韓國數學敎育學會誌〈數學敎育〉
1978. 12. Vol. XVII No. 1

Journal of the Korea Society of Mathematical Education
Dec. 1978. Vol. XVII No. 1

On the finite group of units of a ring

by Jeon, Song Ki

Dan Kook University, Seoul, Korea.

1. Introduction

There are several results in the literature which relate the structure of a ring with identity to that of its group of units.

Gilmer[3] determines all finite commutative rings whose group of units is cyclic.

In this paper we will consider the nature of the finite group of units of a ring whose order is odd and we will find a necessary and sufficient condition for a finite group G of odd order to be the group of units of some ring.

Our main theorems are as follows:

Theorem 1. *If* G *is the group of units of a ring and if* G *is finite of odd order, then the subring* [G] *of* R *generated by* G *is a finite direct sum of Galois field of characteristic* 2. *Thus*

$$[G]=GF(2^{k_1})\oplus GF(2^{k_2})\oplus\cdots\cdots\cdots\oplus GF(2^{k_r}).$$

Theorem 2. *A finite group of odd order is the group of units of some ring if and only if* G *is abelian and is the finite direct product of cyclic groups* G_i, *where the order of each* G_i *is of the form* 2^k-1.

The notation in this paper is standard and taken from [4]. By a ring we mean a ring with identity. The finite field with q elements is called the Galois field, and is denoted by GF(q). The characteristic of a Galois field GF(q) is a prime number p and $q=p^n$ for some positive integer n.

2. Preliminary results

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

Let K be a field. Then the matrix ring $Mat_n(K)$ of $n\times n$ matrices over K is simple, and the group of units of $Mat_n(K)$ is *the general linear group* GL(n, K) consisting of all non-singular $n\times n$ matrices over K.

The following propositions will be needed in the next section.

Proposition 1. (Maschke's theorem) *Let* G *be a finite group of order* n, *and let* K *be a field whose characteristic does not divide* n. *Then the group algebra* K[G] *is a semisimple* *algebra.* [1. p. 16].

Proposition 2. (Wedderburn-Artin's theorem) *Let* A *be a finite dimensional semisimple algebra over a field* K. *Then*

$$A \approx Mat_n(D_1) \oplus Mat_n(D_2) \oplus \cdots\cdots\cdots\cdots \oplus Mat_n(D_r).$$

where each D_i *is a division ring.* [4. Vol. II. p. 156].

Proposition 3. (Wedderburn's theorem) *A finite division ring is necessary a communative field.* [4. Vol. II. p. 203].

If K is the finite field with q elements, then we denote

$$Mat_n(K) = Mat_n(q), \quad GL(n, K) = GL(n, q).$$

If $n=1$, then $Mat_n(q)$ is $GF(q)$ and $GL(n, q)$ is the multiplicative group of the field $GF(q)$.

3. Main theorems

In this section we will prove our main theorems.

Theorem 1. *If* G *is the group of units of a ring* R *and if* G *is finite of odd order, then the subring* [G] *of* R *generated by* G *is a finite direct sum of Galois fields of characteristic* 2, *Thus*

$$[G] = GF(2^{k_1}) \oplus GF(2^{k_2}) \oplus \cdots\cdots\cdots\cdots \oplus GF(2^{k_r}).$$

Proof. Since G has odd order, $-1=1$; otherwise $\{-1, 1\}$ would be a subgroup of G of order 2. Hence the subring [G] generated by G is a finite dimensional algebra over GF (2). [G] is a representation module of G over GF(2) and since 2, the characteristic of GF (2), does not divide the order of G, Maschke's theorem (Prop. 1) implies that [G] is semisimple. By the Wedderburn-Artin's theorem (Prop. 2), we have

$$[G] = Mat_{n_1}(D_1) \oplus Mat_{n_2}(D_2) \oplus \cdots\cdots\cdots\cdots \oplus Mat_{n_r}(D_r)$$

where each D_i is a division ring. Since D_i is finite, it follows from Prop. 3 that D_i is a finite field, and since $-1=1$ in [G], the field D_i is a Galois field of characteristic 2. Therefore,

$$[G] = Mat_{n_1}(2^{k_1}) \oplus Mat_{n_2}(2^{k_2}) \oplus \cdots\cdots\cdots\cdots \oplus Mat_{n_r}(2^{k_r})$$

for some poistive integers $k_1, \cdots\cdots, k_r$. Hence the group of units of [G] is

$$GL(n_1, 2^{k_1}) \times GL(n_2, 2^{k_2}) \times \cdots\cdots\cdots\cdots \times GL(n_r, 2^{k_r}).$$

On the other hand, the order of $GL(n, q)$ is $(q^n-1)(q^n-q)\cdots\cdots(q^n-q^{n-1})$ and when q is even $(q^n-1)(q^n-q)\cdots\cdots(q^n-q^{n-1})$ is odd if and only if $n=1$. Since the group of units of [G] is of odd order, this fact implies that each n_i is 1. Hence we have

$$[G] = GF(2^{k_1}) \oplus GF(2^{k_2}) \oplus \cdots\cdots\cdots\cdots \oplus GF(2^{k_r}).$$

Theorem 2. *A finite group* G *of odd order is the group of units of some ring if and only if* G *is abelian and is the finite direct product of cyclic groups* G_i, *whose order of each* G_i *is of the form* $2^{k_i}-1$.

Proof. The necessary condition follows from Theorem 1 and the fact that the multiplicative group K^* of a finite field K is cyclic. Conversely, if G is abelian and $G = G_1 \times G_2 \times \cdots \times G_r$, where G_i is the multiplicative group of Galois field $GF(2^{k_i})$, then G is the group of units of the ring

$$R=GF(2^{k_1})\oplus GF(2^{k_2})\oplus\cdots\cdots\cdots\cdots\oplus GF(2^{k_r}).$$

Corollary. *A prime power p^m is the number of units of some ring if and only if a prime p is 2 or 2^q-1 for some number q.*

Proof. If $p=2$ (resp. $p=2^q-1$), then $p+1=3$ (resp. $p+1=2^q$), and the m-fold direct sum of GF(3) (resp. GF(2^q)) has precisely p^m units.

Conversely, if a group of prime power order p^m is the group of units of a ring and if $p\neq 2$, then by the theorem 2, p^m is a product of numbers of the form 2^k-1. Therefore, for some positive integers n and $k, p^n=2^k-1$. For n even, $p^n-1=(p-1)\ (p^{n-1}+\cdots\cdots+p+1)$ is divisible by 4, whereas for $k\neq 1$, 2^k-2 is not. Hence n is odd and $p+1$ divides $p^n+1=2^k$, so that $p+1$ is a power of 2.

References

[1] D ornhoff, L. (1971), *Group representation theory*, Part A, Marcel Dekker, Inc., New York.

[2] Eldridge, K. E. (1963), On ring structures determined by groups, *Proc. Amer. Math. Soc.*, 23 pp. 472-477.

[3] Gilmer, R. (1963), Finite rings having a cyclic multiplicative group of units, *Amer. J. Math.* 85 pp. 447-452.

[4] Van der Waerden, B. L. (1949 and 1950), *Modern algebra*, Vol. I and II, Ungar, New York.