Generalized group of units

2 authors:

Abdul-Nasser El-Kassar
Lebanese American University
89 PUBLICATIONS **4,057** CITATIONS

Haissam Chehade
Lebanese International University
14 PUBLICATIONS **16** CITATIONS

Mathematica
Balkanica

New Series Vol. 20, 2006, Fasc. 3-4

Generalized Group of Units

A. N. El-Kassar and H. Y. Chehade

Presented by V. Kiryakova

A generalization of the group of units of a finite commutative ring with identity is presented and the properties of the generalized group of units are examined. Several problems concerning the generalized group of units are considered and solutions for certain special classes of finite commutative rings with identity obtained.

AMS Subject Classification: Primary 16U60; Secondary 16P10,11A25
Key Words: Finite rings, group of units, cyclic groups

1. Introduction

Let R be a finite commutative ring with identity and let $U(R)$ be its group of units. The order of R and the order of its group of units will be denoted by $|R|$ and $|U(R)|$, respectively. In the case when $R = \mathbf{Z}_n$, $|U(R)| = \phi(n)$, where $\phi(n)$ is Euler's phi-function, the number of positive integers less than n and relatively prime to n. If $n = p_1^{a_1}.p_2^{a_2}...p_r^{a_r}$ is the decomposition of n into product of distinct prime powers, then $\phi(n) = (p_1-1)p_1^{a_1-1}.(p_2-1)p_2^{a_2-1}...(p_r-1)p_r^{a_r-1}$.

It is well known that if a finite commutative ring with identity R decomposes as a direct sum $R = R_1 \oplus R_2 \oplus ... \oplus R_i$, then its group of units decomposes naturally as a direct product of groups. That is, $U(R)$ is isomorphic to $U(R_1) \times U(R_2) \times ... \times U(R_i)$. The symbol $\cong$ will be used for both ring and group isomorphism. Note that if two rings R and S are isomorphic, $R \cong S$, then their group of units are isomorphic, $U(R) \cong U(S)$.

The fundamental theorem of finite abelian groups states that any finite abelian group G is isomorphic to a direct product of cyclic groups. That is, $G \cong \mathbf{Z}_{n_1} \times \mathbf{Z}_{n_2} \times ... \times \mathbf{Z}_{n_i}$. Hence, the group of units of a finite commutative ring with identity is isomorphic to a direct product of cyclic groups. The problem of classifying the group of units of an arbitrary finite commutative ring with identity is an open problem. However, the problem is solved for certain classes. In the case when $R = \mathbf{Z}_n$, its group of units is characterized by using the following lemma, see [3].

Lemma 1. *The group of units of* $\mathbf{Z}_n$ *when* n *is a prime power integer is given by*

(1) $U(\mathbf{Z}_2) \cong \{0\}$;

(2) $U(\mathbf{Z}_4) \cong \mathbf{Z}_2$;

(3) $U(\mathbf{Z}_{2^\alpha}) \cong \mathbf{Z}_2 \times \mathbf{Z}_{2^{\alpha-2}}$ *when* $\alpha \geq 3$;

(4) $U(\mathbf{Z}_{p^\alpha}) \cong \mathbf{Z}_{p-1} \times \mathbf{Z}_{p^{\alpha-1}}$ *when* p *is an odd prime.*

Cross [1], gave a characterization of the group of units of $\mathbf{Z}[i]/ <\beta>$, where $\mathbf{Z}[i]$ is the ring of Gaussian integers and β is an element in $\mathbf{Z}[i]$. Smith and Gallian [5], solved the problem when $R = F[x]/ < f(x) >$, where F is a finite field.

The related problem of determining the cyclic groups of units for each of the above classes of rings is completely solved. It is well known that $U(\mathbf{Z}_n)$ is cyclic if and only if $n = 2, 4, p^\alpha$ or $2p^\alpha$, where p is an odd prime integer see [4]. In [1], Cross showed that the group of units of $\mathbf{Z}[i]/ <\beta>$ is cyclic if and only if $\beta = 1+i, (1+i)^2, (1+i)^3, p, (1+i)p, \pi^n, (1+i)\pi^n$, where $p$is a prime integer of the form $4k+3$ and π is a Gaussian prime such that $\pi\overline{\pi}$ is a prime integer of the form $4k+1$. The problem of determining all quotients rings of polynomials over a finite field with a cyclic group of units was solved by El-Kassar et al. [2].

The purpose of this paper is to generalize the group of units of a finite commutative ring with identity and to examine the properties of the generalized group of units. Given a commutative ring with identity R, we define a sequence of rings $R^1, R^2, ...$, and a sequence of groups $U^1(R), U^2(R), ...$ The group $U^k(R)$ is called the k-th group of units of R. In addition, we consider the problem of determining the finite rings with identity having cyclic k-th group of units. Also, we examine the problem of determining the finite rings with identity having a trivial k-th group of units.

2. Preliminaries

Theorem 1. *If a group* $(G, *)$ *is isomorphic to the additive group of a ring* $(R, +, .)$, *then there is an operation* $\otimes$ *on* G *such that* $(G, *, \otimes)$ *is a ring isomorphic to* $(R, +, .)$.

Proof. Let $f : G \to R$ be the group isomorphism. Then, $f(g * h) = f(g) + f(h)$, for all $g, h \in G$. Define the operation $\otimes$ on G by

$$g \otimes h = f^{-1}(f(g).f(h)).$$

Then, $f(g \otimes h) = f(f^{-1}(f(g).f(h))) = f(g).f(h)$. ■

Example 1. The group of positive real numbers under multiplication, $(\mathbf{R}^+, .)$, is isomorphic to the group of real numbers under addition, $(\mathbf{R}, +)$, which is the additive group of the field of real numbers $(\mathbf{R}, +, .)$. Hence, there is an operation $*$ such that $(\mathbf{R}^+, ., *)$ is isomorphic to $(\mathbf{R}, +, .)$. The operation $*$ is defined by $x * y = x^{\ln y}$.

Corollary 1. *Every finite abelian group $(G, *)$ is the additive group of a ring $(G, *, \otimes)$ isomorphic to a direct sum of the form $\mathbf{Z}_{n_1} \oplus \mathbf{Z}_{n_2} \oplus ... \oplus \mathbf{Z}_{n_i}$.*

Note, if the additive groups of two rings $(R, +, .)$ and $(S, +, .)$ are isomorphic, then the two rings obtained by applying theorem 1, $(R, +, \otimes_1) \cong (S, +, .)$ and $(S, +, \otimes_2) \cong (R, +, .)$, are not necessarily isomorphic. For example, if R is the ring $(\mathbf{Z}_n, +, .)$ with usual addition and multiplication modulo n and S is the ring $(\mathbf{Z}_n, +, *)$ with zero multiplication, then $\otimes_1$ is the zero multiplication and $\otimes_2$ is the usual multiplication modulo. However, when $R = \mathbf{Z}_{m_1} \oplus \mathbf{Z}_{m_2} \oplus ... \oplus \mathbf{Z}_{m_j}$ and $S = \mathbf{Z}_{n_1} \oplus \mathbf{Z}_{n_2} \oplus ... \oplus \mathbf{Z}_{n_i}$, then the two rings $(R, +, \otimes_1)$ and $(S, +, \otimes_2)$ are isomorphic. This will be stated in the following lemma.

Lemma 2. *If the groups $\mathbf{Z}_{m_1} \times \mathbf{Z}_{m_2} \times ... \times \mathbf{Z}_{m_i}$ and $\mathbf{Z}_{n_1} \times \mathbf{Z}_{n_2} \times ... \times \mathbf{Z}_{n_j}$ are isomorphic, then the rings $\mathbf{Z}_{m_1} \oplus \mathbf{Z}_{m_2} \oplus ... \oplus \mathbf{Z}_{m_i}$ and $\mathbf{Z}_{n_1} \oplus \mathbf{Z}_{n_2} \oplus ... \oplus \mathbf{Z}_{n_j}$ are isomorphic.*

3. The k-th Group Of Units

Let Rbe a finite commutative ring with identity. Define a sequence of rings R^k, $k = 1, 2, 3, ...$, and a sequence of groups $U^k(R)$ as follows. First, let $R^1 = R$ and $U^1(R) = U(R)$. By the Fundamental theorem of abelian groups, $U(R)$ is isomorphic to a direct product cyclic groups, say $U(R) \cong \mathbf{Z}_{n_1} \times \mathbf{Z}_{n_2} \times ... \times \mathbf{Z}_{n_i}$. By corollary 1, there exits operations $\oplus$ and $\otimes$ defined on $U(R)$ that makes $(U(R), \oplus, \otimes)$ a ring isomorphic to $\mathbf{Z}_{n_1} \oplus \mathbf{Z}_{n_2} \oplus ... \oplus \mathbf{Z}_{n_i}$. The multiplication operation on R serves as the addition of the ring $(U(R), \oplus, \otimes)$; i.e., $a \oplus b = a.b$. The multiplication operation on $(U(R), \oplus, \otimes)$ is defined by $a \otimes b = f^{-1}(f(a).f(b))$ where f is an isomorphism from the group $U(R)$ to $\mathbf{Z}_{n_1} \times \mathbf{Z}_{n_2} \times ... \times \mathbf{Z}_{n_i}$. Note that $U(R) = U^1(R)$ is the underlying set of both the group of units of R and the ring $(U(R), \oplus, \otimes)$, and hence we refer to both simply by $U(R)$ or $U^1(R)$. Define R^2 to be the ring $R^2 = \mathbf{Z}_{n_1} \oplus \mathbf{Z}_{n_2} \oplus ... \oplus \mathbf{Z}_{n_i}$. Thus, the rings R^2 and $U^1(R)$ are isomorphic so that $R^2 \cong U^1(R)$. Now, we define $U^2(R)$ to be the group of units of the ring $U^1(R)$ so that

$$U^2(R) = U(U^1(R)) \cong U(R^2).$$

Then, $U^2(R)$ is a finite abelian group and hence isomorphic to direct product of cyclic groups, $U^2(R) \cong \mathbf{Z}_{m_1} \times \mathbf{Z}_{m_2} \times ... \times \mathbf{Z}_{m_j}$ and by corollary 1, $U^2(R)$ supports a ring structure isomorphic to the ring $R^3 = \mathbf{Z}_{m_1} \oplus \mathbf{Z}_{m_2} \oplus ... \oplus \mathbf{Z}_{m_j}$. Hence, the rings $U^2(R)$ and R^3 satisfy

$$U^2(R) = U(U^1(R)) \cong U(R^2) \cong R^3.$$

Similarly, we define $U^3(R)$ to be the group of units of the ring $U^2(R)$ so that

$$U^3(R) = U(U^2(R)) \cong U(R^2).$$

Continuing in this fashion, we define

$$U^k(R) = U(U^{k-1}(R)) \cong U(R^k), \tag{3.1}$$

where $k > 1$. The group $U^k(R)$ will be referred to as the k-th group of units of the ring R. Also, $U^k(R)$ is a ring satisfying

$$U^k(R) = U(U^{k-1}(R)) \cong U(R^k) = R^{k+1}. \tag{3.2}$$

Example 2. Let p be an odd prime and let $R = \mathbf{Z}_p$. Then $U_p = U(\mathbf{Z}_p)$ is a cyclic group isomorphic to $\mathbf{Z}_{p-1}$. Hence, $R^2 = \mathbf{Z}_{p-1}$. The operations $\oplus$ and $\otimes$ defined on U_p that makes the ring $(U_p, \oplus, \otimes)$ isomorphic to $\mathbf{Z}_{p-1}$ can be described as follows. The multiplication modulo p operation serves as the addition of the ring $(U_p, \oplus, \otimes)$; that is $a \oplus b = a.b (\mathrm{mod}\, p)$. The multiplication operation $\otimes$ on U_p is $a \otimes b = a^{\log_r b} (\mathrm{mod}\, p)$, where r is a primitive root of p. Note that the multiplication operation depends on the choice of the primitive root. The ring $(U_p, \oplus, \otimes)$ is a commutative ring with identity element r and 1 is the zero element.

Lemma 3. *If two rings R and S are isomorphic, then their groups of units are isomorphic and the rings $U(R)$ and $U(S)$ are also isomorphic.*

Proof. The restriction of the ring isomorphism from R onto S to $U(R)$ serves as a group isomorphism from $U(R)$ onto $U(S)$. Now the ring $U(R)$ is isomorphic to $R^2 = \mathbf{Z}_{m_1} \oplus \mathbf{Z}_{m_2} \oplus ... \oplus \mathbf{Z}_{m_j}$ and $U(S)$ is isomorphic to $S^2 = \mathbf{Z}_{n_1} \oplus \mathbf{Z}_{n_2} \oplus ... \oplus \mathbf{Z}_{n_i}$. Since the groups $U(R)$ and $U(S)$ satisfy

$$U(R) \cong \mathbf{Z}_{m_1} \times \mathbf{Z}_{m_2} \times ... \times \mathbf{Z}_{m_j}, U(S) \cong \mathbf{Z}_{n_1} \times \mathbf{Z}_{n_2} \times ... \times \mathbf{Z}_{n_i}$$

and $U(R) \cong U(S)$, we have that $\mathbf{Z}_{m_1} \times \mathbf{Z}_{m_2} \times ... \times \mathbf{Z}_{m_j} \cong \mathbf{Z}_{n_1} \times \mathbf{Z}_{n_2} \times ... \times \mathbf{Z}_{n_i}$. By lemma 2,

$$\begin{aligned} U(R) &\cong R^2 = \mathbf{Z}_{m_1} \oplus \mathbf{Z}_{m_2} \oplus ... \oplus \mathbf{Z}_{m_j} \\ &\cong \mathbf{Z}_{n_1} \oplus \mathbf{Z}_{n_2} \oplus ... \oplus \mathbf{Z}_{n_i} = S^2 \cong U(S). \end{aligned}$$

■

4. k-th Group Of Units Of A Direct Sum

Lemma 4. *If $R \cong R_1 \oplus R_2 \oplus ... \oplus R_i$, then the groups $U(R)$ and $U(R_1) \times U(R_2) \times ... \times U(R_i)$ are isomorphic and the rings $U(R)$ and $U(R_1) \oplus U(R_2) \oplus ... \oplus U(R_i)$ are isomorphic.*

Proof. The group of units of R decomposes into,

$$U(R) \cong U(R_1) \times U(R_2) \times ... \times U(R_i). \tag{4.1}$$

By the fundamental theorem of finite abelian groups, $U(R) \cong \mathbf{Z}_{n_1} \times \mathbf{Z}_{n_2} \times ... \times \mathbf{Z}_{n_s}$ and for each $j, 1 \le j \le i$, $U(R_j) \cong \mathbf{Z}_{n_{j_1}} \times \mathbf{Z}_{n_{j_2}} \times ... \times \mathbf{Z}_{n_{js_j}}$. The rings $U(R)$ and R^2 satisfy

$$U(R) \cong \mathbf{Z}_{n_1} \oplus \mathbf{Z}_{n_2} \oplus ... \oplus \mathbf{Z}_{n_s} = R^2,$$

and for each $j, 1 \le j \le i$, the rings $U(R_j)$ and R_j^2 satisfy

$$U(R_j) \cong \mathbf{Z}_{n_{j1}} \oplus \mathbf{Z}_{n_{j2}} \oplus ... \oplus \mathbf{Z}_{n_{js_j}} = R_j^2.$$

From (4.1),

$$\begin{aligned} U(R) &\cong \mathbf{Z}_{n_1} \times \mathbf{Z}_{n_2} \times ... \times \mathbf{Z}_{n_s} \\ &\cong U(R_1) \times U(R_2) \times ... \times U(R_i) \\ &\cong \mathbf{Z}_{n_{11}} \times \mathbf{Z}_{n_{12}} \times ... \times \mathbf{Z}_{n_{1s_1}} \times ... \times \mathbf{Z}_{n_{i1}} \times \mathbf{Z}_{n_{i2}} \times ... \times \mathbf{Z}_{n_{is_i}}. \end{aligned}$$

By lemma 3, and using the fact that each $U(R_j) \cong R_j^2$, we have

$$\begin{aligned} U(R) &\cong R^2 = \mathbf{Z}_{n_1} \oplus \mathbf{Z}_{n_2} \oplus ... \oplus \mathbf{Z}_{n_s} \\ &\cong \mathbf{Z}_{n_{11}} \oplus \mathbf{Z}_{n_{12}} \oplus ... \oplus \mathbf{Z}_{n_{1s_1}} \oplus ... \oplus \mathbf{Z}_{n_{i1}} \oplus \mathbf{Z}_{n_{i2}} \oplus ... \oplus \mathbf{Z}_{n_{is_i}} \\ &= R_1^2 \oplus R_2^2 \oplus ... \oplus R_i^2 \\ &\cong U(R_1) \oplus U(R_2) \oplus ... \oplus U(R_i). \end{aligned}$$

■

Theorem 2. *If $R \cong R_1 \oplus R_2 \oplus ... \oplus R_i$, then the groups $U^k(R)$ and $U^k(R_1) \times U^k(R_2) \times ... \times U^k(R_i)$ are isomorphic and the rings $U^k(R)$ and $U^k(R_1) \oplus U^k(R_2) \oplus ... \oplus U^k(R_i)$ are isomorphic.*

Proof. By lemma 4, the result is true for $k = 1$. Assume for induction purposes that the result is true for $K - 1$. Then,

$$U^{K-1}(R) \cong U^{K-1}(R_1) \times U^{K-1}(R_2) \times ... \times U^{K-1}(R_i)$$

and

$$U^{K-1}(R) \cong U^{K-1}(R_1) \oplus U^{K-1}(R_2) \oplus ... \oplus U^{K-1}(R_i). \tag{4.2}$$

Applying lemma 4, for the rings in (4.2), we have

$$U(U^{K-1}(R)) \cong U(U^{K-1}(R_1)) \times ... \times U(U^{K-1}(R_i)) \tag{4.3}$$

and

$$U(U^{K-1}(R)) \cong U(U^{K-1}(R_1)) \oplus ... \oplus U(U^{K-1}(R_i)). \tag{4.4}$$

By (3.1) and (3.2), (4.3) and (2.5) become

$$U^K(R)) \cong U^K(R_1) \times U^K(R_2) \times ... \times U^K(R_i)$$

and

$$U^K(R) \cong U^K(R_1) \oplus U^K(R_2) \oplus ... \oplus U^K(R_i)$$

and the result is true for every $k \geq 1$. ■

5. Rings With Trivial k-th Group Of Units

In this section, we consider the problem of determining all finite commutative rings R such that for a fixed k the group of units $U^k(R)$ is trivial, that is $U^k(R) \cong \{0\}$. It is well-known that Boolean rings are the only rings with trivial group of unit. Hence, the problem is solved for $k = 1$. We do not solve this general problem. However, we give partial results for special cases and completely solve the problem when $k = 2$ and $R = \mathbf{Z}_n$.

Lemma 5. *$U(\mathbf{Z}_n) \cong \{0\}$ if and only if $n = 1$ or 2.*

Proof. Suppose that $U(\mathbf{Z}_n) \cong \{0\}$. Then, $U(\mathbf{Z}_n) = \phi(n) = 1$. Since $\phi(n)$ is even for every $n > 2$, we have $n = 1$ or 2. The converse follows directly from lemma 1. ■

In lemmas 6, 7 and 8, we determine the solutions when n is a prime power.

Lemma 6. *Let p be a prime integer. Then, $U^2(\mathbf{Z}_p) \cong \{0\}$ if and only if $p = 2$ or 3.*

Proof. Let p be a prime integer. Suppose that $U^2(\mathbf{Z}_p) \cong \{0\}$. Since $U(\mathbf{Z}_p) \cong \mathbf{Z}_{p-1}$, we have $\{0\} \cong U^2(\mathbf{Z}_p) = U(U(\mathbf{Z}_p)) \cong U(\mathbf{Z}_{p-1})$. By lemma 5, $p - 1 = 1$ or 2. The converse is obtained from lemma 1. ■

Lemma 7. *Let $n = 2^\beta$, where $\beta > 0$. Then, $U^2(\mathbf{Z}_{2^\beta}) \cong \{0\}$ if and only if $\beta = 1, 2$ or 3.*

Proof. By lemma 1, $U^2(\mathbf{Z}_{2^\beta}) \cong \{0\}$ when $\beta = 1, 2$ or 3. Suppose that $\beta > 3$. Then, $U(\mathbf{Z}_{2^\beta}) \cong \mathbf{Z}_2 \times \mathbf{Z}_{2^{\beta-2}}$ and the rings $U(\mathbf{Z}_{2^\beta})$ and $\mathbf{Z}_2 \oplus \mathbf{Z}_{2^{\beta-2}}$ are isomorphic. By lemma 4, we have

$$U^2(\mathbf{Z}_{2^\beta}) \cong U(\mathbf{Z}_2) \oplus U(\mathbf{Z}_{2^{\beta-2}}) \cong U(\mathbf{Z}_{2^{\beta-2}}).$$

Thus, the group $U(\mathbf{Z}_{2^{\beta-2}}) \cong \mathbf{Z}_2 \times \mathbf{Z}_{2^{\beta-4}}$ is nontrivial. ■

Lemma 8. *Let p be an odd prime and let $\beta > 0$. Then, $U^2(\mathbf{Z}_{p^\beta}) \cong \{0\}$ if and only if $p^\beta = 3$.*

Proof. Suppose that $U^2(\mathbf{Z}_{p^\beta}) \cong \{0\}$. By lemma 1, $U(\mathbf{Z}_{p^\beta}) \cong \mathbf{Z}_{p-1} \times \mathbf{Z}_{p^{\beta-1}}$ so that

$$U^2(\mathbf{Z}_{p^\beta}) = U(U(\mathbf{Z}_{p^\beta})) \cong U(\mathbf{Z}_{p-1} \oplus \mathbf{Z}_{p^{\beta-1}}) \cong U(\mathbf{Z}_{p-1}) \oplus U(\mathbf{Z}_{p^{\beta-1}}).$$

Since $U^2(\mathbf{Z}_{p^\beta})$ is trivial, lemma 5 gives that $p-1=2$ and $p^{\beta-1}=1$. ■

Lemma 9. *If $U^2(\mathbf{Z}_n) \cong \{0\}$, then n is a product of at most two prime power factors.*

Proof. Suppose that $U^2(\mathbf{Z}_n) \cong \{0\}$, where $n = q_1^{\alpha_1} q_2^{\alpha_2} ... q_i^{\alpha_i}$ and $q_1 < q_2 < ... < q_i$. Also suppose that $i > 2$, so that $q_3 \geq 5$. Now, $\mathbf{Z}_n \cong \mathbf{Z}_{q_1^{\alpha_1}} \oplus \mathbf{Z}_{q_2^{\alpha_2}} \oplus ... \oplus \mathbf{Z}_{q_i^{\alpha_i}}$ and from theorem 2, we have

$$U^2(\mathbf{Z}_n) \cong U^2(\mathbf{Z}_{q_1^{\alpha_1}}) \oplus U^2(\mathbf{Z}_{q_2^{\alpha_2}}) \oplus U^2(\mathbf{Z}_{q_3^{\alpha_3}}) \oplus ... \oplus U^2(\mathbf{Z}_{q_i^{\alpha_i}}).$$

Since $q_3 \geq 5$, $U(\mathbf{Z}_{q_3-1})$ is nontrivial and so is $U^2(\mathbf{Z}_{q_3^{\alpha_3}}) \cong U(\mathbf{Z}_{q_3-1}) \times U(\mathbf{Z}_{q_3^{\alpha_3-1}})$. Hence, $U(\mathbf{Z}_n)$ is not trivial and $i \leq 2$. ■

Lemma 10. *Let $n = p^\alpha q^\beta$, where $\alpha, \beta > 0$. If $U^2(\mathbf{Z}_n) \cong \{0\}$, then* $p = 2$.

Proof. Let $n = p^\alpha q^\beta$ and let $U^2(\mathbf{Z}_n) \cong \{0\}$. If $p > 2$, then $q \geq 5$ and

$$U(\mathbf{Z}_n) \cong U(\mathbf{Z}_{p^\alpha} \oplus \mathbf{Z}_{q^\beta}) \cong U(\mathbf{Z}_{p^\alpha}) \oplus U(\mathbf{Z}_{q^\beta}).$$

Using lemma 1 and theorem 2,

$$U^2(\mathbf{Z}_n) \cong U^2(\mathbf{Z}_{p^\alpha}) \oplus U(\mathbf{Z}_{q-1}) \oplus U(\mathbf{Z}_{q^{\beta-1}}).$$

By lemma 5, $U(\mathbf{Z}_{q-1})$ is nontrivial and hence $U^2(\mathbf{Z}_n)$ is nontrivial. ■

Lemma 11. *Let $n = 2^\alpha q^\beta$, where $\alpha, \beta > 0$. If $U^2(\mathbf{Z}_n) \cong \{0\}$, then* $\beta = 1$.

Proof. Let $n = 2^\alpha q^\beta$ and let $U^2(\mathbf{Z}_n) \cong \{0\}$. If $\beta > 1$, then

$$U(\mathbf{Z}_n) \cong U(\mathbf{Z}_{2^\alpha}) \oplus \mathbf{Z}_{q^{\beta-1}} \oplus \mathbf{Z}_{q-1}$$

and the group

$$U^2(\mathbf{Z}_n) \cong U^2(\mathbf{Z}_{2^\alpha}) \times U(\mathbf{Z}_{q^{\beta-1}}) \times U(\mathbf{Z}_{q-1}).$$

Since $\beta > 1$ and $q \geq 3$, lemma 5 gives that $U(\mathbf{Z}_{q^{\beta-1}})$ is nontrivial. ■

Lemma 12. *Let $n = 2^\alpha q$, where $\alpha > 0$. If $U^2(\mathbf{Z}_n) \cong \{0\}$, then $q = 3$.*

Proof. Let $n = 2^{\alpha}q$ and let $U^2(\mathbf{Z}_n) \cong \{0\}$. If $q > 3$, then $U(\mathbf{Z}_n) \cong U(\mathbf{Z}_{2^\alpha}) \times \mathbf{Z}_{q-1}$ and $U^2(\mathbf{Z}_n) \cong U^2(\mathbf{Z}_{2^\alpha}) \times U(\mathbf{Z}_{q-1})$. Since $q-1 > 2$, then by lemma 5, $U(\mathbf{Z}_{q-1})$ is nontrivial. Therefore $q = 3$. ■

The following corollary follows from lemmas 7 and 12.

Corollary 2. *Let $n = 2^{\beta}.3$. Then $U^2(\mathbf{Z}_n) \cong \{0\}$ if and only if $\beta = 1, 2$ or 3.*

We summarize of the previous results in the following theorem, which gives the characterization of all values of n for which $U^2(\mathbf{Z}_n)$ is the trivial group.

Theorem 3. *Let $n > 1$ and let $R = \mathbf{Z}_n$. Then, $U^2(R) \cong \{0\}$ if and only if $n = 2, 3, 4, 6, 8, 12$ or 24.*

Next we state without proof some partial solutions to the general problem.

Theorem 4. *Let R be a finite ring with identity with $U^m(R) \cong \{0\}$. Then*

Lemma 13.

(1) $R \cong \mathbf{Z}_2 \oplus \mathbf{Z}_2 \oplus ... \oplus \mathbf{Z}_2$ *iff* $m = 1$;

(2) $R = \mathbf{Z}_{3^k}$ *if and only if* $m = k + 1$;

(3) $R = \mathbf{Z}_{2^k}$ *iff* $m = \dfrac{k}{2} + 1$ *if k is even and* $m = \dfrac{k+1}{2}$ *if k is odd;*

(4) $R = \mathbf{Z}_p$, *where* $p = 2^{2^n} + 1$ *is a Fermat prime, if and only if* $m = 2^{n-1} + 2$;

(5) $R = \mathbf{Z}_{2.3^k}$ *if and only if* $m = k + 1$;

(6) $R = \mathbf{Z}_{2^l.3^k}$ *if and only if* $m = k + 1$ *when* $l < 2k$, *and*

$$m = \begin{cases} \dfrac{l}{2} + 1 & \textit{if } l \textit{ is even} \\[2ex] \dfrac{l+1}{2} & \textit{if } l \textit{ is odd} \end{cases} \qquad \textit{when} \quad l \geq 2k.$$

We close this section by listing some classes of rings R with trivial m^{th} group of units. If $R = \mathbf{Z}_3 \oplus \mathbf{Z}_3 \oplus ... \oplus \mathbf{Z}_3$, then $m = 2$. Also, since $U(GF(4)) \cong \mathbf{Z}_3$, we have $U^3(GF(4) \oplus GF(4) \oplus ... \oplus GF(4)) \cong \{0\}$. Also, if $R = \mathbf{Z}_{2^{k_1}} \oplus \mathbf{Z}_{2^{k_2}} \oplus ... \oplus \mathbf{Z}_{2^{k_i}}$, then $U^m(R) \cong \{0\}$ if and only if

$$m = \begin{cases} \dfrac{k}{2} + 1 \text{ if } k \text{ is even} \\[2ex] \dfrac{k+1}{2} \text{ if } k \text{ is odd} \end{cases}, \quad \text{where } k = \max(k_1, k_2, ..., k_i).$$

Finally, let $R = \mathbf{Z}_{p_1} \oplus \mathbf{Z}_{p_2} \oplus ... \oplus \mathbf{Z}_{p_i}$, where $p_i = 2^{2^{n_i}} + 1$ is a Fermat prime. Then $U^m(R) \cong \{0\}$ if and only if $m = 2^{n-1} + 2$, where $n = \max(n_1, n_2, ..., n_i)$.

6. Rings With Cyclic k-th Group Of Units

In this section, we examine the problem of determining all commutative rings R with cyclic second group of units. Complete characterization is given in the case when $R = \mathbf{Z}_n$.

It is well-know that a direct product of groups $G_1 \times G_2 \times ... \times G_r$ is cyclic iff each G_j is cyclic and $\gcd(|G_i|, |G_j|) = 1$ for $i \neq j$. Thus we have the following useful lemma.

Lemma 14. *Let $G_1, G_2, ..., G_r$ be finite cyclic groups. Then $G_1 \times G_2 \times ... \times G_r$ is not cyclic if and only if $\gcd(|G_i|, |G_j|) \neq 1$ for some $i \neq j$.*

Lemma 15. *If $U^2(\mathbf{Z}_n)$ is cyclic, then n is a product of at most three prime power factors.*

Proof. Let $n = p_1^{\alpha_1}.p_2^{\alpha_2}...p_i^{\alpha_i}$ and suppose that $U^2(\mathbf{Z}_n)$ is cyclic. If $i \geq 4$, then p_3, $p_4 \geq 5$. By theorem 2, we have

$$\begin{aligned} U^2(\mathbf{Z}_n) &\cong U^2(\mathbf{Z}_{p_1^{\alpha_1}}) \times U^2(\mathbf{Z}_{p_2^{\alpha_2}}) \times U(\mathbf{Z}_{p_3^{\alpha_3 - 1}}) \times U(\mathbf{Z}_{p_3 - 1}) \\ &\quad \times U(\mathbf{Z}_{p_4^{\alpha_4 - 1}}) \times U(\mathbf{Z}_{p_4 - 1}) \times ... \times U^2(\mathbf{Z}_{p_i^{\alpha_i}}). \end{aligned}$$

Since the orders of $U(\mathbf{Z}_{p_3 - 1})$ and $U(\mathbf{Z}_{p_4 - 1})$, $\phi(p_3 - 1)$ and $\phi(p_4 - 1)$, are both even, lemma 14 gives that $U^2(\mathbf{Z}_n)$ is not cyclic. ■

In the next three lemmas, we consider the case where n is a product of three prime power factors and $U^2(\mathbf{Z}_n)$ is cyclic.

Lemma 16. *Let $n = p_1^{\alpha_1}.p_2^{\alpha_2}.p_3^{\alpha_3}$. If $U^2(\mathbf{Z}_n)$ is cyclic, then $\alpha_3 = 1$.*

Proof. Let $n = p_1^{\alpha_1}.p_2^{\alpha_2}.p_3^{\alpha_3}$. Suppose that $U^2(\mathbf{Z}_n)$ is cyclic. If $\alpha_3 \geq 2$, then $p_3 \geq 5$ and theorem 2 gives

$$U^2(\mathbf{Z}_n) \cong U^2(\mathbf{Z}_{p_1^{\alpha_1}}) \times U^2(\mathbf{Z}_{p_2^{\alpha_2}}) \times \mathbf{Z}_{p_3^{\alpha_3 - 2}} \times \mathbf{Z}_{p_3 - 1} \times U(\mathbf{Z}_{p_3 - 1}).$$

Since $p_3 - 1$ and $\phi(p_3 - 1)$ are even, we have that $U^2(\mathbf{Z}_n)$ is not cyclic. ■

Lemma 17. *Let $n = p_1^{\alpha_1}.p_2^{\alpha_2}.p_3$. If $U^2(\mathbf{Z}_n)$ is cyclic, then $p_1 = 2$.*

Proof. Let $n = p_1^{\alpha_1}.p_2^{\alpha_2}.p_3$ and let $U^2(\mathbf{Z}_n)$ be cyclic. If $p_1 > 2$, then p_2, $p_3 \geq 5$ and

$$U^2(R) \cong U^2(\mathbf{Z}_{p_1^{\alpha_1}}) \times U(\mathbf{Z}_{p_2^{\alpha_2 - 1}}) \times U(\mathbf{Z}_{p_2 - 1}) \times U(\mathbf{Z}_{p_3 - 1}).$$

Hence, the orders of $U(\mathbf{Z}_{p_2 - 1})$ and $U(\mathbf{Z}_{p_3 - 1})$ are both even and $U^2(\mathbf{Z}_n)$ is not cyclic. ■

Lemma 18. *Let $n = 2^{\alpha_1}p_2^{\alpha_2}p_3$. If $U^2(\mathbf{Z}_n)$ is cyclic, then $p_2^{\alpha_2} = 3$ and $\alpha_1 = 1, 2$ or 3.*

Proof. Let $n = 2^{\alpha_1}p_2^{\alpha_2}p_3$ and let $U^2(\mathbf{Z}_n)$ be cyclic. If $p_2 > 3$, then $p_2, p_3 \geq 5$ and

$$U^2(\mathbf{Z}_n) \cong U^2(\mathbf{Z}_{2^{\alpha_1}}) \times U(\mathbf{Z}_{p_2^{\alpha_2-1}}) \times U(\mathbf{Z}_{p_2-1}) \times U(\mathbf{Z}_{p_3-1})$$

cannot be cyclic. Therefore, $p_2 = 3$ and $n = 2^{\alpha_1}.3^{\alpha_2}.p_3$. Now, suppose that $\alpha_2 \geq 2$. Then

$$U^2(\mathbf{Z}_n) \cong U^2(\mathbf{Z}_{2^{\alpha_1}}) \times \mathbf{Z}_2 \times \mathbf{Z}_{3^{\alpha_2-2}} \times U(\mathbf{Z}_{p_3-1}).$$

But $\mathbf{Z}_2$ and $U(\mathbf{Z}_{p_3-1})$ both have even order, hence $U^2(\mathbf{Z}_n)$ is not cyclic. Thus $n = 2^{\alpha}.3.p$. If $\alpha \geq 4$, then

$$U^2(\mathbf{Z}_n) \cong \mathbf{Z}_2 \times \mathbf{Z}_{2^{\alpha-4}} \times U(\mathbf{Z}_{p-1}).$$

Which is not cyclic. Therefore $\alpha \leq 3$ and we have the result. ■

Next, we examine the case where n is a product of two distinct prime power factors.

Lemma 19. *Let $n = p_1^{\alpha_1}p_2^{\alpha_2}$, where p_1 and p_2 are distinct odd primes. If $U^2(\mathbf{Z}_n)$ is cyclic, then $n = 3.p_2$ where $p_2 = 5$ or $p_2 = 4k+3$ and $2k+1$ is a prime power.*

Proof. Let $n = p_1^{\alpha_1}p_2^{\alpha_2}$, where p_1, p_2 are odd primes and let $U^2(\mathbf{Z}_n)$ be cyclic. If $\alpha_1 \geq 2$, then

$$U^2(\mathbf{Z}_n) \cong \mathbf{Z}_{p_1^{\alpha_1-2}} \times \mathbf{Z}_{p_1-1} \times U(\mathbf{Z}_{p_1-1}) \times U(\mathbf{Z}_{p_2^{\alpha_2-1}}) \times U(\mathbf{Z}_{p_2-1}),$$

which is not cyclic since $\mathbf{Z}_{p_1-1}$ and $U(\mathbf{Z}_{p_2-1})$ are both of even order. Thus, $\alpha_1 = 1$ and $n = p_1.p_2^{\alpha_2}$. A similar argument shows that $\alpha_2 = 1$ so that $n = p_1.p_2$. In the case that $p_1 > 3$, we have $p_1, p_2 \geq 5$, and

$$U^2(\mathbf{Z}_n) \cong U(\mathbf{Z}_{p_1-1}) \times U(\mathbf{Z}_{p_2-1})$$

is not cyclic. Therefore, $p_1 = 3$, $n = 3.p_2$, $U(\mathbf{Z}_n) \cong \mathbf{Z}_2 \times \mathbf{Z}_{p_2-1}$ and $U^2(\mathbf{Z}_n) \cong U(\mathbf{Z}_{p_2-1})$. Thus, $U^2(\mathbf{Z}_n)$ is cyclic when $p_2 - 1 = 2, 4, p^\alpha, 2p^\alpha$ where p is an odd prime integer. Hence, $p_2 = 3, 5, p^\alpha + 1$ or $2p^\alpha + 1$. But the cases where $p_2 = 3$ and $p_2 = p^\alpha + 1$ are dismissed, since $p_1 = 3$ and p_2 is an odd prime integer. Therefore, $p_2 = 5$ or $2p^\alpha + 1$. Now, p is of the form $4k+1$ or $4k+3$. In either case, $2p^\alpha + 1$ is of the form $4k+3$ and

$$U^2(\mathbf{Z}_n) \cong U(\mathbf{Z}_{3-1}) \times U(\mathbf{Z}_{4k+3-1}) \cong U(\mathbf{Z}_{2(2k+1)}) \cong U(\mathbf{Z}_2) \times U(\mathbf{Z}_{2k+1}),$$

which is cyclic only when $2k+1$ is a prime power. ■

The case where n is even and product of two distinct prime powers is given next. The proof can be obtained by a similar argument used in the proof of the above lemma.

Lemma 20. *Let $n = 2^{\alpha_1}p^{\alpha_2}$, where $p > 3$. If $U^2(\mathbf{Z}_n)$ is cyclic, then $\alpha_2 = 1, \alpha_1 < 4$ and $p = 5$ or $p = 2q^{\alpha} + 1$ where q is an odd prime integer.*

Next we examine certain special case when n is of the form $2^{\alpha_1}3^{\alpha_2}$ and $U^2(\mathbf{Z}_n)$ is cyclic.

Lemma 21. *Let $n = 2^{\alpha_1}.3^{\alpha_2}$. If $U^2(\mathbf{Z}_n)$ is cyclic, then $n = 48$, 2.3^{α_2}, $2^2.3^{\alpha_2}$ or $2^3.3^{\alpha_2}$, where α_2 is any positive integer.*

Proof. Let $n = 2^{\alpha_1}.3^{\alpha_2}$ and let $U^2(\mathbf{Z}_n)$ be cyclic. Suppose that $\alpha_2 > 1$. If $\alpha_1 > 3$, then

$$U^2(\mathbf{Z}_n) \cong \mathbf{Z}_2 \times \mathbf{Z}_{2^{\alpha_1-4}} \times U(\mathbf{Z}_{3^{\alpha_2-1}}) \cong \mathbf{Z}_2 \times \mathbf{Z}_{2^{\alpha_1-4}} \times \mathbf{Z}_{3^{\alpha_2-2}} \times \mathbf{Z}_2,$$

which is not cyclic. Hence $\alpha_1 \leq 3$. Now suppose that $\alpha_2 = 1$. If $\alpha_1 > 4$, then $U^2(\mathbf{Z}_n) \cong \mathbf{Z}_2 \times \mathbf{Z}_{2^{\alpha_1-4}}$ which is not cyclic. Therefore, $n = 2.3, 2^2.3, 2^3.3$ or $2^4.3$. ■

Finally, we consider the case where n is a prime power and $U^2(\mathbf{Z}_n)$ is cyclic. In the case when n is even, $n = 2^{\alpha}$, α cannot be greater than 4, since $U^2(\mathbf{Z}_n) \cong \mathbf{Z}_2 \times \mathbf{Z}_{2^{\alpha-4}}$ is not cyclic. Therefore, $\alpha = 1, 2, 3$ or 4 and $n = 2, 4, 8$, or 16.

Lemma 22. *Let $n = p^{\alpha}$. If $U^2(\mathbf{Z}_{p^{\alpha}})$ is cyclic, then $n = 3^{\alpha}$, 5 or $2q^{\beta}+1$, where q is an odd prime.*

Proof. Let $n = p^{\alpha}$ and let $U^2(\mathbf{Z}_{p^{\alpha}})$ be cyclic. If $\alpha = 1$, then $U^2(\mathbf{Z}_p) \cong U(\mathbf{Z}_{p-1})$ is cyclic if and only if $p - 1 = 2, 4, q^{\beta}$ or $2q^{\beta}$, where q is an odd prime. Hence, $p = 3, 5, q^{\beta} + 1$ or $2q^{\beta} + 1$. The case when $p = q^{\beta} + 1$ gives an even value for p. Therefore, $p = 3, 5$,or $2q^{\beta} + 1$. Now, suppose that $\alpha > 1$. If $p > 3$, then $U^2(\mathbf{Z}_{p^{\alpha}}) \cong \mathbf{Z}_{p^{\alpha-2}} \times \mathbf{Z}_{p-1} \times U(\mathbf{Z}_{p-1})$ which is not cyclic. Hence, $n = 3^{\alpha}$ where $\alpha > 1$. ■

We summarize the above results in the following theorem. Note that for each of the special cases, we can easily verify that $U^2(\mathbf{Z}_n)$ is cyclic.

Theorem 5. *Let p and q be an odd prime integers and α be a positive integer. Then, $U^2(\mathbf{Z}_n)$ is cyclic if and only if one of the following is true:*

(1) $n = 2^{\alpha}.3.p$, where $\alpha = 1, 2$ or 3;

(2) $n = 15$;

(3) $n = 3.p$, where $p = 4k + 3$, and $2k + 1 = q^{\alpha}$;

(4) $n = 2.3^{\alpha}, 2^2.3^{\alpha}, 2^3.3^{\alpha}$ or $2^4.3$;

(5) $n = 2, 4, 8$ *or* 16;

(6) $n = 5$ *or* $2p^{\alpha} + 1$, *where* $2p^{\alpha} + 1$ *is a prime integer;*

(7) $n = 3^{\alpha}$.

We close this section by noting some classes of rings satisfying the general problem. The second group of unit of the direct of two rings appearing in the above theorem is cyclic when the orders of the second group of units are relatively prime. Others examples can be provided such as $GF(4)$ and $GF(2^n)$ where $2^n - 1$ is a Mersenne prime.

7. Conclusion

A generalization of the group of units of a finite commutative ring with identity was presented. The k-th group of units was examined. Complete chcracteriztions of the problems of determing all values of n such that the 2nd group of units is cyclic and that of determing all values of n such that the 2nd group of units is trivial were obtained. We leave as problem the complete characterization of rings with cyclic or trivial k-th group of units.

References

[1] Cross, J.T.. The Euler's ϕ-function in the Gaussian Integers:, *Amer. Math. Monthly*, **55**, (1983), 518-528.

[2] El-Kassar, A. N., H.Y. Chehade and D. Zantout. Quotient Rings Of Polynomials Over Finite Fields With Cyclic Groups Of units ,In: *Proceedings of The International Conference On Research Trends In Science and Technology*, RTST2002, Lebanese American University, Beirut Lebanon, (2002) 257–266.

[3] Gallian, Joseph A.. *Contemporary Abstract Algebra*, 5th ed., Houghton Mifflin Co., Boston, (1998).

[4] Niven, Zukerman and Montgomery. *An Introduction To The Theory of Numbers* , 5^{th} ed, Wiley, New York, (1991).

[5] Smith, Judy L. and J.A.Gallian. Factoring Finite Factor Rings , *Mathematics Magazine*, **58**, (1985), 93-95.

Mathematics Department,
Faculty of Science,
BAU, P.O. BOX 11-5020,
Beirut LEBANON

e-mail: ak1@bau.edu.lb

Received 30.06.2004