Bull. Korean Math. Soc. **43** (2006), No. 3, pp. 619–626

THE GENERAL LINEAR GROUP OVER A RING

JUNCHEOL HAN

ABSTRACT. Let m be any positive integer, R be a ring with identity, $M_m(R)$ be the matrix ring of all m by m matrices over R and $G_m(R)$ be the multiplicative group of all m by m nonsingular matrices in $M_m(R)$. In this paper, the following are investigated: (1) for any pairwise coprime ideals $\{I_1, I_2, \ldots, I_n\}$ in a ring R, $M_m(R/(I_1 \cap I_2 \cap \cdots \cap I_n))$ is isomorphic to $M_m(R/I_1) \times M_m(R/I_2) \times \cdots \times M_m(R/I_n)$, and so $G_m(R/(I_1 \cap I_2 \cap \cdots \cap I_n))$ is isomorphic to $G_m(R/I_1) \times G_m(R/I_2) \times \cdots \times G_m(R/I_n)$; (2) In particular, if R is a finite ring with identity, then the order of $G_m(R)$ can be computed.

1. Introduction

Throughout this paper all rings are assumed to be rings with identity. Let I be an ideal in a ring R and $a, b \in R$. Recall that a is said to be congruent to b modulo I (denoted $a \equiv b \pmod{I}$) if $a - b \in I$. Clearly, the congruence relation is an equivalence relation on R. Two ideals I, I' of R are *coprime* if $I + I' = R$. A set of nonzero ideals $\{I_1, I_2, \ldots, I_n\}$ in a ring R is *pairwise coprime* if $I_j + I_k = R$ for all $j, k = 1, 2, \ldots, n$ $(j \neq k)$.

THEOREM 1.1. (Chinese Remainder Theorem) *Let $\{I_1, I_2, \ldots, I_n\}$ be pairwise coprime ideals in a ring R. If $b_1, b_2, \ldots, b_n \in R$, then there exists $b \in R$ such that $b \equiv b_i (\text{mod } I_i)$ $(i = 1, 2, \ldots, n)$. Furthermore, b is uniquely determined up to congruence modulo the ideal $I_1 \cap I_2 \cap \cdots \cap I_n$.*

Proof. See [1, Theorem 2.25]. □

Received October 11, 2005.
2000 Mathematics Subject Classification: Primary 11C20; Secondary 15A36.
Key words and phrases: coprime ideals, general linear group of degree m over a ring, congruence relation $\equiv_m$, order of group.
This work was supported by Pusan National University Research Grant.

COROLLARY 1.2. *Let $\{I_1, I_2, \ldots, I_n\}$ be pairwise coprime ideals in a ring R. Then $R/(I_1 \cap I_2 \cap \cdots \cap I_n)$ is isomorphic to $R/I_1 \times R/I_2 \times \cdots \times R/I_n$ as rings.*

Proof. See [1, Corollary 2.27]. □

REMARK 1. For any pairwise coprime ideals $\{I_1, I_2, \ldots, I_n\}$ in a commutative ring R, $I_1 \cap I_2 \cap \cdots \cap I_n = I_1 \cdot I_2 \cdots I_n$.

Let m be a positive integer and $M_m(R)$ be the matrix ring of all $m \times m$ matrices over a ring R. Consider the following relation $\equiv_m$ defined on $M_m(R)$: For any $A = [a_{ij}]$ and $B = [b_{ij}] \in M_m(R)$, $A \equiv_m B(\text{mod } I)$ (we read this A is congruent to B modulo I) if $a_{ij} \equiv b_{ij}$ (modulo I) for all $i, j = 1, 2, \ldots, m$ (i.e., a_{ij} - $b_{ij} \in I$). We can observe that the congruence relation $\equiv_m$ is an equivalence relation on $M_m(R)$ satisfying the following properties:
For any A, B, C and $D \in M_m(R)$ such that $A \equiv_m B(\text{mod } I)$ and $C \equiv_m D(\text{mod } I)$,

[1] $A + C \equiv_m B + D(\text{mod } I)$.

[2] $AC \equiv_m BD(\text{mod } I)$. In particular, $A^s \equiv_m B^s(\text{mod } I)$ for all positive integers s.

In this paper, we denote $G(R)$ by the multiplicative group of all units in R and $G_m(R)$ by the multiplicative group of all nonsingular matrices in $M_m(R)$.

THEOREM 1.3. *Let m and n be any positive integers, R be a ring and $\{I_1, I_2, \ldots, I_n\}$ be pairwise coprime ideals in a ring R. If $A_1 = [a_{ij}^{(1)}], A_2 = [a_{ij}^{(2)}], \ldots, A_n = [a_{ij}^{(n)}] \in M_m(R)$, then there exists $A \in M_m(R)$ such that $A \equiv A_k(\text{mod } I_k)$ for all $k = 1, 2, \ldots, n$. Furthermore, A is uniquely determined up to congruence modulo the ideal $I_1 \cap I_2 \cap \cdots \cap I_n$.*

Proof. Since $a_{ij}^{(1)}, a_{ij}^{(2)}, \ldots, a_{ij}^{(n)} \in R$ for all $i, j = 1, 2, \ldots, m$, there exists $a_{ij} \in R$ such that $a_{ij} \equiv a_{ij}^{(k)}(\text{mod } I_k)$ $(k = 1, 2, \ldots, n)$ by Theorem 1.1. Let $A = [a_{ij}] \in M_m(R)$. Then $A \equiv_m A_k$ $(\text{mod } I_k)(k = 1, 2, \ldots, n)$. Since a_{ij} is uniquely determined up to congruence modulo the ideal $I_1 \cap I_2 \cap \cdots \cap I_n$ for all $i, j = 1, 2, \ldots, m$, A is also uniquely determined up to congruence modulo the ideal $I_1 \cap I_2 \cap \cdots \cap I_n$. □

COROLLARY 1.4. *Let m and n be any positive integers, R be a ring and $\{I_1, I_2, \ldots, I_n\}$ be ideals in a ring R. Then there is a monomorphism* *of rings* $\theta : M_m(R/(I_1 \cap I_2 \cap \cdots \cap I_n)) \longrightarrow M_m(R/I_1) \times M_m(R/I_2) \times \cdots \times M_m(R/I_n)$. *If* $\{I_1, I_2, \ldots, I_n\}$ *is pairwise coprime, then* θ *is an isomorphism.*

Proof. Consider a map $\theta_1 : M_m(R) \longrightarrow M_m(R/I_1) \times M_m(R/I_2) \times \cdots \times M_m(R/I_n)$ defined by $\theta_1([a_{ij}]) = ([a_{ij}+I_1], [a_{ij}+I_2], \ldots, [a_{ij}+I_n])$ for all $[a_{ij}] \in M_m(R)$. It is straightforward to show that θ_1 is a ring homomorphism and the kernel of θ_1 (denoted by $ker(\theta_1)$) is $M_m(I_1 \cap I_2 \cap \cdots \cap I_n)$. Since $M_m(R)/ker(\theta_1)$ is isomorphic to $M_m(R/(I_1 \cap I_2 \cap \cdots \cap I_n))$, the map $\theta : M_m(R/(I_1 \cap I_2 \cap \cdots \cap I_n)) \longrightarrow M_m(R/I_1) \times M_m(R/I_2) \times \cdots \times M_m(R/I_n)$ is a monomorphism. Suppose that $\{I_1, I_2, \ldots I_n\}$ is a pairwise coprime ideals in a ring R. To show that θ is an isomorphism, it is enough to show that θ is onto. Let $([a_{ij}^{(1)} + I_1], [a_{ij}^{(2)} + I_2], \ldots, [a_{ij}^{(n)} + I_n]) \in M_m(R/I_1) \times M_m(R/I_2) \times \cdots \times M_m(R/I_n)$ be arbitrary. Then by Theorem 1.3, there exists $[a_{ij}] \in M_m(R)$ such that $[a_{ij}] \equiv [a_{ij}^{(k)}] (\text{mod } I_k)$ for all $k = 1, 2, \ldots, n$. Thus $\theta([a_{ij}] + I_1 \cap I_2 \cap \cdots \cap I_n) = ([a_{ij}^{(1)} + I_1], [a_{ij}^{(2)} + I_2], \ldots, [a_{ij}^{(n)} + I_n])$, and so θ is an isomorphism. □

COROLLARY 1.5. *Let* m *and* k *be any positive integers,* $\mathbb{Z}_k$ *be the ring of integers modulo* k. *If* $p_1^{n_1} \cdot p_2^{n_2} \cdots p_s^{n_s}$ *is the prime factorization of* k, *then* $M_m(\mathbb{Z}_k)$ *is isomorphic to* $M_m(\mathbb{Z}_{p_1^{n_1}}) \times M_m(\mathbb{Z}_{p_2^{n_2}}) \times \cdots \times M_m(\mathbb{Z}_{p_s^{n_s}})$.

Proof. Let $I_i = p_i^{n_i}\mathbb{Z}$ be an ideal of $\mathbb{Z}$, the ring of integers, for all $i = 1, 2, \ldots, s$. Since $p_1^{n_1} \cdot p_2^{n_2} \cdots p_s^{n_s}$ is the prime factorization of k, the set of ideals $\{I_1, \ldots, I_s\}$ is pairwise coprime. Since $M_m(\mathbb{Z}/I_i)$ is isomorphic to $M_m(\mathbb{Z}_{p_i^{n_i}})$ for all $i = 1, 2, \ldots, s$, $M_m(\mathbb{Z}_k)$ is isomorphic to $M_m(\mathbb{Z}_{p_1^{n_1}}) \times M_m(\mathbb{Z}_{p_2^{n_2}}) \times \cdots \times M_m(\mathbb{Z}_{p_s^{n_s}})$ by Corollary 1.4. □

COROLLARY 1.6. *Let* m *and* n *be any positive integers and* $\{I_1, I_2, \ldots, I_n\}$ *be ideals in a ring* R. *If* $\{I_1, I_2, \ldots, I_n\}$ *is pairwise coprime, then* $G_m(R/(I_1 \cap I_2 \cap \cdots \cap I_n))$ *is isomorphic to* $G_m(R/I_1) \times G_m(R/I_2) \times \cdots \times G_m(R/I_n)$.

Proof. By Corollary 1.4, $M_m(R/(I_1 \cap I_2 \cap \cdots \cap I_n))$ is isomorphic to $M_m(R/I_1) \times M_m(R/I_2) \times \cdots \times M_m(R/I_n)$. Since $G_m(R/(I_1 \cap I_2 \cap \cdots \cap I_n))$, the multiplicative group of $M_m(R/I_1) \times M_m(R/I_2) \times \cdots \times M_m(R/I_n)$, is $G_m(R/I_1) \times G_m(R/I_2) \times \cdots \times G_m(R/I_n)$, $G_m(R/(I_1 \cap I_2 \cap \cdots \cap I_n))$ is isomorphic to $G_m(R/I_1) \times G_m(R/I_2) \times \cdots \times G_m(R/I_n)$. □

Corollary 1.7. *Let m and k be any positive integers, $\mathbb{Z}_k$ be the ring of integers modulo k. If $p_1^{n_1} \cdot p_2^{n_2} \cdots p_s^{n_s}$ is the prime factorization of k, then $G_m(\mathbb{Z}_k)$ is isomorphic to $G_m(\mathbb{Z}_{p_1^{n_1}}) \times G_m(\mathbb{Z}_{p_2^{n_2}}) \times \cdots \times G_m(\mathbb{Z}_{p_s^{n_s}})$.*

Proof. It follows from Corollary 1.5 and Corollary 1.6. □

2. The order of $G_m(R)$ when R is a commutative ring

Let R be a finite commutative ring. In this section, we will compute the order of $G_m(R)$, the multiplicative group of all nonsingular matrices in $M_m(R)$ (called the general linear group of degree m over R) for all positive integers m. We will denote the order of $G_m(R)$ by $|G_m(R)|$. In [2], the following Theorem has been shown:

Theorem 2.1. *Let R be a finite commutative ring. Then R decomposes (up to order of summands) uniquely as a direct product of local rings. Precisely, $R \simeq (R/P_1^t) \times (R/P_2^t) \times \cdots \times (R/P_n^t)$ for some positive integers n and t, where $P_1, \ldots, P_n$ are all distinct prime (equally maximal) ideals of R.*

Proof. See [2, Theorem VI.2]. □

Lemma 2.2. *Let R and S be any two rings. Then $M_m(R \times S) \simeq M_m(R) \times M_m(S)$.*

Proof. Define $\phi : M_m(R \times S) \to M_m(R) \times M_m(S)$ by $\phi([(a_{ij}, b_{ij})]) = ([a_{ij}], [b_{ij}])$ for all $[(a_{ij}, b_{ij})] \in M_m(R \times S)$. Then it is straightforward to show that ϕ is an isomorphism. □

Corollary 2.3. *Let R be a finite commutative ring such that $R \simeq (R/P_1^t) \times (R/P_2^t) \times \cdots \times (R/P_n^t)$ for some positive integers n and t, where $P_1, P_2, \ldots, P_n$ are all distinct prime ideals of R given in Theorem 2.1. Then $G_m(R) \simeq G_m(R/P_1^t) \times G_m(R/P_2^t) \times \cdots \times G_m(R/P_n^t)$.*

Proof. It follows from Corollary 1.6 and Lemma 2.2. □

Corollary 2.4. *Let R be a finite commutative ring such that $R \simeq (R/P_1^t) \times (R/P_2^t) \times \cdots \times (R/P_n^t)$ for some positive integers n and t, where $P_1, P_2, \ldots, P_n$ are all distinct prime ideals of R given in Theorem 2.1. Then $|G_m(R)| = |G_m(R/P_1^t)| \cdot |G_m(R/P_2^t)| \cdots |G_m(R/P_n^t)|$.*

Proof. It follows from Corollary 2.3. □

To compute $|G_m(R)|$, by Corollary 2.4 it is enough to compute $|G_m(R/P_i^t)|$ for all $i = 1, \ldots, n$, where $P_1, P_2, \ldots, P_n$ are all distinct prime (equally maximal) ideals of R given in Theorem 2.1.

THEOREM 2.5. *Let R be a commutative ring and m be any positive integer. Then $A \in M_m(R)$ is invertible if and only if $|A|$, the determinant of $A \in R$, is a unit in R.*

Proof. See [1, Proposition 3.7]. □

LEMMA 2.6. *Let R be a commutative ring, P be an ideal of R and k $(k \geq 2)$ be a positive integer. Then*

(1) *the map $\sigma : R/P^k \to R/P^{k-1}$ defined by $\sigma(a + P^k) = a + P^{k-1}$ for all $a + P^k \in R/P^k$ is a natural ring homomorphism.*

(2) *$\sigma|_{G(R/P^k)}$, the restriction of σ to $G(R/P^k)$, is a group homomorphism from $G(R/P^k)$ into $G(R/P^{k-1})$.*

(3) *In addition, if R is a local ring with the maximal ideal P, then $\sigma|_{G(R/P^k)}$ is onto.*

Proof. (1) Since $P^k \subseteq P^{k-1}$, the map $\sigma : R/P^k \to R/P^{k-1}$ defined by $\sigma(a + P^k) = a + P^{k-1}$ for all $a + P^k \in G(R/P^k)$ is well-defined. Clearly, σ is a ring homomorphism.

(2) For all $\bar{a} = a + P^k \in G(R/P^k)$, there exists $\bar{b} = b + P^k \in G(R/P^k)$ such that $\bar{a}\bar{b} = \bar{b}\bar{a} = \bar{1} = 1 + P^k$. Thus $1 - ab, 1 - ba \in P^k$. Since $P^k \subseteq P^{k-1}$, $1 - ab, 1 - ba \in P^{k-1}$, and then $a + P^{k-1} \in G(R/P^{k-1})$. Thus the map $\sigma|_{G(R/P^k)}$ is well-defined. For all $a + P^k, c + P^k \in G(R/P^k)$, $\sigma|_{G(R/P^k)}((a + P^k)(c + P^k)) = \sigma|_{G(R/P^k)}(ac + P^k) = ac + P^{k-1} = (a + P^{k-1})(c + P^{k-1})$. Hence $\sigma|_{G(R/P^k)}$ is a group homomorphism.

(3) Let $a + P^{k-1} \in G(R/P^{k-1})$ be arbitrary. Then there exists $b + P^{k-1} \in G(R/P^{k-1})$ such that $ab + P^{k-1} = (a + P^{k-1})(b + P^{k-1}) = (b + P^{k-1})(a + P^{k-1}) = ba + P^{k-1} = 1 + P^{k-1}$. Thus $1 - ab, 1 - ba \in P^{k-1}$. Since $(R/P^k)/(P^{k-1}/P^k) \simeq R/P^{k-1}$ by the Third Isomorphism Theorem of Rings, without loss of generality we can let $(R/P^k)/(P^{k-1}/P^k) = R/P^{k-1}$, i.e., $(a + P^k) + (P^{k-1}/P^k) = \sigma(a + P^{k-1}) = a + P^{k-1}$ for all $a + P^{k-1} \in R/P^{k-1}$, where σ is a natural ring homomorphism given in (1). Since $ab + P^{k-1} = ba + P^{k-1} = 1 + P^{k-1}$, $ab - 1 + P^k, ba - 1 + P^k \in P^{k-1}/P^k$, and so $ab - 1, ba - 1 \in P^{k-1} \subseteq P$. Thus $ab, ba \in 1 + P$. Since R is a local ring with the maximal ideal P, $1 + P \subseteq G(R)$. Therefore, $a \in G(R)$, and so $a + P^k \in G(R/P^k)$. Therefore, $\sigma|_{G(R/P^k)}$ is onto. □

THEOREM 2.7. *Let R be a finite local commutative ring, P be the unique maximal ideal of R and k be a positive integer. Then*

(1) *there exists a normal subgroup N of $G_m(R/P^k)$ such that $G_m(R/P^k)/N \simeq G_m(R/P^{k-1})$.*

(2) *$|G_m(R/P^k)| = (|P^{k-1}|/|P^k|)^{m^2} \cdot |G_m(R/P^{k-1})|$ for all positive integer m.*

(3) *$|G_m(R/P^k)| = (|P/P^k|)^{m^2} \cdot |G_m(R/P)|$ for all positive integer m, where $|G_m(R/P)| = (|R/P|^m - 1)(|R/P|^m - |R/P|) \cdots (|R/P|^m - |R/P|^{m-1})$.*

Proof. (1) Consider the map $\theta : G_m(R/P^k) \to G_m(R/P^{k-1})$ defined by $\theta([a_{ij} + P^k]) = [\sigma(a_{ij} + P^k)] = [a_{ij} + P^{k-1}]$ for all $[a_{ij} + P^k] \in G_m(R/P^k)$, where $\sigma|_{G(R/P^k)}$ is a group homomorphism given in Lemma 2.6. The map θ is well-defined. Indeed, for all $A = [a_{ij} + P^k] \in G_m(R/P^k)$, $|A| \in G(R/P^k)$ by Theorem 2.5, and also $|A| \in G(R/P^{k-1})$. It is easy to show that θ is a group homorphism. Next, we will show that θ is onto. Let $B = (b_{ij} + p^{k-1}) \in G_m(R/P^{k-1})$ be arbitrary. By Theorem 2.5, $|B| \in G(R/P^{k-1})$, where $|B|$ is the determinant of B. By Lemma 2.6, there exists $b_{ij} + P^k \in R/P^k$ such that $\sigma(b_{ij} + P^k) = b_{ij} + P^{k-1}$ for all $i, j = 1, \ldots, m$. Let $B_0 = [b_{ij} + P^k] \in M_m(R/P^k)$. Since $\sigma(|B_0|) = |B|$ and $|B| \in G(R/P^{k-1})$, $|B_0| \in G(R/P^k)$ and so $B_0 \in G_m(R/P^{k-1})$. Thus $\theta(B_0) = B$ and so θ is onto. Let $N = Ker(\theta)$. By the First Isomorphism Theorem of Groups, $G_m(R/P^k)/N \simeq G_m(R/P^{k-1})$.

(2) We can note that $ker(\theta) = \{[a_{ij} + P^k] \in G_m(R/P^k) : a_{ii} \in 1 + P^{k-1}, a_{ij} \in P^{k-1}(i, j = 1, \ldots, m, i \neq j)\}$. Hence the order of $Ker(\theta)$ can be computed by $|Ker(\theta)| = (|P^{k-1}/P^k|)^{m^2} = (|P^{k-1}|/|P^k|)^{m^2}$. By (1), the order of $G_m(R/P^k)$ can be computed by $|G_m(R/P^k)| = |Ker(\theta)| \cdot |G_m(R/P^{k-1})| = (|P^{k-1}|/|P^k|)^{m^2} \cdot |G_m(R/P^{k-1})|$ for all positive integer m.

(3) By (2) and mathematical induction on k, we can compute $|G_m(R/P^k)| = (|P/P^k|)^{m^2} \cdot |G_m(R/P)|$. Since R/P is a finite field, by [2 , Theorem VIII.19], $|G_m(R/P)| = (|R/P|^m - 1)(|R/P|^m - |R/P|) \cdots (|R/P|^m - |R/P|^{m-1})$. Hence we have the result. □

COROLLARY 2.8. *Let p be a prime integer, k and m be any positive integers and $\mathbb{Z}_{p^k}$ be the ring of integers modulo p^k. Then $|G_m(\mathbb{Z}_{p^k})| = p^{m^2} \cdot |G_m(\mathbb{Z}_{p^{k-1}})| = \cdots = p^{(k-1)m^2} \cdot |G_m(\mathbb{Z}_p)|$, where $|G_m(\mathbb{Z}_p)| = (p^m - 1)(p^m - p) \cdots (p^m - p^{m-1})$.*

Proof. Since $\mathbb{Z}_{p^k}$ is a finite local commutative ring and $P = p\mathbb{Z}_{p^k}$ is the unique maximal ideal of $\mathbb{Z}_{p^k}$, we have the result by Theorem 2.7. □

COROLLARY 2.9. *Let m and k be any positive integers. If $p_1^{n_1} \cdot p_2^{n_2} \cdots p_s^{n_s}$ is the prime factorization of k, then the order of $G_m(\mathbb{Z}_k)$ can be computed by $|G_m(\mathbb{Z}_k)| = |G_m(\mathbb{Z}_{p_1^{n_1}})| \cdot |G_m(\mathbb{Z}_{p_2^{n_2}})| \cdots |G_m(\mathbb{Z}_{p_s^{n_s}})|$.*

Proof. It follows from Corollary 1.7 and Corollary 2.8. □

3. The order of $G_m(R)$ when R is a noncommutative ring

Let R be a finite (not necessary commutative) ring and $J(R)$ be the Jacobson radical of R. In this section, we will also compute $|G_m(R)|$, the order of $G_m(R)$, for all positive integers m. By the Wedderburn-Artin Theorem, $M_m(R)/J(M_m(R)) \cong \oplus_{i=1}^n M_i(F_i)$, where $M_i(F_i)$ is the full matrix ring of all n_i by n_i matrices over a finite field F_i for each $i = 1, 2, \ldots, n$ and for some positive integer n_i.

LEMMA 3.1. *Let R be a ring and $G(R)$ be the group of all units in R. Then $G(R)/(1 + J(R)) \cong G(R/J(R))$.*

Proof. Note that the map $\phi : G(R) \to G(R/J(R))$ defined by $\phi(g) = g + J(R)$ for all $g \in G(R)$ is epimorphism and $ker(\phi) = 1 + J(R)$. Hence we have $G(R)/(1+J(R)) \cong G(R/J(R))$ by the First Fundamental Homomorphism Theorem of groups. □

COROLLARY 3.2. *Let R be a finite (not necessary commutative) ring such that $M_m(R)/J(M_m(R)) \cong \oplus_{i=1}^n M_i(F_i)$, where $M_i(F_i)$ is the full matrix ring of all $n_i \times n_i$ matrices over a finite field F_i for each $i = 1, 2, \ldots, n$ and for some positive integer n_i. Then $|G_m(R)| = |J(R)|^{m^2} \cdot \prod_{i=1}^n |G_i(F_i)|$, where $G_i(F_i)$ is the group of all nonsingular matrices in $M_i(F_i)$ for all $i = 1, \ldots, n$.*

Proof. Since $M_m(R)/J(M_m(R)) \cong M_m(R/J(R))$, $M_m(R/J(R)) \cong \oplus_{i=1}^n M_i(F_i)$ and so $G_m(R/J(R)) \cong \oplus_{i=1}^n G_i(F_i)$. Since $J(M_m(R)) = M_m(J(R))$ and $|1 + J(M_m(R))| = |J(M_m(R))|$, by Lemma 3.1 we have $|G_m(R)| = |1+J(M_m(R))| \cdot \prod_{i=1}^n |G_i(F_i)| = |J(M_m(R))| \cdot \prod_{i=1}^n |G_i(F_i)| = |M_m(J(R))| \cdot \prod_{i=1}^n |G_i(F_i)| = |J(R)|^{m^2} \cdot \prod_{i=1}^n |G_i(F_i)|$. □

COROLLARY 3.3. *Let R be a finite (not necessary commutative) local ring. Then $|G_m(R)| = |J(R)|^{m^2} \cdot |G_m(R/J(R))|$.*

Proof. By Lemma 3.1, $G_m(R)/(1+J(M_m(R)) \cong G_m(R/J(R))$. Hence $|G_m(R)| = |J(R)|^{m^2} \cdot |G_m(R/J(R))|$ by the similar argument given in the proof of Corollary 3.2. □

REMARK 2. Let R be a finite commutative local ring. Since the unique maximal ideal of R is the Jacobson radical J of R and $J^k = (0)$ for some positive integer k, by Theorem 2.6 $|G_m(R)| = |G_m(R/J^k)| = (|J/J^k|)^{m^2} \cdot |G_m(R/J)| = |J|^{m^2} \cdot |G_m(R/J)|$ for all positive integer m. Even though R is not commutative, $|G_m(R)| = |J|^{m^2} \cdot |G_m(R/J)|$ holds by Corollary 3.3.

ACKNOWLEDGEMENTS. The author thanks Prof. G. F. Birkenmeier at the University of Louisiana for helpful suggestions for making the paper. The author also thanks Prof. J. Park at the Pusan National University for reading this paper and helpful discussions. The author expresses his thanks to the referee for helpful suggestions for making the paper more readable.

References

[1] T. W. Hungerford, *Algebra*, Springer-Verlag, New York-Belin, 1980.
[2] B. R. McDonald, *Finite Rings with Identity*, Marcel Dekker, Inc, New York, 1974.

DEPARTMENT OF MATHEMATICS EDUCATION, PUSAN NATIONAL UNIVERSITY, PUSAN 609-735, KOREA
E-mail: jchan@pusan.ac.kr