Commun. Korean Math. Soc. **21** (2006), No. 4, pp. 641–652

SOME REMARKS ON THE PRIMARY IDEALS OF $\mathbb{Z}_{p^m}[X]$

SUNG SIK WOO

ABSTRACT. In [2], they found some natural generators for the ideals of the finite ring $\mathbb{Z}_{p^m}[X]/(X^n-1)$, where p and n are relatively prime. If p and n are not relatively prime X^n-1 is not a product of basic irreducible polynomials but a product of primary polynomials. Due to this fact, to consider the ideals of $\mathbb{Z}_{p^m}[X]/(X^n-1)$ in 'inseparable' case we need to look at the primary ideals of $\mathbb{Z}_{p^m}[X]$. In this paper, we find a set of generators of ideals of $\mathbb{Z}_{p^m}[X]/(f)$ for some primary polynomials f of $\mathbb{Z}_{p^m}[X]$.

1. Introduction

If n is not relatively prime to p then the polynomial $X^n-1 \in \mathbb{Z}_{p^m}[X]$ is only a product of primary polynomials instead of a product of basic irreducible polynomials. In the latter case, it was shown that every ideal of $\mathbb{Z}_{p^m}[X]/(X^n-1)$ is principal which is due to the facts that X^n-1 is a product of basic irreducible polynomials and every ideal of $\mathbb{Z}_{p^m}[X]/(f)$ is principal for every basic irreducible polynomials [2]. On the other hand, if p and n has a common factor then it was shown [4] that X^n-1 can be written as a product of 'primary' polynomials in some unique way.

In this paper we propose to describe the ideals of $\mathbb{Z}_{p^m}[X]/(f)$, where f is a primary polynomial. The way to do this will be to define extremal elements by introducing an order structure on the set $\mathbb{Z}_{p^m}[X]/(f)$ which is basically the same method what they used in [2]. But in our case the situation is more complicate when f is primary instead of just being basic irreducible. The results we obtained are far from being satisfactory. We merely indicate a way to describe the primary ideals of $\mathbb{Z}_{p^m}[X]/(f)$

Received August 18, 2005.
2000 Mathematics Subject Classification: 13C12.
Key words and phrases: primary ideal, polynomial over a finite ring.

by choosing certain types of primary polynomials f instead of giving a general statement.

2. Primary polynomials

Unless otherwise stated, throughout this section R will denote a finite commutative local ring with identity and maximal ideal $\mathfrak{m}$. We assume $\mathfrak{m}$ is principal say, $\mathfrak{m} = (p)$ with $R/\mathfrak{m} = k$.

Let $\mu : R \to k$ be the natural map. A polynomial $\Pi \in R[X]$ is called *basic irreducible* if $\mu(\Pi)$ is irreducible in $k[X]$. For a basic irreducible polynomial Π in $R[X]$ we write $\pi = \mu(\Pi)$ which is an irreducible polynomial in $k[X]$.

A polynomial $f(X) \in R[X]$ is called *regular* if it is not a zero divisor. It is well known [4, Theorem XIII.2] that $f(X) = \sum_{i=0}^{n} a_i X^i$ is regular if and only if at least one of the coefficients $a_0, \ldots, a_n$ is a unit of R, that is one of the coefficients is not divisible by p. Equivalently, $\mu(f) \neq 0$. Since μ is a ring homomorphism, we see that *a product of regular polynomials is again regular.*

A nonunit ideal $\mathfrak{q}$ of a ring A is, by definition, *primary* if whenever $xy \in \mathfrak{q}$ we have either $x \in \mathfrak{q}$ or $y^n \in \mathfrak{q}$ for some $n > 0$. A polynomial $f \in R[X]$ is called *primary* if and only if the ideal (f) generated by f is primary.

It is shown in [4] that a regular polynomial can be written as a product of primary polynomials 'uniquely'– less uniquely than the polynomials over a field.

THEOREM 1 ([4] XIII.11). *Let R be a finite ring and f be a regular polynomial in $R[X]$. Then*

(a) *$f = \delta g_1 \cdots g_n$, where δ is a unit in R and $g_1, \ldots, g_n$ are regular primary coprime polynomials.*

(b) *If $f = \delta g_1 \cdots g_n = \beta h_1 \cdots h_m$, where β and δ are units and $\{g_i\}$ and $\{h_j\}$ are regular primary coprime ideals then $n = m$ and, after renumbering $(h_i) = (g_j)$ $(1 \leq i \leq n)$.*

Further a primary polynomial can be written in a certain form:

PROPOSITION 1 ([4] XIII.12]). *A polynomial $f \in R[X]$ is a primary regular non-unit if and only if $f = \delta \Pi^h + \beta$, where δ is a unit in R, Π is a basic irreducible, $h \geq 1$ and $\beta \in \mathfrak{m}[X]$.*

Next we show that any ideal containing a primary polynomial is also

primary. Hence if f is a primary polynomial then every ideal of $R[X]/(f)$ is a primary ideal. For an ideal $\mathfrak{a}$ we denote the *radical* of $\mathfrak{a}$ by $\mathrm{rad}(\mathfrak{a})$.

PROPOSITION 2. *Let $f = \delta\Pi^h + \beta$ be a primary polynomial with $\beta = p^i b \in \mathfrak{m}[X]$ with $\mathfrak{m} = (p)$ and b regular, δ a unit and Π a basic irreducible. Then any ideal containing (f) is primary.*

PROOF. Let J be a nonunit ideal containing (f). Then $p \in \mathrm{rad}(J)$ since $p^n = 0 \in \mathrm{rad}(J)$ for some n, whence $\beta \in \mathrm{rad}(J)$. Hence $\delta\Pi^h = f - \beta \in \mathrm{rad}(J)$ and thus $\Pi \in \mathrm{rad}(J)$. Therefore $\mathrm{rad}(J) = (\Pi, p)$ since an ideal is the unit ideal if and only if its radical is the unit ideal. Since $\mathrm{rad}(J) = (\Pi, p)$ is maximal, we see J is a primary ideal by [1, Cor. 7.16]. □

COROLLARY. *Under the same assumption as in Proposition 2, we have that the ring $R[X]/(f)$ is a local ring with the maximal ideal $(\bar{\Pi}, \bar{p})$.*

PROOF. To check locality of $R[X]/(f)$ let $\mathfrak{m}$ be a maximal ideal. Then $p \in \mathrm{rad}(\mathfrak{m})$. Also, $\delta\Pi^h = f - \beta \in \mathrm{rad}(\mathfrak{m}) = \mathfrak{m}$. Hence $\Pi \in \mathfrak{m}$. Therefore $(p, \Pi) \subseteq \mathfrak{m}$. Since (p, Π) is a maximal ideal we see $(p, \Pi) = \mathfrak{m}$ as desired. □

We will rewrite a primary polynomial in some nice form. For this we will need some well known facts:

LEMMA 1 ([3] THEOREM 1.1 CH.IV). *Let R be a commutative ring. Let $f, g \in R[X]$ with g monic. Then there are unique q and r such that*

$$f = qg + r$$

with $\deg r < \deg g$. (Here we adopt the convention that the degree of the zero polynomial is $-\infty$.)

The following is also well known.

LEMMA 2 ([1] CH.1, EXERCISE 2). *Let R be a commutative ring with identity and let $f(X) = \sum_{i=0}^{n} a_i X^i$ be a polynomial over R. Then $f \in R[X]$ is a unit if and only if a_0 is a unit in R and $a_1, a_2, \ldots, a_n$ are nilpotent in R.*

COROLLARY. *Suppose u is a unit and n is nilpotent. Then $u + n$ is a unit.*

PROOF. Consider the ring homomorphism $\phi : R[X] \to R$ defined by $\phi(f(X))) = f(1)$. By Lemma 2, $u + nX$ is a unit in $R[X]$. Therefore $u + n = \phi(u + nX)$ is also a unit. □

Note that the generator p of $\mathfrak{m}$ is nilpotent. In fact, the set $\{1, p, p^2, \ldots\}$ is finite. Hence $p^a = p^b$ for some $a < b$. Hence $p^a(1 - p^{b-a}) = 0$ and $1 - p^{b-a}$ is a unit by Lemma 2. Therefore $p^a = 0$.

The following is a slight generalization of [2] Lemma 2.1. For any commutative ring R and $a, b \in R$ we will write $(a, b) = 1$ if there are $x, y \in R$ such tat $ax + by = 1$, namely a, b generate the unit ideal.

LEMMA 3 ([2] LEMMA 2.1). *If $f, g \in R[X]$ are regular then $(f, g) = 1$ if and only if $(\mu(f), \mu(g)) = 1$.*

PROOF. If $(f, g) = 1$ then obviously $\mu((f, g)) = (\mu(f), \mu(g)) = (1)$. On the other hand, if $(\mu(f), \mu(g)) = 1$ then there are $\bar{a}, \bar{b} \in k[X]$ such that $\bar{a}f + \bar{b}g = 1$ in $k[X]$. Let a, b be lifts of $\bar{a}, \bar{b}$ in $R[X]$ then $af + bg = 1 + pc$ for some $c \in R[X]$. Since pc is nilpotent we see that $1 + pc$ is a unit by Lemma 2. Therefore the ideal (f, g) contains a unit as desired.□

Applying these facts we will write a primary polynomial in a form we like to have.

PROPOSITION 3. *Let Π be a monic basic irreducible polynomial in $R[X]$. Let $f = \delta\Pi^h + p^i c (i > 0)$ be a polynomial with δ a unit in $R[X]$ and c a regular polynomial. Then there is a unit δ' in $R[X]$ such that $f = \delta'\Pi^h + p^j b$, where b is a regular polynomial of degree $< h \deg \Pi$ and $i \leq j$.*

PROOF. Suppose $\deg c \geq h \deg \Pi$. Then by the Lemma 1, we can find the polynomials q and b such that $f = \delta\Pi^h + p^i c = \delta\Pi^h + p^i(q\Pi^h + b) = \delta(1 + \delta^{-1}p^i q)\Pi^h + p^{i+k}c$ with $\deg b < h \deg \Pi$ and k is the highest power of p in the coefficients of b. Now $(1 + \delta^{-1}p^i q)$ is a unit in $R[X]$ by Lemma 2. Writing $\delta' = \delta(1 + \delta^{-1}p^i q)$ we have the desired result. □

Note the polynomial f in Proposition 3 is necessarily regular and primary. In fact, δ being a unit in $R[X]$ it contains a coefficient which is a unit in R. Hence $\delta\Pi^h$ is regular since it is a product of regular polynomials. Therefore $f = \delta\Pi^h + p^i c$ is regular. To see f is also primary, write $\delta = a_0 + \beta'$ with $a_0 \in R^*$ and $\beta' \in pR[X]$. Since Π is monic, f is of the form $f = a_0\Pi^h + \beta$ with $\beta \in \mathfrak{m}[X]$. Now by Proposition 1, f is primary.

PROPOSITION 4. *Let h be a regular polynomial and Π be a monic basic irreducible polynomial. Then we can write uniquely $h = \Pi^j\Delta + p^i k$, where Δ is regular, $(\Pi, \Delta) = 1$ and k is regular of degree $< j\deg(\Pi)$ and $p^i k \in \mathfrak{m}[X]$.*

PROOF. As remarked above, the polynomial h in the form must be regular. Now to write h in the desired form, let $\mu(h) = \delta\pi^j$ with $(\pi, \delta) = 1$ and $\pi = \mu(\Pi)$. Choose $\Delta \in R[X]$ satisfying $\mu(\Delta) = \delta$. Then $(\Pi, \Delta) = 1$ by Lemma 3 and $\mu(h - \Delta\Pi^j) = 0$. Hence $h - \Delta\Pi^j = p^i k$ for some regular polynomial $k \in R[X]$ and $p^i k \in \mathfrak{m}[X]$. Now suppose $\deg k > j\deg\Pi$. Then we can write $k = \Pi^j\Delta' + r$ for some $r \in R[X]$ of degree $< j\deg\Pi$. Therefore $h = \Pi^j(\Delta + p^i\Delta') + p^i r$ with $\deg r < j\deg(\Pi)$. Now we need to check $(\Pi, \Delta + p^i\Delta') = 1$. For this we need to check the image of $\Delta + p^i\Delta'$ in $R[X]/(\Pi)$ is a unit. But the image of Δ in $R[X]/(\Pi)$ is a unit and $p^i\Delta'$ is nilpotent. Therefore the image of $\Delta + p^i\Delta'$ in $R[X]/(\Pi)$ is a unit by Lemma 2 as desired.

Uniqueness of the expression follows from Lemma 1 which asserts uniqueness of the expression under the same condition on degree. □

THEOREM 2. *Let R be a finite local ring with a maximal ideal $\mathfrak{m}$ and let p be a generator of $\mathfrak{m}$ and m is the smallest positive integer such that $p^m = 0$. Let $f = \Pi^r + \beta$ be a monic primary polynomial over R with Π a monic basic irreducible in $R[X]$ and $\beta \in \mathfrak{m}[X]$. Then any regular polynomial $g \in R[X]$ can be written uniquely in the form*

$$g = af + \Delta_1\Pi^{j_1}p^{i_1} + \Delta_2\Pi^{j_2}p^{i_2} + \cdots + \Delta_l\Pi^{j_l}p^{i_l}$$

for some $a \in R[X]$ and regular polynomials $\Delta_1, \Delta_2, \ldots, \Delta_l$ with $(\Delta_k, \Pi) = 1$ for $k = 1, 2, \ldots, l$ and $r > j_1 \geq j_2 \geq \cdots \geq j_l \geq 0$, $0 \leq i_1 \leq i_2 \leq \cdots \leq i_l < m$.

PROOF. Since f is monic, by Lemma 1 we can write $g = af + p^{i_1}h$ with h regular of degree $< r\deg\Pi = \deg(f)$ and $0 \leq i_1 \leq m$. By Proposition 4, we can write $h = \Delta_1\Pi^{j_1} + p^{i_1'}k_1$ with k_1 regular and $(\Delta_1, \Pi) = 1$ and $\deg(k_1) < j_1\deg(\Pi)$. Hence, we can write $g = af + \Delta_1\Pi^{j_1}p^{i_1} + p^{i_1+i_1'}k_1$ with $\deg(k_1) < j_1\deg(\Pi)$. Also note that $r > j_1$ because $j_1\deg(\Pi) \leq \deg h < r\deg\Pi = \deg(f)$. Again we can write $k_1 = \Delta_2\Pi^{j_2} + p^{i_2'}k_2$ $(j_2 \leq j_1)$ with k_2 regular of $\deg k_2 < j_2\deg\Pi$ and $(\Delta_2, \Pi) = 1$. Thus

$$\begin{aligned} g &= af + \Delta_1\Pi^{j_1}p^{i_1} + p^{i_1+i_1'}(\Delta_2'\Pi^{j_2} + p^{i_2'}k_2) \\ &= af + \Delta_1\Pi^{j_1}p^{i_1} + \Delta_2'\Pi^{j_2}p^{i_1+i_1'} + p^{i_1+i_1'+i_2'}k_2. \end{aligned}$$

Proceeding in this way we get a regular polynomial $k_l = \Delta_l$ with degree $< \deg \Pi$. Then since Π is basic irreducible and k_l is regular of degree $< \deg(\Pi)$, we have $(\Pi, \Delta_l) = 1$ by Lemma 3.

Uniqueness follows by the same reason as in the proof of Proposition 4. □

COROLLARY 1. *Let f, g be as in Theorem 2. Then every $\bar{g} \in R[X]/(f)$ can be written uniquely in the form*

$$\bar{g} = u_1 \bar{\Pi}^{j_1} p^{i_1} + u_2 \bar{\Pi}^{j_2} p^{i_2} + \cdots + u_l \bar{\Pi}^{j_l} p^{i_l},$$

where u_k are units in $R[X]/(f)$ and $r > j_1 \geq j_2 \geq \cdots \geq j_l \geq 0$, $0 \leq i_1 \leq i_2 \leq \cdots \leq i_l < m$. And also write $\bar{\Pi}$ for the image of Π in $R[X]/(f)$.

PROOF. Since $(\Delta_k, \Pi) = 1$ and Δ_k is regular, we have $(\mu(\Delta_k), \pi) = 1$. Hence, we have $(\mu(\Delta_k), \mu(f)) = (\mu(\Delta_k), \pi^r) = (\mu(\Delta_k), \pi) = 1$. Since both Δ_k and f are regular for $k = 1, 2, \ldots, l$, the image of Δ_k in $R[X]/(f)$ is a unit. We simply let u_k be the image of Δ_k in $R[X]/(f)$.□

As another application of the Theorem 2, we can obtain [2, Lemma 3.1] which played an important role in proving one of the main theorem [2, Theorem 3.4] and its corollaries saying that every ideal of $\mathbb{Z}_{p^m}[X]/(X^n - 1)$is principal when p and n are relatively prime.

COROLLARY 2. *Let f be basic irreducible. Then every ideal of $R[X]/(f)$ is of the form (p^i) for some i.*

PROOF. Since f is basic irreducible, we have $r = 1$. Since $r > j_1$ we must have $j_i = 0$ for all i. Let J be an ideal of $R[X]/(f)$ and $g \in J$. Then g is a multiple of p^k modulo f for some k. Now choose the smallest i such that $p^i \in J$. Then obviously $J = (p^i)$ as required. □

REMARK. We may view the expression of Corollary 1 a *Taylor expansion* of $\bar{g}$ in the variables Π and p.

3. Primary ideals of $\mathbb{Z}_{p^m}[X]$

For the rest of this paper we let $R = \mathbb{Z}_{p^m}$ the ring of integers modulo p^m for a prime p. For a commutative ring A we will write A^* for the set of all units of A.

In this section we propose to find the primary ideals which contain a certain primary polynomial. The idea to do this is to use extremal elements in some ordering on the polynomial ring $R[X]$ which can be viewed as a generalization of idea choosing a polynomial of the least degree in an ideal of a polynomial ring over a field as a generator.

Now we endow an order structure on $\{0 = p^m, 1 = p^0, p, p^2, \ldots, p^{m-1}\}$ as

$$0 = p^m < 1 = p^0 < p < p^2 < \cdots < p^{m-1}.$$

Also we endow order structure on the set of n-tuples $(p^{i_1}, p^{i_2}, \ldots, p^{i_n})$ with lexicographic order for every positive integer n. We will often write $i \leq j$ for $p^i \leq p^j$ by abusing the notations. Also we will consider p^m as $p^{-\infty}$.

Let $f = \Pi^r + \beta$ be a monic primary polynomial over R with Π a monic basic irreducible in $R[X]$ and $\beta \in \mathfrak{m}[X]$ as in Theorem 2. By Corollary 1 of Theorem 2, for any $\bar{g} \in R[X]/(f)$ we can write

$$\bar{g} = u_0 \bar{\Pi}^l p^{i_0} + u_1 \bar{\Pi}^{l-1} p^{i_1} + \cdots + u_{l-1} \bar{\Pi} p^{i_{l-1}} + u_l p^{i_l},$$

where u_k are units in $R[X]/(f)$ by allowing i_k to be m. If $\bar{h} = \sum_{k=0}^{l} u_k \bar{\Pi}^k p^{r_k}$ $\in R[X]/(f)$ then we define $\bar{g} \leq \bar{h}$ if and only if

$$(p^{i_0}, p^{i_1}, \ldots, p^{i_l}) \leq (p^{r_0}, p^{r_1}, \ldots, p^{i_l}).$$

This will endow a preordering (a partial ordering without antisymmetry) on $R[X]/(f)$.

To investigate the ideals of $R[X]/(f)$, we begin with a simplest case. We take $\Pi = X$ and $r = 2$ in the previous section. Say let

$$f(X) = X^2 + p^a X + p^b \ (0 \leq a, b \leq m).$$

(For the rest of this section we fix this notation.) First we propose to describe the ideals of $R[X]/(f)$ which are primary by Proposition 2. By Corollary 1 of Theorem 2, every element of $R[X]/(f)$ can be written in the form $up^\alpha X + vp^\beta$ with $\alpha \leq \beta$ and units u, v of $R[X]/(f)$. We defined an order structure on $R[X]/(f)$ by

$$up^\alpha X + vp^\beta \leq u_1 p^\gamma X + v_1 p^\delta$$

if and only if $(p^\alpha, p^\beta) \leq (p^\gamma, p^\delta)$.

Let $\bar{J}$ be an ideal of $R[X]/(f)$ and let

$$p^{i_0} \text{ be the smallest nonnegative power of } p \text{ which belongs to} \bar{J}$$

and let

$$p^i X + up^j \text{ be the smallest linear element in } \bar{J}$$

for some unit $u \in R[X]/(f)$. By Corollary 1 of Theorem 2, we necessarily have $i \leq j$.

First note that since $p^{i_0} \in \bar{J}$ we have that $p^{i_0}X^2 \in \bar{J}$. Therefore, we see that $p^{i_0}X^2 - p^{i_0}f(X) = p^{a+i_0}X + p^{b+i_0} \in \bar{J}$. Which entails

$$p^i X + up^j \leq p^{a+i_0}X + p^{b+i_0}.$$

We consider various cases according to the order relations among i, j, i_0.

PROPOSITION 5. *Let $f(X) = X^2 + p^a X + p^b$ and $\bar{J}$ be a proper ideal of $R[X]/(f)$. Let p^{i_0} be the smallest power of p in $\bar{J}$ and $p^i X + up^j$ is the smallest linear element in $\bar{J}$.*

If $i_0 \leq i$, then $\bar{J} = (p^{i_0})$.

If $i < i_0 \leq j$, then $\bar{J} = (p^{i_0}, p^i X)$.

PROOF. If $i_0 \leq i$ then $p^i X$ and p^j are in (p^{i_0}). Hence in this case we have $\bar{J} = (p^{i_0})$.

On the other hand, suppose now $i < i_0 \leq j$. Then $p^j \in (p^{i_0})$. Hence in this case we have $\bar{J} = (p^{i_0}, p^i X)$. As desired. □

Now we assume $i \leq j < i_0$. Suppose we have $i = j$. Then $p^i X^2 + up^i X = p^i(u - p^a)X - p^{i+b}$ modulo f. Writing $v = (u - p^a)^{-1}$ we have $p^i X - vp^{i+b} \in \bar{J}$. On the other hand, by our assumption $p^i X + up^i \in \bar{J}$. Hence their difference $p^i(u - vp^b)$ is in $\bar{J}$ which contradict to the fact that p^{i_0} is the smallest power of p in $\bar{J}$. Hence this case does not happen.

Therefore we necessarily have $i < j$. And we need to look at the case

$$(*) \qquad i < j < i_0 < m.$$

From these observations we get,

COROLLARY. *If $i_0 = 1$, then an ideal of $R[X]/(f)$ is either of the form $\bar{J} = (p)$ or $\bar{J} = (p, X)$.*

PROOF. From the first case of the Proposition 5 we necessarily have $i_0 = 1$. Hence in this the we obtain $\bar{J} = (p)$. From the second case of Proposition 5, the only possible case is when $i_0 = 1, i = 0$ in which case we have $\bar{J} = (p, X)$.

Now the only possible i, j satisfying (*) with $i_0 = 1$ is when $j = 0$ and $i = -\infty$. But then we have $\bar{J} = (1)$ which in turn implies $i_0 = 0$. This is a contradiction. □

We propose to find the *proper* ideals (i.e., nonzero and nonunit) $\bar{J}$ of $R[X]/(f)$ with $f(X) = X^2 + p^a X + p^b$. As before, we let p^{i_0} be the smallest power of p in $\bar{J}$ and $p^i X + p^j$ be the smallest linear element of $\bar{J}$ satisfying (*). (We set $u = 1$ in Proposition 5 for simplicity.)

Let $g \in \bar{J}$. By Corollary 1 to Theorem 2, we can write $g = vp^\alpha X + up^\beta$ with $\alpha \leq \beta$. By multiplying v^{-1} we may consider g of the form $p^\alpha X + up^\beta$ for some unit u of $R[X]/(f)$ with $\alpha \leq \beta$. We consider the several cases depending on α and β.

LEMMA 4. *With the same assumptions on $\bar{J}$ as above. Suppose $p^i X + up^j$ be an element of $\bar{J}$ with u a unit. Then u is of the form $u = 1 + wp^\alpha$ with $\alpha \geq i_0 - j$ and for some unit w.*

PROOF. First suppose $1 - u$ is a unit. Then since $p^i X + up^j = p^i X + p^j - (1 - u)p^j$ we see $p^j \in \bar{J}$ which contradicts to the fact that p^{i_0} is the smallest power of p in $\bar{J}$.

Now write $1 - u = w_1 p^\alpha X + w_2 p^\beta$ with some units w_1, w_2 and $\alpha \leq \beta$ by Corollary to Theorem 2. (Since $f(X)$ is quadratic we may choose w_1 and w_2 to be units in $\mathbb{Z}_{p^m}$.) Then $p^i X + up^j = (p^i + w_1 p^{\alpha+j})X + (1 + w_2 p^\beta)p^j$. By uniqueness of the expression of Corollary of Theorem 2, we have $w_1 p^{\alpha+j} = 0$ and $u = 1 + w_2 p^\beta$. Now since $(p^i X + up^j) - (p^i X + p^j) = w_2 p^{\beta+j}$ we must have $\beta + j \geq i_0$ i.e., $\beta \geq i_0 - j$ as required. □

Note that in Lemma 4 above we have

$$(**) \qquad (p^\alpha X + up^\beta) = (p^i X + p^j) + wp^\gamma$$

with $\gamma \geq i_0$ and a unit w of $\mathbb{Z}_{p^m}$.

LEMMA 5. *If either $\alpha = i, j < \beta < i_0$ or $\alpha = i, i_0 \leq \beta$, then no element of the form $p^\alpha X + up^\beta$ with a unit u belongs to $\bar{J}$.*

PROOF. In the first case $p^\alpha X + up^\beta - (p^i X + p^j) = -p^j(1 + up^{\beta-j}) < p^{i_0}$ which contradicts to the fact that p^{i_0} is the smallest power of p in $\bar{J}$. Hence there is no element in $\bar{J}$ satisfying the inequality above.

In the second case, since $p^\beta = p^{i_0}p^{\beta-i_0} \in \bar{J}$, we have $(p^\alpha X + up^\beta) - up^{i_0}p^{\beta-i_0} = p^\alpha X \in \bar{J}$. But this contradict to that $p^i X + p^j$ is the smallest linear element of $\bar{J}$. (Remember from (*) that $i < j$.) □

LEMMA 6. *Now suppose $p^\alpha X + up^\beta \in \bar{J}$ with $i < \alpha \leq \beta$.*

(i) *If $\beta \neq \alpha - i + j$ then $\min(\beta, \alpha - i + j) \geq i_0$.*

(ii) *Suppose $\beta = \alpha - i + j$ (i.e., $a := j - i = \beta - \alpha$) and suppose $u = x + wp^\gamma X$ with units x, w of $\mathbb{Z}_{p^m}$ in (**). If $x = 1 + bp^k$ $(k \geq 0)$ with a unit b in $\mathbb{Z}_{p^m}$ then $k \geq i_0 - j - a$.*

PROOF. (i) First suppose $\beta \neq \alpha - i + j$.

First suppose if $\min(\beta, \alpha - i + j) \geq i_0$ then $p^\alpha X + up^\beta - p^{\alpha-i}(p^i X + p^j) = up^\beta - p^{\alpha-i+j} \in \bar{J}$.

If $\min(\beta, \alpha - i + j) < i_0$ then $up^\beta - p^{\alpha-i+j}$ is divisible by a lower power than p^{i_0}. Hence in this case we have $p^\alpha X + up^\beta \notin \bar{J}$.

(ii) Now suppose $\beta = \alpha - i + j$. In this case, we have

$$p^\alpha X + up^\beta = p^a(p^i X + up^j) - p^a(p^i X + p^j) = (u-1)p^{a+j}$$

We consider several cases depending on the unit u.

First suppose $u = x$ and $u - 1 = x - 1 = bp^k$. Then since $(u-1)p^{a+j} \in \bar{J}$ we see that $a + j + k \geq i_0$.

Second suppose $\gamma \geq 0$ and $x - 1$ is a unit i.e., $k = 0$. Then $u - 1$ is a unit since X is nilpotent. Therefore we also see that $a + j + k \geq i_0$ with $k = 0$.

Now suppose $\gamma \geq 0$ and $x - 1$ is not a unit. For this we consider two cases; when $k \leq \gamma$ and $k > \gamma$.

Case 1: $k \leq \gamma$

In this case we have $(u-1)p^{a+j} = (b + w_1 X p^{\gamma-k})p^{a+k+j} \in \bar{J}$. Hence we have $a + j + k \geq i_0$.

Case 2: $k > \gamma$.

Since

$$\begin{aligned} p^a(p^i X + up^j) &= p^a(p^i X + (p^k b + w_1 X p^\gamma + 1)p^j) \\ &= p^a((p^i + w_1 p^{\gamma+j})X + (p^k b + 1)p^j) \end{aligned}$$

we see $u = 1 + p^k b$ and $w_1 p^{\gamma+j} = 0$ by the uniqueness of the expression of Corollary to Theorem 2. Therefore $p^a(p^i X + up^j) = p^a(p^i X + p^j) + bp^{a+j+k}$. Hence again we have $a + j + k \geq i_0$. □

REMARK. In any case of Lemma 6, the elements of the form $p^{\alpha}X + up^{\beta} \in \bar{J}$ is a linear combination of p^{i_0} and $p^iX + p^j$.

Consider all R-linear combinations in $R[X]/(f)$ of

$$p^{i_0} \quad \text{and} \quad p^iX + p^j$$

which we denote by $\bar{H}$. Then $\bar{H}$ is an additive group. In order that an additive group A of a ring to be an ideal we need to check that A is stable under multiplication by X.

We have a simple lemma we omit its straight forward verification.

LEMMA 7. *Let A be an additive subgroup of $R[X]/(f)$ then $A + AX$ is an ideal of $R[X]/(f)$, where $f(X) = X^2 + p^aX + p^b$ as before.*

Let $\bar{J}$ be an ideal of $R[X]/(f)$ having the smallest elements p^{i_0} and $p^iX + p^j$. It turns out that we need restrictions on the exponents i_0, i, j, a, b of p.

THEOREM 3. *Let $f(X) = X^2 + p^aX + p^b$ and $\bar{J}$ be a proper ideal of $R[X]/(f)$. Let p^{i_0} be the smallest power of p in $\bar{J}$ and $p^iX + p^j$ is a minimal linear element in $\bar{J}$ with $i < j < i_0 < m$.*

(i) *If $j - i < a$ then we need $j - i \leq b$ also and we require*

$$\begin{cases} j \geq i_0 & \text{if } b \neq 2(j-i) \\ i + 2a \geq i_0 & \text{if } b = 2(j-i) \end{cases}$$

(ii) *If $j - i = a$, then we necessarily have $i + b \geq i_0$.*

(iii) *If $j - i > a$, then we also need $a \leq b$ and*

$$\begin{cases} 2j - i \geq i_0, i + b = j & \text{if } a = 0 \\ a + j \geq i_0 & \text{if } b - a \neq j - i \\ 2j - i \geq i_0 & \text{if } b - a = j - i \end{cases}$$

In each case, we have $\bar{J} = \bar{H} + \bar{H}X$.

PROOF. First note that since $i < j < i_0$ we have $p^{i_0}X \geq p^iX + p^j$. And we see $p^{i_0}X \in \bar{J}$. Next consider $X(p^iX + p^j)$.

(i) First suppose $j - i < a$. To be an element of an ideal having the smallest element p^{i_0} and $p^iX + p^j$ it must be of type in Lemma 4 and Lemma 6.

By using the relation $X^2 + p^aX + p^b = 0$ we have $(p^iX + p^j)X = p^j(1 - p^{i+a-j})X - p^{i+b}$ which is of the form $p^jX + up^{i+b}$ with u a unit

of the form $u = 1 + bp^{i+b-j}$ for some unit b of R. This is not of the type in Lemma 4. Hence it must be of the type considered in Lemma 6. Thus we necessarily have $j - i \leq b$.

If $i + b - j \neq j - i$ i.e., $b \neq 2(j - i)$, then by Lemma 6 (i), we must have $\min(j, i + b - i + j) \geq i_0$ i.e., $j \geq i_0$.

If $b = 2(j - i)$, then by Lemma 6 (ii), we have $i + a - j \geq i_0 - j - a$ i.e., $i + 2a \geq i_0$.

(ii) If $j - i = a$, then $(p^i X + p^j)X = -p^{i+b}$. Since p^{i_0} is the smallest power of p in $\bar{H}$ we have $i + b \geq i_0$.

(iii) If $j - i > a$, then $(p^i X + p^j)X = p^{i+a}(p^{j-i-a} - 1)X - p^{i+b}$. If $a = 0$ then this is an element considered in Lemma 4. Hence we must have $i + b = j$ and $j - i - a \geq i_0 - j$ i.e., $2j - i \geq i_0$.

If $a \neq 0$, then this is again the type of element considered in Lemma 6. We omit the routine verification. □

COROLLARY. *Under the same assumptions of Theorem 3, the ideal $\bar{J}$ is completely determined by the extremal elements p^{i_0} and $p^i X + p^j$. In fact, they generate the ideal $\bar{J}$.*

PROOF. From the proof of Theorem 3, we see that the elements of $\bar{J}$ consists of the linear combinations of p^{i_0} and $p^i X + p^j$ whenever $\bar{J}$ becomes an ideal. □

If we replace the smallest linear element by $p^i X + vp^j$ for some unit instead of $p^i X + p^j$ we will get more complicate conditions on i_0, i, j, a, b's.

References

[1] M. Atiyah, Addison-Wesley (1965).
[2] P. Kanwar and Sergio, *Cyclic codes over integer modulo p^n*, finite fields and their applications **3(2)** (1997).
[3] S. Lang, *Algebra, 3rd ed.*, Addison Wesley, 1993.
[4] B. R. McDonalds, *Finite rings with identity*, Dekker, New York, 1974.

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