by using relation $b_{q-1}b_i = b_ib_{q-1}$.

By using the above observations and relations in the group $G$, we see that the relations in the group $H$ can be obtained. Hence $H$ is a subgroup of the group $G$, in fact normal subgroup of $G$. Corollary 2.4 and Theorem 2.5, give that the group $H$ is isomorphic to $SL(2, \mathbb{F}_q)$. Now we consider the quotient group $G/H$.

Case 1. When $\frac{q-1}{2}$ is even we have,

$$G/H = \langle c | c^{q-1} \rangle.$$ 

Case 2. When $\frac{q-1}{2}$ is odd we have,

$$G/H = \langle b, c | b^q, c^{\frac{q+1}{2}}, bc = cb \rangle.$$ 

In both cases we see that $o(G/H) = q - 1$. This proves that $G \cong GL(2, \mathbb{F}_q)$. ■

**Corollary 5.2.** When $q = 3$, a presentation of $GL(2, \mathbb{F}_q)$ is

$$\langle a, b, c | a^2, b^2, c^2, a^2c^2 \in center, (ab)^3, (bca)^3, (bc)^2, a^2 = a_2, b_{q-1}b_i = b_ib_{q-1}, a_{q-1}b_{q-1}a_{q-1}^{-1} = b(bc)^{\frac{q-1}{2}}, a_2a = a_{q-1}b_1a_{q-1}, (a_{q-1}b_{q-1}a_{q-1}^{-1})m(a_{q-1}b_{q-1}a_{q-1}^{-1})^{-1} = a_m^{-1} \rangle,$$

where $1 \leq m \leq 2$.

In the following corollary we are giving a presentation of $GL(2, \mathbb{F}_9)$. In this case, we have a primitive polynomial, $2 + x + x^2$.

**Corollary 5.3.** A presentation of $GL(2, \mathbb{F}_9)$ is

$$\langle a, b, c | a^2, b^2, c^{16}, a^2, c^2 \in center, (ab)^3, (bca)^3, (bc)^8, a_1a_2 = a_2a_1 = a_8, a_2^2 = a_5, b_8b_1 = b_1b_8, a_8^{-1}b_8a_8^{-1} = b(bc)^4, a_2a = a_8^{-1}b_8a_8, (a_8b_8^{-1}a_8)b_8(a_8b_8^{-1}a_8)^{-1} = a_m^{-1} \rangle.$$ 

Thus we have found presentations for $GL(2, \mathbb{F}_{2^n})$ and $GL(2, \mathbb{F}_{p^n})$ in terms of Lie regular units. The exciting thing about these generators is that these elements have a fixed form \(\begin{pmatrix} 0 & \alpha \\ 1 & 0 \end{pmatrix}\) for some $\alpha \in \mathbb{F}_q \setminus \{0\}$, except \(\begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}\) and \(\begin{pmatrix} 1 & 0 \\ -1 & -1 \end{pmatrix}\).

All results are verified with MAGMA software.

**References**


