Commun. Korean Math. Soc. **26** (2011), No. 3, pp. 427–443
DOI 10.4134/CKMS.2011.26.3.427

IDEALS OF $\mathbb{Z}_{p^n}[X]/(X^l-1)$

Sung Sik Woo

Abstract. In [6, 8], we showed that any ideal of $\mathbb{Z}_4[X]/(X^l-1)$ is generated by at most two polynomials of the 'standard' forms when l is even. The purpose of this paper is to find the 'standard' generators of the cyclic codes over $\mathbb{Z}_{p^a}$ of length a multiple of p, namely the ideals of $\mathbb{Z}_{p^a}[X]/(X^l-1)$ with an integer l which is a multiple of p. We also find an explicit description of their duals in terms of the generators when $a=2$.

1. Introduction

In [4], a complete description of the ideals of $\mathbb{Z}_{p^n}[X]/(X^l-1)$ (i.e., the cyclic codes of length l over $\mathbb{Z}_{p^n}$) is given when l is prime to p. When $p^n=4$ and l is of the form $l=2^k$, it was shown that $S'=\mathbb{Z}_4[X]/(X^{2^k}-1)$ is isomorphic to $S=\mathbb{Z}_4[X]/(X^{2^k}-2X^{2^{k-1}})$ and the ideals of the latter ring are generated by two elements of some special type [7]. More generally, the cyclic codes of even length was described in [6].

The purpose of this paper is to find a description of the cyclic code of length divisible by p over $\mathbb{Z}_{p^a}$, that is the ideals of $\mathbb{Z}_{p^a}[X]/(X^l-1)$ with $l=p^nm, a\geq 1, (m,p)=1$ and $n\geq a$. Also, we find a description of the dual of the cyclic codes when $a=2$ and $l=p^n$.

For this we will show, in §5, that the ring $\mathbb{Z}_{p^a}[X]/(X^l-1)$ $(l=p^nm)$ is isomorphic to $S[Y]/(Y^m-u)$ where $S=\mathbb{Z}_{p^a}[X]/(X^{p^n}-ph(X))$ for some $h(X)\in\mathbb{Z}_{p^a}[X]$ and $u\in S$ is a unit. Using the fact that $(p,m)=1$ we then show that $S[Y]/(Y^m-u)$ is isomorphic to a direct sum of the rings of the type $S[Y]/(f)$ for some $f\in S[X]$ in which every ideal is a 'descent' of an ideal of S.

In §2, we start investigating the rings S of the form $\mathbb{Z}_{p^a}[X]/(X^{p^n}-ph(X))$ where $h(X))\in\mathbb{Z}_{p^a}[X]$. We show that every ideal of S is generated by some special forms, like $X^k-ph(X)$ for some $h(X)\in\mathbb{Z}_{p^a}[X]$ and pX^r's.

Next we show that the ring $\mathbb{Z}_{p^a}[X]/(X^{p^n}-1)$ is isomorphic to the ring of the form $S=\mathbb{Z}_{p^a}[X]/(X^{p^n}-ph(X))$ for some $h(X)\in\mathbb{Z}_{p^a}[X]$ by using some combinatorial facts (§3).

Received April 6, 2010.
2010 *Mathematics Subject Classification.* 13M05, 11T71.
Key words and phrases. cyclic code over $\mathbb{Z}_{p^a}$, ideals of $\mathbb{Z}_{p^n}[X]/(X^l-1)$.

In §4, we show that the dual $C^{\perp}$ of a cyclic code C over $\mathbb{Z}_{p^2}$ of length p^n generated by the ideal I is generated by the annihilator ideal $\mathrm{Ann}(I)$ of I. And the explicit generators for $\mathrm{Ann}(I)$ is given in terms of generators of I.

A ring means a commutative ring with the identity element 1 throughout this paper. The characteristic of a ring R is the smallest nonnegative integer n such that $nx = 0$ for all $x \in R$. The characteristic of a ring is assumed to be a power of a prime p. We assume p to be an *odd prime* in §4.

After this paper was written the author come to know that S. T. Dougherty and Y. H. Park [3] worked over the same subject using coding theoretic methods. However the author thinks that a purely algebraic approach is still worth for publication.

2. Algebras generated by a nilpotent element over $\mathbb{Z}_{p^a}$ and the ideals

We consider a ring of the form $S = \mathbb{Z}_{p^a}[X]/(\alpha(X))$ where $\alpha(X)$ is a monic polynomial of degree m such that $X^n \in (\alpha(X))$ for some n. If this happens, we show that the polynomial $\alpha(X)$ assumes some special form.

Lemma 1. *Let $S = \mathbb{Z}_{p^a}[X]/(\alpha(T))$ for some $\alpha(T) \in \mathbb{Z}_{p^a}[X]$. Then the canonical image x of X in S satisfies $x^n = 0$ if and only if $\alpha(X) = X^m + ph(X)$ for some $h(X) \in \mathbb{Z}_{p^a}[X]$.*

Proof. If $S = \mathbb{Z}_{p^a}[X]/(\alpha(T))$ with $\alpha(X) = X^m + ph(X)$ for some $h(X) \in \mathbb{Z}_{p^a}[X]$, then the canonical image x of X in S satisfies $x^{m+a} = 0$.

Conversely, suppose S satisfies the condition. If we reduce modulo the ideal (p), then $x^n = 0$ implies $\bar{\alpha}(X)$ divides X^n where $\bar{\alpha}(X)$ denotes the image of $\alpha(X)$ under $\mathbb{Z}_{p^a}[X] \to \mathbb{Z}_p[X]$. Since $\mathbb{Z}_p[X] = \mathbb{F}_p[X]$ is a UFD, we see that $\bar{\alpha}(X) = X^m$ for some m, i.e., $X^m - \alpha(X) \in p\mathbb{Z}_{p^a}[X]$. Therefore $\alpha(X)$ has the required form. □

In this section, a ring S will mean a cyclic $\mathbb{Z}_{p^a}$-algebra of the form $S = \mathbb{Z}_{p^a}[X]/(\alpha(X))$ where $\alpha(X)$ is a monic polynomial of degree m such that $X^n \in (\alpha(X))$ for some n unless otherwise states. Whenever we talk about a polynomial $f(X)$ in S we shall choose a representative with degree less than m. In this section we fix the degree of $\alpha(X)$, say $\deg(\alpha(X)) = m$.

As in [8], our first observation is that the ring S we are interested in is a local ring and every ideal of S is primary. The same proof of the corresponding assertion works as well in our case also. We include the proof just for completeness.

Proposition 1. *The ring $S = \mathbb{Z}_{p^a}[X]/(\alpha(X))$ is a local ring with the maximal ideal (p, X). Every ideal J of S is primary with the radical $\mathrm{rad}(J) = (p, X)$.*

Proof. Let $\mathfrak{m}$ be a maximal ideal. Any nilpotent element is contained in every prime ideal [1]. Since p, X are nilpotent, we see that p and X belong to $\mathfrak{m}$. Hence (p, X) is contained in $\mathfrak{m}$. Since (p, X) is a maximal ideal as well, $\mathfrak{m} =$

(p, X) and it is unique. Let J be an ideal of S. Then p and X, being nilpotent, belong to the radical $\mathrm{rad}(J)$ of J. Therefore $\mathrm{rad}(J) = (p, X)$. It is well known that if the radical of J is a maximal ideal, then J is primary [1, Proposition 4.2]. □

We will use the following well known fact freely.

Lemma 2. *Let R be a commutative ring with the identity. If u is a unit and $\nu \in R$ is nilpotent, then $u + \nu$ is a unit.*

We will show that if an ideal J of $S = \mathbb{Z}_{p^a}[X]/(\alpha(X))$ is contained in the principal ideal (p) generated by p, then J is generated by at most $(a-1)$ elements. We define an ordering on the set $\mathcal{P} = \{(i,j) | 1 \le i < a, 0 \le j < m\}$ of pairs of integers by furnishing lexicographic order.

Proposition 2. *Let J be an ideal of S contained in (p). Choose a subset $\mathcal{P}_J = \{(i_1, j_1), (i_2, j_2), \ldots, (i_r, j_r)\}$ of $\mathcal{P}$ satisfying the properties*
(i) *$i_1 < i_2 < \cdots < i_r$ and $j_1 > j_2 > \cdots > j_r$,*
(ii) *(i_1, j_1) is the smallest pair such that $p^{i_1}X^{j_1} \in J$ and*
(iii) *$p^{i_s}X^{j_s} \in J$ but $p^{i_s}X^{j_s-1} \notin J$ $(s = 1, 2, \ldots, r)$.*
Then $J = (p^{i_1}X^{j_1}, p^{i_2}X^{j_2}, \ldots, p^{i_r}X^{j_r})$. In particular, J is generated by at most $(a-1)$ elements.

Proof. Suppose $p^iX^j \in J$. Then $i_a \le i \le i_{a+1}$. If $i = i_a$ (resp. $i = i_{a+1}$), then $j \ge j_a$ (resp. $j \ge j_{a+1}$). Hence p^iX^j is a multiple of one of the elements in $\{p^{i_1}X^{j_1}, p^{i_2}X^{j_2}, \ldots, p^{i_k}X^{j_k}\}$.

Now suppose $i_a < i < i_{a+1}$. Then $j \ge j_a$. For otherwise the pair (i, j) must be in the list. Hence p^iX^j is a multiple of $p^{i_a}X^{j_a}$. □

Remark. We can choose the pairs $\mathcal{P}_J$ in the following way: Let $A = \{(i, j_i)\}$ be the pairs such that $p^iX^{j_i} \in J$ and for each fixed i $(1 \le i < a)$, j_i is the smallest integer such that $p^iX^{j_i} \in J$. Let (i_1, j_1) be the smallest pair in A. If $j_{i_1+1} \ge j_{i_1}$, then do not include the pair $(i_1 + 1, j_{i_1+1})$ in $\mathcal{P}_J$ because $p^{i_1+1}X^{j_{i_1+1}}$ is a multiple of $p^{i_1}X^{j_1}$. Hence the pair (i_2, j_2) among the pairs in A will be in $\mathcal{P}_J$ if and only if i_2 is the first integer after i_1 such that $j_2 < j_1$. And so on.

Definition 1. Let us call the element of the form pX^r a *pxr form.*

By using something similar to the Euclidean algorithm on $\mathbb{Z}_{p^a}[X]$ we will show that if the ideal J is not contained in the ideal (p) generated by p in S, then J is generated by elements of the pxr forms in Proposition 2 and polynomials of the form $X^k + ph(X)$. The following proposition and theorem are easy generalizations over $\mathbb{Z}_{p^a}$ of corresponding assertions in [8, 9] and their proofs are carried out with *mutatis mutandis.*

Proposition 3. *Let S be as before. Let J be a nonzero ideal of S which is not contained in the ideal (p). Then there are nonzero elements of the form $X^k + ph(X)$ where $h \in S$ of degree $< k$.*

Proof. If $f(X) = \sum_{i<m} a_i X^i$ is a nonzero polynomial in J with a_0 a unit, then f is a unit since $X \in S$ is nilpotent, i.e., J is the unit ideal.

Hence we may assume there is $f(X) = \sum_{i=0}^{m-1} a_i X^i \in J$ such that a_0 is a multiple of p. If the coefficients of every $f(X) = \sum_{i=0}^{m-1} a_i X^i \in J$ are divisible by p, then $J \subset (p)$ which is a contradiction. Thus we may assume there is $f(X) = \sum_{i=0}^{m-1} a_i X^i \in J$ such that a_0 is divisible by p and a_j is a unit for some $j > 0$. Let a_i be the unit coefficient of the lowest degree, i.e., $a_{i-1}, a_{i-2}, \dots$ are in $p\mathbb{Z}_{p^a}$. Let l be the smallest integer such that $X^l = 0$. Then $X^{l-i-1} f(X)$ is a desired form after multiplying a unit if necessary. □

Definition 2. The polynomials of the form

$$g(X) = X^k + pa_h X^h + pa_{h-1} X^{h-1} + \cdots + pa_0$$

with $a_h, a_{h-1}, \dots, a_0 \in \mathbb{Z}_{p^a}$ will be called an *xkp form.*

We will prove something similar to the Euclidean algorithm on $\mathbb{Z}_{p^a}[X]$. Let us agree that the degree of the zero polynomial is $-\infty$ and $X^k = 0$ if $k = -\infty$.

Theorem 1 (Euclidean algorithm modulo p^a). *Let J be an ideal of S which is not contained in the ideal (p) generated by $p \in S$. Suppose that $g(X) = X^k + ph(X)$ is an xkp form of the least degree in J. Then for $f(X) = \sum_{i<m} a_i X^i$ in J, we can write uniquely*

$$f(X) = g(X)q(X) + r(X)$$

with $q(X), r(X) \in S$, $\deg(r) < k$ and $r(X) \in p\mathbb{Z}_{p^a}[X]$.

Proof. Since g is monic, we can write $f = gq + r$ for some $r \in S$ with $\deg(r) < \deg(g) = k$ uniquely by Euclidean algorithm over a commutative ring. We need to prove that the coefficients of $r(X)$ are in $p\mathbb{Z}_{p^a}$.

Assume that this is not true. If the coefficient of the lowest degree term is a unit, then $r(X)$ is of the form $X^i \cdot$(unit) with $i < k$ since X is nilpotent. Hence $X^i \in J$ with $i < k$. But this contradicts to the fact that $g(X) = X^k + ph(X)$ is of lowest degree.

Hence we may assume that the coefficient of the lowest degree term is p say, $r(X) = a_j X^j + a_{j-1} X^{j-1} + \cdots + pa_l X^l$ with $j < k$ and $a_j \neq 0$. Let $a_s X^s$ be the lowest degree term with a unit a_s, that is, $a_{s-1}, a_{s-2}, \dots \in p\mathbb{Z}_{p^a}$. If $s = j$, then $a_s^{-1} r(X)$ is an xkp form which is of lower degree than $g(X)$ which is a contradiction.

Then we see that $X^{k-j} r(X) - a_j g(X) \in J$ is a polynomial of degree $< k$ in which the divisibility of the coefficients of $X^{s+k-j-1}, X^{s+k-j-2}, \dots$ by p remain the same as those of $a_{s-1}, a_{s-2}, \dots$ since the coefficient of terms of degree $< k$ in $a_j g(X)$ is in $p\mathbb{Z}_{p^a}$.

Let $ph(X) = \sum_i ph_i X^i$. If the coefficients of $X^{k-1}, X^{k-2}, \dots, X^{s+k-j+1}$ in $X^{k-j} r(X) - a_j g(X)$ happen to vanish namely, $X^{k-j} r(X) - a_j g(X) = (a_s + pa_j h_s) X^{s+k-j} + (a_{s-1} + pa_j h_{s-1}) X^{s+k-j-1} + \cdots + (p + pa_j h_l) X^l$. Then $a_s + pa_j h_s$ is a unit and $a_{s-i} + pa_j h_{s-i} \in p\mathbb{Z}_{p^a}$ for $i \geq 1$. But this gives us an element

in J whose degree is lower than $g(X)$ after multiplying some unit if necessary. This is a contradiction.

If this is not the case, then we can repeat the same process until all the coefficients of the terms but the last $(s-l)$ terms vanish without changing the divisibility by p of the coefficients of the last $(s-l)$ terms to get an element of J with degree $< \deg(X^{k-j}r(X) - a_j g(X))$. Then, the resulting element is obviously an xkp form which is smaller than $g(X)$ belonging to J. □

Let J be a nonzero ideal of S which is not contained in (p). Choose an xkp form $g(X) = X^k + ph(X) \in J$ with $h(X) \in S$, $\deg(h) < k$ of the lowest degree. We will show that J is generated by $g(X)$ and $p^i X^j$'s in Proposition 2.

As before, we let S is of the form $\mathbb{Z}_{p^a}/(\alpha(X))$ where $\alpha(X) \in \mathbb{Z}_{p^a}[X]$ is of the form $X^m + ph(X)$.

Theorem 2. *Let J be an ideal of S which is not contained in (p). Let $g(X) = X^k + ph(X)$ be an xkp form of the lowest degree in J. Then there are $\{p^{i_1}X^{j_1}, p^{i_2}X^{j_2}, \ldots, p^{i_r}X^{j_r}\}$ such that*

$$J = (g(X), p^{i_1}X^{j_1}, p^{i_2}X^{j_2}, \ldots, p^{i_r}X^{j_r}),$$

where $i_1 < i_2 < \cdots < i_r$, $j_1 > j_2 > \cdots > j_r$ and $-\infty \le j_s < l$ $(s = 1, 2, \ldots, r), r < a$. In particular, any ideal of S can be generated by at most a elements.

Proof. Let $g(X) = X^k + ph(X) \in J$ be an xkp form of the lowest degree in J. Then by Theorem 1, every $f(X) \in J$ can be written as $f = qg + r$ with $r \in p\mathbb{Z}_{p^a}[X]$. Let J' be the set of all remainders of elements of J upon division by g. Then it is easy to show that J' is an ideal of S contained in (p). By Proposition 2, $J' = (p^{i_1}X^{j_1}, p^{i_2}X^{j_2}, \ldots, p^{i_r}X^{j_r})$. Now it is obvious that $J = (g(X), p^{i_1}X^{j_1}, p^{i_2}X^{j_2}, \ldots, p^{i_r}X^{j_r})$. □

If $a = 2$, then an ideal of S is generated by at most two elements. Hence we have the following simple result.

Corollary. *Let $S = \mathbb{Z}_{p^2}/(\alpha(X))$ and J be an ideal of S. If $g(X) \in J$ be an xkp form of the lowest degree and pX^r is the pxr form of the lowest degree, then $J = (g(X), pX^r)$.*

Even though the Eisenstein's Irreducibility Criterion is usually stated over a unique factorization domain the same proof works for the polynomials over $\mathbb{Z}_{p^a}$.

Theorem 3 (Eisenstein's Criterion over $\mathbb{Z}_{p^a}$). *Let $f(X) = \sum_{i=0}^{n} a_i X^i$ be a polynomial in $\mathbb{Z}_{p^a}[X]$ $(a \ge 2)$. Suppose*

$$p^2 \nmid a_0, \quad p | a_i \ (i = 0, \ldots, (n-1)) \quad \text{and} \quad p \nmid a_n.$$

Then f is irreducible in $\mathbb{Z}_{p^a}[X]$.

Proof. Suppose f is reducible; $f = gh$ with $g = s_l X^l + \cdots + s_0$ and $h = t_m X^m + \cdots + t_0$. Since $p|a_0 = s_0 t_0$ and $p^2 \nmid a_0$ only one of s_0 or t_0 is divisible by p, say $p \nmid s_0$ and $p|t_0$. Also since $p \nmid a_n = s_l t_m$, we see that $p \nmid t_m$. Let t_i $(i < n)$ be the coefficient of the lowest degree term such that $p \nmid t_i$. Then since

$$a_i = s_0 t_i + s_1 t_{i-1} + \cdots ,$$

and since $p \nmid s_0 t_i$ and $p|(s_1 t_{i-1} + \cdots)$ we have $p \nmid a_i$, which is a contradiction. □

Corollary. *Every xkp form whose nonzero constant term is not divisible by p^2 in $\mathbb{Z}_{p^a}[X]$ $(a \geq 2)$ is irreducible.*

3. Cyclic codes of length p^n over $\mathbb{Z}_{p^a}$

A *cyclic code* over $\mathbb{Z}_{p^a}$ is an ideal of $\mathbb{Z}_{p^a}[X]/(X^{p^n} - 1)$. To deal with the polynomial $X^{p^n} - 1 \in \mathbb{Z}_{p^a}$, we will need some combinatorial facts.

For a rational number k, let us write $v_p(k) = n$ if $k = p^n \alpha$ with α a quotient of integers which are prime to p. The following combinatorial fact may be well known.

Proposition 4. *For an odd prime p, let $X_i = \{p^{n-i}, 2p^{n-i}, \ldots, (p-1)p^{n-i}\}$, $(1 \leq i < a)$ be a subset of $\mathbb{Z}_{p^n}$. Then for $n \geq 2, a \leq n$ and for a positive integer r with $0 \leq r \leq p^n$ we have*

$$\binom{p^n}{r} \equiv \begin{cases} 1 & (\mathrm{mod}\ p^a)\ \textit{if}\ \ r = 0,\ p^n \\ (-1)^j j^{-1} p^i & (\mathrm{mod}\ p^a)\ \textit{if}\ \ r = jp^{n-i} \in X_i, 1 \leq i < a \\ 0 & (\mathrm{mod}\ p^a)\ \textit{otherwise}, \end{cases}$$

where j^{-1} is taken in $\mathbb{Z}_{p^a}$.

If $p = 2$, we have

$$\binom{2^n}{r} \equiv \begin{cases} 1 & (\mathrm{mod}\ 2^a)\ \textit{if}\ \ r = 0,\ 2^n \\ 2^i & (\mathrm{mod}\ 2^a)\ \textit{if}\ \ r = 2^{n-i}, 1 \leq i < a \\ 0 & (\mathrm{mod}\ 2^a)\ \textit{otherwise.} \end{cases}$$

Proof. We recall

$$\binom{p^n}{r} = \frac{p^n (p^n - 1)(p^n - p) \cdots (p^n - r + 1)}{1 \cdot 2 \cdots r}.$$

If $r = 0$ or $r = p^n$, then our result is obvious. Now we rewrite

$$(\dagger) \qquad \binom{p^n}{r} = \frac{(p^n - 1)}{1} \cdot \frac{(p^n - 2)}{2} \cdots \frac{(p^n - (r-1))}{r-1} \cdot \frac{p^n}{r}.$$

Note that for any $k < p^n$ the power of p in k is the same as the power of p in $p^n - k$, i.e., $v_p(k) = v_p(p^n - k)$. On the other hand, $p^n - k \equiv -k \pmod{p^a}$ for $1 \leq k \leq (r-1)$. First suppose p is odd. Then we have $\binom{p^n}{r} \equiv (-1)^{jp^{n-i}} \frac{p^n}{r} \equiv (-1)^j \frac{p^n}{jp^{n-i}} \equiv (-1)^j j^{-1} p^i \pmod{p^a}$.

Now suppose $p=2$. Then for $r=0$ or $r=2^n$ our result is obvious. For $0<r<2^n$ we see that $\binom{p^n}{r}$ is nonzero only when $r=2^i(1\le i<a)$ by looking at (†) and the sign is positive. □

We record the special case, when $a=2$ for later use.

Corollary. *Let p be an odd prime. Let $X=\{p^{n-1},2p^{n-1},\dots,(p-1)p^{n-1}\}$. For $n\ge 2$ and a positive integer r with $0\le r\le p^n$, we have*

$$\binom{p^n}{r}\equiv\begin{cases}1 & (\mathrm{mod}\ p^2)\ \textit{if}\ \ r=0,\ p^n\\ (-1)^j j^{-1}p & (\mathrm{mod}\ p^2)\ \textit{if}\ \ r=jp^{n-1}\in X\\ 0 & (\mathrm{mod}\ p^2)\ \textit{otherwise},\end{cases}$$

where j^{-1} is taken in $\mathbb{Z}_{p^2}$.

If $p=2$, we have

$$\binom{2^n}{r}\equiv\begin{cases}1 & (\mathrm{mod}\ 4)\ \textit{if}\ \ r=0,\ 2^n\\ 2 & (\mathrm{mod}\ 4)\ \textit{if}\ \ r=2^{n-1}\\ 0 & (\mathrm{mod}\ 4)\ \textit{otherwise}.\end{cases}$$

Theorem 4. *Let p be prime and let $X^{p^n}-1\in\mathbb{Z}_{p^a}[X](n\ge a\ge 2)$. Let $h(T)$ and $\bar{h}(T)$ be the polynomials in $\mathbb{Z}_{p^a}[T]$ defined by*

$$h(T)=\begin{cases}\displaystyle\sum_{\substack{1\le j<p\\ 1\le i<a}}(-1)^j j^{-1}p^{i-1}T^{jp^{n-i}} & \textit{if } p \textit{ is odd}\\ \displaystyle\sum_{1\le i<a}2^{i-1}T^{2^{n-i}} & \textit{if } p=2\end{cases}$$

and $T^{p^{n-a+1}}\bar{h}(T)=h(T)$. Then we have the decomposition

$$(*)\qquad X^{p^n}-1=(X-1)^{p^{n-a+1}}\left((X-1)^{p^n-p^{n-a+1}}+p\bar{h}(X-1)\right).$$

Furthermore, if $a=2$, then the decomposition $(*)$ above are product of irreducible polynomials.

Proof. First suppose p is odd. Then by Proposition 4, we have

$$\begin{aligned}X^{p^n}&=((X-1)+1)^{p^n}\\ &=(X-1)^{p^n}+\sum_{\substack{1\le j<p\\ 1\le i<a}}(-1)^j j^{-1}p^i(X-1)^{jp^{n-i}}+1.\end{aligned}$$

Hence we have

$$X^{p^n}-1=(X-1)^{p^n}+\sum_{\substack{1\le j<p\\ 1\le i<a}}(-1)^j j^{-1}p^i(X-1)^{jp^{n-i}}.$$

Now the coefficients of the last term is divisible by p. Hence we can define a polynomial $\bar{h}(T)$ by

$$\frac{(X^{p^n}-1)-(X-1)^{p^n}}{(X-1)^{p^{n-a+1}}}=p\cdot\bar{h}(X-1).$$

Hence we have decomposition $(*)$.

If $p = 2$ we can be proved similarly and we omit its proof.

When $a = 2$, irreducibility of the second factor in $(*)$ follows from the corollary of the Eisenstein Criterion. □

Corollary. *With the same notations of Theorem 4, we have an isomorphism*

$$\psi : \mathbb{Z}_{p^a}[X]/(X^{p^n} - 1) \ \to \ \mathbb{Z}_{p^a}[T]/(T^{p^n} + ph(T))$$

of rings which maps $f(X)$ to $f(T+1)$. The inverse of ψ maps $f(T)$ to $f(X-1)$.

Proof. Simply make a substitution $T = X - 1$. □

Remark. (1) We note that the ring $S = \mathbb{Z}_{p^a}[T]/(T^{p^n} + ph(T))$ is a finite local ring with the maximal ideal $\mathfrak{m} = (p, T)$ and is generated by the canonical image t of T in S which is nilpotent, namely $t^{ap^n} = 0$.

(2) For $a > 2$, the polynomials $T^{p^n - p^{n-a+1}} + p\bar{h}(T) \in \mathbb{Z}_{p^a}[T]$ are not irreducible. For example, if we take $p = 2, a = 3$, then

$$T^{3\cdot 2^{n-2}} + 2T^{2^{n-1}} + 4 = (T^{2^{n-2}} - 2)(T^{2^{n-1}} + 2T^{2^{n-2}} - 2)$$

is a factorization into irreducible polynomials in $\mathbb{Z}_8[T]$, say by Eisenstein's Criterion. It appears that there is no simple way to factor the polynomial $T^{p^n - p^{n-a+1}} + p\bar{h}(T) \in \mathbb{Z}_{p^a}[T]$ into irreducible polynomials, in general.

Example. Let $p^n = 3^6 = 729$. Consider $X^{729} - 1 \in \mathbb{Z}_9[X]$. By Theorem 4, we see

$$\begin{aligned} X^{3^6} - 1 &= (X-1)^{3^6} + 3(X-1)^{2\cdot 3^5} + 3(X-1)^{3^5} \\ &= (X-1)^{3^5}\left((X-1)^{2\cdot 3^5} + 3(X-1)^2 + 3\right). \end{aligned}$$

Hence the irreducible divisors of $X^{729} - 1 \in \mathbb{Z}_9[X]$ are

$$(X-1)^{2\cdot 3^5} + 3(X-1)^2 + 3 \text{ and } (X-1).$$

For later use we record the special case when $a = 2$. Now suppose p is an odd prime. Then for $n \geq 2$, we have

$$X^{p^n} - 1 = (X-1)^{p^n} + p\left(\sum_{j=1}^{p-1}(-1)^j j^{-1}(X-1)^{jp^{n-1}}\right)$$

in $\mathbb{Z}_{p^2}[X]$ by Corollary to Proposition 4. Hence we obtain the following result.

Proposition 5. *Let p be a prime and let $X^{p^n} - 1 \in \mathbb{Z}_{p^2}[X]$ $(n \geq 2)$. Let $h(T) \in \mathbb{Z}_{p^2}[T]$ be the polynomial defined by*

$$h(T) = \begin{cases} \sum_{j=1}^{p-1}(-1)^j j^{-1} T^{jp^{n-1}} & \text{if } p \text{ is odd} \\ T^{2^{n-1}} & \text{if } p = 2, \end{cases}$$

where j^{-1} is taken in $\mathbb{Z}_{p^2}$. Then we have

$$\begin{aligned} X^{p^n}-1 &= (X-1)^{p^n}+ph(X-1) \\ &= (X-1)^{p^{n-1}}\left((X-1)^{(p-1)p^{n-1}}+p\bar{h}(X-1)\right), \end{aligned}$$

where $\bar{h}(T)$ is defined by $T^{p^{n-1}}\bar{h}(T)=h(T)$. The latter factorization is into monic irreducible polynomials. Also we have an isomorphism

$$\mathbb{Z}_{p^2}[X]/(X^{p^n}-1)\to\mathbb{Z}_{p^2}[T]/(T^{p^n}+ph(T))$$

sending $f(X)$ to $f(T+1)$.

By finding the irreducible factors of $X^{p^n}-1$, we can characterize free cyclic codes over $\mathbb{Z}_{p^a}$ of length p^n [7, Theorem 2, Theorem 3].

Theorem 5 ([7])**.** *Let $T=\mathbb{Z}_{p^a}$. Let C be a cyclic code of length m over T. Then C is T-free if and only if there is a polynomial g such that $g|(X^m-1)$ that generate C. In this case, we have* $\operatorname{rank}_T(C)=m-\deg(g)$.

Corollary. *Let C be a cyclic code of length p^n over $T=\mathbb{Z}_{p^a}$. Then C is T-free if C is generated by a polynomial g of a product of the following form*

$$\frac{(X^{p^n}-1)}{(X-1)^{p^{n-a+1}}} \text{ and } (X-1)^r \ (r=0,1,\dots,p^n).$$

If $a=2$, then these are only free cyclic codes. In this case, we have $\operatorname{rank}_T(C)=p^n-\deg(g)$.

Proof. Immediately follows from Theorem 4 and Theorem 5 □

4. Annihilating polynomials of the cyclic codes over $\mathbb{Z}_{p^2}$ and the duality

From the previous sections we know that the cyclic codes length p^n over $\mathbb{Z}_{p^2}$ is generated by at most two elements. The purpose of this section is to identify the dual of the cyclic codes length p^n over $\mathbb{Z}_{p^2}$. We assume p is an odd prime since the case $p=2$ was worked out in [8].

In this section, we let $S=\mathbb{Z}_{p^2}[T]/(\alpha(T))$ with

$$\alpha(T)=T^{pl}+\sum_{j=1}^{p-1}(-1)^j j^{-1}pT^{jl},$$

where i^{-1} is taken in $\mathbb{Z}_{p^2}$ and $l=p^{n-1}$.

Also we let

$$h(T)=\sum_{j=1}^{p-1}(-1)^j j^{-1}T^{jl}=u(T)T^l$$

with $u(T)=-1+2^{-1}T^l-\cdots+(p-1)^{-1}T^{(p-1)l}$ which is a unit in S. Therefore $T^{lp}=-pu(T)T^l$ in S.

Recall the annihilator $\mathrm{Ann}(I)$ of an ideal I of a commutative ring R is given by

$$\mathrm{Ann}(I) = \{r \in R | rx = 0 \text{ for all } x \in I\}.$$

To find the annihilator of an ideal I of S, we will find xkp form and pxr form which annihilates the generators of I in the 'most economical' way. It will turn out that they generates the ideal $\mathrm{Ann}(I)$ as well as the dual of the cyclic codes generated by the ideal I.

Proposition 6. *Let $S = \mathbb{Z}_{p^2}[T]/(\alpha(T))$. Then the annihilator of the ideal (pT^r) is given by (T^{pl-r}, p).*

Proof. By Corollary to Theorem 2, we need to find an xkp and pxr forms of the lowest degree which annihilate pT^r. Now we have $T^{pl-r}(pT^r) = pT^{pl} = 0$ and $p(pT^r) = 0$. It is clear that T^{pl-r} is an xkp form of the lowest degree which annihilates $g(T)$ and p is a pxr form of the lowest degree which annihilates pT^r. □

We will use the following notation for the rest of this section:

$$\begin{aligned} g(T) &= T^k + pa_hT^h + \cdots + pa_1T + pa_0 \ (h < k < pl,\ a_i \in \mathbb{Z}_{p^2}) \\ T^{pl-k}g(T) &= pb_{h_1}T^{h_1} + \cdots + pb_{h_t}T^{h_t} \qquad (b_{h_i} \in \mathbb{Z}_{p^2}^*) \end{aligned}$$

where $\mathbb{Z}_{p^2}^*$ denotes the units in $\mathbb{Z}_{p^2}$ and $h_i > h_{i+1}$. For a polynomial $f(T)$ we denote $\deg_L(f(T))$ to be the degree of the nonzero term in $f(T)$ of the lowest degree. Hence $h_t = \deg_L(T^{pl-k}g(T))$.

Theorem 6. *Let $S = \mathbb{Z}_{p^2}[T]/(\alpha(T))$ and let $g(T) \in S$. Then the annihilator $\mathrm{Ann}(g(T))$ of the ideal generated by $g(T)$ is given by the following*:

(i) *if $h_t \geq k$, then $\mathrm{Ann}(g(T)) = (g_1^\perp(T))$ where*

$$g_1^\perp(T) = T^{pl-k} - pb_{h_1}T^{h_1-k} - \cdots - pb_{h_t}T^{h_t-k}.$$

(ii) *if $h_t \leq k$, then $\mathrm{Ann}(g(T)) = (g_2^\perp(T), pT^{pl-k})$ where $g_2^\perp(T)$ is given by*

$$g_2^\perp(T) = T^{pl-h_t} - pb_{h_1}T^{h_1-h_t} - \cdots - pb_{h_t}.$$

Proof. We need to find an xkp form $T^a + ph'(T)$ of the lowest degree such that $T^a g(T) = ph'(T)g(T)$. Hence we need to find the smallest a such that $T^a g(T) \in p\mathbb{Z}_{p^2}[T]$ and $\deg_L(T^a g(T)) \geq k$.

(i) If $h_t \geq k$, then obviously $a = pl - k$ is the smallest such that $T^a g(T)$ belongs to $p\mathbb{Z}_{p^2}[T]$. And since $h_t \geq k$, we see that

$$\begin{aligned} T^{pl-k}g(T) &= pb_{h_1}T^{h_1} + \cdots + pb_{h_t}T^{h_t} \\ &= (pb_{h_1}T^{h_1-k} + \cdots + pb_{h_t}T^{h_t-k})g(T). \end{aligned}$$

Therefore we see that $g_1^\perp(T)$ is an xkp form of the lowest degree that annihilates $g(T)$.

A pxr form of the lowest degree that annihilates $g(T)$ is pT^{pl-k} but it already belongs to the ideal $(g_1^\perp(T))$. Therefore $\mathrm{Ann}(g(T)) = (g_1^\perp(T))$.

(ii) Now suppose $h_t \le k$. Then we have

$$\begin{aligned} T^{(pl-k)+(k-h_t)}g(T) &= pb_{h_1}T^{k+h_1-h_t} + \cdots + pb_{h_t}T^k \\ &= (pb_{h_1}T^{h_1-h_t} + \cdots + pb_{h_t})g(T). \end{aligned}$$

Hence $g_2^{\perp}(T)g(T) = 0$ and $g_2^{\perp}(T)$ is an xkp form of the lowest degree that annihilates $g(T)$.

On the other hand, we have $pT^{pl-k}g(T) = 0$ and pT^{pl-k} is a pxr form of the lowest degree that annihilates $g(T)$. Therefore we see $\mathrm{Ann}(g(T))$ is given by $(g_2^{\perp}(T), pT^{pl-k})$. □

Remark. Consider the ideal $I = (g(T), pT^r)$. Then we may assume that $k \ge r$ and $h_t \ge r$. In fact, if $k < r$, then we can write $pT^r = pT^{r-k}g(T)$ and hence $I = (g(T))$. Also, we may assume $h_t \ge r$. For otherwise we have $T^{pl-k}g(T) = pT^{h_t}(b_1T^{h_1-h_t} + \cdots + b_t) \in (g(T))$ where $(b_1T^{h_1-h_t} + \cdots + b_t)$ is a unit and $h_t < r$. Hence $pT^r \in (g(T))$.

Theorem 7. *Let $S = \mathbb{Z}_{p^2}[T]/(\alpha(T))$, $g(T) \in S$ as before. Let $I = (g(T), pT^r)$ with $k \ge r$ and $h_t \ge r$. Then the annihilator* $\mathrm{Ann}(I)$ *of the ideal is given by the following*:

(i) *if $h_t \ge k$, then* $\mathrm{Ann}(I) = (T^{k-r}g_1^{\perp}(T), pT^{pl-k})$ *where $g_1^{\perp}(T)$ is given in Theorem 6.*

(ii) *if $h_t \le k$, then* $\mathrm{Ann}(I) = (T^{h_t-r}g_2^{\perp}(T), pT^{pl-k})$ *where $g_2^{\perp}(T)$ is given in Theorem 6.*

Proof. (i) Suppose $h_t \ge k$. We saw in the proof of Theorem 6 that $g_1^{\perp}(T)$ is an xkp form of the lowest degree that annihilates $g(T)$. However the lowest degree xkp form that annihilates pT^r as well will be $T^{k-r}g_1^{\perp}(T)$.

A pxr form of the lowest degree that annihilates $g(T)$ as well as pT^r is pT^{pl-k}. Therefore $\mathrm{Ann}(I) = (T^{k-r}g_1^{\perp}(T), pT^{pl-k})$.

(ii) Now suppose $h_t \le k$. We saw in the proof of Theorem 6 that $g_2^{\perp}(T)$ is an xkp form of the lowest degree that annihilates $g(T)$. However the lowest degree xkp form that annihilates pT^r as well will be $T^{h_t-r}g_2^{\perp}(T)$.

A pxr form of the lowest degree that annihilates $g(T)$ as well as pT^r is pT^{pl-k}. Therefore $\mathrm{Ann}(I) = (T^{h_t-r}g_2^{\perp}(T), pT^{pl-k})$. □

We will count the number of elements in the cyclic codes. Let

$$g(T) = T^k + pa_hT^h + pa_{h-1}T^{h-1} + \cdots + pa_0 \ (h < k)$$

with $a_h, a_{h-1}, \ldots, a_0 \in \mathbb{Z}_{p^2}$. For each basis element $\{1, T, \ldots, T^{pl-1}\}$ (in this order) of S express $T^ig(T)$ as a linear combination of the basis $\{T^{pl-1}, \ldots, T, 1\}$ (in this order) of S. Then its matrix expression is of the form

$$G = \begin{pmatrix} A & B \\ C & D \end{pmatrix},$$

where A is a $(pl-k)\times(pl-k)$ matrix of the form

$$A=\begin{pmatrix}0&\cdots&\cdots&1\\0&\cdots&1&*\\0&\cdot&*&*\\1&*&*&*\end{pmatrix}$$

with 1's on the opposite diagonal and $*$'s below the opposite diagonals which consist of the elements of $p\mathbb{Z}_{p^2}$. The matrix B is of size $(pl-k)\times k$ over $p\mathbb{Z}_{p^2}$ and C is a $k\times(pl-k)$ matrix over $p\mathbb{Z}_{p^2}$.

And D is a $k\times k$ matrix of the form

$$D=\begin{pmatrix}*&*&\cdots&pb_{h_t}&0&\cdots&0\\&\cdots&pb_{h_t}&0&\cdots\cdots&&0\\*&\cdot&0&\cdots\cdots\cdots\cdots&&&0\\pb_{h_t}&0&0&\cdots\cdots\cdots\cdots&&&0\\0&0&0&\cdots\cdots\cdots\cdots&&&0\\&&\cdots\cdots\cdots\cdots\cdots\cdots&&&&\\0&0&\cdots\cdots\cdots\cdots\cdots\cdots&&&&0\end{pmatrix},$$

where $*$'s are in $p\mathbb{Z}_{p^2}$ and b_{h_t} is a unit. Hence the upper left corner of D is a square matrix whose opposite diagonals are multiples of p.

The moral is that adding a constant multiple of a row to another one does not change the submodule generated by the rows.

We consider two cases. The first case is when $D=0$. This is equivalent to $\deg_L(T^{pl-k}g(T))\geq k$. The second case we consider is when $D\neq 0$. This is equivalent to that $\deg_L(T^{pl-k}g(T))<k$.

Theorem 8. *Let $S=\mathbb{Z}_{p^2}[T]/(\alpha(T))$ and let $g(T)\in S$. Then the ideal I generated by $g(T)$ is isomorphic, as $\mathbb{Z}_{p^2}$-modules, to the following*:

(i) *if $h_t\geq k$, then I is $\mathbb{Z}_{p^2}$-free of rank $(pl-k)$,*

(ii) *if $h_t\leq k$, then I is isomorphic to the sum of $(pl-k)$ copies of $\mathbb{Z}_{p^2}$ and $(k-h_t)$ copies of $\mathbb{Z}_p$.*

Proof. (i) Suppose $h_t\geq k$. Then we have $D=0$. And in this case, the number of 1's is $pl-k$. And, using these 1's, we can get rid of multiples of p's in C. Hence the ideal generated by $g(T)$ is free over $\mathbb{Z}_{p^2}$ of rank $pl-k$.

(ii) Now suppose $h_t<k$. As before, we can make all entries below the 1's on the opposite diagonal of A. Also we can get rid of multiples p's in C without changing D since the entries in B and C are the multiples of p. We can get rid of all entries above the pb_{h_t} on the opposite diagonal of a square matrix on the upper left corner of D. It is clear that the ideal generated by the rows is isomorphic to the sum of $(pl-k)$ copies of $\mathbb{Z}_{p^2}$ which correspond to the 1's in A and $s-k$ copies of $\mathbb{Z}_p$ which correspond to pb_{h_t}'s in D. □

Proposition 7. *Let $S=\mathbb{Z}_{p^2}[T]/(\alpha(T))$. Then the ideal (pT^r) generated by pT^r is isomorphic to $(pl-r)$ copies of $\mathbb{Z}_p$.*

Proof. It is easy to show and we omit its proof. □

Theorem 9. *Let $S=\mathbb{Z}_{p^2}[T]/(\alpha(T))$ and let $g(T)\in S$. Let $I=(g(T),pT^r)$ be the ideal generated by $g(T)$ and pT^r with $k\geq r$ and $h_t\geq r$. Then the ideal I is isomorphic, as $\mathbb{Z}_{p^2}$-modules, to $(pl-k)$ copies of $\mathbb{Z}_{p^2}$ and $k-r$ copies of $\mathbb{Z}_p$.*

Proof. The generator matrix for $(g(T),pT^r)$ is

$$G=\begin{pmatrix} A & B \\ C & D \\ F_1 & F_2 \end{pmatrix},$$

where $F=(F_1,F_2)$ is a matrix of the same form as D of size $(pl-r)\times pl$.

If $h_t\geq k$, then $D=0$. And using 1's in A we get rid of all entries below the 1's in A. The number of p's in F_2 is $k-r$ which gives the $k-r$ copies of $\mathbb{Z}_p$.

Now if $h_t\leq k$, then the number of pb_{h_t}'s in the opposite diagonal of D is $(k-h_t)$ and the number of p's in the opposite diagonal of F_2 is $(k-r)$. Since we assumed $h_t\geq r$ we see $k-r\geq k-h_t$. Now it is easy to see that the p's in F_2 contribute to the factor of $k-r$ copies of $\mathbb{Z}_p$. □

We want to identify the dual of the cyclic code corresponding to the ideal I is the cyclic code of the ideal corresponding to the ideal $\mathrm{Ann}(I)$. Let C (resp. C') be the cyclic code corresponding to the ideal I (resp. $\mathrm{Ann}(I)$). To show $C'=C^\perp$ we need to show $C'\imath C^\perp$ and C' has the right number of elements as given by the lemma below.

Lemma 3. *Let C be a $\mathbb{Z}_{p^2}$-submodule of $\mathbb{Z}_{p^2}^n$. Define*

$$C^\perp=\{b\in\mathbb{Z}_{p^2}^n \mid a\cdot b=0 \text{ for all } a\in C\},$$

where $a=(a_1,\ldots,a_n), b=(b_1,\ldots,b_n)$ and $a\cdot b=a_1b_1+\cdots+a_nb_n$. Then the number of elements of C is of the form $\#C=(p^2)^{k_1}p^{k_2}$ and then $\#C^\perp=(p^2)^{n-k_1-k_2}p^{k_2}$.

Proof. By the classification of finite abelian groups we may assume C is isomorphic to $(\mathbb{Z}_{p^2})^{k_1}\times(\mathbb{Z}_p)^{k_2}$. Now it is easy to show that $C^\perp$ is isomorphic to the abelian group $(\mathbb{Z}_{p^2})^{n-k_1-k_2}\times(\mathbb{Z}_p)^{k_2}$. □

Proposition 8. *Let $S=\mathbb{Z}_{p^2}[T]/(\alpha(T))$. Let C be the cyclic code generated by pT^r. Then the dual $C^\perp$ is given by the ideal (T^{pl-r},p).*

Proof. We see that the number of elements of C is p^{pl-r} by Proposition 7. It is obvious that T^{pl-r} and p annihilates pT^r. By Theorem 9, the number of elements in the ideal (T^{pl-r},p) is $(p^2)^r p^{pl-r}$. Now that is the right number of elements for the dual. □

Theorem 10. *Let $S=\mathbb{Z}_{p^2}[T]/(\alpha(T))$. Let $g(T)\in S$ be as before. Let C be the cyclic code generated by $g(T)$ then the dual $C^\perp$ is generated by;*

(i) *if $h_t\geq k$, then $C^\perp$ is generated by $g_1^\perp(T)$ where $g_1^\perp$ is given in Theorem 6.*

(ii) *if $h_t\leq k$, then $C^\perp$ is generated by $g_2^\perp(T)$ and pT^{pl-k} where $g_2^\perp$ is given in Theorem 6.*

Proof. (i) Suppose $h_t \geq k$. Since we know that $g_1^{\perp} g = 0$ we need to check that $(g_1^{\perp}(T))$ has the right number of elements. By Theorem 9, we have $\#(g_1^{\perp}(T)) = (p^2)^k$. On the other hand, $\#(g(T)) = (p^2)^{pl-k}$ as required.

(ii) Now suppose $k \geq h_t$. We need to count the number of elements of $(g_2^{\perp}(T), pT^{pl-k})$. First we have $\#(g(T)) = (p^2)^{pl-k}p^{k-h_t}$. On the other hand, $\#(g_2^{\perp}(T), pT^{pl-k}) = (p^2)^{pl-(pl-h_t)}p^{(pl-h_t)-(pl-k)} = (p^2)^{h_t}p^k$ by Theorem 9. As required. □

Theorem 11. *Let $S = \mathbb{Z}_{p^2}[T]/(\alpha(T))$. Let $g(T) \in S$ be as before. Let C be the cyclic code generated by the ideal $I = (g(T), pT^r)$ with $k \geq r$ and $h_t \geq r$ as before. Then the dual $C^{\perp}$ is generated by*

(i) *$T^{k-r}g_1^{\perp}(T)$ and pT^{pl-k} if $h_t \geq k$ where $g_1^{\perp}$ is given in Theorem 6.*

(ii) *$T^{h_t-r}g_2^{\perp}(T)$ and pT^{pl-k} if $h_t \leq k$ where $g_2^{\perp}$ is given in Theorem 6.*

Proof. (i) Suppose $h_t \geq k$. Since we know that $g_1^{\perp}g(T) = 0 = pT^{pl-k}g(T)$ we need to check that $(g_1^{\perp}(T), pT^{pl-k})$ has the right number of elements. By Theorem 9, we obtain $\#(T^{k-r}g_1^{\perp}(T), pT^{pl-k}) = (p^2)^r p^{k-r}$. On the other hand, $\#(g(T), pT^r) = (p^2)^{pl-k}p^{k-r}$ as required.

(ii) Now suppose $k \geq h_t$. Again we need to count the number of elements of $(T^{h_t-r}g_2^{\perp}(T), pT^{pl-k})$. First we have $\#(g(T), pT^r) = (p^2)^{pl-k}p^{k-r}$. On the other hand, $\#(T^{h_t-r}g_2^{\perp}(T), pT^{pl-k}) = (p^2)^{pl-(pl-r)}p^{(pl-r)-(pl-k)} = (p^2)^r p^{k-r}$ by Theorem 9. As desired. □

5. Cyclic codes of length $\lambda = p^n m$ over $\mathbb{Z}_{p^a}$ with $(p, m) = 1$

Let p be a prime and write $\lambda = p^n m$ with $(p, m) = 1$. When $p^a = 4$ we showed, in [6], how one can find the ideals of $\mathbb{Z}_4[X]/(X^{\lambda} - 1)$ from the ideals of $S' = \mathbb{Z}_4[X]/(X^{2^n} - 1)$ and the ideals of $S'[Y]/(Y^m - t)$. And we showed that the latter ring decomposes as a direct sum of the rings of the form $S'[X]/(f)$ in which every ideal comes from the ideals of S'. Since the same method as in [6] applies to our case, we will merely indicate how this can be done.

We first show that the ring $\mathbb{Z}_{p^a}[X]/(X^{\lambda} - 1)$ is isomorphic to the ring $S[Y]/(Y^m - x - 1)$ where $S = \mathbb{Z}_{p^a}[T]/(T^{p^n} - ph(T))$.

Theorem 12. *We have an isomorphism*

$$\mathbb{Z}_{p^a}[X]/(X^{\lambda} - 1) \to S[Y]/(Y^m - t - 1),$$

where $S = \mathbb{Z}_{p^a}[T]/(T^{p^n} - ph(T))$ and t denotes the canonical image of T in S.

Proof. Let $S' = \mathbb{Z}_{p^a}[\overline{T}]/(\overline{T}^{p^n} - 1)$. By letting $\overline{T} = X^m$, we can identify $\mathbb{Z}_{p^a}[X]/((X^m)^{p^n} - 1) = \mathbb{Z}_{p^a}[\overline{T}]/(\overline{T}^{p^n} - 1)[\sqrt[m]{\overline{T}}\,] = S'[\sqrt[m]{\overline{T}}\,]$. And we have an isomorphism

$$\alpha : S'[\sqrt[m]{\overline{T}}\,] \stackrel{\cong}{\to} S'[Y]/(Y^m - \bar{t}),$$

where $\bar{t}$ is the canonical image of T in S'. Composing α with the isomorphism

$$\psi : \mathbb{Z}_{p^a}[X]/(X^{p^n} - 1) \ \to \ \mathbb{Z}_{p^a}[T]/(T^{p^n} + ph(T))$$

of Corollary to Theorem 4, we have the desired isomorphism. □

As we remarked in §3, S is a finite local ring with the maximal ideal $\mathfrak{m} = (p, T)$ with characteristic a power of p. Recall some definitions on finite local rings [4]. Let $\mu : S \to S/\mathfrak{m}$ be the natural map and let $k = S/\mathfrak{m}$ be the residue field. A polynomial $f(Y) \in S[Y]$ is called *regular* if the coefficients of f generates the unit ideal of S. And f is called *basic irreducible* if $\mu(f) \in k[Y]$ is irreducible. Two polynomials $f(Y), g(Y) \in S[Y]$ are said to be *coprime* if there are $f_1(Y), g_1(Y)$ such that $f_1 f + g_1 g = 1$.

Proposition 9 ([6, Proposition 1])**.** *Let S be a finite ring of characteristic p and $u \in S$ be a unit. If m is prime to p, then the polynomial $f(X) = X^m - u$ in $S[X]$ can be written as a product of regular basic irreducible coprime polynomials.*

Since $(p, m) = 1$ and $t + 1 \in S$ is a unit, we see that $Y^m - t - 1 \in S[Y]$ can be factored into regular basic irreducible pairwise coprime polynomials $f_1, f_2, \ldots, f_r$. By the Chinese Remainder Theorem we see that

$$S[Y]/(Y^m - x - 1) \overset{\cong}{\to} \oplus_{i=1}^{r} S[Y]/(f_i).$$

Now we can generalize Lemma 2.1 of [4] in the following form.

Lemma 4 ([6, Lemma 4])**.** *Let S be a finite local ring. Let f be a basic irreducible in $S[T]$ and let $\pi : S \to S[T]/(f)$ be the natural map. If I is an ideal of $S[T]/(f)$, then there is an ideal J of S such that $I = \pi(J)$.*

Since f_i's are regular basic irreducible polynomials we see that the ideals of $S[Y]/(f_i)$ come from the ideals of S. By Theorem 2, we know how to find the ideals of S. Therefore we can find the ideals of $\mathbb{Z}_{p^a}[X]/(X^\lambda - 1)$.

Factorization of the polynomial $f(Y) = Y^m - t - 1$ into basic irreducible polynomials in $S[Y]$ is, in general, not so easy. However, if we reduce $f(Y)$ modulo the maximal ideal $\mathfrak{m}$, then we obtain $\bar{f}(Y) = Y^m - 1 \in \mathbb{F}_p[Y]$ and we can factor $\bar{f}(Y)$ rather easily by using the theory of finite fields.

Now, we recall some basic facts about roots of unity and cyclotomic polynomials over a finite fields from [5]. Let F be a field of characteristic $p > 0$ and m a positive integer. Let $F^{(m)}$ be the splitting field of $X^m - 1$ over F and μ_m be the set of roots of unity. If $(m, p) = 1$, then μ_m is a cyclic group of order m [5, p. 59]. Let ζ be a primitive m-th root of unity, i.e., a generator of μ_m. We define the *m-th cyclotomic polynomial* to be

$$Q_m(X) = \prod_{(s,m)=1} (X - \zeta^s).$$

Then it is well known that $Q_m(X) \in \mathbb{F}_p[X]$ is a polynomial of degree $\phi(m)$ where $\mathbb{F}_p$ is the field of p elements, i.e., the prime field of F.

Theorem 13 ([5, pp. 60–61])**.** *Let $F = \mathbb{F}_p$ be the field of p elements and m be a positive integer not divisible by p. Then*

(i) $X^m - 1 = \prod_{k|m} Q_k(X)$.

(ii) *Let d be the least positive integer such that $p^d \equiv 1 \mod m$. Then $Q_m(X)$ factors into $\phi(m)/d$ irreducible polynomials in $F[X]$ of degree d and $[F^{(m)} : F] = d$.*

Now, we can use the Hensel's Lemma to lift the factorization of the polynomial $Y^m - 1 \in \mathbb{F}_p[Y]$ to the factorization of $Y^m - t \in S'[Y]$. In [2, III.4.3], the Hensel's Lemma is stated in very general form. We adapt it for our purpose.

Hensel's Lemma [2]**.** *Let S be an Artin local ring with the maximal ideal $\mathfrak{m}$. Let $k = S/\mathfrak{m}$ be the residue field and $\mu : S \to k$ be the natural map. Let $P(X) \in S[X]$ be a polynomial. Let $g \in k[X]$ be a monic polynomial and $h(X) \in k[X]$ be a polynomial such that g, h are coprime. Suppose that $\mu(P) = g \cdot h$. Then there exist unique coprime polynomials $G, H \in S[X]$ such that $\mu(G) = g, \mu(H) = h$ and $P(X) = G(X)H(X)$ in $S[X]$.*

Using the isomorphism of Theorem 12, we apply these results with the Artin local ring $S' = \mathbb{Z}_{p^a}[\overline{T}]/(\overline{T}^{p^n} - 1)$ to find the ideals of $\mathbb{Z}_{p^a}[X]/(X^\lambda - 1)$.

Theorem 14. *Let $\lambda = p^n m$ with $n \geq 1$ and $(m, p) = 1$. For each divisor k of m let d_k be the smallest positive integer such that $p^{d_k} \equiv 1 \pmod{k}$. Then $Y^m - t - 1$ is a product of $r := \sum_{k|m} \frac{\phi(k)}{d_k}$ irreducible polynomials $\{f_1, f_2, \ldots, f_r\}$ in $S[Y]$ where $S = \mathbb{Z}_{p^a}[T]/(T^{p^n} - ph(T))$ $(n \geq a)$. Further, we have an isomorphism*

$$\mathbb{Z}_{p^a}[X]/(X^\lambda - 1) \overset{\cong}{\to} \oplus_{i=1}^r S[Y]/(f_i)$$

and the ideals of $S[Y]/(f_i)$ comes from the ideals of S which are generated by at most a elements.

Proof. By Theorem 13 and the Hensel's Lemma we have the required factorization of $Y^m - t - 1$. By Lemma 4, the ideals of $S[Y]/(f_i)$ comes form the ideals of S and by Theorem 2, they are generated by at most a elements. □

Remark. By using the same method in [4, Corollary 3.6] it can be shown that the ideals of $\mathbb{Z}_{p^a}[X]/(X^\lambda - 1)$ are generated by at most a elements.

Example. Let $\lambda = 5^3 6 = 750$. We saw $\mathbb{Z}_{5^2}[X]/(X^\lambda - 1)$ is isomorphic to $S'[Y]/(Y^6 - t)$ where $S' = \mathbb{Z}_{5^2}[\overline{T}]/(\overline{T}^{5^3} - 1)$. Reduce $Y^6 - \bar{t} \in S'[Y]$ modulo the maximal ideal $\mathfrak{m}' = (5, \overline{T} - 1)$ of S', we obtain $Y^6 - 1 \in \mathbb{F}_5[Y]$. By Theorem 13, we can factor it as $Y^6 - 1 = Q_1 Q_2 Q_3 Q_6$. By using [4, Theorem 3.27] we have $Q_1 = Y - 1, Q_2 = Y + 1, Q_3 = Y^2 + Y + 1, Q_6 = Y^2 - Y + 1$. By Theorem 13, we conclude that Q_1, Q_2, Q_3 and Q_6 are irreducible. Hence we obtain an irreducible factorization

$$Y^6 - 1 = (Y - 1)(Y + 1)(Y^2 + Y + 1)(Y^2 - Y + 1)$$

in $\mathbb{F}_5[X]$. By Hensel's Lemma we can lift the factorization in $S'[Y]$. In fact,

$$Y^6 - \bar{t} = (Y - \bar{t}^{21})(Y + \bar{t}^{21})(Y^2 + \bar{t}^{21} Y + \bar{t}^{42})(Y^2 - \bar{t}^{21} Y + \bar{t}^{42})$$

is the factorization into basic irreducible polynomials in $S'[Y]$. By writing $\overline{Q}_1 = Y - \bar{t}^{21}$, $\overline{Q}_2 = Y + \bar{t}^{21}$, $\overline{Q}_3 = Y^2 + \bar{t}^{21}Y + \bar{t}^{42}$ and $\overline{Q}_6 = Y^2 - \bar{t}^{21}Y + \bar{t}^{42}$ we see, by Theorem 14, that $\mathbb{Z}_{5^2}[X]/(X^{750}-1)$ is isomorphic to the direct sum $S'/\overline{Q}_1 \oplus S'/\overline{Q}_2 \oplus S'/\overline{Q}_3 \oplus S'/\overline{Q}_6$ and the ideals of each factor are the descents of the ideals of S' by Lemma 4. And we saw that the ring S' is isomorphic to the rings we investigated in § 2 where we showed how to find the ideals of such rings.

Acknowledgement. Publication of this paper has been long delayed. It was written sometime during the February of 2006. The editors of the journals delayed their decisions for acceptance and/or didn't want to publish in their journal with one reason or the other. And finally CKMS agreed to publish the paper.

References

[1] M. Atiyah and I. G. Macdonald, *Introduction to Commutative Algebra*, Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont. 1969.
[2] N. Bourbaki, *Elements of Mathematics. Commutative Algebra*, Addison-Wesley Publishing Co., Reading, Mass., 1972.
[3] S. T. Dougherty and Y. H. Park, *On modular cyclic codes*, Finite Fields Appl. **13** (2007), no. 1, 31–57.
[4] P. Kanwar and S. R. López-Permouth, *Cyclic codes over the integers modulo p^m*, Finite Fields Appl. **3** (1997), no. 4, 334–352.
[5] R. Lidl and H. Niederreiter, *Introduction to Finite Fields and Their Applications*, Cambridge University Press, Cambridge, 1994.
[6] S. S. Woo, *Cyclic codes of even length over $\mathbb{Z}_4$*, J. Korean Math. Soc. **44** (2007), no. 3, 697–706.
[7] ———, *Free cyclic codes over finite local rings*, Bull. Korean Math. Soc. **43** (2006), no. 4, 723–735.
[8] ———, *Cyclic codes of length 2^n over $\mathbb{Z}_4$*, preprint, 2005.
[9] ———, *Algebras with a nilpotent generator over $\mathbb{Z}_{p^2}$*, Bull. Korean Math. Soc. **43** (2006), no. 3, 487–497.

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