On the group of units of the finite ring $\text{Mat}_2(\mathbb{F}^n)$

By Rhee Min Surp

Dan Kook University, Seoul, Korea

1. Introduction

Let $\text{Mat}_2(\mathbb{F}^n)$ be the set of all $2 \times 2$-matrices over a finite field with $\mathbb{F}^n$ elements. Then $\text{Mat}_2(\mathbb{F}^n)$ forms a finite ring with identity of characteristic $p$. It is well known that $\text{GL}(2, \mathbb{F}^n)$ is the group of units of $\text{Mat}_2(\mathbb{F}^n)$.

In this paper we will characterize the finite ring with identity whose group of units is isomorphic to $\text{GL}(2, \mathbb{F}^n)$, where $\mathbb{F}^n$ is a prime number. Our main theorems are the following:

**Theorem 3.2.** Let $R$ be a finite ring with identity. Suppose that the group $R^*$ of units of the ring $R$ is isomorphic to $\text{GL}(2, \mathbb{F}^n)$. Then

$$R \cong \text{Mat}_2(\mathbb{F}^n) \oplus \mathbb{Z}_2 \oplus \cdots \oplus \mathbb{Z}_2$$

**Theorem 3.4.** Let $R$ be a finite Semisimple ring with identity. Suppose that the group $R^*$ of units of the ring $R$ is isomorphic to $\text{GL}(2, \mathbb{F}^n)$. Then:

1. If $p=2$, then $R \cong \text{Mat}_2(\mathbb{F}^n) \oplus \mathbb{Z}_2 \oplus \cdots \oplus \mathbb{Z}_2$
2. If $p$ is an odd prime, then $R \cong \text{Mat}_2(\mathbb{F}^n)$.

The above theorems will be proved in Section 3. In Section 2 we will discuss some properties of a ring and the structure of the group $\text{GL}(n, q)$ which will be used in the proof of our main theorems.

There are several results in the literature, which are related to our paper. They have been proved by Gilmer, Ditor, Eldridge, and Fisher.

The notation in this paper is standard. It is taken from [3] and [4] for the groups and the rings. We will denote by $|S|$ the number of elements of a finite set $S$.

2. Preliminary results

In this section We will discuss some properties of a ring and the structure of $\text{GL}(n, q)$.

Let $R$ be a ring with identity. An element $r$ of $R$ is called a unit if $r$ has the multiplicative inverse in the ring $R$. The set of all units of a ring $R$ forms a multiplicative group, which is called the group of units of $R$ and is denoted by $R^*$. 

--- 31 ---
Let $\text{Mat}_n(F)$ be the set of all $n \times n$-matrices over a field $F$. If $F$ is the finite field with $q$ elements, we will use the symbol $\text{Mat}_n(q)$ for $\text{Mat}_n(F)$. Note that if $p$ is the characteristic of $F$, then $q$ is a power of $p$. The group $\text{GL}(n, q)$ is the group of units of $\text{Mat}_n(q)$.

The following known results are useful in the proof of our main theorems.

**Proposition 2.1.** A finite semisimple ring with identity is isomorphic to a finite direct sum of the full matrix rings over finite fields. That is, 

$$R \cong \text{Mat}_n(q_1) \oplus \cdots \oplus \text{Mat}_n(q_r),$$

where $q_i = p_i^{n_i}$ and $p_i$ is a prime number for all $i = 1, 2, \ldots, r$.

**Proof.** The proof follows from Wedderburn-Artin theorem [3, p. 13, Theorem 2.17] and Wedderburn’s theorem [1, p. 138, Theorem 3].

**Proposition 2.2.** Let $n \geq 2$ and $q = p^n$, $p$ prime. Then:

1. $\text{GL}(n, q)$ has no nontrivial normal $p$-subgroups.
2. A $Sylow$ $p$-subgroup of $\text{GL}(n, q)$ is elementary abelian if and only if $n = 2$.

**Proof.** It follows from [5, p. 54, Proposition 2.3].

**Proposition 2.3.** Let $F$ be a finite field with $p^n$ elements. Then the group $\text{SL}(2, p^n)$ is generated by two Sylow $p$-subgroups $S_1$ and $S_2$, where

$$S_1 = \left\{ \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} \middle| \lambda \in F \right\} \quad \text{and} \quad S_2 = \left\{ \begin{pmatrix} 1 & 0 \\ \lambda & 1 \end{pmatrix} \middle| \lambda \in F \right\}$$

**Proof.** This is proved in [2, p. 81, Lemma 6.1.1].

**Proposition 2.4.** Let $N$ be a normal subgroup of the group $\text{SL}(2, p^n)$, $p^n \geq 4$. If $|N| > 2$, then $N = \text{SL}(2, p^n)$.

**Proof.** The proof may be found in [5, p. 55, Proposition 2.5].

**Proposition 2.5.** Let $K$ be a normal subgroup of $\text{GL}(2, p^n)$ whose order is $|\text{SL}(2, p^n)|$. Then $K = \text{SL}(2, p^n)$.

**Proof.** Let $S_1$ and $S_2$ be Sylow $p$-subgroups which are defined in Proposition 2.3. It follows from $(\text{GL}(2, p^n) : \text{SL}(2, p^n)) = 1$ that $S_1$ and $S_2$ are Sylow $p$-subgroups of $\text{GL}(2, p^n)$. Also $K$ contains at least one Sylow $p$-subgroup $S$ of $\text{GL}(2, p^n)$ since $|K| = |\text{SL}(2, p^n)|$ and Sylow’s theorem. By Sylow’s theorem we have $xSx^{-1} = S_1$ and $ySx^{-1} = S_2$ for some $x, y \in \text{GL}(2, p^n)$. Hence $K$ contains $S_1$ and $S_2$ since $K$ is a normal subgroup of $\text{GL}(2, p^n)$. Thus $\text{SL}(2, p^n)$ is a subgroup of $K$ by Proposition 2.3. Therefore $K = \text{SL}(2, p^n)$.

3. Main theorems

In this section we will prove our main theorems.

**Proposition 3.1.** Let $R$ be a finite ring with identity of characteristic $p$, $p$ prime. Suppose that the group $R^*$ of units of the ring $R$ is isomorphic to $\text{GL}(2, p^n)$. Then:

1. If $p = 2$, then $R \cong \text{Mat}_2(2^n) \oplus \mathbb{Z}_2 \oplus \cdots \oplus \mathbb{Z}_2$.
2. If $p$ is an odd prime, then $R \cong \text{Mat}_2(p^n)$.

**Proof.** The proof may be found in [5, pp. 55-57].

**Theorem 3.2.** Let $R$ be a finite ring with identity. Suppose that the group $R^*$ of units of the ring $R$ is isomorphic to $\text{GL}(2, 2^m)$. Then
\[ R \cong \text{Mat}_2(2^m) \oplus \mathbb{Z}_2 \oplus \cdots \oplus \mathbb{Z}_2 \]

Proof. Let \( k \) be the characteristic of \( R \) and \( R_0 \) be the subring of \( R \) generated by the identity. Then \( R_0 \) is isomorphic to \( \mathbb{Z}_k \). Hence \( R_0^* \cong \mathbb{Z}_k^* \) is a subgroup of the center \( Z(R^*) \) of \( R^* \). Thus we know that \( |\mathbb{Z}_k^*| = |R_0^*| = \varphi(k) \) is a divisor of \( |Z(R^*)| = 2^m - 1 \). Hence \( \varphi(k) \) is odd and \( k = 2 \). By Proposition 3.1, this theorem holds.

Proposition 3.3. Let \( H \) be a subgroup of \( R^* \) which is isomorphic to \( SL(2, p^m) \). Then \( H \cong SL(n_1, p_1^{k_1}) \times \cdots \times SL(n_r, p_r^{k_r}) \).

Proof. It is clear that \( |SL(n_1, p_1^{k_1}) \times \cdots \times SL(n_r, p_r^{k_r})| = |SL(2, p^m)| \).

Also the group \( SL(n_1, p_1^{k_1}) \times \cdots \times SL(n_r, p_r^{k_r}) \) is a normal subgroup of \( GL(n_1, p_1^{k_1}) \times \cdots \times GL(n_r, p_r^{k_r}) \). Hence by Proposition 2.5, we have

\[ H \cong SL(n_1, p_1^{k_1}) \times \cdots \times SL(n_r, p_r^{k_r}) \]

Theorem 3.4. Let \( R \) be a finite semisimple ring with identity. Suppose that the group \( R^* \) of units of the ring \( R \) is isomorphic to \( GL(2, p^m) \). Then:

1. If \( p = 2 \), then \( R \cong \text{Mat}_2(2^m) \oplus \mathbb{Z}_2 \oplus \cdots \oplus \mathbb{Z}_2 \).
2. If \( p \) is an odd prime, then \( R \cong \text{Mat}_2(p^m) \).

Proof. Assume that \( p = 2 \). It follows from Theorem 3.2 that \( R \cong \text{Mat}_2(2^m) \oplus \mathbb{Z}_2 \oplus \cdots \oplus \mathbb{Z}_2 \).

Assume that \( p \) is an odd prime. It follows from Proposition 2.1 that \( R \cong \text{Mat}_n(p_1^{k_1}) \oplus \cdots \oplus \text{Mat}_n(p_r^{k_r}) \),

where \( p_i \) is a prime number for, \( i = 1, 2, \ldots, r \). Hence we have \( R^* \cong GL(n_1, p_1^{k_1}) \times \cdots \times GL(n_r, p_r^{k_r}) \).

Let \( H \) be the subgroup of \( R^* \) which is isomorphic to \( SL(2, p^m) \). Hence by Proposition 3.3, we have

\[ H \cong SL(n_1, p_1^{k_1}) \times \cdots \times SL(n_r, p_r^{k_r}) \]

Since \( SL(2, p^m) \) is nonabelian, there exists at least one number \( n_i \geq 2 \), say \( n_1 \). It follows from Proposition 2.4 that \( SL(n_1, p_1^{k_1}) \times \cdots \times SL(n_r, p_r^{k_r}) \) has no normal subgroup whose order is more than 2. Hence we have \( n_2 = n_3 = \cdots = n_r = 1 \) and \( k_2 = k_3 = \cdots = k_r = 0 \).

Thus \( GL(2, p^m) \cong GL(n_1, p_1^{k_1}) \). It is clear that \( m = 2 \) by Proposition 2.2.

Since \( |Z(GL(2, p^m))| = |Z(GL(2, p_1^{k_1}))| \), we have \( p^m - 1 = p_1^{k_1} - 1 \).

Hence \( p_1 = p \) and \( k_1 = m \). Therefore \( R \cong \text{Mat}_2(p^m) \).

References