J. Korean Math. Soc. **46** (2009), No. 2, pp. 295–311

THE GROUP OF UNITS OF SOME FINITE LOCAL RINGS I

Sung Sik Woo

Abstract. The purpose of this paper is to identify the group of units of finite local rings of the types $\mathbb{F}_2[X]/(X^k)$ and $\mathbb{Z}_4[X]/I$, where I is an ideal. It turns out that they are 2-groups and we give explicit direct sum decomposition into cyclic subgroups of 2-power order and their generators.

1. Introduction

The purpose of this paper is to find the isomorphism type of the group of units of a finite local ring of some special types namely the ring of the form $R = \mathbb{Z}_4[X]/(X^k + 2X^a, 2X^r)$. This is not a chain ring unless $a = 0$ ([1]). An ideal of such ring is generated by two elements in general ([2]). We needed to require a to be rather 'big' to find the group of units.

It turns out that the group of units of the rings we consider are all 2-groups. By the classification of abelian groups they can be written as a direct sum of cyclic subgroups of 2-power order. Therefore we need to find the generators of each cyclic factor.

In Section 2, we collect some general information on the properties of rings of the type we will consider. In Section 3, we compute the group of units of the ring $\mathbb{F}_2[X]/(X^k)$ by finding explicit generators of cyclic subgroups which gives a clue to compute the group of units of a finite local ring of the form $R = \mathbb{Z}_4[X]/(X^k + 2X^a, 2X^r)$.

In Section 4, we compute the group of unit of the ring $R = \mathbb{Z}_4[X]/(X^k)$ by showing that the liftings of the generators of the group of units of $\mathbb{F}_2[X]/(X^k)$ and some extra elements of order 2 form a generating set for the group.

In Section 5, we compute the group of units of the ring of the type $\mathbb{Z}_4[X]$ / $(X^k + 2X^a)$ with a certain restriction on a and in Section 6 we compute the group of units of the ring $R = \mathbb{Z}_4[X]/(X^k + 2X^a, 2X^r)$.

Received June 28, 2007; Revised July 22, 2008.
2000 *Mathematics Subject Classification.* 13C12.
Key words and phrases. finite local ring, group of units.

2. Finite local rings over $\mathbb{Z}_4$

In this section we collect the properties of the rings of the type we are going to deal with. First we show that the rings of the type $R = \mathbb{Z}_4[X]/(X^k+2X^a, 2X^r)$ can be characterized as a $\mathbb{Z}_4$-algebra generated by a nilpotent element.

We briefly recall some of the result of [2, 3]. Consider a ring of the form $R = \mathbb{Z}_4[x]$ with $x^m = 0$ for some m. Then R is a quotient $\mathbb{Z}_4[X]/I$ for some ideal I of $\mathbb{Z}_4[X]$. If I is an ideal which is contained in (2), the ideal generated by 2, then it turns out that I is of the form $(2X^r)$.

Now suppose the ideal I not contained in (2). We define an order on the set $\mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$ in the usual way

$$0 < 1 < 2 < 3,$$

where we omitted the bars as we will do from now on. On the set $C = \{(a_0, a_1, \ldots, a_{m-1}) | a_i \in \mathbb{Z}_4\}$ we define an ordering by endowing the lexicographic order. Let

$$f(X) = \sum_{i=0}^{m-1} a_i X^i, \quad g(X) = \sum_{i=0}^{m-1} b_i X^i$$

be polynomials in $\mathbb{Z}_4[X]$ with $\deg(f), \deg(g) < m$. Then we define

$$f \leq g \text{ if and only if } (a_0, a_1, \ldots, a_{m-1}) \leq (b_0, b_1, \ldots, b_{m-1}).$$

Let us call the element of the form $2X^r$ a 2xr form. And let us call the polynomials of the form

$$g(X) = X^k + 2X^{h_1} + 2X^{h_2} + \cdots + 2X^{h_t}$$

with $h_t < \cdots < h_1 < k < m$ an xk2 form.

The following theorem is one of the fundamental result in [2].

Theorem 2.1. *Let J be an ideal of $\mathbb{Z}_4[X]/I$ which is not contained in* (2). *Let $g(X) = X^k + 2h(X) \in J$ be the smallest* xk2 *form in J and $2X^r$ be the smallest* 2xr *form in J. Then $J = (g(X), 2X^r)$, where $-\infty \leq r < l$. Here we let $X^{-\infty} = 0$.*

Thereby we obtain easily the following fact.

Lemma 2.2. *Let R be a finite local ring over $\mathbb{Z}_4$ generated by a nilpotent element $x \in R$ as $\mathbb{Z}_4$-algebra. Then R is of the form $R = \mathbb{Z}_4[X]/(X^k + 2h(X), 2X^r)$, where $h(X)$ is of degree $< k$.*

Proof. First we write $R = \mathbb{Z}_4[X]/I$ for some ideal I. Then $I \not\subset (2)$ for otherwise we have a surjection $\mathbb{Z}_4[X]/I \to \mathbb{Z}_4[X]/(2)$. This is impossible since $\mathbb{Z}_4[X]/(2)$ is infinite. Since $X \in R$ is nilpotent say, $X^m = 0$ we have a surjection $\phi : \mathbb{Z}_4[X]/(X^m) \to R$. By Theorem 2.1, $\mathrm{Ker}(\phi)$ is generated by the form described above. □

First we will state a simple lemma ([2]).

Lemma 2.3. *For a positive integer n and r $(1 \leq 2^n < r)$ we have*

$$\binom{2^n}{r} \equiv \begin{cases} 0 \pmod 4 \text{ if } r \neq 2^{n-1}, \\ 2 \pmod 4 \text{ if } r = 2^{n-1}. \end{cases}$$

In particular,

$$(a+b)^{2^n} = a^{2^n} + 2(ab)^{2^{n-1}} + b^{2^n}.$$

Let $U(R)$ be the group of units of the ring $R = \mathbb{Z}_4[X]/(X^k + 2X^a)$ with $a > 0$ and $U_1(R)$ be the subgroup of $U(R)$ of the form $1 + Xf(X)$, $f(X) \in \mathbb{Z}_4[X]$ whenever it is well defined. Using Lemma 2.2 it is easy to show that the group of units of the ring $R = \mathbb{Z}_4[X]/I$ in which X is nilpotent is a 2-group.

Lemma 2.4. *Let $R = \mathbb{Z}_4[X]/I$, where X is nilpotent. Then the group of units $U(R)$ and $U_1(R)$ are 2 groups.*

Proof. Suppose $X^l = 0$ for some l. It suffices to show that $a^{2^n} = 1$ $(a \in R^*)$ for some n. But $a \in R^*$ is of the form $\epsilon + Xf(X)$ for some $\epsilon = 1, 3$ and $f(X) \in \mathbb{Z}_4[X]$. Then $\epsilon^2 = 1$ and by the lemma above we have $(\epsilon + Xf(X))^{2^n} = \epsilon^{2^n} + 2(\epsilon Xf)^{2^{n-1}} + (Xf)^{2^n} = 1$ for suitably chosen 2^n bigger than l. □

Theorem 2.5 ([1, XVII.3])**.** *If R is a local commutative ring of characteristic p^n, then R is generated by its units as an algebra over $\mathbb{Z}_{p^n}$.*

Hence we can say that the group of units of R takes a 'large' portion of the ring. However our results show that the functor from the category of finite local rings over $\mathbb{Z}_4$ to the category of abelian groups which sends R to the group of units $U(R)$ is not faithful. In fact, we can construct nonisomorphic rings by:

Proposition 2.6. *Let $R = \mathbb{Z}_4[X]/(X^k + 2X^a, 2X^r)$ with $a < r < k$. Then distinct triples (k, a, r) gives rise to nonisomorphic rings.*

Proof. Obviously $k + r - a \geq 2$. Hence $X^k = 2X^a$ and so $X^{k+r-a} = 2X^r = 0$ and we see that the nilpotency of X is $k+r-a$. On the other hand, the additive structure of R is isomorphic to $\mathbb{Z}_4^r \oplus \mathbb{Z}_2^{k-r}$. Hence $r, k-r$ and $k+r-a$ are invariants of R. Therefore distinct triples (k, a, r) gives rise to nonisomorphic rings. □

Now we will see, by using Theorem 6.5 of Section 6, quite a few of them give rise to isomorphic group of units.

For the rest of the paper we restrict our attention to the rings of the types $R = \mathbb{F}_2[X]/(X^k)$, $R_1 = \mathbb{Z}_4[X]/(X^k + 2X^a)$ and $R_2 = \mathbb{Z}_4[X]/(X^k + 2X^a, 2X^r)$. We have surjective ring homomorphisms

$$\mathbb{Z}_4[X]/(X^k + 2X^a) \to \mathbb{Z}_4[X]/(X^k + 2X^a, 2X^r) \to \mathbb{F}_2[X]/(X^k),$$

which induces surjective group homomorphisms on the groups of units since a unit in $\mathbb{Z}_4[X]/(X^k + 2X^a, 2X^r)$ (resp. $\mathbb{F}_2[X]/(X^k)$) can be lifted to the units of the same expression in $\mathbb{Z}_4[X]/(X^k + 2X^a)$ (resp. $\mathbb{Z}_4[X]/(X^k + 2X^a, 2X^r)$).

3. The group of units of the ring $R = \mathbb{F}_2[X]/(X^k)$

In this section we determine the group of units of the ring $R = \mathbb{F}_2[X]/(X^k)$. First we observe that the order of the group of units $U(R)$ of R is 2^{k-1}. By the classification of finite abelian groups we know that $U(R)$ is a product of cyclic groups of order a power of 2. To find the isomorphism type of the group we need to determine the exact order of the cyclic subgroups and their generators. Throughout this section we let $R = \mathbb{F}_2[X]/(X^k)$.

Definition 3.1. For a rational number a let $\lfloor r \rfloor_2$ to be the smallest integer greater than or equal to $\log_2(a)$. Hence $2^{\lfloor r \rfloor_2}$ is the smallest power of 2 which is greater than or equal to a.

If the order $o(G)$ of a group G is 2^n, then we will say the 2-*logarithmic order* of G is n and we will write $lo_2(G) = n$. For $x \in G$ we will write $lo_2(x) = n$ for the 2-logarithmic order of the subgroup is generated by x. *To simplify our notation we will write* $lo(G)$ *for* $lo_2(G)$.

First we observe that a unit of $R = \mathbb{F}_2[X]/(X^k)$ is of the form $1 + Xf(X)$.

Lemma 3.2. *Let* $R = \mathbb{F}_2[X]/(X^k)$. *Then*
(i) $o(U(R)) = 2^{k-1}$,
(ii) $lo(1 + X^i) = \lfloor \frac{k}{i} \rfloor_2$.

Proof. (i) We already remarked on this.

(ii) Since $U(R)$ is a 2-group we know that the order of $1 + X^i$ is a 2-power. Let $k_i = \lfloor \frac{k}{i} \rfloor_2$. Then $i2^{k_i} \geq k$ and $(1 + X^i)^{2^{k_i}} = 1 + X^{i2^{k_i}} = 1$ by Lemma 2.2. On the other hand, if b is a 2-power less than $2^{\lfloor \frac{k}{i} \rfloor_2}$, then obviously $(1+X^i)^b = 1 + X^b \neq 1$. □

Lemma 3.3. *If a subgroup of* $U(R)$ *contains all* $\{(1+X^n) |\, n$ *is odd less than* $k\}$ *then it contains* $(1 + X^i)$ *for each positive integer* i *smaller than* k.

Proof. For each even integer a write $a = 2^b c$ with an odd integer c. Then $(1 + X^c)^{2^b} = 1 + X^a$. □

For each odd integer $< k$ we let G_i be the subgroup of $U(R)$ generated by $1 + X^i$. We will show that $U(R)$ is the direct sum of G_i's.

Theorem 3.4. *Let* $R = \mathbb{F}_2[X]/(X^k)$. *Let* G_i *be the subgroup generated by* $(1 + X^i)$, *where* i *is an odd positive integer* $< k$. *Then the group* $U(R)$ *of units of the ring* R *is the direct sum*

$$U(R) = G_1 \oplus G_3 \oplus \cdots \oplus G_m,$$

where m *is the largest odd integer smaller than* k. *Further, the logarithmic order of the cyclic subgroup generated by* $(1 + X^i)$ *is* $\lfloor \frac{k}{i} \rfloor_2$.

Proof. First we show that $(G_1+G_3+\cdots+G_i)\cap G_{i+2} = 1$. Suppose $(1+X^{i+2})^l \in (G_1 + G_3 + \cdots + G_i)$ with $l < 2^{\lfloor \frac{k}{i+2} \rfloor_2}$. Then since $G/(G_1 + G_3 + \cdots + G_i)$

is a 2-group we can assume l (by choosing the smallest such) is a power of 2, namely, $(1+X^{i+2})^{2^r}$ belongs to $(G_1+G_3+\cdots+G_i)$. Hence we can write

$$(1+X^{(i+2)2^r}) = (1+X)^{a_1}(1+X^3)^{a_3}\cdots(1+X^i)^{a_i}$$

for some $0 \le a_j < \lfloor \frac{k}{j} \rfloor_2$ for each odd j smaller than k. Write $a_j = 2^{c_j}b_j$, where b_j is odd. Then we can write

$$(1+X^{(i+2)2^r}) = (1+X^{2^{c_1}})^{b_1}(1+X^{3\cdot 2^{c_3}})^{b_3}\cdots(1+X^{i\cdot 2^{c_i}})^{b_i}.$$

The right hand side must contain more than one factor for otherwise $(1+X^{(i+2)2^r}) = (1+X^{2^{c_j}})^{b_j}$ for some j which is not possible.

Note that $2^{c_1}, 3\cdot 2^{c_3}, \ldots, i\cdot 2^{c_i}$ are all distinct. Hence we can choose the smallest one which we call m. Obviously, $m < (i+2)2^r$ since the right hand side contains more than one factor. Then the right hand side of the above equality contains X^m, but there is no such term in $(1+X^{(i+2)2^r})$. This contradiction shows that $(G_1+G_3+\cdots+G_i)\cap G_{i+2} = 1$.

Now we prove that $U(R) = G_1+G_3+\cdots+G_m$. Let $f(X) = 1+X^{a_1}+X^{a_2}+\cdots+X^{a_j}$ be a unit with $a_1 < a_2 < \cdots < a_j < k$. We induct on $\deg(f)$. If $\deg(f) = 1$, then our result is obvious. Hence we assume $g(X) = 1+X^{a_1}+X^{a_2}+\cdots+X^{a_{j-1}} \in G_1+G_3+\cdots+G_m$ and we proceed to prove $f(X) = 1+X^{a_1}+X^{a_2}+\cdots+X^{a_j} \in G_1+G_3+\cdots+G_m$. By Lemma 3.3 we need to express f as a product of $(1+X^i)$'s with various integers i's. First note that $g(X)(1+X^{a_j}) = f(X)+X^{a_1+a_j}+\cdots+X^{a_{j-1}+a_j}$. Next, if we multiply $(1+X^{a_1+a_j})$ by $f(X)+X^{a_1+a_j}+\cdots+X^{a_{j-1}+a_j}$, then the term $X^{a_1+a_j}$ drops out and we get $g(X)(1+X^{a_j})(1+X^{a_1+a_j}) = f(X)+X^{2a_1+a_j}+\cdots$. If we repeat this, then the lowest degree of nonzero terms in the tail of this expression gets bigger and bigger. By using the fact that $X^k = 0$ when we keep multiplying the elements of the form $(1+X^i)$ we come up with an expression of $f(X)$ as a product of the form $f(X) = g(X)(1+X^{b_1})(1+X^{b_2})\cdots(1+X^{b_s})$. □

Corollary 3.5. *Let $R = \mathbb{F}_2[X]/(X^k)$. Then the group of units of the ring R is of order 2^{k-1} and it is isomorphic to the direct sum of cyclic groups of orders $2^{\lfloor k \rfloor_2}, 2^{\lfloor \frac{k}{3} \rfloor_2}, \ldots, 2^{\lfloor \frac{k}{l} \rfloor_2}$, where l is the largest odd integer $< n$.*

Corollary 3.6. *If l is the largest odd integer $< n$,*

$$\lfloor k \rfloor_2 + \lfloor \frac{k}{3} \rfloor_2 + \lfloor \frac{k}{5} \rfloor_2 + \cdots + \lfloor \frac{k}{l} \rfloor_2 = k-1.$$

Remark. It is interesting that there seems to be no rather easy way to show this identity directly.

Example 3.7. Let $R = \mathbb{F}_2[X]/(X^{10})$. We have $\lfloor 10 \rfloor_2 = 4, \lfloor \frac{10}{3} \rfloor_2 = 2, \lfloor \frac{10}{5} \rfloor_2 = 1, \lfloor \frac{10}{7} \rfloor_2 = 1, \lfloor \frac{10}{9} \rfloor_2 = 1$. Hence the group of units $U(R)$ of R is the direct sum of cyclic subgroups generated by $1+X, 1+X^3, 1+X^5, 1+X^7, 1+X^9$ whose respective orders are $2^4, 2^2, 2, 2, 2$. Therefore

$$U(R) \cong \mathbb{Z}/2^4 \times \mathbb{Z}/2^2 \times \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2.$$

4. The group of units of the ring $R = \mathbb{Z}_4[X]/(X^k)$

In this section, we determine the group of units of the ring $R = \mathbb{Z}_4[X]/(X^k)$ with $k \geq 2$. For this it suffices to determine the subgroup $U_1(R)$ of $U(R)$. Since $U(R)$ consists of elements of the form $u+Xf(X)$ with $u = 1$ or $u = 3$, and $U_1(R)$ of elements of $u + Xf(X)$ with $u = 1$, it is not hard to see $U(R) \cong U_1(R) \times \langle 3\rangle$ and, of course, $\langle 3\rangle$ is a cyclic group of order 2.

When i is odd $< k$ we let G_i be the subgroup of $U_1(R)$ generated by $1+X^i$. When i is even with $i = b2^c$ we let G_i to be the cyclic subgroup of $U_1(R)$ generated by $(1 + X^{b2^c})(1 + X^b)^{-2^c}$;

$$G_i = \begin{cases} \langle 1 + X^i\rangle \ \ (\text{if } i \text{ is odd}), \\ \langle (1 + X^{b2^c})(1 + X^b)^{-2^c}\rangle \ (\text{for even } i = b2^c \text{ with } b \text{ odd}). \end{cases}$$

Lemma 4.1. *Let $R = \mathbb{Z}_4[X]/(X^k)$. Then*
(i) *if i is odd, $lo(1 + X^i) = \lfloor \frac{k}{i} \rfloor_2 + 1$,*
(ii) *if i is even, G_i is cyclic of order 2.*

Proof. (i) We know that the order of every element of $U(R)$ a power of 2 since $U(R)$ is a 2-group. Now we have $(1 + X^i)^{2^n} = 1 + 2X^{i2^{n-1}} + X^{i2^n} = 1$ if $2^{n-1} > \frac{k}{i}$. The smallest such power of 2 is $2^{\lfloor \frac{k}{i} \rfloor_2 + 1}$.

(ii) If $i = b2^c$ with an odd b, then

$$\begin{aligned}(1 + X^i)^2 =& 1 + 2X^{b2^c} + X^{b2^{c+1}} \\ =& (1 + X^b)^{2^{c+1}}\end{aligned}$$

by Lemma 2.2. □

We have a natural ring homomorphism $\phi : R = \mathbb{Z}_4[X]/(X^k) \to \mathbb{F}_2[X]/(X^k)$. The map ϕ induces group homomorphisms on the groups of units

$$\phi_0 : U(\mathbb{Z}_4[X]/(X^k)) \to U(\mathbb{F}_2[X]/(X^k))$$

and

$$\phi_1 : U_1(\mathbb{Z}_4[X]/(X^k)) \to U(\mathbb{F}_2[X]/(X^k)).$$

Let T_0 be the kernel of ϕ_0 and T be the kernel of ϕ_1. Then the elements of T are of the form $1 + 2Xf(X)$ with $\deg(f) < k$. Let

$$T_i = \{1 + 2(X^i + (\text{hdt}))\} = \{1 + 2X^i f(X)\} \ (i = 1, 2, \ldots, k - 1),$$

where hdt stand for 'higher degree term' (terms with degree higher than i). Then T_i is a subgroup of T such that $T_i \supset T_{i+1}$. Further

$$T_i \cdot T_j \subset T_i \text{ whenever } i \leq j.$$

Lemma 4.2. *Let i be an odd integer. Then $G_i \cap T \subseteq T_{i2^{k_i-1}}$, where $k_i = \lfloor \frac{k}{i} \rfloor_2$.*

Proof. Obviously, $G_i \cap T = \langle (1 + X^i)^{2^{k_i}}\rangle$. But $(1 + X^i)^{2^{k_i}} = 1 + 2X^{i2^{k_i-1}} \in T_{i2^{k_i-1}}$. □

Lemma 4.3. *Let $2n = b2^c$ be an even integer $< k$. Then $(1+X^{2n})(1+X^b)^{-2^c} \in T_n$ but $(1+X^{2n})(1+X^b)^{-2^c} \notin T_{n+1}$.*

Proof. Since we know that $(1+X^{2n})(1+X^b)^{-2^c} \in T$ we write $(1+X^{2n})(1+X^b)^{-2^c} = 1+2(X^d+\text{hdt})$, where hdt stand for "higher degree terms". Hence

$$\begin{aligned}(1+X^{2n}) &= (1+X^b)^{2^c}(1+2(X^d+\text{hdt})) \\ &= 1+2X^{b2^{c-1}}+2(X^d+\text{hdt})+2X^{2n}(X^d+\text{hdt})+X^{2n}.\end{aligned}$$

Now the middle terms $2X^i$'s have to vanish. Since the degrees of the 4th term gets bigger they has to cancel off with the higher degree terms of the third term. And therefore $2X^{b2^{c-1}}$ has to cancel off with $2X^d$. Thus $d = b2^{c-1} = n$. □

Lemma 4.4. *Let $R = \mathbb{Z}_4[X]/(X^k)$. Then the group $U_1(R)$ of 1-unit of R is of order $2^{2(k-1)}$.*

Proof. The number of elements of the form $1+a_iX^i$, where $a_i \in \mathbb{Z}_4$ and $i < k$ is $2^{2(k-1)}$. □

Using these lemmas we can write $U_1(R)$ as a direct sum of cyclic subgroups.

Theorem 4.5. *Let $R = \mathbb{Z}_4[X]/(X^k)$. Then the group $U_1(R)$ of 1-unit of R is isomorphic to the direct sum*

$$G_1 \oplus G_3 \oplus \cdots \oplus G_{2n+1} \oplus G_2 \oplus G_4 \oplus \cdots \oplus G_{2m},$$

where $2n+1$ is the largest odd integer less than k and $2m$ is the largest even integer less than k. If i is odd, then the group G_i is cyclic group of order $2^{\lfloor \frac{k}{i} \rfloor_2 + 1}$ and if i is even, then G_i is cyclic of order 2.

Proof. First we need to show

$$(G_1 + G_3 + \cdots + G_{2l-1}) \cap G_{2l+1} = (1).$$

Suppose $y \in (G_1 + G_3 + \cdots + G_{2l-1}) \cap G_{2l+1}$. Then it is of the form,

$$(1+X^{2l+1})^{a_{2l+1}} = (1+X)^{a_1}(1+X^3)^{a_3}\cdots(1+X^{2l-1})^{a_{2l-1}}.$$

Reducing the equality modulo 2 we see that both sides are equal to 1 since $U(\mathbb{F}_2[X]/(X^k)) = G_1 \oplus G_3 \oplus \cdots \oplus G_{2n+1}$ by Theorem 3.4. Therefore $a_i = 2^{k_i}$ or where $k_i = \lfloor \frac{k}{i} \rfloor_2$. Now we have

$$1 + 2X^{(2l+1)2^{k_{2l+1}-1}} = \prod_{i<l}\left(1+2X^{(2i-1)2^{k_{2i-1}-1}}\right) = 1 + \sum_{i<l} 2X^{(2i-1)2^{k_{2i-1}-1}}.$$

But by Lemma 4.2 no power of X in the above equation are the same. Hence the equality above is impossible. This proves that $(G_1+G_3+\cdots+G_{2l-1})\cap G_{2l+1} = (1)$.

Now we need to show that $(G_1 + G_3 + \cdots + G_{2n+1} + G_{2m} + G_{2m-2} + \cdots + G_{2l+2}) \cap G_{2l} = (1)$, where $2n+1$ is the largest odd integer $< k$ and $2m$ is the largest even integer which is $< k$. Write $2l = b2^c$. Suppose y belongs to the intersection then, since G_{2l} is of order 2, it must be of the form

$(1+X^{2l})(1+X^b)^{-2^c}$ and it must be an element in $(G_1+G_3+\cdots+G_{2n+1}+G_{2m}+G_{2m-2}+\cdots+G_{2l+2})$. For each even $2i$ write $2i=b_i2^{c_i}$. As before it is of the form

$$(1+X^{2l})(1+X^b)^{-2^c}=\prod_{j \text{ odd}}(1+X^j)^{a_j}\cdot\prod_{2i>2l}\left\{(1+X^{2i})(1+X^{b_i})^{-2^{c_i}}\right\}.$$

Reducing modulo 2 both sides must be equal to 1 by Theorem 3.4. Hence we have $a_j=2^{k_j}$, where $k_j=\lfloor\frac{k}{j}\rfloor_2$ or 0. Now by Lemma 4.2, $(1+X^j)^{a_j}\in T_{j2^{k_j-1}}$ with $j2^{k_j-1}>\frac{k}{2}$. On the other hand, for each $2i$ appearing in the product $\prod_{2i<2l}\{(1+X^{2i})(1+X^{b_i})^{-2^{c_i}}\}$ we have $(1+X^{2i})(1+X^{b_i})^{-2^{c_i}}\in T_i$ with $i>l$. Therefore the righthand side is in T_α with $\alpha>l$ since $l<\frac{k}{2}$. But the left hand side contains the term $2X^l$. This is a contradiction. Hence we conclude that the intersection $(G_1+G_3+\cdots+G_{2n+1}+G_{2m}+G_{2m-2}+\cdots+G_{2l+2})\cap G_{2l}=(1)$.

Finally, we need to check that the group $G_1\oplus G_3\oplus\cdots\oplus G_{2n+1}\oplus G_2\oplus G_4\oplus\cdots\oplus G_{2m}$ has the right order. By Lemma 4.4, we need to show that it has order 2^{2k-2}. We see easily that

$$\#\{\text{positive odd integers}<k\}=\begin{cases}\frac{k}{2} & \text{if } k \text{ is even},\\ \frac{k-1}{2} & \text{if } k \text{ is odd},\end{cases}$$

and

$$\#\{\text{positive even integers}<k\}=\begin{cases}\frac{k-2}{2} & \text{if } k \text{ is even},\\ \frac{k-1}{2} & \text{if } k \text{ is odd}.\end{cases}$$

By Corollary 3.6, we see that $\lfloor k\rfloor_2+\lfloor\frac{k}{3}\rfloor_2+\lfloor\frac{k}{5}\rfloor_2+\cdots+\lfloor\frac{k}{2n+1}\rfloor_2=k-1$. In either case, the order of the direct sum of cyclic groups is 2^{2k-2}. □

Example 4.6. Consider the ring $R=\mathbb{Z}_4[X]/(X^{10})$. The group $U_1(R)$ of 1-units of R is isomorphic to

$$\mathbb{Z}/2^5\oplus\mathbb{Z}/2^3\oplus\mathbb{Z}/2^2\oplus\mathbb{Z}/2^2\oplus\mathbb{Z}/2^2\oplus\mathbb{Z}/2\oplus\mathbb{Z}/2\oplus\mathbb{Z}/2\oplus\mathbb{Z}/2,$$

where the first five cyclic groups are generated by the units

$$1+X, 1+X^3, 1+X^5, 1+X^7, 1+X^9$$

and the last four groups are generated by

$$(1+X^2)(1+X)^{-2}, (1+X^4)(1+X)^{-4}, (1+X^6)(1+X^3)^{-2}, (1+X^8)(1+X)^{-8}$$

in this order.

5. The group of units of the ring $R=\mathbb{Z}_4[X]/(X^k+2X^a)$

Now consider the group of units of the ring $R=\mathbb{Z}_4[X]/(X^k+2X^a)$ with $(0<a<k)$. As before, we have the natural surjection $\phi: R\to\mathbb{F}_2[X]/(X^k)$ which induces surjective group homomorphism on the groups of units and the groups of 1-units. As in the previous section we denote the kernel of ϕ_1 by T and $\{T_i\}$ be the filtration of T which was introduced in the previous section.

For each positive odd integer i, let G_i be the cyclic subgroup of $U_1(R)$ generated by $1+X^i$; and for each positive even integer $2i = b2^c$, let G_i be the cyclic subgroup of $U_1(R)$ generated by $(1+X^{2i})(1+X^b)^{-2^c}$. Write

$$G_{\text{odd}} = \sum_{\text{odd } i<k} G_i \text{ and } G_{ev} = \sum_{\text{even } i<k} G_i.$$

Lemma 5.1. *Let $R = \mathbb{Z}_4[X]/(X^k + 2X^a)$. Then $1+X^{2n} \notin G_{\text{odd}}$.*

Proof. Let $2n = b2^c$ with $c \geq 1$. Assume the contrary and write

$$1 + X^{2n} = \prod_{i\text{odd}} \left(1+X^i\right)^{a_i}.$$

Reducing the expression modulo 2 we see that it should of the form

$$1 + X^{2n} = \left(1+X^b\right)^{2^c} \prod_{\substack{i:\text{odd} \\ i\neq b}} \left(1+X^i\right)^{2^{k_i}},$$

where $k_i = \lfloor \frac{k}{i} \rfloor_2$. Expanding the right hand side we have

$$\left(1 + 2X^{b2^{c-1}} + X^{b2^c}\right)\left(1 + \sum_{i\neq b}(2X^{i2^{k_i-1}} + 2X^{i2^{k_i}-k+a})\right).$$

To simply the notation, let $K = (2^{k_1-1}, 3\cdot 2^{k_3-1}, \ldots, m2^{k_m-1})$ and $2X^K = \sum_{i\neq b} 2X^{i2^{k_i-1}}$. Using this notation if we expand the right hand side we have

$$1 + 2X^{b2^{c-1}} + 2X^K + 2X^{2K-k+a} + 2X^{2n}(X^K + X^{2K-k+a}) + X^{2n}.$$

Now $2X^{b2^{c-1}}$ cannot cancel off with a term in $2X^K$ since the sum runs over i such that $i \neq b$. Hence either $2X^{b2^{c-1}}$ cancels off with a term in $2X^{2K-k+a}$ or does not vanish. (It cannot cancel off with a term in $2X^{2n}(X^K + X^{K-k+a})$ since $b2^{c-1} < 2n$.) If $2X^{b2^{c-1}}$ cancel off with a term of $2X^{2K-k+a}$, then the number of terms in $2X^{b2^{c-1}} + 2X^{2K-k+a}$ is less than the number of terms in $2X^K$. (Some of the exponents $i2^{k_i} - k + a$ may be bigger than k so that $X^{i2^{k_i}-k+a} = 0$) Hence $2X^K + (2X^{b2^{c-1}} + 2X^{2K-k+a}) \neq 0$. Therefore it contains at least a term of the form $2X^\alpha$. If $2X^{b2^{c-1}}$ does not cancel off with a term of $2X^{K-k+a}$, then it contains the term $2X^{b2^{c-1}}$. In either case, the right hand side contains a term of the form $2X^\alpha$ whereas the right hand side does not contain such term. This is a contradiction. □

Lemma 5.2. *Let $2n = b2^c$ be an even integer $< k$. Then $(1+X^{2n})(1+X^b)^{-2^c} \in T_n$ but $(1+X^{2n})(1+X^b)^{-2^c} \notin T_{n+1}$.*

Proof. The same proof of Lemma 4.3 works for our case. □

Lemma 5.3. *Let $R = \mathbb{Z}_4[X]/(X^k + 2X^a)$ and i be an odd integer less than k. Then*

$$lo(1+X^i) = \begin{cases} k_i & \text{if } k-a = i2^{k_i-1}, \\ k_i+1 & \text{otherwise,} \end{cases}$$

where $k_i = \lfloor \frac{k}{i} \rfloor_2$. If $a > \frac{k}{2}$, then $lo(1+X^i) = \lfloor \frac{k}{i} \rfloor_2 + 1$. Furthermore, there are at most one odd i satisfying $k-a = i2^{k_i-1}$.

Proof. First suppose $2X^{i2^{n-1}} + X^{i2^n} = 0$. This happens only when $i2^n \geq k$ and $i2^{n-1} = k-a$. The smallest such one is when $n = k_i$. In this case, if we let $n = k_i$ in the equality

$$(1+X^i)^{2^n} = 1 + 2X^{i2^{n-1}} + X^{i2^n}.$$

Then $X^{i2^{k_i}} = 2X^{i2^{k_i}-k+a} = 2X^{i2^{k_i}-i2^{k_i-1}} = 2X^{i2^{k_i-1}}$ and hence $(1+X^i)^{k_i} = 1$. And obviously no smaller power can make it to be 1.

Now suppose $2X^{i2^{n-1}} + X^{i2^n} \neq 0$. Then we must have $2X^{i2^{n-1}} = 0$ and $X^{i2^n} = 0$ for the equality above reduces to 1. Note $X^{2k-a} = 2X^k = 0$ and these are the smallest such power. Let $n = k_i + 1$ in the equality above. Then $i2^{k_i+1} \geq 2k \geq 2k-a$ and $ik_i \geq k$. Hence $(1+X^i)^{2^{k_i+1}} = 1+2X^{2^{k_i}}+X^{2^{k_i+1}} = 1$. And obviously 2^{k_i+1} is the smallest such power. If $a > \frac{k}{2}$, then $i2^{k_i-1} = k-a$ is impossible since $i2^{k_i-1} \geq \frac{k}{2}$.

For the last part simply note that if $i2^{\lfloor \frac{k}{i} \rfloor_2 - 1} = j2^{\lfloor \frac{k}{j} \rfloor_2 - 1}$ with odd integers i, j, then we must have $i = j$. □

Lemma 5.4. *Let $R = \mathbb{Z}_4[X]/(X^k + 2X^a)$. Then the order of the group of 1-unit $U_1(R)$ is $2^{2(k-1)}$.*

Proof. Similar to the proof of Lemma 4.4. □

Combining these lemmas we can decompose the group of units of $R = \mathbb{Z}_4[X]/(X^k + 2X^a)$ into a direct sum of cyclic groups.

Theorem 5.5. *Let $R = \mathbb{Z}_4[X]/(X^k+2X^a)$. If $a > \frac{k}{2}$, then the group of 1-units $U_1(R)$ of R is isomorphic to the direct sum*

$$G_1 \oplus G_3 \oplus \cdots \oplus G_{2n+1} \oplus G_2 \oplus G_4 \oplus \cdots \oplus G_{2m},$$

where $2n+1$ is the largest odd integer less than k and $2m$ is the largest even integer less than k. If i is odd, then the group G_i is cyclic group of order $2^{\lfloor \frac{k}{i} \rfloor_2 + 1}$ generated by $1 + X^i$ and if i is even, then G_i is cyclic of order 2 generated by $(1+X^{2n})(1+X^b)^{-2^c}$ with $2n = b2^c < k$.

Proof. First we show

$$(G_1 + G_3 + \cdots + G_{2l-1}) \cap G_{2l+1} = (1).$$

Suppose $y \in (G_1 + G_3 + \cdots + G_{2l-1}) \cap G_{2l+1}$. Then it is of the form,

$$(1+X^{2l+1})^{a_{2l+1}} = (1+X)^{a_1}(1+X^3)^{a_3} \cdots (1+X^{2l-1})^{a_{2l-1}}.$$

If we reduce modulo 2, then both sides are equal to 1 by Theorem 3.4. Therefore $a_i = 2^{k_i}$, where $k_i = \lfloor \frac{k}{i} \rfloor_2$. But $lo(1+X^i) = k_i + 1$ by Lemma 5.3. Hence we have

$$(1+X^{2l+1})^{2^{k_{2l+1}}} = \prod_{\substack{i<2l+1 \\ i=\text{odd}}} (1+X^i)^{2^{k_i}},$$

where the product is taken over odd integers i with $i < 2l+1$.

$$\begin{aligned} &1 + 2X^{(2l+1)2^{k_{2l+1}}-1} + 2X^{(2l+1)2^{k_{2l+1}}-k+a} \\ &= \prod_{\substack{i<2l+1 \\ i=\text{odd}}} (1 + 2X^{i2^{k_i-1}} + 2X^{i2^{k_i}-k+a}) = 1 + \sum_{\substack{i<2l+1 \\ i=\text{odd}}} (2X^{i2^{k_i-1}} + 2X^{i2^{k_i}-k+a}). \end{aligned}$$

Hence we must have

$$\sum_{\substack{i\le 2l+1 \\ i=\text{odd}}} \left(2X^{i2^{k_i-1}} + 2X^{i2^{k_i}-k+a}\right) = 0.$$

But the equality above is impossible. This follows from the observation: If $K = \{a_1, a_2, \ldots, a_n\}$ strictly increasing numbers with a's are of the form $i2^{k_i-1}$, then $2K - \alpha = \{2a_1 - \alpha, 2a_2 - \alpha, \ldots, 2a_n - \alpha\}$ is also a strictly increasing numbers. In order that the two sets to be equal $a_i = 2a_i - \alpha$, namely $a_i = \alpha$ for all i. We apply this with $\{a_i\}$ to be the exponents $\{i2^{k_i-1}\}$ appearing in the sum which are all distinct. Hence we see $(G_1 + G_3 + \cdots + G_{2l-1}) \cap G_{2l+1} = (1)$.

Now we need to show that $(G_1 + G_3 + \cdots + G_{2n+1} + G_{2m} + G_{2m-2} + \cdots + G_{2l+2}) \cap G_{2l} = (1)$, where $2n+1$ is the largest odd integer $< k$ and $2m$ is the largest integer which is $< k$. Write $2l = b2^c$. Suppose y belongs to the intersection then, since G_{2l} is of order 2, it must be of the form $(1+X^{2l})(1+X^b)^{-2^c}$ and it must be an element in $(G_1 + G_3 + \cdots + G_{2n+1} + G_{2m} + G_{2m-2} + \cdots + G_{2l+2})$. For each even $2i$ write $2i = b_i 2^{c_i}$. Then, as before, it is of the form

$$(1+X^{2l})(1+X^b)^{-2^c} = \prod_{j \text{ odd}} (1+X^j)^{a_j} \cdot \prod_{2i=b_i2^{c_i}>2l} \left\{(1+X^{2i})(1+X^{b_i})^{-2^{c_i}}\right\}.$$

Suppose there is no right hand side product $\prod_{i \text{ even}>2l}\{(1+X^i)(1+X^{b_i})^{-2^{c_i}}\}$. Then we have $1+X^{2l} \in G_{\text{odd}}$ which contradicts to Lemma 5.1. Hence the right hand side product is nontrivial. Let $(1+X^{2i})(1+X^{b_i})^{2^{c_i}} = 2X^{b_i2^{c_i-1}} + (\text{hdt})$ and let $B = \{b_i 2^{c_i-1}\}$. Then $b_i 2^{c_i-1} > l$. Now by reducing modulo 2, we see that $a_j = k_j = j2^{\lfloor \frac{k}{j} \rfloor_2}$. Hence the left hand side product can be written

$$\prod (1+X^i)^{k_i} = 1 + 2\sum (X^{i2^{k_i-1}} + X^{i2^{k_i}-k+a}).$$

If we write $K = \{i2^{k_i-1}\}$, then we can write the sum simply by

$$\prod (1+X^i)^{k_i} = 1 + 2(X^K + X^{2K-k+a}).$$

Note that $i2^{k_i-1} > \frac{k}{2}$ and $i2^{k_i} - k + a \geq a > \frac{k}{2}$ by our assumption on a. Therefore the whole product is of the form $1+2(X^B+(\text{hdt})+X^K+X^{2K-k+a})$ and is contained in T_α for some α with $\alpha > l$. On the other hand, the left hand side is of the form $1 + 2(X^l + (\text{hdt})) \in T_l$ by Lemma 5.2.

This proves that $(G_1 + G_3 + \cdots + G_{2n+1} + G_2 + \cdots + G_{2l-2}) \cap G_{2l} = (1)$, where $2n + 1$ is the largest odd integer $< k$.

To finish our proof we need to check that the order of the subgroup $G_{\text{odd}} \oplus G_{ev}$ is $2^{2(k-1)}$. However, the same proof of last part of Theorem 4.5 also works for this case also. □

Question† **and Remark.** Is Theorem 5.5 true without assuming $a > \frac{k}{2}$? Under our assumption on a Theorem 5.5 asserts that the group of 1-unit of the ring $R = \mathbb{Z}_4[X]/(X^k + 2X^a)$ depends only on k.

Example 5.6. Let $R = \mathbb{Z}_4[X]/(X^5 + 2X^3)$. Then $o(U_1(R)) = 2^8$. Now we have

$$lo(1 + X) = 4, lo(1 + X^3) = 2,$$
$$lo((1 + X^2)(1 + X)^{-2}) = 1,\ lo((1 + X^4)(1 + X)^{-4}) = 1.$$

Hence

$$U_1(R) \cong G_1 \oplus G_3 \oplus G_2 \oplus G_4 \cong \mathbb{Z}/2^4 \oplus \mathbb{Z}/2^2 \oplus \mathbb{Z}/2 \oplus Z/2 \oplus Z/2.$$

Here we note that $(1 + X^4)(1 + X)^{-4} = (1 + X^4)(1 + X)^{12} = (1 + X^4)(1 + 2X^2 + 3X^4) = 1 + 2X^2$. And $(1 + X)^8 = 1 + 2X^4$.

6. The group of units of the ring $R = \mathbb{Z}_4[X]/(X^k + 2X^a, 2X^r)$

Let $R = \mathbb{Z}_4[X]/(X^k + 2X^a, 2X^r)$, where $0 < a < r < k$. We have surjective ring homomorphisms

$$\mathbb{Z}_4[X]/(X^k + 2X^a) \xrightarrow{\phi_1} \mathbb{Z}_4[X]/(X^k + 2X^a, 2X^r) \xrightarrow{\phi_2} \mathbb{F}_2[X]/(X^k).$$

They induces surjective maps on the groups of units and their kernels are

$$\text{Ker}(\phi_1) = \{1 + 2(X^r + \text{hdt})\},$$
$$\text{Ker}(\phi_2) = \{1 + 2(X + \text{hdt})\}.$$

Lemma 6.1. *Let $R = \mathbb{Z}_4[X]/(X^k + 2X^a, 2X^r)$ with $0 < a < r < k$. Then the number of elements of R is 2^{k+r} and the number of elements of $U(R)$ is 2^{k+r-1} and the group of 1-units $U_1(R)$ has order 2^{k+r-2}.*

Proof. The number of elements of $S = \mathbb{Z}_4[X]/(X^k+2X^a)$ is 4^k. Since the number of elements of the ideal $(2X^r)$ in S is 2^{k-r}. Hence the number of elements of R is $4^k/2^{k-r} = 4^r 2^{k-r}$. On the other hand, note that $R = U(R) \cup (1+U(R))$ is a disjoint union and they have the same number of elements. Therefore the number of elements of $U(R)$ is $4^r 2^{k-r-1}$ and $o(U_1(R)) = \frac{1}{2}o(U(R))$. □

†This question is resolved in [4, 5].

Lemma 6.2. *Let $R = \mathbb{Z}_4[X]/(X^k + 2X^a, 2X^r)$ with $0 < a < r < k$. Then for each odd integer i less than k we have*

(i) *If $k \le r + a$ and $k - a \neq i2^{\lfloor \frac{r}{i} \rfloor_2}$, then $lo(1 + X^i) = \lfloor \frac{2r}{i} \rfloor_2$.*

(ii) *If $k \ge r + a$, then*

$$lo(1 + X^i) = \begin{cases} \lfloor \frac{k+r-a}{i} \rfloor_2, \\ \lfloor \frac{k}{i} \rfloor_2 \quad \text{if} \quad k - a = i2^{k_i - 1}, \end{cases}$$

where $k_i = \lfloor \frac{k}{i} \rfloor_2$. There are at most one positive odd integer i less than k satisfying the condition $k - a = i2^{k_i - 1}$.

Proof. Note that $X^{k+r-a} = 2X^r = 0$ and these are the least such exponents. Now we have $(1 + X^i)^{2^n} = 1 + 2X^{i2^{n-1}} + X^{i2^n} = 1$ if $i2^{n-1} \ge r$ and $i2^n \ge k + r - a$. Hence if $2r \ge k + r - a$, i.e., $k \le r + a$, then $lo(1 + X^i) = \lfloor \frac{2r}{i} \rfloor_2$.

On the other hand, suppose $k \ge r + a$. Consider the case $k - a = i2^{k_i - 1}$. If we let $n = k_i$ in the equality

$$(1 + X^i)^{2^n} = 1 + 2X^{i2^{n-1}} + X^{i2^n},$$

then $X^{i2^{k_i}} = 2X^{i2^{k_i} - k + a} = 2X^{i2^{k_i} - i2^{k_i - 1}} = 2X^{i2^{k_i - 1}}$ and hence $(1 + X^i)^{k_i} = 1$ and obviously no smaller 2-power can make it to be 1. Hence $lo(1 + X^i) = \lfloor \frac{k}{i} \rfloor_2$. And this is the only case when $2X^{i2^{n-1}}$ cancels off with X^{i2^n} for if j is another odd such that $k - a = j2^{k_j - 1}$, then $j2^{k_j - 1} = i2^{k_i - 1}$ and hence $i = j$. If $k - a \neq i2^{k_i - 1}$, then there is no chance that $2X^{i2^{n-1}}$ cancels off with X^{i2^n}. Hence the smallest power of 2 that makes $(1 + X^i)$ to be 1 will be $\lfloor \frac{k+r-a}{i} \rfloor_2$. □

Let $R = \mathbb{Z}_4[X]/(X^k + 2X^a, X^r)$ with $0 < a < r < k$. As before we have the natural surjective map $\phi_2 : R \to \mathbb{F}_2[X]/(X^k)$ which induces surjective group homomorphism on the groups of 1-units. As in the previous section, we denote the kernel of ϕ_1 by T and T_i be the filtration of T as defined there.

Again as in the previous section, for each odd i less than k, let G_i be the cyclic subgroup of $U_1(R)$ generated by $1 + X^i$ and for even $2i = b2^c$ let G_i be the cyclic subgroup of $U_1(R)$ generated by $(1 + X^{2i})(1 + X^b)^{-2^c}$. Write

$$G_{\text{odd}} = \sum_{\text{odd } i<k} G_i \quad \text{and} \quad G_{ev} = \sum_{\text{even } i<k} G_i.$$

Lemma 6.3. *Let $R = \mathbb{Z}_4[X]/(X^k + 2X^a, 2X^r)$. Then $1 + X^{2n} \notin G_{\text{odd}}$.*

Proof. We slightly modify the proof of Lemma 5.1. Let $2n = b2^c$, $c \ge 1$. Assume the contrary and write

$$1 + X^{2n} = \prod_{i:\text{odd}} \left(1 + X^i\right)^{a_i}.$$

Reducing the expression modulo 2 we see that it should of the form

$$1 + X^{2n} = (1 + X^b)^{2^c} \prod_{\substack{i:\text{odd} \\ i \neq b}} \left(1 + X^i\right)^{2^{k_i}}$$

where $k_i = \lfloor \frac{k}{i} \rfloor_2$. Expanding the right hand side we have

$$\left(1 + 2X^{b2^{c-1}} + X^{b2^c}\right)\left(1 + \sum_{i \neq b}(2X^{i2^{k_i-1}} + 2X^{i2^{k_i}-k+a})\right).$$

To simplify the notation let $K = (2^{k_1-1}, 3 \cdot 2^{k_3-1}, \ldots, m2^{k_m-1})$ and $2X^K = \sum_{i \neq b} 2X^{i2^{k_i-1}}$. Using this notation if we expand the right hand side we have

$$1 + 2X^{b2^{c-1}} + 2X^K + 2X^{2K-k+a} + 2X^{2n}(X^K + X^{2K-k+a}) + X^{2n}.$$

If $b2^{c-1} \geq r$, then since $K \neq 2K - k + a$ the above sum contains a nonzero term of the form $2X^\alpha$. Now let $b2^{c-1} < r$. As before $2X^{b2^{c-1}}$ cannot cancel off with a term in $2X^K$ since the sum runs over i such that $i \neq b$. Hence either $2X^{b2^{c-1}}$ cancels off with a term in $2X^{2K-k+a}$ or does not vanish. (It cannot cancel off with a term in $2X^{2n}(X^K + X^{K-k+a})$ since $b2^{c-1} < 2n$.) If $2X^{b2^{c-1}}$ cancel off with a term of $2X^{2K-k+a}$, then the number of terms in $2X^{b2^{c-1}} + 2X^{2K-k+a}$ is less than the number of terms in $2X^K$. (Some of the exponents $i2^{k_i} - k + a$ may be bigger than r so that $X^{i2^{k_i}-k+a} = 0$.) Hence $2X^K + (2X^{b2^{c-1}} + 2X^{2K-k+a}) \neq 0$. Therefore it contains at least a term of the form $2X^\alpha$. If $2X^{b2^{c-1}}$ does not cancel off with a term of $2X^{K-k+a}$, then it contains the term $2X^{b2^{c-1}}$. In either case the right hand side contains a term of the form $2X^\alpha$ whereas the right hand side does not contain such term. This is a contradiction. □

Lemma 6.4. *Let $2n = b2^c$ be an even integer $< r$. Then $(1+X^{2n})(1+X^b)^{-2^c} \in T_n$ but $(1 + X^{2n})(1 + X^b)^{-2^c} \notin T_{n+1}$.*

Proof. The same proof of Lemma 4.3 works for our case. □

Finally we compute the group of units of the ring $R = \mathbb{Z}_4[X]/(X^k + 2X^a, 2X^r)$ with a certain restriction on a.

Theorem 6.5. *Let $R = \mathbb{Z}_4[X]/(X^k + 2X^a, 2X^r)$. Suppose $\frac{k}{2} < a < r$ then the group $U_1(R)$ of 1-units of R is isomorphic to the direct sum*

$$G_1 \oplus G_3 \oplus \cdots \oplus G_{2n+1} \oplus G_2 \oplus G_4 \oplus \cdots \oplus G_{2m},$$

where $2n + 1$ is the largest odd integer less than k and $2m$ is the largest even integer less than r. If i is odd $< k$, then the group G_i is cyclic group of order $2^{\lfloor \frac{2r}{i} \rfloor_2}$ generated by $1+X^i$ and if i is even, then G_i is cyclic of order 2 generated by $(1 + X^{2n})(1 + X^b)^{-2^c}$ with $2n = b2^c < k$.

Proof. First we show

$$(G_1 + G_3 + \cdots + G_{2l-1}) \cap G_{2l+1} = (1).$$

Suppose $y \in (G_1 + G_3 + \cdots + G_{2l-1}) \cap G_{2l+1}$. Then it is of the form,

$$(1 + X^{2l+1})^{a_{2l+1}} = (1 + X)^{a_1}(1 + X^3)^{a_3} \cdots (1 + X^{2l-1})^{a_{2l-1}}.$$

If we reduce modulo 2, then both sides are equal to 1 since $\mathbb{F}_2[X]/(X^k) = G_1 \oplus G_3 \oplus \cdots \oplus G_{2n+1}$. Therefore $a_i = 2^{k_i}$ or 0, where $k_i = \lfloor \frac{k}{i} \rfloor_2$. Hence the equality above is of the form

$$(1+X^{2l+1})^{2^{k_{2l+1}}} = \prod_{\substack{i<2l+1 \\ i=\text{odd}}} (1+X^i)^{2^{k_i}}.$$

In other words,

$$\begin{aligned} &1 + 2X^{(2l+1)2^{k_{2l+1}}-1} + 2X^{(2l+1)2^{k_{2l+1}}-k+a} \\ &= \prod_{\substack{i<2l+1 \\ i=\text{odd}}} (1 + 2X^{i2^{k_i}-1} + 2X^{i2^{k_i}-k+a}) = 1 + \sum_{\substack{i<2l+1 \\ i=\text{odd}}} (2X^{i2^{k_i}-1} + 2X^{i2^{k_i}-k+a}). \end{aligned}$$

Hence we have

$$\sum_{\substack{i\le 2l+1 \\ i=\text{odd}}} (2X^{i2^{k_i}-1} + 2X^{i2^{k_i}-k+a}) = 0.$$

But the equality above is impossible. This follow from the observation: If $K = \{a_1, a_2, \ldots, a_n\}$ strictly increasing numbers, then $2K - a = \{2a_1 - a, 2a_2 - a, \ldots, 2a_n - a\}$ is also a strictly increasing numbers. In order that the two sets are the same $a_i = 2a_i - a$ namely $a_i = a$ for all i. We apply this with $\{a_i\}$ to be the exponents $\{i2^{k_i-1}\}$ appearing in the sum which are all distinct. This proves that $(G_1 + G_3 + \cdots + G_{2l-1}) \cap G_{2l+1} = (1)$.

Now we need to show that $(G_1 + G_3 + \cdots + G_{2n+1} + G_{2m} + G_{2m-2} + \cdots + G_{2l+2}) \cap G_{2l} = (1)$, where $2n+1$ is the largest odd integer $< k$ and $2m$ is the largest integer which is $< r$. Write $2l = b2^c$. Suppose $y(\neq 1)$ belongs to the intersection then, since G_{2l} is of order 2, it must be of the form $(1+X^{2l})(1+X^b)^{-2^c}$ and it must be an element in $(G_1 + G_3 + \cdots + G_{2n+1} + G_{2m} + G_{2m-2} + \cdots + G_{2l+2})$. For each even i write $i = b_i 2^{c_i}$. As before it is of the form

$$(1+X^{2l})(1+X^b)^{-2^c} = \prod_{j \text{ odd}} (1+X^j)^{a_j} \cdot \prod_{r>2i=b_i 2^{c_i}>2l} \left\{(1+X^{2i})(1+X^{b_i})^{-2^{c_i}}\right\}.$$

Suppose there is no right hand side product $\prod_{i \text{ even}>2l}\{(1+X^i)(1+X^{b_i})^{-2^{c_i}}\}$. Then we have $1 + X^{2l} \in G_{\text{odd}}$ which contradicts to Lemma 6.3. Hence the right hand side product expression is nontrivial. Let $(1+X^{2i})(1+X^{b_i})^{2^{c_i}} = 2X^{b_i 2^{c_i-1}} + (\text{hdt})$ and let $B = \{b_i 2^{c_i-1}\}$. Then $b_i 2^{c_i-1} > l$. Now by reducing modulo 2, we see that $a_j = k_j = j2^{\lfloor \frac{k}{j} \rfloor_2}$. Hence

$$\prod \left(1+X^i\right)^{k_i} = 1 + 2\sum \left(X^{2^{k_i-1}} + X^{2^{k_i}-k+a}\right).$$

If we write $K = \{i2^{k_i-1}\}$, then we can write the sum simply by

$$\prod \left(1+X^i\right)^{k_i} = 1 + 2\left(X^K + X^{2K-k+a}\right).$$

Note that $i2^{k_i-1} > \frac{k}{2}$ and $2^{k_i} - k + a \geq a > \frac{k}{2}$ by our assumption on a. Therefore the whole product is of the form $1+2(X^B+(\mathrm{hdt})+X^K+X^{2K-k+a})$ and is contained in T_α with $\alpha > l$. On the other hand, the left hand side is of the form $1+2(X^l+(\mathrm{hdt})) \in T_l$ by Lemma 6.4 which is impossible. This proves that $(G_1 + G_3 + \cdots + G_{2n+1} + G_2 + \cdots + G_{2l-2}) \cap G_{2l} = (1)$, where $2n+1$ is the largest odd integer $< k$.

To finish our proof we need to show that the direct sum of our subgroups has the right order. In fact we know that

$$\sum_{\text{odd } i \geq 1}^{2r-1} \lfloor \frac{2r}{i} \rfloor_2 = 2r - 1.$$

If i is odd $\geq k$, then $\lfloor \frac{2r}{i} \rfloor_2 = 1$. Since the numbers of such i's are

$$\begin{cases} \frac{2r-k-1}{2} & \text{if } k \text{ is odd,} \\ \frac{2r-k}{2} & \text{if } k \text{ is even.} \end{cases}$$

Hence

$$\sum_{i \,\text{odd}} lo(G_i) = \begin{cases} (2r-1) - \frac{2r-k+1}{2} & \text{if } k \text{ is odd,} \\ (2r-1) - \frac{2r-k}{2} & \text{if } k \text{ is even.} \end{cases}$$

On the other hand,

$$\sum_{i \,\text{even}} lo(G_i) = \#(\text{even} < k) = \begin{cases} \frac{k-1}{2} & \text{if } k \text{ is odd,} \\ \frac{k-2}{2} & \text{if } k \text{ is even.} \end{cases}$$

Therefore $lo(G_{\text{odd}})+lo(G_{ev}) = k+r-2$ which is exactly the order of $U_1(R)$. □

Example 6.6. Let $R = \mathbb{Z}_4[X]/(X^5 + 2X^3, 2X^4)$. Then the order of $U_1(R)$ is 2^7 and

$$U_1(R) \cong G_1 \oplus G_3 \oplus G_2 \oplus G_4,$$

where $G_1 = \langle 1+X \rangle$ with order 2^3 and $G_3 = \langle 1+X^3 \rangle$ having order 2^2; G_2, G_4 are cyclic groups of order 2 generated by $(1+X^2)(1+X)^{-2}$ and $(1+X^4)(1+X)^{-4}$ respectively. Therefore,

$$U_1(R) \cong \mathbb{Z}/2^3 \oplus \mathbb{Z}/2^2 \oplus \mathbb{Z}/2 \oplus \mathbb{Z}/2.$$

Acknowledgement. In the sequel of this paper [4, 5] we will remove the restrictions imposed in the paper by modifying the set of generators.

References

[1] B. R. McDonald, *Finite Rings with Identity*, Pure and Applied Mathematics, Vol. 28. Marcel Dekker, Inc., New York, 1974.
[2] S. S. Woo, *Algebras with a nilpotent generator over $\mathbb{Z}_{p^2}$*, Bull. Korean Math. Soc. **43** (2006), no. 3, 487–497.
[3] ———, *Cyclic codes of even length over Z_4*, J. Korean Math. **44** (2007), no. 3, 697–706.
[4] ———, *The group of units of some finite local rings II*, J. Korean Math. **46** (2009), no. 3, 475–491.

[5] ———, *The group of units of some finite local rings III*, J. Korean Math. **46** (2009), no. 4, 675–689.

Department of Mathematics
Ewha Women's University
Seoul 120-750, Korea
E-mail address: sswoo@ewha.ac.kr