

## MULTIPLICATIVE GROUP IN A FINITE RING

JUNCHEOL HAN

### 1. Introduction and basic definitions

Let  $R$  be a finite ring with identity 1 and let  $G$  denote the multiplicative group of all units of  $R$ . An element  $e$  in  $R$  is said to be idempotent if  $e^2 = e$ . A nonzero idempotent is said to be primitive if it cannot be written as the sum of two orthogonal nonzero idempotents.

In [4], Artinian proved that if  $R$  is a semisimple Artinian ring, then  $R$  is isomorphic to a direct product of finite number of matrix rings over division rings. In particular, if  $R$  is finite, then we obtain the following;

**THEOREM 1.1.** (*Wedderburn-Artin's Structure Theorem for a finite ring*)

If  $R$  is a finite ring and  $J$  is the Jacobson radical of  $R$ , then  $R/J \cong \bigoplus_{i=1}^n M_i$  where  $M_i$  is the ring of all  $n_i \times n_i$  matrices over a finite field  $F_i$ .

In this paper, we will show that the multiplicative group  $G$  in a finite ring  $R$  with identity 1 has a  $(B, N)$ -pair satisfying the following conditions;

- (1)  $G = BNB$  where  $B$  and  $N$  are subgroups of  $G$ .
- (2)  $B \cap N$  is a normal subgroup of  $N$  and  $W = N/(B \cap N)$ , is generated by a set  $S = \{s_1, s_2, \dots, s_r\}$  where  $s_i \in N/(B \cap N)$ ,  $s_i^2 \equiv 1$  and  $s_i \neq 1$ .
- (3) For any  $s \in S$  and  $w \in W$ , we have  $sBw \subset BwB \cup BswB$ .
- (4) We have  $sBs \not\subseteq B$  for any  $s \in S$ .

When  $G, B, N$  and  $S$  satisfy the above conditions, we say that the quadruple  $(G, B, N, S)$  is a Tits system. The group  $W$  is called the Weyl group of the Tits system.

**2. Muultiplicative group in a matrix ring over a (finite) field**

Let  $R = M_n(F)$  be the ring of all  $n \times n$  matrices over a (finite) field  $F$  and let  $G$  the multiplicative group of  $R$ . Let  $E$  be the set of all primitive idempotents in  $R$  and let  $I(E)$  be the set of all right ideals in  $R$  which is generated by the subset  $S$  of  $E$  such that each member of  $S$  is orthogonal to another. Let  $\Delta(E)$  be the set of all chains in  $I(E)$ . Let  $\sum = \{e_1, e_2, \dots, e_n\}$  be a subset of  $E$  satisfying that  $e_i e_j = 0$  for  $i \neq j$  and  $e_1 + e_2 + \dots + e_n = 1$ .

Let  $\sum_{\Delta}$  be the set of all chains in  $\Delta(E)$  constructed by  $\sum$ . Pick a maximal chain  $c$  in  $\sum_{\Delta}$ ;

$$c : e_1 R + \dots + e_{n-1} R \supset e_1 R + \dots + e_{n-2} R \supset \dots \supset e_1 R.$$

For each  $g \in G$ , define  $g(C)$  by

$$g(e_1 R + \dots + e_{n-1}) R \supset g(e_1 R + \dots + e_{n-2} R) \supset \dots \supset g(e_1 R).$$

Note that by the Proposition 3 in [6,pp 77],  $g(C)$  is also a maximal chain in  $\Delta(E)$  constructed by a set  $\{f_1, f_2, \dots, f_n\}$  satisfying that  $f_i f_j = 0$  for  $i \neq j$  and  $f_1 + f_2 + \dots + f_n = 1$  where  $f_i = g e_i g^{-1}$  for each  $i = 1, 2, \dots, n$ .

LEMMA 2.1. *Let  $R$  be the ring of all  $n \times n$  matrices over a (finite) field  $F$  and let  $G$  the multiplicative group of  $R$ . Let  $B = \{g \in G : g(C) = C\}$ . Then  $B$  is a subgroup of  $G$  and  $B = \{g \in G : g \text{ is upper-triangular}\}$ .*

*Proof.* Let  $g = (g_{ij}) \in B$ . Without loss of generality, we may take  $e_i = E_{ij} = (a_{ij})$  where  $a_{ij} = 1$  and  $a_{ij} = 0$  for  $i \neq j (1 \leq i, j \leq n)$ , which is assured by the Proposition 3 in [6,p 77]. From the equality  $g(C) = C$ , we have

$$\begin{aligned} g(e_1 R) &= e_1 R - (1) \\ g(e_1 R + e_2 R) &= e_1 R - (2) \\ &\dots\dots\dots \\ g(e_1 R + \dots + e_{n-1}) R &= e_1 R + \dots + e_{n-2} R - (n - 1). \end{aligned}$$

## Multiplicative Group in a Finite Ring

From the equality (1),  $g_{1j} = 0$  for  $2 \leq j \leq n$ . From the equality (2),  $g_{2j} = 0$  for  $3 \leq j \leq n$ . By induction on  $n$  and the equality  $(n - 1)$ ,  $g_{ij} = 0$  for  $i \leq j \leq n$ . Hence  $g = (g_{ij})$  is upper-triangular. On the other hand, it is clear that  $g(C) = C$  for all upper-triangular  $g \in G$ . Consequently,  $B = \{g \in G : g \text{ is upper-triangular}\}$  and clearly,  $B$  is a subgroup of  $G$ .

**LEMMA 2.2.** *Let  $R$  be the ring of all  $n \times n$  matrices over a (finite) field  $F$  and let  $G$  the multiplicative group of  $R$ . Let  $N = \{g \in G : g(\sum_{\Delta}) = \sum_{\Delta}\}$ . Then  $N$  is a subgroup of  $G$  and  $N = \{g \in G : g \text{ has only one nonzero entry for each row}\}$ .*

*Proof.* Clearly,  $N$  is a subgroup of  $G$ . Let  $g = (g_{ij}) \in N$ . Without loss of generality, we may assume that the first row of  $g$  has two nonzero entries  $g_{1r}, g_{1s} (1 \leq r < s \leq n)$ . Let  $C$  be a maximal chain in  $\sum_{\Delta}$ :

$$C : e_1R + \dots + e_{r-1}R + e_{r+1}R + \dots + e_sR + \dots + e_nR \supset \dots \supset e_1R.$$

Then we have  $g(e_1R + \dots + e_{r-1}R + e_{r+1}R + \dots + e_sR + \dots + e_nR) = R$ , which means that  $g(C)$  is not a maximal chain in  $\sum_{\Delta}$ , a contraction.

On the other hand, it is clear that if  $g \in G$  has only one nonzero entry for each row, then  $g(\sum_{\Delta}) = \sum_{\Delta}$ . Hence we have the result.

**LEMMA 2.3.** *Let  $R$  be the ring of all  $n \times n$  matrices over a (finite) field  $F$  and let  $G$  the multiplicative group of  $R$ . Let  $N_G(D) = \{g \in G : gDg^{-1} \subseteq D\}$  where  $D = \{a \in R : a \text{ is diagonal matrix}\}$ . Then  $N_G(D) = N$  where  $N$  is given in Lemma 2.2.*

*Proof.* First, we will show that  $N \subseteq N_G(D)$ . Indeed, For any  $g = (g_{ij}) \in N, d = (d_{ij}\delta_{ij}) \in D$  and  $g^{-1} = (h_{ij})$ , we have

$$\begin{aligned} gdg^{-1} &= \sum_{k=1}^n (g_{ik}h_{kj})d_{kk} = ((g_{is}h_{sj})d_{ss}) \text{ (for some } s, 1 \leq s \leq n) \\ &= \sum_{k=1}^n (g_{ik}h_{kj})d_{ss} = (d_{ss}\delta_{ij}) \in D. \end{aligned}$$

Hence  $g \in N_G(D)$ . Assume that  $N \neq N_G(D)$ . Then there exists  $g = (g_{ij}) \in N_G(D) \setminus N$ . Without loss of generality, we may assume that

some row of  $g$ , say  $i$ -th row, has two non-zero entries  $g_{ir}, g_{is} (1 \leq r < s \leq n)$ . Choose a diagonal matrix  $d = (d_{ij}\delta_{ij})$  so that  $d_{ii} = 0$  for  $i \neq r, s$  and  $d_{rr}, d_{ss} \neq 0$  and  $d_{rr} \neq d_{ss}$ . Since  $g \in N_G(D)$ , there exists  $d_1 = (x_{ij}\delta_{ij}) \in D$  such that  $gd = d_1g - (*)$ . Note that  $(i, r)$ -entry of  $gd = g_{ir}d_{rr}$ ,  $(i, s)$ -entry of  $gd = g_{is}d_{ss}$ ,  $(i, r)$ -entry of  $d_1g = x_{ii}g_{rr}$  and  $(i, s)$ -entry of  $d_1g = x_{ii}g_{ss}$ . From  $(*)$ , we have  $d_{rr} = x_{ii}$  and  $d_{ss} = x_{ii}$ , and so  $d_{rr} = d_{ss}$ , a contraction. Hence  $N = N_G(D)$ .

**PROPOSITION 2.4.** *Let  $R$  be the ring of all  $n \times n$  matrices over a (finite) field  $F$  and let  $G$  the multiplicative group of  $R$ . Let  $B = \{g \in G : g(C) = C\}$  and  $N = \{g \in G : g(\sum_{triangle}) = \sum_{\Delta}\}$ . Then  $G = BNB$ .*

*Proof.* Let  $g$  be any element in  $G$ . To make each row of  $G$  have different number of zeroes beginning from the left, consider an invertible matrix obtained from  $g$  by means of a sequence of elemently row operation which is defined by replacing  $i$ -th row with  $i$ -th row  $+ a \cdot (j$ -th row) for some nonzero  $a \in F (i < j)$ . Note that the matrices obtained from identity matrix by the operations given above are upper-triangular, and so  $bg = g_1$  for some  $b \in B$  by Lemma 2.1.

Next, we can make an invertible matrix obtained from  $g_1$  by means of a sequence of some rotation of two rows be upper-triangular. Note that the matrices obtained from identity matrix by the operations given above are contained in  $N$  by Lemma 2.2. Hence  $ng_1 = nbq = b_1$  for some  $b_1 \in B$ , so  $g = (nb)^{-1}b_1 = b^{-1}n^{-1}b_1 \in BNB$ .

**PROPOSITION 2.5.** *Let  $R$  be the ring of all  $n \times r$  matrices over a (finite) field  $F$  and let  $G$  the multiplicative group of  $R$ . Let  $B = \{g \in G : g(C) = C\}$  and  $N = \{g \in G : g(\sum_{\Delta}) = \sum_{\Delta}\}$ . Then  $B \cap N$  is a normal subgroup of  $G$ .*

*Proof.* It is clear from Lemma 2.1 and Lemma 2.2 to show that  $B \cap N = G \cap D$ . For all  $n \in N$  and all  $a \in B \cap N, nan^{-1} \in D$  since  $a \in D$  and  $n \in N$ . Clearly,  $nan^{-1} \in G$ . Hence  $nan^{-1} \in G \cap D = B \cap N$ , and so  $B \cap N$  is a normal subgroup of  $G$ .

**PROPOSITION 2.6.** *Let  $R$  be the ring of all  $n \times r$  matrices over a (finite) field  $F$  and let  $G$  the multiplicative group of  $R$ . Let  $B = \{g \in G : g(C) = C\}$  and  $N = \{g \in G : g(\sum_{\Delta}) = \sum_{\Delta}\}$ . Then  $N/(B \cap N)$*

is generated by a set  $S = \{s_1, s_2, \dots, s_k\}$  for some positive integer  $k$  where  $s_i \in N/(B \cap N)$ ,  $s_i^2 \equiv 1$  and  $s_i \neq 1$ .

*Proof.* Let  $t_{ij}$  be the matrix obtained by interchanging two different rows,  $i$ -th and  $j$ -th rows, on the identity matrix  $I$ . Then  $t_{ij}^2 = I$  and  $t_{ij} \neq I$ . Let  $s_{ij} = t_{ij}(B \cap N)$ . Since  $t_{ij} \in N/(B \cap N)$ .

We will show that  $N/(B \cap N)$  is generated by the set  $\{s_{ij} | 1 \leq i, j \leq n, i \neq j\}$ . Let  $n(B \cap N) \in N/(B \cap N)$  and  $t = (d_{ij}\delta_{ij}) \in B \cap N$  where  $d_{ii}$  is the inverse of nonzero entry of  $i$ -th column of  $n$ . Then  $nt$  can be expressed by a product of some elements of  $\{t_{ij} | 1 \leq i, j \leq n, i \neq j\}$ . Therefore,  $nt(B \cap N) = (n(B \cap N))(t(B \cap N))$  can be also expressed by a product of some element of  $\{s_{ij} | 1 \leq i, j \leq n, i \neq j\}$ .

**COROLLARY 2.7.** Let  $R$  be the ring of all  $n \times n$  matrices over a (finite) field  $F$  and let  $G$  the multiplicative group of  $R$ . Let  $B = \{g \in G : g(C) = C\}$  and  $N = \{g \in G : g(\sum_{\Delta}) = \sum_{\Delta}\}$ . Then  $N/(B \cap N)$  is generated by a set  $S_0 = \{s_{ii+1} | i = 1, 2, \dots, n-1\}$  where  $s_{ii+1} = t_{ii+1}(B \cap N) \in N/(B \cap N)$  and  $t_{ii+1}$  be the matrix obtained by interchanging two rows,  $i$ -th and  $i+1$ -th rows, on the identity matrix  $I$ .

*Proof.* Since the symmetric group  $S_n$  of degree  $n$  is generated by all the  $n-1$  transposition  $(ii+1)$  for  $i = 1, 2, \dots, n-1$ , each  $s_i$  in the set  $S$  given in Proposition 2.6 is generated by  $S_0$ .

**DEFINITION 2.8.** An element  $s_{ij} \in W = N/(B \cap N)$  satisfying  $s_{ij}^2 \equiv 1$  and  $s_{ij} \neq 1$  (1 is an identity of  $W$ ) is called the involution with respect to  $B$ . The group  $W$  generated by the involutions is called the Weyl group of the  $\sum_{\Delta}$ .

The equality  $G = BNB$  which is proved in proposition 2.4 shows that  $G$  is a union of the double cosets with respect to  $(B, B)$  and that we can take an element of  $N$  as representative from each  $(B, B)$ -double coset. For  $w = n(B \cap N) \in W$ , we can define  $BwB = BnB$ . We also use notations such as  $Bw = Bn$  when  $w = n(B \cap N)$ .

**PROPOSITION 2.9.** Let  $R$  be the ring of all  $n \times n$  matrices over a (finite) field  $F$  and let  $G$  the multiplicative group of  $R$ . Let  $B = \{g \in G : g(C) = C\}$  and  $N = \{g \in G : g(\sum_{\Delta}) = \sum_{\Delta}\}$ . Then  $s_{ij}Bs_{ij} \subseteq B$

for any  $s_{ij} \in S$ , a generating set for  $W = N/(B \cap N)$  given in the proof of proposition 2.6.

*Proof.* Assume that there exists some  $s_{ij} \in S$  such that  $s_{ij}Bs_{ij} \subseteq B$ . Let  $s_{ij} = t_{ij}(B \cap N)$  where  $t_{ij}$  is the matrix obtained by interchanging two rows,  $i$ -th and  $j$ -th rows ( $i < j$ ), on the identity matrix  $I$ . Choose  $b \in B$  so that  $(i, j)$ -entry of  $b = b_{ij} \neq 0$ . Then  $t_{ij}ot_{ij}^{-1} \notin B$ . Hence  $s_{ij}Bs_{ij}^{-1} = s_{ij}Bs_{ij} \not\subseteq B$  for any  $s_{ij} \in S$ .

**PROPOSITION 2.10.** *Let  $R$  be the ring of all  $n \times n$  matrices over a (finite) field  $F$  and let  $G$  the multiplicative group of  $R$ . Let  $B = \{g \in G : g(C) = C\}$  and  $N = \{g \in G : g(\sum_{\Delta} = \sum_{\Delta})\}$ . Then  $sBw \subset BsB \cup BswB$  for any  $s \in S$ , a generating set for  $W$ , and for any  $w \in W$ .*

*Proof.* Since  $W$  is generated by  $S$ ,  $w = s_1s_2 \dots s_k$  for some  $s_i \in S$  and positive integer  $k$  ( $i = 1, 2, \dots, k$ ). We will prove the result by induction on  $k$ . By straight forward calculation,  $sBs_1 \subset BsB$  if  $s = s_1$  and  $sBs_1 \subset Bss_1B$  if  $s \neq s_1$ . Moreover,  $sBs_1s_2 \subset BsB$  if  $s = s_1 = s_2$  and  $sBs_1s_2 \subset Bss_1s_2B$  otherwise. Hence by induct on  $k$ ,  $sBw = sBs_1s_2 \dots s_k \subset BsB$  if  $s = s_i$  for all  $i = 1, 2, \dots, k$  and  $sBw \subset BswB$  otherwise.

**DEFINITION 2.11.** Let  $G$  be a group. Two subgroups  $B$  and  $N$  of  $G$  are said to be a  $(B, N)$ -pair of  $G$  if the following conditions are satisfied:

- (1)  $G = BNB$  where  $B$  and  $N$  are subgroups of  $G$ .
- (2)  $B \cap N$  is a normal subgroup of  $N$  and  $W = N/(B \cap N)$  is generated by the set  $S = \{s_1, s_2, \dots, s_k\}$  where  $s_i \in W$ ,  $s_i^2 \equiv 1$  and  $s_i \neq 1$  ( $1$  is the identity of  $W$ ).
- (3) For any  $s \in S$  and  $w \in W$ , we have  $sBw \subset BwB \cup BswB$ .
- (4) For any  $s \in S$ , we have  $sBs \not\subseteq B$ .

When  $G, B, N$ , and  $S$  satisfy the above conditions, we say that the quadruple  $(G, B, N, S)$  is a Tits system. The group  $W$  is called the Weyl group of the Tits system.

In this section, we have shown that if  $R$  is the ring of all  $n \times n$  matrices over a (finite) field  $F$  and  $G$  is the multiplicative group of  $R$ , then there is a Tits system  $(G, B, N, S)$ .

### Multiplicative Group in a Finite Ring

**COROLLARY 2.12.** *If  $G$  is the multiplicative group of a finite semisimple ring  $R$ , then there is a Tits system  $(G, B, N, S)$ .*

*Proof.* By Theorem 1.1,  $R \cong \bigoplus_{i=1}^n M_i$  where  $M_i$  is the matrix ring of all  $n_i \times n_i$  matrices over a finite field  $F_i$ . For the simplicity of notation, we can assume that  $R = \bigoplus_{i=1}^n M_i$ . Let  $G_i$  be the multiplicative group of  $M_i$  for each  $i = 1, 2, \dots, n$ . By the above argument, there is a Tits system  $(G_i, B_i, N_i, S_i)$  for each  $i = 1, 2, \dots, n$ .

Note that  $G = \bigoplus_{i=1}^n G_i$ . Let  $B = \bigoplus_{i=1}^n B_i$ ,  $N = \bigoplus_{i=1}^n N_i$ , and  $S = \bigoplus_{i=1}^n S_i$ . It is easy to show that  $(G, B, N, S)$  is a Tits system for  $G$ .

### 3. Multiplicative Group in a Finite Ring with Identity

In this section, we will show that in the multiplicative group  $G$  of a finite ring with identity 1, there is a Tits system  $(G, B, N, S)$ .

**LEMMA 3.1.** *Let  $R$  be a finite ring with identity 1, let  $J$  the Jacobson radical of  $R$ , let  $G$  the multiplicative group of  $R$  and let  $\overline{G}$  the multiplicative group of  $\overline{R} = R/J$ . Then  $g \in G$  if and only if  $g + J \in \overline{G}$ .*

*Proof.*  $(\Rightarrow)$  Clear.

$(\Leftarrow)$  Suppose that  $\overline{g} = g + J \in \overline{G}$ . Then there exists  $\overline{h} = h + J$  such that  $\overline{g}\overline{h} = \overline{h}\overline{g} = \overline{1}$  (where  $\overline{1}$  is the identity of  $\overline{G}$ ), and so  $1 - gh$  and  $1 - hg \in J$ . Since  $J$  is a two-sided quasi left ideal of  $R$  and  $R$  has identity 1,  $1 - (1 - gh) = gh$  and  $1 - (1 - hg) = hg$  are invertible in  $G$  by Theorem 2.3 through Lemma 2.8, in [4, pp.426-428]. Hence  $(gh)x = y(hg) = 1$  for some  $x$  and  $y \in G$ . Therefore,  $g \in G$ .

**LEMMA 3.2.** *Let  $\phi : A \rightarrow B$  be a ring homomorphism which is onto. If  $P$  and  $Q$  are subsets of  $B$ , then  $\phi^{-1}(PQ) = \phi^{-1}(P)\phi^{-1}(Q)$ .*

*Proof.* If  $a \in \phi^{-1}(PQ)$ , then  $\phi(a) \in PQ$ ,  $\phi(a) = pq$  for some  $p \in P$  and  $q \in Q$ . Since  $\phi$  is onto, there exist  $p_0$  and  $q_0 \in A$  such that  $\phi(p_0) = p$  and  $\phi(q_0) = q$ . Then  $\phi(a) = \phi(p_0)\phi(q_0) \in \phi(\phi^{-1}(P)\phi^{-1}(Q))$ , and so  $a \in \phi^{-1}(P)\phi^{-1}(Q)$ .

If  $a \in \phi^{-1}(P)\phi^{-1}(Q)$ , then  $a = xy$  for some  $x \in \phi^{-1}(P)$  and  $y \in \phi^{-1}(Q)$ . Thus  $\phi(a) = \phi(xy) = \phi(x)\phi(y) \in PQ$ , and so  $a \in \phi^{-1}(PQ)$ .

**PROPOSITION 3.3.** *Let  $R$  be a finite ring with identity and  $G$  be the multiplicative group of  $R$ . Then  $G$  has a  $(B^*, N^*)$ -pair satisfying the following conditions;*

- (1)  $G = B^*N^*B^*$  where  $B^*$  and  $N^*$  are subgroups of  $G$ .
- (2)  $B^* \cap N^*$  is a normal subgroup of  $N^*$  and  $W^* = N^*/(B^* \cap N^*)$  is generated by a set  $S^* = \{s_1^*, s_2^*, \dots, s_k^*\}$  where  $s_i \in N^*/(B^* \cap N^*)$ ,  $s_i^2 \equiv 1$  and  $s_i^* \neq 1$ .
- (3) For any  $s^* \in S^*$  and  $w^* \in W^*$ , we have  $s^*B^*w^* \subset B^*w^*B^* \cup B^*s^*w^*B^*$ .
- (4) We have  $s^*B^*s^* \not\subseteq B^*$  for any  $s^* \in S^*$ .

*Proof.* Let  $\pi : R \rightarrow \overline{R} = R/J$  be the canonical ring homomorphism where  $J$  is the Jacobson radical of  $R$ . For any  $g \in G$ ,  $\pi(g) = g + J = \overline{g} \in \pi(G) = \overline{G}$  by Lemma 3.1. By Corollary 2.12,  $\overline{G} = \overline{B}\overline{N}\overline{B}$  for some subgroups  $B$  and  $N$  of  $\overline{G}$ . Thus it follows from Lemma 3.2 that  $g \in \pi^{-1}(\overline{G}) = \pi^{-1}(B\overline{N}B) = \pi^{-1}(B)\pi^{-1}(N)\pi^{-1}(B)$ . Hence  $G = \pi^{-1}(B)\pi^{-1}(N)\pi^{-1}(B)$ . Clearly,  $B^* = \pi^{-1}(B)$  and  $N^* = \pi^{-1}(N)$  are subgroups of  $G$ . If  $n \in N^*$  and  $a \in B^* \cap N^*$ , then  $\pi(n) \in N$  and  $\pi(a) \in B \cap N$ . Note that  $\pi(n)\pi(a)\pi(n)^{-1} = \pi(nan^{-1}) \in B \cap N$  since  $B \cap N$  is a normal subgroup of  $N$ . Thus  $nana^{-1} \in \pi^{-1}(B \cap N) = \pi^{-1}(B) \cap \pi^{-1}(N) = B^* \cap N^*$ , and so  $B^* \cap N^*$  is a normal subgroup of  $N^*$ .

Let  $n_0(B^* \cap N^*)$  be arbitrary element of  $N^*/(B^* \cap N^*)$ . By Corollary 2.12,  $N^*/(B^* \cap N^*)$  is generated by a subset  $S = \{\overline{s}_1, \overline{s}_2, \dots, \overline{s}_k\}$  of  $N^*/(B^* \cap N^*)$  where  $\overline{s}_i^2 \equiv 1$  and  $\overline{s}_i \neq 1$ . Let  $n = \pi(n_0) \in N$ . Then  $n(B \cap N)$  can be a finite product of elements of  $S$ , say  $n(B \cap N) = \overline{s}_1 \cdot \overline{s}_2 \dots \overline{s}_t = s_1 \cdot s_2 \dots s_t(B \cap N)$  where  $\overline{s}_i = s_i(B \cap N)$ ,  $i = 1, 2, \dots, t$  for some positive integer  $t$ . Note that  $n(s_1 \cdot s_2 \dots s_t)^{-1} \in B \cap N$ . Since  $\pi$  is onto, there exists  $s_i^* \in N^*$  such that  $\pi(s_i^*) = s_i$  for each  $i = 1, 2, \dots, t$ . Thus  $n(s_1 \cdot s_2 \dots s_t)^{-1} = \pi(n_0)\pi(s_1^* \cdot s_2^* \dots s_t^*)^{-1} = \pi(n_0(s_1^* \dots s_t^*)^{-1}) \in (B \cap N)$ , and hence  $n_0(s_1^* \cdot s_2^* \dots s_t^*)^{-1} = \pi^{-1}(B \cap N) = B^* \cap N^*$ ,  $n_0(B^* \cap N^*) = (s_1^* \cdot s_2^* \dots s_t^*)(B^* \cap N^*) = s_1^*(B^* \cap N^*) \cdot s_2^*(B^* \cap N^*) \dots s_t^*(B^* \cap N^*)$ , which means that  $n_0(B^* \cap N^*)$  can be a finite product of elements of  $S = \{\overline{s}_1, \overline{s}_2, \dots, \overline{s}_k\}$ . Therefore,  $N^*/(B^* \cap N^*)$  is generated by a subset  $S^* = \{s_1^*, s_2^*, \dots, s_k^*\}$ .

Since  $\overline{s}B\overline{s} \not\subseteq B$  for any  $\overline{s} \in S$ , it is easy to show that  $\overline{s}^*B\overline{s}^* \not\subseteq B^*$



## Multiplicative Group in a Finite Ring

for any  $\bar{s} \in S^*$ . It remains to show that  $\bar{s}^*B\bar{w}^* \subset B^*\bar{w}^*B^* \cup B^*\bar{s}^*\bar{w}^*B^*$  for any  $\bar{s}^* \in S^*$  and  $\bar{w}^* \in W^*$ . Let  $\pi(\bar{s}^*) = \bar{s}$  and  $\pi(\bar{w}^*) = \bar{w}$  for any  $\bar{s}^* \in S^*$  and  $\bar{w}^* \in W^*$ . Then  $\bar{s} \in S$  and  $\bar{w} \in W$ , and so by Corollary 2.12, we have  $\bar{s}B\bar{w} \subset B\bar{w}B \cup B\bar{s}\bar{w}B$ . Hence it follows from Lemma 3.2 that  $\bar{s}^*B^*\bar{w}^* \subset \pi^{-1}(\bar{s})\pi^{-1}(B)\pi^{-1}(\bar{w}) = \pi^{-1}(\bar{s}B\bar{w}) \subset \pi^{-1}(B\bar{s}B \cup B\bar{s}\bar{w}B) \subset \pi^{-1}(B\bar{s}B) \cup \pi^{-1}(B\bar{s}\bar{w}B) = \pi^{-1}(B)\pi^{-1}(\bar{s})\pi^{-1}(B) \cup \pi^{-1}(B)\pi^{-1}(\bar{s})\pi^{-1}(\bar{w})\pi^{-1}(B) = B^*\bar{w}^*B^* \cup B^*\bar{s}^*B^* \cup B^*\bar{s}^*\bar{w}^*B^*$ .

## References

1. Anderson, F.W. and Fuller, K.R., *Rings and Category of Modules*, New York, Springer-Verlag, 1974.
2. Cohen, J and Koh, K., *The subring Generated by the Units in a Compact Ring*, *Communications in Algebra* . **18(5)** (1990), 1617-1620.
3. Cohen, J and Koh, K., *The Group of Units in a Compact Ring*, *Journal of Pure and Applied Algebra* **54** (1988), 167-179.
4. Hungerford, T.W., *Algebra*, New-York, Holt, Rinehart and Winston Inc., 1976.
5. Jacobson, N., *Structure of rings*, Amer. Math. Soc. Colloq. Publ. Rev. Ed. Providence: AMS **37** (1964).
6. Lambek, J., *Lectures on rings and Modules*, New-York, Chelsea Publ. Com., 1976.
7. Suzuki, M., *Group Theory I*, New-York, Springer-Verlag, 1982.

DEPARTMENT MATHEMATICS, KOSHIN UNIVERSITY, PUKJAN 606-080, KOREA