Bull. Korean Math. Soc.
Vol. 15, No. 2, 1979.

A CHARACTERIZATION OF A FINITE RING $\mathrm{Mat}_2(p^m)$

BY MIN SURP RHEE

1. Introduction

Let $\mathrm{Mat}_2(p^m)$ be the set of all $n\times n$-matrices over a finite field with p^m elements, where p is a prime number. Then the set $\mathrm{Mat}_2(p^m)$ forms a finite ring with identity of characteristic p. The group of units of the ring $\mathrm{Mat}_2(2,p^m)$ is the general linear group (in dimension 2) $\mathrm{GL}(2,p^m)$.

The main object of this paper is to characterize the finite rings with identity of characteristic p, whose group of units is isomorphic to $\mathrm{GL}(2,p^m)$, where p is a prime number. Our main theorem is the following:

THEOREM 3.1. *Let R be a finite ring with identity of characteristic p, where p is a prime number.*

Suppose that the group R^* of units of R is isomorphic to $\mathrm{GL}(2,p^m)$. *Then*

(1) *If $p=2$, then* $R\cong\mathrm{Mat}_2(2^m)\oplus\mathbf{Z}_2\oplus\cdots\oplus\mathbf{Z}_2$.

(2) *If p is odd, then* $R\cong\mathrm{Mat}_2(p^m)$.

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

There are several results in the literature, which are related to our paper. Gilmer [8] gave a complete description of all finite, commutative rings with identity whose group of units is cyclic. Eldridge and Fisher [6] determined the rings satisfying the descending chain condition for left (right) ideals, whose group of units is finite. Also, they showed that there is only one noncommutative ring satisfying this condition. Eldridge [5] have showed that the structure of an artinian ring is determined by knowing that it has either a solvable, torsion, simple, nilpotent, supersolvable, or finitely generated quasi-regular group. For the case of a simple quasi-regular group, the rings are completely determined. Ditor [3] has determined a finite ring whose group of units is of odd order.

The notation in this paper is standard. It is taken from [4] and [9] for the groups and the rings. We will denote by $|S|$ the number of elements of a finite set S. Let G be a group and H be a subgroup of G. Then we will denote by $|G:H|$ the index of H in G.

2. Preliminary results

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

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^*.

Let $\mathrm{Mat}_n(F)$ 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 $\mathrm{Mat}_n(q)$ for $\mathrm{Mat}_n(F)$. Note that if p is the characteristic of F, then q is a power of p.

The general linear group $\mathrm{GL}(n,q)$ is the group of units of $\mathrm{Mat}_n(q)$. The subgroup of $\mathrm{GL}(n,q)$ consisting of matrices of determinant 1 is called the special linear group, which is denoted by $\mathrm{SL}(n,q)$. The center Z of $\mathrm{SL}(n,q)$ consists of the scalar matrices of determinant 1 and the corresponding factor group $\mathrm{PSL}(n,q)=\mathrm{SL}(n,q)/Z$ is called the projective special linear group.

The following known results are useful in the proof of our main theorem of this paper.

PROPOSITION 2.1. *Let R be a ring with identity and let* Rad$R$ *be the Jacobson radical of R. Then* $1+\mathrm{Rad}R$ *is a normal subgroup of R^*, the group of units of R.*

Proof. The proof may be found in [9, pp. 74–75].

PROPOSITION 2.2. *A finite semisimple ring R with identity is isomorphic to a finite direct sum of the full matrix rings over finite fields. That is,* $R\cong\mathrm{Mat}_{n1}(q_1)\oplus\cdots\oplus\mathrm{Mat}_{n_r}(q_r)$, *where each q_i is a power of a prime number.*

Proof. The proof follows from Wedderburn-Artin theorem [4, p. 13, Theorem 2.17] and Wedderburn's theorem [1, p. 138, Theorem 3].

PROPOSITION 2.3. *Let $n\geq 2$ and $q=p^m$, p prime. Then*

(1) $\mathrm{GL}(n,q)$ *has no nontrivial normal p-subgroup.*

(2) *A Sylow p-subgroup of* $\mathrm{GL}(n,q)$ *is elementary abelian if and only if $n=2$.*

Proof. Let S_1 be the set of all elements of $\mathrm{GL}(n,q)$ of the form

$$\begin{pmatrix} 1 & & & 0 \\ & 1 & & \\ & & \ddots & \\ * & & & 1 \end{pmatrix}$$

and let S_2 be the set of all elements of $\mathrm{GL}(n,q)$ of the form

$$\begin{pmatrix} 1 & & * \\ & 1 & \\ & & \ddots \\ 0 & & & 1 \end{pmatrix}$$

Then S_1 and S_2 are Sylow p-subgroups of $\mathrm{GL}(n,q)$. Let N be a normal p-subgroup of $\mathrm{GL}(n,q)$. By Sylow's theorem, N is contained in all Sylow p-subgroups of $\mathrm{GL}(n,q)$. In particular, $N\subseteq S_1\cap S_2=\{1\}$. Therefore, the assertion (1) holds.

The assertion (2) can be proved by an easy calculation.

PROPOSITION 2.4. *Let F be a finite field with p^m elements. Then the group* $\mathrm{SL}(2,p^m)$ *is generated by two Sylow p-subgroups S_1 and S_2, where*

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

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

PROPOSITION 2.5. *Let N be a normal subgroup of the group* $\mathrm{SL}(2,p^m)$, $p^m\geq 4$. *If* $|N|>2$, *then* $N=\mathrm{SL}(2,p^m)$.

Proof. The group $\mathrm{PSL}(2,p^m)$, $p^m\geq 4$, is simple [4, p. 205, Theorem 35.8]. Assume that $p=2$. Note that $\mathrm{SL}(2,p^m)=\mathrm{PSL}(2,p^m)$. It is easy to show that $N=\mathrm{SL}\ (2,p^m)$. Assume that p is odd. Let N be a normal subgroup of $\mathrm{SL}(2,p^m)$ and Z be the center of $\mathrm{SL}(2,p^m)$. If $Z\subseteq N$, then N must be $\mathrm{SL}(2,p^m)$ since the order of Z is 2 and $\mathrm{SL}(2,p^m)/Z$ is simple. Suppose that $Z\not\subseteq N$. Then $Z\cap N=\{1\}$ and $N\neq\{1\}$. Hence N is a normal subgroup of $\mathrm{SL}(2,p^m)$ of index 2. Since 2 and p are relatively prime, any Sylow p-subgroup of N is a Sylow p-subgroup of $\mathrm{SL}(2,p^m)$. By Sylow's theorem, N contains all the Sylow p-subgroups of $\mathrm{SL}(2,p^m)$. By Proposition 2.4, $N=\mathrm{SL}(2,p^m)$. Therefore, this proposition holds.

3. Main theorem

In this section we will prove the following theorem.

THEOREM 3.1. *Let R be a finite ring with identity of characteristic p, where p is a prime number. Suppose that the group R^* of units of R is isomorphic to* $\mathrm{GL}(2,p^m)$. *Then*

(1) *If $p=2$, then* $R\cong\mathrm{Mat}_2(2^m)\oplus\mathbf{Z}_2\oplus\cdots\oplus\mathbf{Z}_2$.

(2) *If p is odd, then* $R\cong\mathrm{Mat}_2(p^m)$.

The above theorem will be proved by a series of propositions. Throughout this section, R is a finite ring satisfying the assumption in Theorem 3.1.

PROPOSITION 3.2. *The number of elements of R is a power of p.*

Proof. Suppose that $|R|$ is not a power of p. Then there exists a prime number p', $p' \neq p$, which is a divisor of $|R|$. Since $(R, +)$ is a group, it follows from Cauchy theorem that there exists a nonzero element $a \in R$ such that $p' \cdot a = 0$. On the other hand, the characteristic of R is p. Hence $p \cdot a = 0$. These two equations implies $a = 0$. This is a contradiction.

PROPOSITION 3.3. *We have*

$$R \cong \mathrm{Mat}_{n_1}(q_1) \oplus \cdots \oplus \mathrm{Mat}_{n_r}(q_r)$$

and

$$R^* \cong \mathrm{GL}(n_1, q_1) \times \cdots \times \mathrm{GL}(n_r, q_r),$$

where r and n_i are positive integers, and $q_i = p^{k_i}$ for some positive integer k_i.

Proof. Since $(\mathrm{Rad}R, +)$ is a subgroup of $(R, +)$, $|\mathrm{Rad}\, R|$ is a power of p by Proposition 3.2. By Proposition 2.1, the subgroup $1+\mathrm{Rad}R$ is normal in R^*. Therefore, $1+\mathrm{Rad}R$ is a normal p-subgroup of R^*, and $1+\mathrm{Rad}R = \{1\}$ by Proposition 2.3. This implies that $\mathrm{Rad}R = \{0\}$ and R is a semisimple ring. By Proposition 2.2, $R \cong \mathrm{Mat}_{n_1}(q_1) \oplus \cdots \oplus \mathrm{Mat}_{n_r}(q_r)$. Since the characteristic of R is p, each q_i must be a power of p. Thus, Proposition 3.3 holds.

PROPOSITION 3.4. *There exists a normal subgroup H of R^*, which is isomorphic to* $\mathrm{SL}(2, p^m)$. *And there exist normal subgroups $G_1, \cdots, G_r$ of R^* such that $R^* = G_1 \times \cdots \times G_r$, where $G_i \cong \mathrm{GL}(n_i, p^{k_i})$.*

Proof. The first assertion is easy and the second assertion follows from Proposition 3.3.

PROPOSITION 3.5. *Theorem* 3.1 *holds.*

Proof. Let $G_1, \cdots, G_r$ and H be normal subgroups of R^*, which are defined in Proposition 3.4. Since $R^* = G_1 \times \cdots \times G_r$ is not abelian, at least one of the G_i is not abelian. Thus, without loss of generality, we may assume that G_1 is not abelian. Note that $R^* \cong \mathrm{GL}(2, p^m)$, $H \cong \mathrm{SL}(2, p^m)$, and $G_1 \cong \mathrm{GL}(n, p^k)$ for some positive integers $n \geq 2$ and k.

First we will prove that $G_1 = R^*$. Since G_1 and H are normal subgroups of R^*, both G_1H and $G_1 \cap H$ are normal subgroups of R^*. By the second isomorphism theorem, $G_1H/H \cong G_1/G_1 \cap H$ and $|G_1 : G_1 \cap H| = |G_1H : H|$. Since $|R^* : H|$ and p are relatively prime, it follows that $|G_1 : G_1 \cap H|$ and p are relatively prime. Hence any Sylow p-subgroup of $G_1 \cap H$ is a Sylow p-subgroup of the group G_1. Any Sylow p-subgroup of $G_1 \cap H$ is a p-subgroup of H, and $G_1 \cap H$ is elementary abelian. Hence a Sylow p-subgroup of $G_1 \cap H$ is elementary abelian. By Proposition 2.3, we have $n=2$ and $G_1 \cong \mathrm{GL}(2, p^k)$. Moreover, the normality of $G_1 \cap H$ in G_1 implies that any Sylow p-subgroup of G_1 is contained in $G_1 \cap H$. By Proposition 2.4, the group $G_1 \cap H$. By Proposition 2.4, the group $G_1 \cap H$ contains a subgroup which is isomorphic to $\mathrm{SL}(2, p^k)$. Note that $|\mathrm{SL}(2, p^k)| \geq p^k$. In particular, $|G \cap H| \geq |\mathrm{SL}(2, p^k)| > 2$. Assume that $m=1$. Then the group R^* is isomorphic to the group $\mathrm{GL}(2, p)$. Since the group G_1 is isomorphic to the group $\mathrm{GL}(2, p^k)$ and G_1 is a subgroup of R^*, we have $k=1$ and $R^*=G$. Assume that $m \geq 2$. Then since $p^m \geq 4$ and $|G_1 \cap H| > 2$, it follows from Proposition 2.5 that $G_1 \cap H = H$. Hence the group H is a subgroup of the group G_1. On the other hand, the order of a Sylow p-subgroup of H is p^m and the order of a Sylow p-subgroup of G_1 is p^k. Hence we have $k=m$ and $R^*=G_1$.

Finally we will show that this proposition holds. By Proposition 3.3, we have $R \cong \mathrm{Mat}_{n_1}(q_1) \oplus \cdots \oplus \mathrm{Mat}_{n_r}(q_r)$. Suppose that $r=1$. Then $R \cong \mathrm{Mat}_2(p^m)$.

Now suppose that $r>1$. Then $|G_2| = \cdots = |G_r| = 1$, and it follows that $n_2 = \cdots = n_r = 1$, $k_2 = \cdots = k_r = 1$, and $p=2$. This implies that

$$R \cong \mathrm{Mat}_2(2^m) \oplus \mathbf{Z}_2 \oplus \cdots \oplus \mathbf{Z}_2.$$

Thus we have proved Theorem 3.1.

References

1. Behrens F. A., *Ring Theory*, Academic Press, 1972.
2. Carter R. W., *Simple groups of Lie type*, J. Wiley & Sons, 1972.
3. Ditor S., *On the group of units of a ring*, Amer. Math. Monthly **78** (1971), 522-523.
4. Dornhoff L., *Group Representation Theory* (Part A), Marcel Dekker Inc., 1971.
5. Eldridge K. E., *On ring structures determined by groups*, Proc. Amer. Math. Soc. **23** (1969), 472-477.
6. Eldridge K. E., and Fisher I., *D. C. C. rings with a cyclic group of units*, Duke Math. J. **34** (1967), 243-248.
7. Farahat H., *The multiplicative groups of a ring*, Math. Z. **87** (1965), 378-384.
8. Gilmer R. W., *Finite rings having a cyclic multiplicative group of units*, Amer. J. Math. **85** (1963), 447-452.
9. McDonald B. R., *Finite ring with identity*, Marcel Dekker Inc., 1974.

Sogang University