

## THE GROUP OF UNITS OF SOME FINITE LOCAL RINGS II

SUNG SIK WOO

ABSTRACT. In [2], we identified the group of units of finite local rings  $\mathbb{Z}_4[X]/(X^k + 2X^a, 2X^r)$  with certain restrictions on  $a$ . In this paper we find direct sum decomposition of the group of units of such rings without restrictions on  $a$  into cyclic subgroups by finding their generators. And further generalization is considered.

### 1. Introduction

In [2], we observed that any finite  $\mathbb{Z}_4$ -algebra which is generated by a single element is of the form  $R = \mathbb{Z}_4[X]/(X^k + 2u(X)X^a, 2X^r)$  with  $a < r < k$  and a polynomial  $u(X)$  such that  $u(0) = 1$  and  $\deg(u) < r - a$ . The group of units  $U(R)$  of  $R$  is easily seen to be a 2-group and we will decompose it into a direct sum of cyclic subgroups by finding their generators explicitly. If  $a = 0$ , then  $R$  is a chain ring [1, Chapter XVII].

In Section 2, we show that the surjective ring homomorphism

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

induces a surjective group homomorphism which we still call  $\phi$ ,

$$\phi : U(\mathbb{Z}_4[X]/(X^k + 2u(X)X^a, 2X^r)) \rightarrow U(\mathbb{F}_2[X]/(X^k))$$

on the groups of units and find its kernel. And then we set up our notations and prove technical lemmas to be used in the next sections.

In Section 3, we consider the rings of the form  $R = \mathbb{Z}_4[X]/(X^k + 2u(X)X^a)$  with  $u = 1$  and find a decomposition of the group of units  $U(R)$  of  $R$  into a direct sum of cyclic subgroups. The generators we are going to use will be different from those used in [2]. It turns out that those generators do not give us a direct sum decomposition of the group of units for  $u \neq 1$ . Hence further investigation is needed when  $u \neq 1$ .

In Section 4, we consider the ring  $R = \mathbb{Z}_4[X]/(X^k + 2u(X)X^a, 2X^r)$ . When  $u = 1$ , a complete description of the group of units of  $R$  into a direct sum of cyclic subgroups with explicit generators is given.

---

Received July 25, 2007.

2000 *Mathematics Subject Classification.* 13C12.

*Key words and phrases.* finite local ring, group of units.

We will use the following notations: For a finite set  $S$  of positive integers and a nonnegative integer  $\alpha$  we will write  $S + \alpha = \{i + \alpha \mid i \in S\}$ . And  $X^S = \sum_{i \in S} X^i$  as an element of  $\mathbb{Z}_4[X]$ . If  $S = \emptyset$ , then we define  $X^S = 0$ .

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

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  $lo_2(G) = n$  or simply  $lo(G) = n$ . For  $x \in G$  we will write  $lo_2(x)$  for the 2-logarithmic order of the subgroup generated by  $x$ .

Any unexplained notations are in [2].

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

Now consider the group of units of the ring  $R = \mathbb{Z}_4[X]/(X^k + 2u(X)X^a, 2X^r)$ , where  $u(X) = \sum_{i=0}^s a_i X^i$ , where  $a_0 = 1$ , and  $\deg(u) < k - a$ . We will adopt the convention that  $X^{-\infty} = 0$  so that our ring can be  $R = \mathbb{Z}_4[X]/(X^k)$  if  $a = r = -\infty$ ; or  $R = \mathbb{Z}_4[X]/(X^k + 2X^a)$  if  $r = -\infty$ . If  $a > 0$ , then the elements of the form  $1 + Xf(X)$ , where  $f \in \mathbb{Z}_4[X]$  form a subgroup  $U_1(R)$  which we call the group of 1-units. If  $a = 0$ , then the set of 1-units does not form a subgroup and in that case we will only consider the group of units of  $R$ .

In [2, Theorem 3.4], we identified the group of units of the ring  $\mathbb{F}_2[X]/(X^k)$  as the direct sum of cyclic subgroups generated by  $1 + X^i$  for all odd integers  $i$  with  $0 < i < k$ . And the 2-logarithmic order of  $1 + X^i$  is  $\lfloor \frac{k}{i} \rfloor_2$ .

Consider the surjective ring homomorphism  $\mathbb{Z}_4[X]/(X^k + 2uX^a, 2X^r) \xrightarrow{\phi} \mathbb{F}_2[X]/(X^k)$ . Then  $\phi$  induces a surjective map on the group of units since a unit of  $\mathbb{F}_2[X]/(X^k)$  is of the form  $1 + Xf(X)$  and the same expression in  $R = \mathbb{Z}_4[X]/(X^k + 2uX^a, 2X^r)$  will give rise to a lift. Hence we have an exact sequence

$$(1) \rightarrow T_0 \rightarrow U(\mathbb{Z}_4[X]/(X^k + 2uX^a, 2X^r)) \xrightarrow{\phi} U(\mathbb{F}_2[X]/(X^k)) \rightarrow (1),$$

where  $T_0$  is the kernel of  $\phi$ . Then  $T_0$  will be generated by  $\Delta = \{-1 + 2X^i \mid 0 \leq i < n\}$ , where  $n = k$  if  $r = -\infty$ ; and  $n = r$  if  $r > 0$ . Note that we could also choose the generators of  $T_0$  by  $\{-1\} \cup \{1 + 2X^i \mid 0 < i < n\}$ .

When  $a > 0$ , we can construct a similar exact sequence for 1-units

$$(1) \rightarrow T \rightarrow U_1(\mathbb{Z}_4[X]/(X^k + 2uX^a, 2X^r)) \xrightarrow{\phi_1} U(\mathbb{F}_2[X]/(X^k)) \rightarrow (1),$$

where  $T$  is the kernel of  $\phi_1$ . Then  $T$  will be generated by  $\Delta_1 = \{1 + 2X^i \mid 0 < i < n\}$ , where  $n = k$  if  $r = -\infty$ ; and  $n = r$  if  $r > 0$ .

We let

$$\begin{aligned} G_i &= \langle 1 + X^i \rangle \text{ if } i \text{ is odd with } 0 < i < k, \\ H_j &= \langle 1 + 2X^j \rangle \text{ if } j \text{ an integer with } 0 < j < k \text{ and,} \\ H_0 &= \langle -1 \rangle, \end{aligned}$$

and let

$$G = \sum_{1 \leq i: \text{odd} < k} G_i, H_{(l)} = \sum_{0 < i < l} H_i \text{ and } H_{(l)}^+ = \sum_{0 \leq i < l} H_i.$$

Also note that if  $U_1(R)$  is well defined, then  $U(R) = H_0 \oplus U_1(R)$  and  $T_0 = H_0 \oplus T$ .

We will prove a crucial fact which we will use repeatedly in the proofs of our assertions in the following sections.

**Lemma 2.1.** *Let  $k$  be a positive integer and let  $k_i = \lfloor \frac{k}{i} \rfloor_2$ . Then*

$$\{i2^{k_i-1} \mid 0 < i : \text{odd} < k\} = \left\{ i \mid \frac{k}{2} \leq i < k \right\}.$$

*Proof.* Consider the set  $\{i2^{k_i-1} \mid 0 < i : \text{odd} < k\}$  which we call  $K$ . Observe that the elements of  $K$  are all distinct since  $i$ 's are distinct odd numbers. Further every element of  $K$  is  $< k$  by the very definition of  $\lfloor \frac{k}{i} \rfloor_2$ . On the other hand, every element of  $K$  is  $\geq \frac{k}{2}$  since  $i2^{k_i} \geq k$ .

Now the number of elements of  $K$  is  $\frac{k-1}{2}$  if  $k$  is odd and  $\frac{k}{2}$  if  $k$  is even. Since these are precisely the numbers of elements in  $\{i \mid \frac{k}{2} \leq i < k\}$  we have the equality above.  $\square$

In [2, Corollary 3.5] we proved the following fact.

**Lemma 2.2.** *If  $k$  is a positive integer, then*

$$\sum_{0 < i: \text{odd} < k} \lfloor \frac{k}{i} \rfloor_2 = k - 1.$$

Using these facts we can prove some interesting formula as a byproduct.

**Corollary 2.3.** *Let  $k$  be a positive integer. Then*

$$\frac{\prod \{i \mid \frac{k}{2} \leq i : \text{even} < k\}}{\prod \{i \mid 1 \leq i : \text{odd} < \frac{k}{2}\}} = \begin{cases} 2^{\frac{k-1}{2}} & \text{if } k \text{ is odd,} \\ 2^{\frac{k-2}{2}} & \text{if } k \text{ is even.} \end{cases}$$

*Proof.* Let  $k_i = \lfloor \frac{k}{i} \rfloor_2$ . By the lemma above and the fact  $\sum \{k_i \mid 0 < i : \text{odd} < k\} = k - 1$ , we have

$$\begin{aligned} \sum \log_2 \{2j \mid k \leq 2j < 2k\} &= \sum \log_2 \{i2^{k_i} \mid 0 < i : \text{odd} < k\} \\ &= \sum_{0 < i: \text{odd} < k} \log_2(i) + \sum_{0 < i: \text{odd} < k} k_i \\ &= \sum_{0 < i: \text{odd} < k} \log_2(i) + (k - 1). \end{aligned}$$

On the other hand,

$$\begin{aligned} \sum \log_2\{2j \mid k \leq 2j < 2k\} &= \sum_{\frac{k}{2} \leq j < k} \{(\log_2 j) + 1\} \\ &= \sum_{\frac{k}{2} \leq j < k} (\log_2 j) + \begin{cases} \frac{k-1}{2} & \text{if } k \text{ is odd,} \\ \frac{k}{2} - 1 & \text{if } k \text{ is even.} \end{cases} \end{aligned}$$

Therefore we have

$$\sum_{\frac{k}{2} \leq j < k} (\log_2 j) - \sum_{0 < i: \text{odd} < k} \log_2(i) = \sum_{\frac{k}{2} \leq j: \text{even} < k} (\log_2 j) - \sum_{0 < i: \text{odd} < \frac{k}{2}} \log_2(i)$$

and this is equal to

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

**Lemma 2.4.** *Let  $\mathbb{Z}_4[X]/(X^k + 2X^a)$  with  $0 < a < k$  and let  $H$  be a subgroup of  $U(R)$ .*

(i) *For each  $i$  with  $0 < i < k$  let  $S_i$  be a subset of  $\{1, 2, \dots, k-1\}$  consisting of at most a single element such that  $i \notin S_i$ . If  $H$  contains the elements  $1 + 2X^i + 2X^{S_i}$ , then  $H$  contains  $1 + 2X^i$  for all  $0 < i < k$ . (Recall that when  $S_i = \emptyset$  we defined  $X^{S_i} = 0$ .)*

(ii) *If  $H$  contains all*

$$1 + 2(X^j + (\text{hdt})) \quad (0 < j < k),$$

*where hdt stand for ‘higher degree terms’, then  $H$  contains  $1 + 2X^i$  for all  $0 < i < k$ .*

*Proof.* (i) First note that  $1 + 2X^{k-1} \in H$ . If there is  $S_i$  containing  $k-1$ , then we have  $(1 + 2(X^i + X^{S_i}))(1 + 2X^{k-1}) = 1 + 2X^i \in H$ . Hence, in particular, we see that  $1 + 2X^{k-2} \in H$ . In this way, we arrive, eventually, at the conclusion that  $1 + 2X^i \in H$  for all  $i < k$ .

(ii) If  $j = k-1$ , then  $1 + 2(X^j + (\text{hdt})) = 1 + 2X^j$ . Hence  $1 + 2X^j \in H$ . Therefore if there an element having  $2X^j$  as a higher degree term, then we can cancel it off by multiplying  $1 + 2X^j$  to it. And so on. □

**Lemma 2.5.** *Let  $R = \mathbb{Z}_4[X]/(X^k + 2u(X))$ , where  $u(X) = X^{a_0} + \dots + X^{a_s}$  with  $0 < a_0 < \dots < a_s$  and  $a_s < k$ . Let  $A = \{i \mid \frac{k}{2} \leq i < k\}$  and let  $H$  be a subgroup of  $U(R)$  containing*

$$\left\{ 1 + 2X^i + \sum_{0 \leq j \leq s} 2X^{2i-k+a_j} \mid \frac{k}{2} \leq i < k \right\}.$$

*Let  $B = \{i \mid 0 < i < \frac{k}{2}\}$  and let  $b$  be the number of elements of  $B$ .*

(i) *If  $a_0 > \frac{k}{2}$ , then  $\sum_{0 < i < \frac{k}{2}} H_i$  together with  $G \cap T$  generate  $T$ .*



**Proposition 2.6.** *Let  $R = \mathbb{Z}_4[X]/(X^k + 2u(X))$ , where  $u(X) = X^{a_0} + \dots + X^{a_s}$  with  $0 < a_0 < \dots < a_s$  and  $a_s < k$ . Assume  $u \neq 1$  and  $a_0 \leq \frac{k}{2}, a_0 \neq 1$ . Then the sum  $\sum_{0 < i: \text{odd} < k} G_i$  is not a direct sum.*

*Proof.* Consider the matrix formed by the coefficients of

$$\left\{ 2X^i + \sum_{0 \leq j \leq s} 2X^{2i-k+a_j} \mid \frac{k}{2} \leq i < k \right\}$$

as in the proof of the lemma above.

Obviously the row containing 0 is a linear combination of the rows below. If the element corresponding to the row containing 0 is the element in  $G_i \cap T$  and the elements below the row containing 0 is the element in  $G_{a(j)} \cap T$ , then our assertion about matrix implies that  $\sum_j G_{a(j)} \cap G_i \neq (1)$ . Hence the sum  $\sum G_i$  is not a direct sum.  $\square$

We will make use of the following simple observation.

**Lemma 2.7.** *Let  $G$  be a finite abelian group. Let  $G_i$  be subgroups of  $G$  such that  $\sum G_i = G$  and  $\prod o(G_i) = o(G)$ . Then  $G = \oplus G_i$ .*

**3. Decomposing the group of units of  $\mathbb{Z}_4[X]/(X^k + 2u(X)X^a)$**

We apply the results of the previous section to choose the simpler generators for the direct sum decomposition of  $U_1(R)$  than we used in [2].

**Theorem 3.1.** *Let  $R = \mathbb{Z}_4[X]/(X^k)$ . Then the group  $U_1(R)$  of 1-units of  $R$  is isomorphic to the direct sum*

$$U_1(R) = \bigoplus_{1 \leq i: \text{odd} < k} G_i \oplus \bigoplus_{0 < i < \frac{k}{2}} H_i,$$

where  $G_i$  is the cyclic subgroup generated by  $1 + X^i$  of order  $2^{k_i+1}$  with  $k_i = \lfloor \frac{k}{i} \rfloor_2$  for each odd integer  $i$ , and  $H_i$  is cyclic of order 2 generated by  $1 + 2X^i$  ( $0 < i < \frac{k}{2}$ ).

*Proof.* By the exact sequence

$$(1) \rightarrow T \rightarrow U_1(\mathbb{Z}_4[X]/(X^k)) \xrightarrow{\phi} U(\mathbb{F}_2[X]/(X^k)) \rightarrow (1)$$

we need to prove that  $\phi(G + H_{(\frac{k}{2})})$  generate  $U(\mathbb{F}_2[X]/(X^k))$  and  $(G + H_{(\frac{k}{2})}) \cap T$  generate  $T$ . The first assertion is [2, Theorem 3.4] and hence we only need to show that  $(G + H_{(\frac{k}{2})}) \cap T$  generate  $T$ , i.e.,  $G \cap T$  together with  $H_{(\frac{k}{2})}$  generate  $T$ . First note that  $(1 + X^i)^{2^{k_i}} = 1 + 2X^{i2^{k_i-1}} \in G \cap T$ . Therefore  $H_j \subset G \cap T$  for  $\frac{k}{2} \leq j < k$  by Lemma 2.1. Hence it is clear that  $G \cap T$  together with  $H_{(\frac{k}{2})}$  generate  $T$ .

Finally we need to check that the sum of the logarithmic orders of the subgroups is the right number, i.e.,

$$\sum lo(G_i) + \sum lo(H_i) = 2(k - 1) = lo(U_1(\mathbb{Z}_4[X]/(X^k))).$$

We see easily that

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

and

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

By Lemma 2.2, we see that  $\sum_{0 < i: \text{odd} < k} \lfloor \frac{k}{i} \rfloor_2 = k - 1$ . In either case, the sum of the logarithmic order of the cyclic groups is  $2k - 2$ .  $\square$

**Example 3.2.** Consider the example  $\mathbb{Z}_4[X]/(X^{10})$ . 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

$$(1 + 2X), (1 + 2X^2), (1 + 2X^3), (1 + 2X^4)$$

in this order.

Now consider the group of units of the ring  $R = \mathbb{Z}_4[X]/(X^k + 2X^a)$  with  $0 \leq a < k$ . We can remove the assumption  $a > \frac{k}{2}$  in [2, Theorem 5.5] by using different generators. First consider the ring  $R = \mathbb{Z}_4[X]/(X^k + 2)$ . In this case, the group of 1-units is not well defined. Hence we decompose the group of units  $U(R)$  into a direct sum of cyclic subgroups.

**Theorem 3.3.** *Let  $R = \mathbb{Z}_4[X]/(X^k + 2)$ . Then*

$$U(R) = \bigoplus_{1 \leq i: \text{odd} < k} G_i \oplus \bigoplus_{0 \leq i < \frac{k}{2}} H_i,$$

where  $G_i$  is a cyclic group generated by  $1 + X^i$  of order  $2^{k_i+1}$  with  $k_i = \lfloor \frac{k}{i} \rfloor_2$  for each odd integer  $i$ ; and  $H_i$  is cyclic of order 2 generated by  $1 + 2X^i$  ( $0 < i < \frac{k}{2}$ ) and  $H_0 = \langle -1 \rangle$ .

*Proof.* As before by the exact sequence

$$(1) \rightarrow T_0 \rightarrow U(\mathbb{Z}_4[X]/(X^k + 2)) \xrightarrow{\phi} U(\mathbb{F}_2[X]/(X^k)) \rightarrow (1)$$

we need to prove that  $\phi(G + H_{(\frac{k}{2})}^+)$  generate  $U(\mathbb{F}_2[X]/(X^k))$  and  $G \cap T_0$  together with  $H_{(\frac{k}{2})}^+$  generate  $T_0$ . By [2, Theorem 3.4], we only need to prove the second

assertion. By [2, Lemma 5.1],  $lo(1 + X^i) = k_i + 1$  with  $k_i = \lfloor \frac{k}{i} \rfloor_2$ . Then since  $i2^{k_i} \geq k$  we have

$$\begin{aligned} (1 + X^i)^{2^{k_i}} &= 1 + 2X^{i2^{k_i-1}} + X^{i2^{k_i}} \\ &= 1 + 2X^{i2^{k_i-1}} + 2X^{i2^{k_i-k}} \in T_0. \end{aligned}$$

Hence  $G_i \cap T_0 = \langle (1 + X^i)^{2^{k_i}} \rangle$ . Therefore it suffice to show that  $T_0$  is generated by the elements

$$\begin{cases} 1 + 2X^{i2^{k_i-1}} + 2X^{i2^{k_i-k}}, \text{ where } 0 < i \text{ odd} < k, \\ (-1 + 2X^i), \text{ where } 0 \leq i < \frac{k}{2}. \end{cases}$$

We know  $\{i2^{k_i-1} \mid 0 < i : \text{odd} < k\} = \{i \mid \frac{k}{2} \leq i < k\}$  by Lemma 2.1. Therefore  $G \cap T_0$  contains  $\{1 + 2X^i + 2X^{2i-k} \mid \frac{k}{2} \leq i < k\}$ . Now we use Lemma 2.4 to conclude that  $T_0 \cap (G + H_{(\frac{k}{2})}^+)$  contains  $\{-1 + X^n \mid 0 \leq n < k\}$ .

Since we know  $G$  and  $H_{\frac{k}{2}}^+$  generate  $U(R)$  we need to show that sum of logarithmic order is  $lo(U(R)) = 2k - 1$ . Now we have

$$\sum lo(H_i) = \# \left\{ i \mid 0 \leq i < \frac{k}{2} \right\} = \begin{cases} \frac{k+1}{2} & \text{if } k \text{ is odd,} \\ \frac{k}{2} & \text{if } k \text{ is even.} \end{cases}$$

Therefore, by Lemma 2.2,

$$\sum lo(G_i) + \sum lo(H_i) = \sum_{1 \leq i: \text{odd} < k} \lfloor \frac{2k}{i} \rfloor_2 + \# \left\{ i \mid 0 \leq i < \frac{k}{2} \right\} = 2k - 1$$

as required. □

Now we consider the group of 1-units of  $R = \mathbb{Z}_4[X]/(X^k + 2X^a)$  with  $a > 0$  and decompose it into a direct sum of cyclic subgroups.

**Theorem 3.4.** *Let  $R = \mathbb{Z}_4[X]/(X^k + 2X^a)$  with  $a > 0$  and let  $k_i = \lfloor \frac{k}{i} \rfloor_2$ . Then the group of 1-units  $U_1(R)$  of  $R$  can be decomposed into the direct sum of the following cyclic subgroups:*

(i) *If  $\frac{k}{2} < a$ , then*

$$U_1(R) = \bigoplus_{0 < i: \text{odd} < k} G_i \oplus \bigoplus_{0 < i < \frac{k}{2}} H_i,$$

where  $G_i$  is cyclic of order  $2^{k_i+1}$  generated by  $1 + X^i$  for each odd integer  $< k$  and  $H_i$  is the cyclic subgroup of order 2 generated by  $1 + 2X^i$ .

(ii) *If  $\frac{k}{2} \geq a$ , then*

$$U_1(R) = \bigoplus_{0 < i: \text{odd} < k} G_i \oplus \bigoplus_{0 < i < \frac{k}{2}} H_i \oplus H_{k-a},$$



where  $H$ 's are cyclic group of order 2 and for each odd  $i$  the cyclic subgroup  $G_i$  is generated by  $1 + X^i$  with

$$lo(G_i) = \begin{cases} k_i + 1 & \text{if } i \neq j, \\ k_j & \text{if } i = j. \end{cases}$$

*Proof.* We first prove (ii). As before by the exact sequence

$$(1) \rightarrow T \rightarrow U_1(\mathbb{Z}_4[X]/(X^k + 2X^a)) \xrightarrow{\phi} U(\mathbb{F}_2[X]/(X^k)) \rightarrow (1)$$

we need to prove that  $G \cap T$  together with  $H_{(\frac{k}{2})} + H_{k-a}$  generate  $T$  since we already know that  $\phi(G)$  generate  $U(\mathbb{F}_2[X]/(X^k))$ . Since  $\frac{k}{2} \geq a$  we have  $k - a \geq \frac{k}{2}$ . By Lemma 2.1, there is a  $j$  such that  $k - a = j2^{k_j-1}$ . If  $i \neq j$ , then

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

But for  $j$  we have  $(1 + X^j)^{2^{k_j}} = 1$  and hence  $lo(1 + X^j) = k_j$ ; but note that  $(1 + X^j)^{2^{k_j-1}} = 1 + 2X^{j2^{k_j-2}} + X^{j2^{k_j-1}} \notin T$  and thus  $G_j \cap T = (1)$ . Hence  $T \cap (G + H_{k-a})$  is generated by

$$\begin{cases} 1 + 2X^{i2^{k_i-1}} + 2X^{i2^{k_i}-k+a} & (i \neq j), \\ 1 + 2X^{k-a}, & \text{where } k - a = j2^{k_j-1}. \end{cases}$$

And by Lemma 2.1,  $\{i2^{k_i-1} | i \neq j\} \cup \{k - a\} = \{i | \frac{k}{2} \leq i < k\}$ . By Lemma 2.4, we conclude that  $H_{(\frac{k}{2})} \oplus H_{k-a}$  together with  $T \cap G$  generate  $T$ .

(i) Suppose now  $\frac{k}{2} < a$ , i.e.,  $k - a < \frac{k}{2}$ . Then by Lemma 2.1, there is no  $j$  such that  $k - a = j2^{k_j-1}$ . Therefore  $(1 + X^i)^{2^{k_i}} = 1 + 2X^{i2^{k_i-1}} + 2X^{i2^{k_i}-k+a} \in T$  for each odd  $i$  with  $0 < i < k$ . By Lemma 2.4, we see that  $\{(1 + X^i)^{2^{k_i}} | 0 < i : \text{odd} < k\}$  and  $H_{(\frac{k}{2})}$  generate  $T$ .

To finish our proof we need to check that the sum of the logarithmic order of the subgroups  $\sum_{0 < i: \text{odd} < k} lo(G_i) + \sum_{0 < i < \frac{k}{2}} lo(H_i)$  is equal to  $2(k - 1)$  in (i). However, the same proof of Theorem 3.3 also works for this case also. In the case of (ii), we need to show  $\sum_{0 < i: \text{odd} < k} lo(G_i) + \sum_{0 < i < \frac{k}{2}} lo(H_i) + lo(H_{k-a}) = 2(k - 1)$ . But since  $lo(G_j) = k_j$  the sum  $\sum_{0 < i: \text{odd} < k} lo(G_i)$  drops by 1 which is compensated by adding  $lo(H_{k-a}) = 1$ .  $\square$

**Example 3.5.** Let  $R = \mathbb{Z}_4[X]/(X^8 + 2X^4)$ . Then  $lo(U_1(R)) = 14$ . For  $i = 1$  we have  $k_i = 3$  and  $i2^{k_i-1} = 4 = k - a$ . Now we have

$$\begin{aligned} lo(1 + X) &= 3, \quad lo(1 + X^3) = 3, \quad lo(1 + X^5) = 2, \quad lo(1 + X^7) = 2, \\ lo((1 + 2X)) &= lo((1 + 2X^2)) = lo((1 + 2X^3)) = lo((1 + 2X^4)) = 1. \end{aligned}$$

Hence

$$\begin{aligned} U_1(R) &\cong G_1 \oplus G_3 \oplus G_5 \oplus G_7 \oplus H_1 \oplus H_2 \oplus H_3 \oplus H_4 \\ &\cong \mathbb{Z}/2^3 \oplus \mathbb{Z}/2^3 \oplus \mathbb{Z}/2^2 \oplus \mathbb{Z}/2^2 \oplus \mathbb{Z}/2 \oplus \mathbb{Z}/2 \oplus \mathbb{Z}/2 \oplus \mathbb{Z}/2. \end{aligned}$$

For the rest of this section, we consider the ring of the type  $R = \mathbb{Z}_4[X]/(X^k + 2u(X)X^a)$ , where  $u(X)$  is a polynomial of the type

$$u(X) = \sum_{i=0}^s X^{b_i}, \text{ where } b_0 = 0, u(X) \neq 1 \text{ and } \deg(u) < k - a$$

and write  $X^a u(X) = X^{a_0} + X^{a_1} + \dots + X^{a_s}$ . If  $u = 1$ , then  $R$  reduces to the rings we already considered. And if  $u \neq 1$  we need some restrictions on  $a$  to decompose the group of units into a direct sum of cyclic subgroups.

**Lemma 3.6.** *Let  $R = \mathbb{Z}_4[X]/(X^k + 2u(X)X^a)$  with  $a \geq 0$ . For an odd integer  $i$  less than  $k$  let  $k_i = \lfloor \frac{k}{i} \rfloor_2$ . Then*

- (i) *If  $a > \frac{k}{2}$ , then  $lo(1 + X^i) = k_i + 1$ .*
- (ii) *If  $a = 1$  and  $j$  is an odd integer such that  $k - 1 = j2^{k_j - 1}$ , then*

$$lo(1 + X^i) = \begin{cases} k_i + 1 & \text{if } i \neq j, \\ k_j & \text{if } i = j. \end{cases}$$

*Proof.* (i) Note  $X^{2k-a} = 2uX^k = 0$  and these are the smallest such power. Then  $i2^{k_i+1} \geq 2k \geq 2k - a$  and  $i2^{k_i} \geq k$ . Hence  $(1 + X^i)^{2^{k_i+1}} = 1 + 2X^{2^{k_i}} + X^{2^{k_i+1}} = 1$ . Now check the possibility that  $(1 + X^i)^{2^{k_i}} = 1$ . This happens only when

$$2X^{i2^{k_i-1}} + X^{i2^{k_i}} = 2X^{i2^{k_i-1}} + 2(X^{i2^{k_i-k+a_0}} + X^{i2^{k_i-k+a_1}} + \dots) = 0,$$

where  $X^a u(X) = X^{a_0} + X^{a_1} + \dots + X^{a_s}$ . But  $\{i2^{k_i-1} \mid 0 < i : \text{odd} < k\} = \{n \mid \frac{k}{2} \leq n < k\}$  by Lemma 2.1, and since  $a > \frac{k}{2}$  we see that  $i2^{k_i} - k + a_0 > i2^{k_i-1}$ . Therefore  $2X^{i2^{k_i-1}} + X^{i2^{k_i}}$  cannot vanish.

(ii) Existence of an odd integer  $j$  with  $k - 1 = j2^{k_j - 1}$  is guaranteed by Lemma 2.1. Now we have

$$\begin{aligned} (1 + X^j)^{2^{k_j}} &= 1 + 2X^{j2^{k_j-1}} + X^{j2^{k_j}} \\ &= 1 + 2X^{j2^{k_j-1}} + 2(X^{j2^{k_j-k+a}} + \dots). \end{aligned}$$

Then  $2X^{j2^{k_j-1}} + 2X^{j2^{k_j-k+a}} = 0$  and the rest vanishes because the exponents of  $X$  become  $\geq k$ . Therefore we see that  $lo(1 + X^j) = k_j$ . □

**Theorem 3.7.** *Let  $R = \mathbb{Z}_4[X]/(X^k + 2u(X)X^a)$  with a polynomial  $u$  of the type described above and let  $k_i = 2^{\lfloor \frac{k}{i} \rfloor_2}$ .*

- (i) *If  $a > \frac{k}{2}$ , then*

$$U_1(R) = \bigoplus_{0 < i : \text{odd} < k} G_i \oplus \bigoplus_{0 < i < \frac{k}{2}} H_i,$$

where  $G_i$  is cyclic of  $lo(G_i) = k_i + 1$  with the generator  $1 + X^i$  and  $H_i$  is cyclic of  $lo(H_i) = 1$  with the generator  $1 + 2X^i$ .

(ii) If  $a = 1$  and if  $j$  is an odd integer with  $k - 1 = j2^{k_j-1}$ , then

$$U_1(R) = \bigoplus_{0 < i: \text{odd} < k} G_i \oplus \bigoplus_{0 < i < \frac{k}{2}} H_i \oplus H_{k-1}$$

with  $lo(G_j) = k_j$  and  $lo(G_i) = k_i + 1$  ( $i \neq j$ ) and  $H_i$ 's are the same as before.

(iii) If  $a = 0$ , then the group of units of  $R$  is

$$U(R) = \bigoplus_{0 < i: \text{odd} < k} G_i \oplus \bigoplus_{0 \leq i < \frac{k}{2}} H_i,$$

where  $G_i$  is cyclic group of order  $2^{k_i+1}$  generated by  $1 + X^i$  for each odd integer  $< k$  and  $H_i$  is the cyclic subgroup of order 2 generated by  $1 + 2X^i$ .

*Proof.* (i) Since there is no  $i$  such that  $k - a = i2^{k_i-1}$  we see that  $lo(G_i) = k_i + 1$ . The same proof of Theorem 3.4(i) will works for this case.

(ii) follows from Lemma 2.5 together with the fact that the direct sum of the subgroups generate  $U_1(R)$  with the right order.

(iii) is similarly proved. □

*Remark.* For  $1 < a \leq \frac{k}{2}$  the sum  $\sum_i G_i$  is not direct as we saw in Proposition 2.6. Further investigation is needed for this case<sup>†</sup>.

#### 4. Decomposing the group of units of $\mathbb{Z}_4[X]/(X^k + 2X^a, 2X^r)$

Let  $R = \mathbb{Z}_4[X]/(X^k + 2X^a, 2X^r)$ , where  $0 \leq a < r < k$ . In [2, Lemma 6.1, Lemma 6.2] we show that the number of elements of  $U(R)$  is  $2^{k+r-1}$  and the group of 1-units  $U_1(R)$  has order  $2^{k+r-2}$  when  $a > 0$ . And we showed that for each odd integer  $i$  with  $0 < i < k$

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

$$k_i \leq \lfloor \frac{2r}{i} \rfloor_2 \leq k_i + 1$$

since  $k \leq r + a \leq 2r \leq 2k$ .

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

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

where  $k_i = \lfloor \frac{k}{i} \rfloor_2$ . There are at most one positive odd integer  $i$  less than  $k$  satisfying the condition  $k - a = i2^{k_i-1}$  with  $k_i > 1$ . Note that if we let  $\alpha_i = \lfloor \frac{k+r-a}{i} \rfloor_2$ , then since  $k < k + r - a < 2k$  we have

$$k_i \leq \alpha_i \leq k_i + 1.$$

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

---

<sup>†</sup>See the paper [3].

**Theorem 4.1.** *Let  $R = \mathbb{Z}_4[X]/(X^k + 2X^a, 2X^r)$  with  $0 < a < r < k$ . If  $k \geq r + a$ , then the group of 1-units  $U_1(R)$  decomposes into the direct sum:*

$$U_1(R) = \bigoplus_{1 \leq i: \text{odd} < k} G_i \oplus \bigoplus_{i \in S} H_i,$$

where  $S = \{i \mid 0 < i < a\} \cup \{a + i \mid i : \text{odd}, a < a + i < r\}$ . Here,  $G_i$  is cyclic generated by  $1 + X^i$  of order  $2^{\alpha_i}$ , where  $\alpha_i = \lfloor \frac{\alpha}{i} \rfloor_2$  with  $\alpha = k + r - a$ ; and  $H_i$  is cyclic generated by  $1 + 2X^i$  of order 2.

*Proof.* First we look at  $G \cap T$ . Since the elements of  $T$  are order 2, the only possible elements in  $G_i$  which are in  $T$  are of the form  $(1 + X^i)^{\alpha_i - 1} = 1 + 2X^{i2^{\alpha_i - 2}} + X^{i2^{\alpha_i - 1}}$ . This will belong to  $T$  only if  $i2^{\alpha_i - 1} \geq k$ . Now  $\{i2^{\alpha_i - 1} \mid 1 \leq i : \text{odd} < \alpha\} = \{j \mid \frac{\alpha}{2} \leq j < \alpha\}$ , by Lemma 2.1, which we will call  $\mathfrak{S}$ . If  $j$  is odd such that  $j \geq k$ , then  $\alpha_j = 1$  and  $(1 + X^j)^{\alpha_j - 1} = (1 + X^j) \notin T$ . Hence the even numbers  $\geq k$  in  $\mathfrak{S}$  is of the form  $S' = \{i2^{\alpha_i - 1} \mid i : \text{odd}, \alpha_i > 1, i2^{\alpha_i - 1} \geq k\} = \{j : \text{even} \mid k \leq j < \alpha\}$ . And therefore,  $G \cap T = \langle 1 + 2X^{\frac{j}{2}} + 2X^{j - k + a} \mid j \in S' \rangle$ .

On the other hand,  $k \geq r + a$  implies that  $a < \frac{k}{2}$ . Therefore  $k - a > \frac{k}{2} \geq \frac{j}{2}$ . Hence  $\frac{j}{2} > j - k + a$  and consequently  $(1 + X^i)^{2^{\alpha_i - 1}} = 1 + 2X^{j - k + a} + (\text{hdt}) \neq 1$  ( $j = k, k + 2, \dots$ ). Hence  $G \cap T$  is generated by  $\{1 + 2X^{a + 2i} \mid i = 0, 1, \dots\}$ .

Thus if we let  $S = \{i \mid 0 < i < a\} \cup \{a + i \mid i : \text{odd}, a < a + i < r\}$ , then  $T$  is generated by  $G \cap T$  together with  $\sum_{i \in S} H_i$  by Lemma 2.4. As we already know that  $\phi(G)$  generate  $U(\mathbb{F}_2[X]/(X^k))$  we conclude that  $G$  together with  $\bigoplus_{i \in S} H_i$  generate  $U_1(R)$ .

Now we need to show that  $\sum_{0 < i: \text{odd} < k} lo(G_i) + \sum_{i \in S} lo(H_i) = k + r - 2$ . First note  $\#S = \#\{i \mid 1 \leq i < r\} \setminus S' = (r - 1) - \#S'$ . Hence

$$\begin{aligned} & \sum lo(G_i) + \sum lo(H_i) \\ &= (\alpha - 1) - \#\{i : \text{odd} \mid k \leq i < \alpha\} + \#S \\ &= (\alpha - 1) - \#\{i : \text{odd} \mid k \leq i < \alpha\} \cup S' + \#\{i \mid 1 \leq i < r\} \\ &= \#\{i \mid 1 \leq i < k\} + \#\{i \mid 1 \leq i < r\} = (k - 1) + (r - 1) \\ &= k + r - 2 \end{aligned}$$

as required. □

*Remark.* In the proof of Theorem 4.1, suppose there is an odd integer  $i$  satisfying the condition  $k - a = i2^{k_i - 1}$ . As observed above, the only possible elements in  $G$  which are in  $T$  are of the form  $(1 + X^i)^{\alpha_i - 1} = 1 + 2X^{i2^{\alpha_i - 2}} + X^{i2^{\alpha_i - 1}}$  and it belong to  $T$  only if  $i2^{\alpha_i - 1} \geq k$ . But since  $k - a = i2^{k_i - 1} < k$  the corresponding element  $(1 + X^i)^{k_i}$  does not belong to  $T$  and existence of such  $i$  does not affect the decomposition of the group of units.

**Theorem 4.2.** *Let  $R = \mathbb{Z}_4[X]/(X^k + 2X^a, 2X^r)$  with  $0 < a < r < k$ . Let  $r_i = \lfloor \frac{r}{i} \rfloor_2$ . Suppose  $k < r + a$ . Then the group of 1-units  $U_1(R)$  decomposes into the direct sum:*

(i) If  $a > \frac{k}{2}$ , then

$$U_1(R) = \bigoplus_{0 < i: \text{odd} < k} G_i \oplus \bigoplus_{0 < i < \frac{k}{2}} H_i,$$

where  $G_i$  is cyclic generated by  $1 + X^i$  with  $lo(G_i) = r_i + 1$  and  $H_i$  is cyclic generated by  $1 + 2X^i$  with  $lo(H_i) = 1$ .

(ii) If  $a \leq \frac{k}{2}$ , then there is an odd integer  $j$  ( $0 < j < k$ ) such that  $k - a = j2^{r_j - 1}$  and

$$U_1(R) = \bigoplus_{0 < i: \text{odd} < k} G_i \oplus \bigoplus_{i \in S} H_i,$$

where  $S = \{i \mid 0 < i < a\} \cup \{k - a\} \cup \{a + l\}$ , where  $l$  is odd such that  $a < a + l < r$  if  $k$  is even; and  $l$  is even such that  $a + 1 < a + l < r$  if  $k$  is odd. Here,  $G_i$  is cyclic generated by  $1 + X^i$  with  $lo(G_i) = r_i + 1$  for  $i \neq j$  and  $lo(G_j) = r_j$ ; and  $H_i$  is cyclic generated by  $1 + 2X^i$  with  $lo(H_i) = 1$ .

*Proof.* (i) As before consider the exact sequence

$$(1) \rightarrow T \rightarrow U_1(\mathbb{Z}_4[X]/(X^k + 2X^a, 2X^r)) \xrightarrow{\phi} U(\mathbb{F}_2[X]/(X^k)) \rightarrow (1),$$

where  $T$  is generated by  $1 + 2X^i$ , where  $0 < i < r$ . As usual we need to show that  $G \cap T$  together with  $\bigoplus_{0 < i < \frac{k}{2}} H_i$  (resp.  $\bigoplus_{0 < i < \frac{k}{2}} H_i \oplus H_{k-a}$ ) generate  $T$  when  $a > \frac{k}{2}$  (resp.  $a \leq \frac{k}{2}$ ).

By Lemma 2.1, we see that

$$\{i2^{r_i} \mid 0 < i: \text{odd} < 2r\} = \{n \mid r \leq n < 2r\}$$

which we call  $\mathfrak{R}$ . If  $i \in \mathfrak{R}$  is odd such that  $i \geq k$ , then  $r_i = 0$  and hence  $(1 + X^i)^{2^{r_i}} \notin T$ . And therefore if  $n \in \mathfrak{R}$  is even such that  $n \geq k$ , then it is of the form  $n = i2^{r_i}$  with  $r_i \geq 1$  and  $i$  is odd such that  $0 < i < 2r$  (we only need  $i$  for which  $0 < i < k$ ). For an odd  $i$  with  $k \leq i2^{r_i}$  and  $0 < i < k$  we have

$$\begin{aligned} (1 + X^i)^{2^{r_i}} &= 1 + 2X^{i2^{r_i-1}} + X^{i2^{r_i}} \\ &= 1 + 2X^{i2^{r_i-1}} + 2X^{i2^{r_i} - k + a} \in T. \end{aligned}$$

Since  $\frac{k}{2} < a$  we see that  $k - a < \frac{k}{2}$  and as  $k \leq j$  we conclude that  $k - a < \frac{j}{2}$ . This in turn implies that  $j - k + a > \frac{j}{2}$ . Thus  $(1 + X^i)^{2^{r_i}} = 1 + 2X^{\frac{j}{2}} + 2X^{S_n}$ , where  $S_n = \{i2^{r_i} - k + a\}$  if  $i2^{r_i} - k + a < r$  and  $S_n = \emptyset$  if  $i2^{r_i} - k + a \geq r$ . Thus we conclude that

$$\begin{cases} 1 + 2X^i & (0 < i < \frac{k}{2}) \\ 1 + 2X^n + 2X^{S_n} & (\frac{k}{2} \leq n < r) \end{cases}$$

generate  $T$  by Lemma 2.4.

On the other hand, if  $k - a = j2^{r_j - 1}$  for some  $j$ , in the situation above, then  $(1 + X^j)^{2^{r_j}} = 1$  and  $lo(G_j) = r_j$  and  $G_j \cap T = 1$ . (Every element of  $T$  is of order 2 and the only element of  $G_i$  is  $(1 + X^j)^{2^{r_j - 1}}$  but this does not belong to

$T$ .) Hence  $G \cap T$  contains  $\{1 + 2X^n + 2X^{S_n} \mid \frac{k}{2} \leq n < r, n \neq k - a\}$ . Therefore  $G \cap T$  together with  $H_{(\frac{k}{2})} + H_{k-a}$  generate  $T$  by Lemma 2.4.

To finish our proof we need to show that the sum of the logarithmic order of our subgroups is the right number. In fact, we know that

$$\sum_{1 \leq i: \text{odd} < 2r} \lfloor \frac{2r}{i} \rfloor_2 = 2r - 1.$$

If  $i$  is odd  $\geq k$ , then  $\lfloor \frac{2r}{i} \rfloor_2 = 1$ . Since the number of elements of  $\{i \mid k \leq i < 2r\}$  are

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

Hence

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

On the other hand,

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

Therefore  $lo(G_{\text{odd}}) + lo(H_i) = k + r - 2$  which is exactly the order of  $U_1(R)$ . (We could have used the similar argument we used in the proof of Theorem 4.1.)

(ii) Now suppose  $a \leq \frac{k}{2}$ . Then  $k \leq 2(k - a) < 2r$  since  $k < r + a$ . Hence there is an odd integer  $j$  for which  $k - a = j2^{r_j-1}$ . And if  $n \in \mathfrak{R}$  is even such that  $\frac{n}{2} < k - a$ , then  $n - k + a < \frac{n}{2}$  and; if  $\frac{n}{2} > k + a$ , then  $\frac{n}{2} < n - k + a$ .

Now we have  $(1 + X^j)^{2^{r_j}} = 1 + 2X^{j2^{r_j-1}} + X^{j2^{r_j}} = 1$ . Therefore  $G \cap T$  is generated by

$$\begin{cases} 1 + 2X^{n-k+a} + (\text{hdt}), & \text{where } n \in \mathfrak{R} \text{ is even such that } k \leq n < 2(k - a), \\ 1 + 2X^{\frac{n}{2}} + (\text{hdt}), & \text{where } n \in \mathfrak{R} \text{ is even such that } n > 2(k - a). \end{cases}$$

Hence, by Lemma 2.4,  $T$  is generated by  $G \cap T$  together with

$$\begin{cases} 1 + 2X^i & (0 < i < a) \\ 1 + 2X^{k-a} \\ 1 + 2X^{a+l}, \end{cases}$$

where  $l$  is odd such that  $a < a + l < r$  if  $k$  is even; and  $l$  is even such that  $a + 1 < a + l < r$  if  $k$  is odd.

To count the order we notice that the number of  $i$  such that  $G_i \cap T \neq (1)$  is one less than that in (i) since  $G_{k-a} \cap T = (1)$ . And we can resort to the proof of (i). □

*Remark.* We have freedom to choose the generators of the form  $1 + 2X^i$ 's. Say we could have chosen  $\{1 + 2X^{\frac{i}{2}} \mid j \in S'\}$  instead of  $S' - k + a$  when we form the set  $S = \{i \mid 0 < i < r\} \setminus S' - k + a$ . But our choice seems to be rather natural.

**Theorem 4.3.** *Let  $R = \mathbb{Z}_4[X]/(X^k + 2, 2X^r)$ . Then the group of units  $U(R)$  of  $R$  is isomorphic to*

$$U(R) = \bigoplus_{1 \leq i: \text{odd} < k} G_i \oplus \bigoplus_{i \in S} H_i,$$

where

$$S = \begin{cases} \{i : \text{even} \mid 0 \leq i < r\} & \text{if } k \text{ is odd,} \\ \{i : \text{odd} \mid 0 < i < r\} \cup \{0\} & \text{if } k \text{ is even.} \end{cases}$$

*Proof.* As before we need to show that  $\{1 + 2X^i \mid i \in S\}$  together with  $G \cap T_0$  with  $\bigoplus_{i \in S} H_i$  generate  $T_0$  and the sum of logarithmic order of our subgroups has the right number.

First we look at  $G \cap T_0$ . Let  $\alpha = k + r$  and  $\alpha_i = \lfloor \frac{\alpha}{i} \rfloor_2$ . Since the elements of  $T_0$  are of order 2, the only possible elements in  $G$  which are in  $T_0$  are of the form

$$(1 + X^i)^{\alpha_i - 1} = 1 + 2X^{i2^{\alpha_i - 2}} + X^{i2^{\alpha_i - 1}}$$

which belong to  $T_0$  only if  $i2^{\alpha_i - 1} \geq k$ . Now by Lemma 2.1, we know that  $\{i2^{\alpha_i - 1} \mid 1 \leq i : \text{odd} < \alpha\} = \{j \mid \frac{\alpha}{2} \leq j < \alpha\}$  which we will call  $\mathfrak{S}$ . If  $i$  is odd such that  $i \geq k$ , then  $\alpha_i = 1$ ;  $i2^{\alpha_i - 1} = i$  and  $(1 + X^i)^{\alpha_i - 1} = 1 + X^i \notin T_0$ . Therefore the even numbers  $\geq k$  in  $\mathfrak{S}$  is of the form  $S' = \{i2^{\alpha_i - 1} \mid i : \text{odd}, \alpha_i > 1, i2^{\alpha_i - 1} \geq k\} = \{j : \text{even} \mid k \leq j < \alpha\}$ . And hence  $G \cap T_0 = \{1 + 2X^{\frac{j}{2}} + 2X^{j-k} \mid j \in S'\}$ . Let  $S = \{i \mid 0 \leq i < r\} \setminus S' - k$ . Then  $S = \{i : \text{even} \mid 0 \leq i < r\}$  if  $k$  is odd; and  $S = \{i : \text{odd} \mid 0 < i < r\} \cup \{0\}$  if  $k$  is even. Thus  $T_0$  is generated by  $G \cap T_0$  and  $\sum_{i \in S} H_i$  by Lemma 2.4. As we already know that  $\phi(G)$  generate  $U(\mathbb{F}_2[X]/(X^k))$  we conclude that  $G$  together with  $\bigoplus_{i \in S} H_i$  generate  $U_1(R)$ .

Now we need to show that

$$\sum_{0 < i: \text{odd} < k} lo(G_i) + \sum_{i \in S} lo(H_i) = k + r - 1.$$

First note  $\#S = \#\{i \mid 0 \leq i < r\} \setminus S' = r - \#S'$ . Hence

$$\begin{aligned} & \sum lo(G_i) + \sum lo(H_i) \\ &= (\alpha - 1) - \#\{i : \text{odd} \mid k \leq i < \alpha\} + \#S \\ &= (\alpha - 1) - \#\{i : \text{odd} \mid k \leq i < \alpha\} \cup S' + \#\{i \mid 0 \leq i < r\} \\ &= \#\{i \mid 1 \leq i < k\} + \#\{i \mid 0 \leq i < r\} = (k - 1) + r \\ &= k + r - 1 \end{aligned}$$

as required. □

**Example 4.4.** Let  $R = \mathbb{Z}_4[X]/(X^{20} + 2X^2, 2X^{12})$ . Here we have  $k + r - a = 30$ ,  $k \geq r + a$  and  $lo(U_1(R)) = k + r - 2 = 30$ . Let  $\alpha = k + r - a$  and  $\alpha_i = \lfloor \frac{k+r-a}{i} \rfloor_2$ .

We look at the possible elements of  $T$  of the form  $(1 + X^i)^{2^{\alpha_i-1}}$ .

$1 \leq i : \text{odd} < \alpha$	$\alpha_i$	$i2^{\alpha_i-1}$	$(1 + X^i)^{2^{\alpha_i-1}}$	
1	5	$2^4 = 16$	$1 + 2X^8 + X^{16}$	not in $T$
3	4	$3 \cdot 2^3 = 24$	$1 + 2X^6$	
5	3	$5 \cdot 2^2 = 20$	$1 + 2X^{10} + 2X^2$	not in $T$
7	3	$7 \cdot 2^2 = 28$	$1 + 2X^{10}$	
9	2	$9 \cdot 2 = 18$	$1 + 2X^9 + X^{18}$	not in $T$
11	2	$11 \cdot 2 = 22$	$1 + 2X^{11} + 2X^4$	
13	2	$13 \cdot 2 = 26$	$1 + 2X^8$	not in $T$
15	1	15	$1 + X^{15}$	
17	1	17	$1 + X^{17}$	not in $T$
19	1	19	$1 + X^{19}$	not in $T$
21		21		$i \geq k$
23		23		
25		25		
27		27		
29		29		

In the blank space there were terms of the form  $2X^l$  with  $l > r$ .

Now

$$\sum_{1 \leq i: \text{odd} < 20} lo(G_i) = \sum_{1 \leq i: \text{odd} < k} \alpha_i = 5 + 4 + \dots + 1 = 24$$

and

$$G \cap T = \bigoplus \{H_{2j-k+a} \mid k \leq 2j < k+r-a\} \\ = \{1 + 2X^{10} + 2X^2, 1 + 2X^{11} + 2X^4, 1 + 2X^6, 1 + 2X^8, 1 + 2X^{10}\}$$

which correspond to even numbers  $i2^{\alpha_i-1}$  which is bigger than  $k$ . Therefore to generate  $T$  we need to adjoin the generators

$$\{1 + 2X^i \mid 1 \leq i < r, i \neq 2, 4, 6, 8, 10\}$$

which consists of  $(r-1) - \frac{r-a}{2} = \frac{r+a}{2} - 1 = 6$  elements. Letting  $S' = \{2j - k + a \mid k \leq 2j < k+r-a\}$  we have

$$U_1(R) = \bigoplus_{1 \leq i: \text{odd} < k} G_i \oplus \bigoplus \{H_i \mid i \notin S', 1 \leq i < r\} \\ = \bigoplus_{1 \leq i: \text{odd} < 30} G_i \oplus \bigoplus_{1 \leq i: \text{odd} < 12} H_i.$$

**Example 4.5.** Let  $R = \mathbb{Z}_4[X]/(X^{20} + 2X^6, 2X^{15})$ . Here we have  $r + a = 21$ ,  $k \leq r + a$  and  $lo(U_1(R)) = k + r - 2 = 33$ . Let  $r_i = \lfloor \frac{r}{i} \rfloor_2$  so that  $r_i + 1 = \lfloor \frac{2r}{i} \rfloor_2$ . Note that  $r_7 = \lfloor \frac{15}{7} \rfloor_2 = 2$  and  $k - a = 14 = 7 \cdot 2^{r_7-1}$ . Hence  $lo(G_7) = r_7 = 2$



and for an odd  $i$  other than 7 we have  $lo(G_i) = r_i + 1$ . Now

$$\sum_{1 \leq i: \text{odd} < k} lo(G_i) = r_7 + \sum_{i: \text{odd} \neq 7} (r_i + 1) = 23.$$

We look at the possible elements of  $T$  of the form  $(1 + X^i)^{2^{r_i}}$ .

$1 \leq i : \text{odd} < 2r$	$r_i$	$i2^{r_i}$	$(1 + X^i)^{2^{r_i}}$	
1	4	$2^4 = 16$	$1 + 2X^8 + X^{16}$	not in $T$
3	3	$3 \cdot 2^3 = 24$	$1 + 2X^{12} + 2X^{10}$	
5	2	$5 \cdot 2^2 = 20$	$1 + 2X^{10} + 2X^6$	
7	2	$7 \cdot 2^2 = 28$	$1 + 2X^{14} + 2X^{14} = 1$	$lo(G_7) = 2$
9	1	$9 \cdot 2 = 18$	$1 + 2X^9 + X^{18}$	not in $T$
11	1	$11 \cdot 2 = 22$	$1 + 2X^{11} + 2X^8$	
13	1	$13 \cdot 2 = 26$	$1 + 2X^{13} + 2X^{12}$	
15	0	15	$1 + X^{15}$	not in $T$
17	0	17	$1 + X^{17}$	not in $T$
19	0	19	$1 + X^{19}$	not in $T$
21		21		
23		23		
25		25		$i \geq k$
27		27		
29		29		

Therefore  $G \cap T$  is generated by

$$\{1 + 2X^{12} + 2X^{10}, 1 + 2X^{10} + 2X^6, 1 + 2X^{11} + 2X^8, 1 + 2X^{13} + 2X^{12}\}.$$

Hence if we let  $H' = H_{14} \oplus \bigoplus_{0 < i < 10} H_i$ , then  $(G \cap T) + H' = T$ . Therefore  $U_1(R) = G \oplus H'$ .

**Acknowledgment.** In the sequel of this paper [3] we will remove the restrictions imposed in the paper by modifying the set of generators.

**References**

[1] Bernard R. McDonald, *Finite Rings with Identity*, Pure and Applied Mathematics, Vol. 28. Marcel Dekker, Inc., New York, 1974.  
 [2] S. S. Woo, *The group of units of some finite local rings I*, J. Korean Math. Soc. **46** (2009), no. 2, 295–311.  
 [3] ———, *The group of units of some finite local rings III*, J. Korean Math. Soc. **46** (2009), no. 4, 675–689.

DEPARTMENT OF MATHEMATICS  
 EWHA WOMEN'S UNIVERSITY  
 SEOUL 120-750, KOREA  
*E-mail address:* sswoo@ewha.ac.kr