Finite rings with identity having $GL(2^m)$ as the group of units

Kim, Eung-Tae and Shin, Hyun-Yong
(Department of Mathematics)

要 約

주어진 환에 있어서 가역원 전체의 집합은 곱셈군을 이룬다. 이 곱셈군이 순회인 유한환은 그 구조가 완전히 결정된다는 것은 이미 알려져 있다.

본 논문에서는 다음 정리를 증명한다.

정리 (3.1)

가역원 전체로 이루어진 곱셈군이 일반선형군 $GL_2(2^m)$ 과 동형인 유한환 R은 다음과 같다. 즉,

$$R\cong M_2(2^m)\oplus Z_2\oplus\cdots\cdots\oplus Z_2.$$

1. Introduction.

In this paper, we will determine the finite rings having the general linear group $GL_2(2^m)$ as the group of units.

Our main theorem is as follows:

Theorem 3.1. Let R be a finite ring with identity. Suppose that the group R^* of all units is isomorphic to $GL_2(2^m)$. Then

$$R\cong M_2(2^m)\oplus Z_2\oplus\cdots\cdots\oplus Z_2,$$

where $M_2(2^m)$ is the 2×2 matrix ring over the Galois field $GF(2^m)$.

There are several results in the literature which is related to our theorem. Gilmer (1963) determined all finite commutative rings with identity such that the group of units is cyclic.

Eldridge and Fischer (1967) showed that a ring satisfying the descending chain condition for left (right) ideals and having a cyclic group of units must be finite. Furthermore,

they showed that there is essentially only one non-commutative ring satisfying these conditions. Eldridge (1969) showed that part of the structure of an artinian ring is determined when it has a solvable, simple, nilpotent, supersolvable, torsion, or finitely generated quasi-regular group and that for the case of a simple quasi-regular group, the rings are completely determined. Ditor (1971) has characterized a finite ring whose group of units is of odd order.

The structure of $GL_2(2^m)$ is useful for our discussion.

The notations in this paper are standard. Most of them are taken from McDonald (1974) for the ring theory and from Gorenstein (1968) for the group theory.

2. Preliminary results.

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

In this section we will give some results which will be used in this paper.

The following two propositions are well-known.

Proposition 2.1. Let $Rad(R)$ be the Jacobson radical of a ring R. Then $1+Rad(R)$ is a normal subgroup of R^*.

Proof. The proof may be found in McDonald (1974).

Proposition 2.2. A finite semi-simple ring R is isomorphic to a finite direct sum of the full matrix rings over fields, that is,

$$R\cong M_{n_1}(F_1)\oplus\cdots\cdots\oplus M_{n_r}(F_r).$$

In particular,

$$R^*\cong GL_{n_1}(F_1)\times\cdots\cdots\times GL_{n_r}(F_r).$$

Proof. This is proved in Barshay (1969).

Now we consider the ring $M_2(F)$ of all 2×2 matrices over a field F. The *general linear group* $GL_2(F)$ is the group of units of $M_2(F)$. The subgroup of $GL_2(F)$ consisting of matrices of determinant 1 is called the *special linear group*, and is denoted by $SL_2(F)$.

The center Z of $GL_2(F)$ consists of the scalar matrices and the corresponding factor group $PGL_2(F)=GL_2(F)/Z$ is called the *projective linear group*. The image $PSL_2(F)$ of

$SL_2(F)$ in $PGL_2(F)$ is called the *projective special linear group.*

Note that $GL_2(2)=SL_2(2)$, and it is isomorphic to the symmetric group of degree 3.

Proposition 2.3. Let F be a finite field with q elements. Then

$$|GL_2(F)|=q(q^2-1)(q-1)$$

and

$$|SL_2(F)|=q(q^2-1).$$

Proof. This is a well-known result. The proof may be found in Gorenstein (1968).

Proposition 2.4. The projective special linear group $PGL_n(F)$ is simple for $n\geqq 2$ except in the case $n=2$, $|F|=2$ or 3. In particular, $SL_2(2^m)$ is simple if $m\geqq 2$.

Proof. This is proved in Gorenstein (1968).

We conclude this section with the following proposition.

Proposition 2.5. Let S be a Sylow 2-subgroup of $GL_n(2^m)$, $n\geqq 2$. Then S is an elementary abelian if and only if $n=2$.

Proof. Let S be the set of all elements of $GL_n(2^m)$ of the form

$$\begin{bmatrix} 1 & 1 & \cdot & 0 \\ * & & \cdot & 1 \end{bmatrix}.$$

Then it is clear that S is a Sylow 2-subgroup of $GL_n(2^m)$. By an easy calculation, the above assertion follows.

3. Main theorem.

In this section we will prove the following theorem.

Theorem 3.1. Let R be a finite ring such that the group R^* of units is isomorphic to $GL_2(2^m)$. Then

$$R\cong M_2(2^m)\oplus Z_2\oplus\cdots\cdots\oplus Z_2.$$

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

Proposition 3.2. The characteristic of R is 2.

Proof. Let k be the characteristic of R and let R_0 be the subring of R generated by 1. Then $R_0\cong Z_k$, the ring of integers modulo k, and $Z_k^*\cong R_0^*$ is a subgroup of the center

$Z(R^*)$ of R^*. Since $|Z(R^*)|=2^m-1$ is an odd integer, $|Z_k^*|=\varphi(k)$ must be odd. Therefore, $k=2$.

Proposition 3.3. The order of R is a power of 2.

Proof. Suppose that the order of R is not a power of 2. Then there exists a prime number p, $p\neq 2$, such that p divides the order of R.

By the Cauchy's theorem, there exists an element of R with order p. This is a contradiction to the Proposition 3.2. Hence the order of R is a power of 2.

Proposition 3.4. The Jacobson radical $Rad(R)$ of R is 0. Moreover,

$$R\cong M_{n_1}(q_1)\oplus\cdots\cdots\oplus M_{n_r}(q_r),\ q_i=2^{k_i}.$$

Proof. Let $S_1=\left\{\begin{bmatrix}1&\alpha\\0&1\end{bmatrix}:\alpha\in GF(2^m)\right\}$ and $S_2=\left\{\begin{bmatrix}1&0\\\alpha&1\end{bmatrix}:\alpha\in GF(2^m)\right\}$

Then S_1 and S_2 are Sylow 2-subgroups of R^*. Now $1+Rad(R)$ is a normal 2-subgroup of R^*. Thus $1+Rad(R)$ is contained in all Sylow 2-subgroups. Hence $1+Rad(R)=S_1\cap S_2=1$. This implies that $Rad(R)=0$.

The second assertion follows from Proposition 2.2 and 3.2.

Proposition 3.5. There are normal subgroups $G_1,\cdots\cdots,G_r$ of R^* such that

$$R^*=G_1\times\cdots\cdots\times G_r,$$

where $G_i=GL_{n_i}(q_i)$, $q_i=2^{k_i}$.

Proof. By Proposition 3.4, $R\cong M_{n_1}(q_1)\oplus\cdots\cdots\oplus M_{n_r}(q_r)$. Hence

$$R^*=GL_{n_1}(q_1)\times\cdots\cdots\times GL_{n_r}(q_r).$$

Therefore the assertion holds.

Proposition 3.6. Let H be the normal subgroup of R^* which is isomorphic to the normal subgroup $SL_2(2^m)$ of $GL_2(2^m)$, and let $Z(R^*)$ be the center of R^*. Then

$$R^*=Z(R^*)H.$$

Proof. The assertion follows from the structure of $GL_2(2^m)$.

Proposition 3.7. If $m=1$, then $R\cong M_2(2)\oplus Z_2\oplus\cdots\cdots\oplus Z_2$.

Proof. By Proposition 3.4, we have

$$R^*\cong GL_{n_1}(q_1)\times\cdots\cdots\times GL_{n_r}(q_r).$$

Since R^* is non-abelian, at least one of the n_i, say n_1, is not equal to 1. Since $|R^*|=6$, counting the number of elements of the right side, we know that $n_1=2$ and $n_j=1$

for $j \neq 1$.

Moreover, $k_i=1$ for all $i=1, 2, \cdots\cdots, n$. Therefore,

$$R \cong M_2(Z_2) \oplus Z_2 \oplus \cdots\cdots \oplus Z_2.$$

Proposition 3.8. If $m>1$, then $R \cong M_2(2^m) \oplus Z_2 \oplus \cdots\cdots \oplus Z_2$.

Proof. By Proposition 3.5, we have $R^*=G_1 \times G_2 \times \cdots\cdots \times G_r$. Since R^* is not abelian, at least one of the G_i is not abelian. Assume that G_1 is not abelian.

First, we will prove that $R^*=Z(R^*)G_1$.

The subgroup $Z(R^*)G_1$ is a normal subgroup of R^*. Let H be the subgroup of R^* defined in Proposition 3.6. Since the index $|R^*: H|$ of H in R^* is 2^m-1 and $|Z(R^*)G_1| > 2^m-1$, we have $Z(R^*)G_1 \cap H \neq 1$. It follows from Proposition 2.4 that $Z(R^*)G_1 \supseteq H$, and hence $Z(R^*)G_1 \supseteq Z(R^*)H=R^*$. Therefore, $R^*=Z(R^*)G_1$.

Secondly, we will prove that $G_1 \cong GL_2(2^m)$.

Since $Z(R^*)=Z(G_1) \times \cdots\cdots \times Z(G_r)$, we have

$$R^*=G_1 \times Z(G_2) \times \cdots\cdots \times Z(G_r).$$

Therefore, $G_i=Z(G_i)$ for all $i \geqq 2$. Since $G_i=GL_{n_i}(q_i)$, this implies that for any $i \geqq 2$, $n_i=1$ and $|G_i|=q_i-1$. But q_i-1 is an odd integer. Hence any Sylow 2-subgroup of R^* is contained in G_1. Now, by Proposition 2.5 and the above arguments, we can conclude that $n_1=2$ and $q_1=2^m$. This yields $G_1 \cong GL_2(2^m)$.

By the above arguments, we have $G_i=1$ for all $i \geqq 2$. Hence $q_i=2$ for all $i \geqq 2$. Therefore, by Proposition 3.4, we have

$$R \cong M_2(2^m) \oplus Z_2 \oplus \cdots\cdots \oplus Z_2.$$

Proposition 3.9. Theorem 3.1 holds.

Proof. This is a consequence of Proposition 3.7 and 3.8. We have completed the proof of our main theorem.

References

Barshay, J. 1969, *Topics in ring theory*, W.A. Benjamin, INC

Ditor, S. 1971, *On the group of units of a ring*, Amer. Math. Monthly, 78:322-323.

Eldridge, K.E. 1969, *On ring structures determined by groups*, Proc. Amer. Math. Soc., 23:472-477.

Eldridge, K.E. and Fischer, I. 1967, D.C.C. *Rings with a cyclic group of units*, Duke Math. J., 34:243-248.

Farahat, H. 1965, *The multiplicative groups of a ring*, Math. Zeitschr. 87:378-384.

Gilmer, R.W. 1963, *Finite rings having a cyclic multiplicative group of units*, Amer. J. Math., 85:447-452.

Gorenstein, D. 1968, *Finite groups*, Harper and Row.

McDonald, B.R. 1974, *Finite rings with identity*, Marcel Dekker, INC.