On The Structure Of Primary Ideals Of A Non-Laskerian Group Ring

Reza DastBasteh*,Hamed Mousavi**,Taher Abualrub*** ,Javad Haghighat**
*Department of Mathematics, Sabanci university, Istanbul, Turkey
**Department of Electrical Engineering, Shiraz University of Technology, Shiraz, Iran
*** Department of Mathematics and Statistics, American University of Sharjah, Sharjah, UAE
E-mails:
r.dastbasteh@sabanciuniv.edu, h.moosavi@sutech.ac.ir, abualrub@aus.edu, haghighat@sutech.ac.ir

December 4, 2016

Abstract

In this paper, we study the structure of $R_n = (\mathbb{F}_p + u\mathbb{F}_p)[\mathbb{Z}_n; \theta]$ where $u^2 = 0$ and $\theta(u) = -u$. As a main result, we prove that this group ring is not Laskerian. Also, we classify the maximal ideals, prime ideals, and primary ideals and find the ideals that have primary decomposition. We also find $J(R_n)$, $Nil_*(R_n)$, $Nil^*(R_n)$, and $Nil(R_n)$ as additional results.

1 Introduction

We say an ideal I in R has a primary decomposition, if there exists $t \in \mathbb{N}$ and primary ideals like $Q_1, \cdots, Q_t$ such that $I = Q_1 Q_2 \cdots Q_t$. The primary ideals can be defined in different ways for a non-commutative ring. One of the typical and the most common way to define them is that Q is primary in R, if for each ideals A, B in R such that $AB \subseteq Q$, then $A \subseteq Q$ or $B^n \subseteq Q$ for some $n \in \mathbb{N}$. The existence of primary decomposition (i.e. being a Laskerian ring) in the monoid rings and group rings is very important. Because it can help to study the structure of an arbitrary ideal in more detail. Some examples of existence of primary decomposition can be found in [30, 31, 29]. In [34], the author investigates the Laskerian condition over the characteristic one algebras. This subject becomes very interesting, if applied to the decomposition of ideals in group rings. There has been increasing attention to the group rings and their properties when the group is finite. Some examples of such works are [15, 16, 17, 18]. Also, some works appearing in literature, study the primary decomposition in the graded rings and group rings. As an example, the author in [32] studies the existence of primary decomposition over a special ring $R \oplus R$. Also, in [33], the author aims to find G-primary decomposition for the G-graded rings, since these rings do not have primary decomposition in general cases. Some finite group rings are very important in applications such as coding theory and cryptography. For example, the group rings of the form $R[\mathbb{Z}_n] \simeq \frac{R[x]}{<x^n-1>}$ generate the cyclic codes over a ring R with length n. Some examples can be found in [2, 12, 6, 4, 11, 10, 3, 8, 13, 7, 14]. Typically, the ring R is finite in these applications; therefore, the group ring $R[\mathbb{Z}_n]$ is also finite. We know that if a ring is commutative Noetherian, then the primary decomposition exists. Thus, there exists a primary decomposition for each ideal of a finite group ring. However, the structure of primary ideals in special rings such as $R[\mathbb{Z}_n]$ is very important. This is due the fact that the structure of primary ideals of a ring can help to develope fast algorithms to find the primary decomposition, which in turn has a key role in numerous coding and cryptographic applications. Some examples of these algorithms can be found in [25, 23, 26, 27, 28].

Another interesting topic is the structure of primary decomposition in the monoid rings like $R[\mathbb{Z}] \simeq R[x]$. We know that if R is finite, then $R[x]$ is Noetherian by Hilbert basis theorem. Also, if S is a totally strictly positively ordered monoid, we also know that $R[[S^{,\leq}]]$ is Noetherian, if and only if R is Noetherian and S is finite generated (see [35]). However, these results are not directly applicable to skew group rings and skew monoid rings. This is due the fact that these rings are no longer commutative, and therefore they are not necessarily Laskerian. This means that even existence of primary decomposition in these rings is not guaranteed. Therefore, proving the existence of primary decomposition and studying the structure of primary ideals in these rings are not straightforward. There are some previous works on non-commutative rings or modules to find necessary or sufficient conditions of being Laskerian. As examples of these works, we refer the reader to [21, 20, 19, 22] and references therein.

In this paper, we aim to show that the rings $R_n := (\mathbb{F}_p + u\mathbb{F}_p)[\mathbb{Z}_n;\theta]$ and $R := (\mathbb{F}_p + u\mathbb{F}_p)[x;\theta]$ are not Laskerian, where $u^2 = 0$, p is a prime number, θ is an automorphism of $\mathbb{F}_p + u\mathbb{F}_p$ and $n \in \mathbb{N}$. We also give an explicit form for the prime, maximal and primary ideals of both rings R, R_n. We also find $J(R), J(R_n)$ and $Nil_*(R), Nil_*(R_n), Nil^*(R), Nil^*(R_n), Nil(R), Nil(R_n)$ and $Z(R), U(R)$ as additional results.

2 Over the ring $(\mathbb{F}_p + u\mathbb{F}_p)[x;\theta]$

2.1 The center and units of R

From now on, θ will denote an automorphism of S of order $o(\theta) = |\langle\theta\rangle| = e > 1$.

Since R is a non-commutative ring, it is worth to find its center. The following theorem can be proved as the Theorem in [14].

Theorem 2.1. *The center of $R = S[x;\theta]$ is $\mathbb{F}_p[x^e]$ for $\theta \in Aut(S)$ of order e.*

So $x^n - 1 \in Z(R)$ if and only if $e|n$. The other useful property is division algorithm. The left and the right division algorithm hold for some elements of R. The proof of the following theorem is straightforward.

Theorem 2.2. *Let $f, g \in R$ such that the leading coefficent of g is a unit. Then there exist unique polynomials q and r in R such that $f = qg + r$, where $r = 0$ or $deg(r) < deg(g)$.*

Now we shall determine, $U(R)$, the set of all unit elements of R. First we shall prove the following lemma, which is crucial in over studies later on.

Lemma 2.3. *For every $g(x) \in R$, there exists $g'(x) \in \mathbb{F}_p[x]$ such that $ug = g'u$.*

Proof. Let $g(x) = \sum_{i=0}^{n} g_i x^i \in R$. Since $g_i \in S$ for each i, there exist g_i' and g_i'' in $\mathbb{F}_p$ such that $g_i = g_i' + ug_i''$. So $g(x) = \sum (g_i' + ug_i'')x^i$. Since $u^2 = 0$, we have

$$ug(x) = \sum u(g_i' + ug_i'')x^i = \sum ug_i'x^i = \sum_{e\nmid i} \alpha^{-i} g_i' x^i u + \sum_{e|i} g_i' x^i u = g'(x)u \tag{2.1}$$

for some $g'(x) \in R$. □

Notation. For a fixed element $g \in R$, the element $g' \in \mathbb{F}_p[x]$ in lemma 2.3 is unique and hence we call it the *partaker* of g.

Lemma 2.4. *Let $A \trianglelefteq \mathbb{F}_p[x]$ and $A' \subseteq \mathbb{F}_p[x]$, such that $uA = A'u$. Then $A' \trianglelefteq \mathbb{F}_p[x]$.*

Proof. Let $f, g \in A'$ and $h \in R$. So there exist polynomials $l, k \in A$ such that $fu = uk$ and $gu = ul$. So $(f + g)u = u(l + k) \in uA = A'u$. Hence $f + g \in A'$. Also $hfv = hvk = uh'k$, for some $h' \in \mathbb{F}_p[x]$. Since $h'k \in A$, $hf \in A'$. Thus A' is an ideal of R. □

Note 1. From now on, we shall call A' in lemma 2.4, the *partaker set* of A.

First we shall find $U(S)$. Let $a + bu \in S$ be a unit. So there exists $c + du \in S$ such that $(a+bu)(c+du) = 1$. So $ac = 1$ and $ad+bc = 0$. One can show that these equations have unique solutions for c and d, if and only if $a \in \mathbb{F}_p^*$. So $U(S) = \mathbb{F}_p^* + u\mathbb{F}_p$. In the next step, we try to find $U(R)$.

Theorem 2.5. *$U(R) = \{a + uh(x) | a \in \mathbb{F}_p^*, h \in \mathbb{F}_p[x]\}$.*

Proof. Let $h(x) = \sum_{i=0}^{n} h_i x^i \in \mathbb{F}_p[x]$. Write $h = b + g(x)$, where $b = h_0$ and $g(x) \in \mathbb{F}_p[x]$. We show that $a + uh(x)$, where $a \in \mathbb{F}_p^*$ has the inverse $t = (a + bu)^{-1} - (a + bu)^{-1}ug(a + bu)^{-1}$.

$$\begin{aligned}
&((a + bu) + ug)[(a + bu)^{-1} - (a + bu)^{-1}ug(a + bu)^{-1}] \\
&= 1 - ug(a + bu)^{-1} + ug(a + bu)^{-1} - ug(a + bu)^{-1}ug(a + bu)^{-1} \\
&= 1 - ug(a + bu)^{-1}ug(a + bu)^{-1} = 1 - u^2k(x) = 1 \qquad (2.2)
\end{aligned}$$

for some $k(x) \in \mathbb{F}_p[x]$.

Similarly, t is the left inverse of $a + uh(x)$. Thus $a + uh$ is a unit in R. Conversly, let $f \in U(R)$. Then there exists $g \in R$ such that $fg = gf = 1$. Let $f = f_1 + uf_2$ and $g = g_1 + ug_2$ for $f_i, g_i \in \mathbb{F}_p[x]$. So $fg = (f_1 + uf_2)(g_1 + ug_2) = 1$ implies that $f_1g_1 = 1$ and $uf_2g_1 + f_1ug_2 = 0$. Hence f_1 is a non-zero constant polynomial. That is, $f_1 \in \mathbb{F}_p^*$. Thus $f = f_1 + uf_2$, where $f_1 \in \mathbb{F}_p^*$ and $f_2 \in \mathbb{F}_p[x]$. □

2.2 The left maximal and prime ideals of R

In this section, we shall determine the sets $Max(R)$ and $Spec(R)$, the set of all left maximal and prime ideals of R respectively. For the sake of semplicity, from now on, by an ideal of R we mean a left ideal of R.

First, we shall show that u is irreducible in R.

Lemma 2.6. *Ru is a maximal ideal in R.*

Proof. Let $u = fg$, for some $f, g \in R$. Let $f = f_1 + uf_2$ and $g = g_1 + ug_2$. Then $f_1g_1 = 0$ and

$$f_1ug_2 + uf_2g_1 = u. \qquad (2.3)$$

From $f_1g_1 = 0$, we have that $f_1 = 0$ or $g_1 = 0$. If $f_1 = 0$, then $uf_2g_1 = u$. So $f_2g_1 = 1$. Hence g is a unit in $\mathbb{F}_p[x]$. If $g_1 = 0$, then by equation (2.3), $f_1ug_2 = u$. Let g_2' be the partaker if g_2. Thus $fg_2'u = u$ so $f_1g_2' = 1$. This implies that $f = f_1 + uf_2$ is a unit by theorem 2.5. Therefore, Rv is a maximal ideal in R. □

Now, to determine the sets $Max(R)$ and $Spec(R)$, we shall introduce the following sets, which in fact are ideals of $\mathbb{F}_p[x]$.

Definition 2.7. Let $A \trianglelefteq R$. Define

$$A_{[1]} = \{f \in \mathbb{F}_p[x] | \exists g \in \mathbb{F}_p[x] \quad such\ that \quad f + ug \in A\}$$
$$A_{[2]} = \{g \in \mathbb{F}_p[x] | \exists f \in \mathbb{F}_p[x] \quad such\ that \quad f + ug \in A\}$$

Let $f \in A$ and $f = f_1 + uf_2$, for some $f_1, f_2 \in \mathbb{F}_p[x]$. Since $f_1 \in A_{[1]}$ and $f_2 \in A_{[2]}$, we conclude that $A \subset A_{[1]} + uA_{[2]}$.

Lemma 2.8. *Let $A \trianglelefteq R$. Then $A_{[1]}$ and $A_{[2]}$ are ideals of $\mathbb{F}_p[x]$.*

Proof. Let $f_1, f_2 \in A_{[1]}$. Then there exist $g_1, g_2 \in \mathbb{F}_p[x]$ such that $f_1 + ug_1, f_2 + ug_2 \in A$. Thus $f + g = (f_1 + f_2) + u(g_1 + g_2) \in A$ since $A \trianglelefteq R$. Hence $f_1 + f_2 \in A_{[1]}$. Now for $f \in A_{[1]}$ and $g \in \mathbb{F}_p[x]$, we show that fg is an element of $A_{[1]}$. There exists $h \in \mathbb{F}_p[x]$ such that $f_1 + uh \in A$. So $g(f + uh) \in A$. So $gh \in A_{[1]}$ and hence $A_{[1]} \trianglelefteq \mathbb{F}_p[x]$. Similarly, $A_{[2]} \trianglelefteq \mathbb{F}_p[x]$. □

Lemma 2.9. *For $A \trianglelefteq R$, we have*

i) $uA_{[1]} \trianglelefteq R$.
ii) $uA_{[1]} \subseteq A$.
iii) $A_{[1]} \subseteq A_{[2]}$.
iv) If $A_{[1]} = A_{[2]} = \mathbb{F}_p[x]$, then $A = R$.

Proof. i) By lemma 2.8, A_1 is an ideal of $\mathbb{F}_p[x]$ and since $\mathbb{F}_p[x]$ is a PID, there exists $a \in \mathbb{F}_p[x]$ such that $A_{[1]} = \langle a \rangle$.

We only show that if $f \in R$ and $ug \in uA_{[1]}$, then $fug \in uA_{[1]}$. Let $f = f_1 + uf_2$ and $ug = uak$ for some $k \in \mathbb{F}_p[x]$. Then $fug = (f_1 + uf_2)uka = uf_1'ka$, where f_1' is the partaker of f_1. Since $f_1', k, a \in \mathbb{F}_p[x]$, $fuak \in uA_{[1]}$, which shows that $uA_{[1]} \trianglelefteq R$.

ii) Let $uk_1 \in uA_{[1]}$. Then there exists $k_2 \in A_{[2]}$ such that $k_1 + uk_2 \in A$. So $uk_1 = u(k_1 + uk_2) \in A$ (since $A \trianglelefteq R$). So $uA_{[1]} \subseteq A$.

iii) Since $\mathbb{F}_p[x]$ is a PID, $A_{[1]} = \langle f \rangle$ and $A_{[2]} = \langle g \rangle$ for some $f, g \in \mathbb{F}_p[x]$. Thus there exists $h \in \mathbb{F}_p[x]$ such that $g + uh \in A$. So $u(g + uh) = ug \in A$. Thus $g \in A_{[2]}$. That is, $A_{[1]} \subseteq A_{[2]}$.

iv) Since $1 \in A_{[1]}$, $1 + ug(x) \in A$ is a unit in R for $g(x) \in A_{[2]}$ by theorem 2.9. Thus $A = R$. □

We showed that $A \subseteq A_{[1]} + uA_{[2]}$. This inclusion can be strict, as the following example shows.

Example 2.10. Let $A = R(u + x)$. Then $A_{[1]} =< x >$ and $A_{[2]} =< 1 >$. We claim that u is not in A. Otherwise, let $u = (f_1 + uf_2)(x + u)$ for some $f_1, f_2 \in \mathbb{F}_p[x]$. So $xf_1 = 0$ which means that $f_1 = 0$. Thus $uf_2x = u$. So $xf_2 = 1$, which is not possible. So there is no such $f = f_1 + uf_2 \in R$ such that $u = f(u + x)$, which means that u is not in A. However, $u \in A_{[1]} + uA_{[2]}$. So $A \subsetneqq A_{[1]} + uA_{[2]}$.

Definition 2.11. Let $A \trianglelefteq R$. A is called a first type ideal of R, if $A = A_{[1]} + uA_{[2]}$, and it is called a second type if $A \subsetneqq A_{[1]} + uA_{[2]}$.

Example 2.12. This example is a generalization of Example 2.10. We show that $A = (f + u)R$ is a second type ideal for every $0 \neq f \in \mathbb{F}_p[x]$ which is not unique. Let $A = A_{[1]} + uA_{[2]}$. Since $f + u \in A$, $1 \in A_{[2]}$. So $u \in A$. That is, $u = (h_1 + uh_2)(f + u)$ for some $h_1, h_2 \in \mathbb{F}_p[x]$. Hence $fh_1 = 0$, which means that $h_1 = 0$. So $u = (uh_2)(f + u) = ufh_2$. So f is a unit in $\mathbb{F}_p[x]$ which is a contradiction. Therefore, A is a second type ideal of $\mathbb{F}_p[x]$.

In the following example, we propose a second type ideal which is not principle.

Example 2.13. In this example, we give a non principle second type ideal A which $x^n - 1 \in A$ for some $n \in \mathbb{N}$. Note that these ideals are so applicable in encoding and decoding which we discuss later.

Consider $A = R((x^3-1)+u)+u\mathbb{F}_p[x](x^n-1)$. In this ideal, $A_{[1]} =< x^3-1 >$ and $A_{[2]} = \mathbb{F}_p[x]$. First, we show that A is not first ype ideal. Suppose in contrary, A is a first type ideal. Then $u \in A$ which means that there are $f, g, h, k \in \mathbb{F}_p[x]$ such that

$$(f + ug)(x^3 - 1 + u) + (h + uk)(u(x - 1)) = u \tag{2.4}$$

So, $f = 0, g(x^3 - 1) + h'(x - 1) = 1$. Hence, $x - 1|1$ and it is impossible.

Now, we show that there is no generator for A. Suppose that $A = R(f + ug)$ for some $f, g \in \mathbb{F}_p[x]$. We know that $f = x^3 - 1$ (Otherwise, $A_{[1]} \neq< x^3 - 1 >$). Also, $u(x - 1) \in A$. So there exists $h, k \in \mathbb{F}_p[x]$ such that

$$(h + uk)(x^3 - 1 + ug) = h(x^3 - 1) + uk(x^3 - 1) + uh'g = u(x - 1) \tag{2.5}$$

So $h = 0$ and therefor the left side is equal to $uk(x^3 - 1)$ for some $k \in \mathbb{F}_p[x]$ which is not equal to $u(x - 1)$. This contradiction complete the example.

Now we are in a position to give a chacterization of maximal ideals of R.

Theorem 2.14. *Let $A \trianglelefteq R$. Then A is a maximal ideal of R if and only if*

i) $A_{[1]} =< f >$, for some irreducible polynomial $f \in \mathbb{F}_p[x]$.

ii) $A_{[2]} = \mathbb{F}_p[x]$.

iii) A is of the first type, that is, $A = A_{[1]} + u\mathbb{F}_p[x]$.

Proof. $\Rightarrow$) i) We show that $A_{[1]}$ is maximal in $\mathbb{F}_p[x]$. Let $A_{[1]} \subsetneqq B \subsetneqq \mathbb{F}_p[x]$. Then $A \subseteq A_{[1]} + u\mathbb{F}_p[x] \subsetneqq B + u\mathbb{F}_p[x] \subsetneqq R$, which is a contradiction. So $A_{[1]}$ is maximal in $\mathbb{F}_p[x]$ and hence is generated by an irreducible polynomial $f \in \mathbb{F}_p[x]$.

ii) Suppose that $A_{[2]} \subsetneqq \mathbb{F}_p[x]$. We know that $A_{[1]}$ is maximal in $\mathbb{F}_p[x]$. Let $B = A_{[1]} + u\mathbb{F}_p[x]$. Then $A \subsetneqq B \subsetneqq R$ (since $u \in B - A$ and $1 \in \mathbb{F}_p[x] - B$), which is a contradiction.

iii) Let $A \neq A_{[1]} + uA_{[2]}$. Then $A \subsetneqq A_{[1]} + u\mathbb{F}_p[x] \subsetneqq R$, which is a contradiction.

$\Leftarrow$) Since A is a proper ideal, there exists a maximal ideal B containing A. By hypothesis $A_{[2]} = \mathbb{F}_p[x]$. Since $A \subseteq B$, $A_{[2]} = \mathbb{F}_p[x] \subseteq B_{[2]}$. That is, $B_{[2]} = \mathbb{F}_p[x]$. Also $A_{[1]} \subseteq B_{[1]}$. Since B is proper in R , $B_{[1]} \neq \mathbb{F}_p[x]$ by lemma 2.9(iv). But $A_{[1]} =< f >$, where f is irreducible in $\mathbb{F}_p[x]$ and if $B_{[1]} =< g >$, then $g|f$, which implies that $f = ug$, for some unit $u \in \mathbb{F}_p[x]$. Hence $B_{[1]} = A_{[1]}$.

Finally $B_{[1]} = A_{[1]} =< f >$, and $B_{[2]} = A_{[2]} = \mathbb{F}_p[x]$. So by Theorem 2.14, we have $B \subseteq B_{[1]} + uB_{[2]} = A_{[1]} + uA_{[2]} = A$, as required. □

Lemma 2.15. *For $A, B \trianglelefteq R$, we have*

$$A \cap B = (A_{[1]} \cap B_{[1]}) + u(A_{[2]} \cap B_{[2]}).$$

In particular, the intersection of two first type ideals is again a first type ideal.

Proof. Let $A_{[1]} = a_1\mathbb{F}_p[x]$, $A_{[2]} = a_2\mathbb{F}_p[x]$, $B_{[1]} = b_1\mathbb{F}_p[x]$ and $B_{[2]} = b_2\mathbb{F}_p[x]$. Since $a_1 \in A$ and $b_1 \in B$, $lcm(a_1, b_1) \in A \cap B$. Similarly, $lcm(a_2, b_2) \in A \cap B$. Thus $lcm(a_1, b_1)\mathbb{F}_p[x] + u\mathbb{F}_p[x]lcm(a_2, b_2) \subseteq A \cap B$. Hence

$$(A_{[1]} \cap B_{[1]}) + u(A_{[2]} \cap B_{[2]}) \subseteq A \cap B. \tag{2.6}$$

Now, let $f \in A \cap B$. If $f = f_1 + uf_2$, for some $f_1, f_2 \in \mathbb{F}_p[x]$, then $f_1 = a_1h$, $f_1 = b_1g$, $f_2 = a_2h'$ and $f_2 = b_2g'$.

So $lcm(a_1, b_1)|f_1$ and $lcm(a_2, b_2)|f_2$. Hence, $f_1 \in A_{[1]} \cap B_{[1]}$ and $f_2 \in A_{[2]} \cap B_{[2]}$. So $f \in (A_{[1]} \cap B_{[1]}) + u(A_{[2]} \cap B_{[2]})$, as required. □

Corollary 2.16. $J(R) = u\mathbb{F}_p[x]$.

Proof. By lemma 2.15 and Theorem 2.14, we have

$$J(R) = \bigcap_{M \lhd_m R} M = \bigcap_{f:irreducible in \mathbb{F}_p[x]} < f > +u\mathbb{F}_p[x] = J(\mathbb{F}_p[x]) + u\mathbb{F}_p[x] = u\mathbb{F}_p[x]$$

□

Now, we shall find the set of all left prime ideals of R. Note that for any $A \lhd R$, the equation $< u > A =< uA >$ holds.

Lemma 2.17. *Let $Spec(A)$ be the set of all left prime ideals of R. Then $Spec(A) \subseteq Max(R) \cup u\mathbb{F}_p[x]$.*

Proof. Let P be a prime ideal of R. We shall show that $P_{[1]} \subseteq P$. We know that $uP_{[1]}$ is an ideal of R such that $uP_{[1]} \subseteq P$ by lemma 2.9. Also we know that $< u >< P_{[1]} >\subseteq< uP_{[1]} >\subseteq P$. So $< u >\subseteq P$ or $< P_{[1]} >\subseteq P$ which means that $u \in P$ or $P_{[1]} \subseteq P$. Assume that $u \in P$. Then let $f \in P_{[1]}$. So $f + ug \in P$ for some $g \in \mathbb{F}_p[x]$. Since $u \in P$, $f \in P$ which means that $P_{[1]} \subseteq P$.

We show that $P_{[1]}$ is prime in $\mathbb{F}_p[x]$. Let $BC \subseteq P_{[1]}$, for some ideals B, C in $\mathbb{F}_p[x]$. Thus $uB(C + uC) \subseteq P$. So $uB \subseteq P$ or $C + uC \subseteq P$. Hence $uB \subseteq P$ or $C \subseteq P_{[1]}$.

If $uB \subseteq P$, then $(C + uC)(B + uB) = (BC + uBC) + CuB \subseteq P + uP + CP \subseteq P$. So $B + uB \subseteq P$ or $C + uC \subseteq P$, which implies that $B \subseteq P_{[1]}$ or $C \subseteq P_{[1]}$. So in any case $B \subseteq P_{[1]}$ or $C \subseteq P_{[1]}$, which means that $P_{[1]}$ is prime in $\mathbb{F}_p[x]$. But $\mathbb{F}_p[x]$ is a PID, so $P_{[1]}$ is maximal or the zero ideal. By lemma 2.9(*iii*), $P_{[1]} \subseteq P_{[2]}$. So we can have three cases.

i) $P_{[1]} = P_{[2]}$ maximal in $\mathbb{F}_p[x]$.

ii) $P_{[2]} = \mathbb{F}_p[x]$.

iii) $P_{[1]} = 0$, that is, $P = uP_{[2]}$.

Suppose that $P_{[1]} = P_{[2]} = \langle\pi\rangle$ for some irreducible polynomial $\pi \in \mathbb{F}_p[x]$. Let $k \in \mathbb{F}_p[x]$ be an irreducible polynomial in $\mathbb{F}_p[x]$ which is different from π. Then $(0+uk\mathbb{F}_p[x])(\pi\mathbb{F}_p[x]+u\mathbb{F}_p[x]) \subseteq uk\pi\mathbb{F}_p[x] \subseteq u\pi\mathbb{F}_p[x] \subseteq P$. But neither $uk\mathbb{F}_p[x] \subseteq P$ nor $\pi\mathbb{F}_p[x] + u\mathbb{F}_p[x]$, since $k \neq \pi$. So P is not prime in this case.

Suppose that $P_{[2]} = \mathbb{F}_p[x]$ and $P_{[1]} = \langle\pi\rangle$ for some irreducible $\pi \in \mathbb{F}_p[x]$. So $\pi + us \in P$ for some $s \in \mathbb{F}_p[x]$. Thus $u(\pi + us) = u\pi \in P$. We show that $< u >< \pi + u >\subseteq P$. Let $a \in< u >< \pi + u >$. Then

$$a = \sum_i (f_i + ug_i)v(k_i + ul_i)(\pi + u) = \sum f_iuk_i\pi \in< u\pi >\subseteq P. \tag{2.7}$$

Hence $< u >\subseteq P$ or $< \pi + u >\subseteq P$. If $u \in P$, then by Theorem 2.14, P is maximal, since $\pi \in P_{[1]} \subseteq P$ and hence $P = \pi\mathbb{F}_p[x] + u\mathbb{F}_p[x] = P_{[1]} + uP_{[2]}$. But if $\pi + u \in P$, then $u\pi = u(\pi + u) \in P$ and so $< u\pi >\subseteq P$. Since $< u >< \pi >\subseteq< u\pi >\subseteq P$, $< u >\subseteq P$ or $< \pi >\subseteq P$, in each case P is maximal.

Finally, let $P_{[1]} = 0$. Then $P = uP_{[2]}$. Thus $P = u\rho\mathbb{F}_p[x]$, for some non-zero $\rho \in \mathbb{F}_p[x]$. We show that ρ is a unit. P can not be zero, as $u^2 = 0 \in P$, but $u \notin P$. So

$$(u\mathbb{F}_p[x])(\rho\mathbb{F}_p[x] + u\rho\mathbb{F}_p[x]) \subseteq v\rho\mathbb{F}_p[x] = P. \tag{2.8}$$

Thus $(\rho\mathbb{F}_p[x] + u\rho\mathbb{F}_p[x]) \subseteq P$ or $u\mathbb{F}_p[x] \subseteq P$. So $\rho + uh \in P$ for some $h \in \mathbb{F}_p[x]$ or $u \in P$. Since $\rho \in P_{[1]} = 0$, which in impossible as $\rho \neq 0$. Hence $u \in P$. So $1 \in P_{[2]}$ (since $0 + u.1 \in P$) and hence $P_{[2]} = \mathbb{F}_p[x] = \rho\mathbb{F}_p[x]$. That is, ρ is a unit. Therefore, $P = u\mathbb{F}_p[x]$ is required in this case. □

Lemma 2.18. *The ideal $P = u\mathbb{F}_p[x]$ is prime in R.*

Proof. Suppose that $AB \subseteq P$ for $A, B \trianglelefteq R$. So $A_{[1]}B_{[1]} \subseteq P_{[1]} = 0$. Hence, $A_{[1]} = 0$ or $B_{[1]} = 0$. Thus $A = uA_{[2]}$ or $B = uB_{[2]}$. Therefore, $A \subseteq P$ or $B \subseteq P$. □

Now by the above results we can give a characterisation of all left prime ideals of R.

Theorem 2.19. *$Spec(R) = Max(R) \cup u(\mathbb{F}_p[x])$.*

Finally, we try to find $Nil(R), Nil_*(R), Nil^*(R)$.

Corollary 2.20. *$Nil_*(R) = Nil(R) = Nil^*(R) = u\mathbb{F}_p[x]$*

Proof. Since $Nil_*(R) = \bigcap_{P\in Spec(R)} P$, It is easy to see that $Nil_*(R) = u\mathbb{F}_p[x]$ by corollary 2.16 and Theorem 2.19. Thus

$$u\mathbb{F}_p[x] = Nil_*(R) \subseteq Nil(R) \subseteq Nil^*(R) \subseteq J(R) = u\mathbb{F}_p[x].$$

So the result follows. □

2.3 The primary ideals of R

In this section, we shall give some characterisations of left primary ideals of R. Recall that a left (respectively, right) proper ideal Q is called primary if for each left(respectively, right) ideals A and B such that $AB \subseteq Q$, then $A \subseteq Q$ or there exists $n \in \mathbb{N}$ such that $B^n \subseteq Q$. (respectively, $B \subseteq Q$ or $A^n \subseteq Q$ for some $n \in \mathbb{N}$), see, for example, [?]. First, we shall show that the irreducible polynomials of $\mathbb{F}_p[x]$ are irreducible in R.

Lemma 2.21. *An element $f \in \mathbb{F}_p[x]$ is irreducible in R if and only if f is irreducible in $\mathbb{F}_p[x]$.*

Proof. $\Rightarrow$) Let $f \in \mathbb{F}_p[x]$ be irreducible in $\mathbb{F}_p[x]$, but $f = gh$, for some $g, h \in R$. Let $g = g_1 + ug_2$ and $h = h_1 + uh_2$, where $f_i, g_i, h_i \in \mathbb{F}_p[x]$ for $i = 1, 2$. Then $f_1 = g_1h_1$. So g_1 or h_1 is a unit in $\mathbb{F}_p[x]$ and hence g or h is a unit by Theorem 2.5.

$\Leftarrow$) Obvious. □

Note 2. Recall that if R is a UFD and π is an irreducible element of R, then $< \pi >$ is a prime ideal and $< \pi^n >$,$n \geq 1$, is a primary ideal, with radical $< \pi >$. Conversely, every primary ideal Q whose radical is $< \pi >$ is of the form $< \pi^n >$, $n \geq 1$. (see, for example, [1], P.155.)

Lemma 2.22. *Let S be a PID. Then $Q \lhd S$ is primary if and only if for each ideals $B, C \unlhd S$, if $BC \subseteq Q$, then $B \subseteq \sqrt{Q}$ or $C \subseteq \sqrt{Q}$.*

Proof. $\Rightarrow$) Obvious.

$\Leftarrow$) Let $Q = \prod_{i=1}^{k} P_i^{a_i}$, the prime factorization of Q into prime ideals of S. If $k > 1$, then $\prod_{i=1}^{k} P_i^{a_i} \subseteq Q$, but neither $P_1^{a_1} \nsubseteq \prod_{i=1}^{k} P_i = \sqrt{Q}$ nor $\prod_{i=2}^{k} P_i^{a_i} \nsubseteq \prod_{i=1}^{k} P_i = \sqrt{Q}$, which is a contradiction with hypothesis. So $k = 1$ and hence Q is primary, since Q is a power of a maximal ideal in S. □

Theorem 2.23. *Let Q be a left primary ideal of R. Then only one of the following cases occures.*

i) There exists a prime ideal $P \unlhd \mathbb{F}_p[x]$ with partaker P', where $P' \subseteq P$ and positive integers a, b such that $a \geq b$, $Q_{[1]} = P^a$ and $Q_{[2]} = P^b$.

ii) There exists a prime ideal $P \unlhd \mathbb{F}_p[x]$ and integer $a > 0$ such that $Q_{[1]} = P^a$ and $Q_{[2]} = \mathbb{F}_p[x]$.

iii) $Q = u\mathbb{F}_p[x]$

iv) $Q = 0$.

Proof. First, we show that $Q_{[1]}$ is a primary ideal of $\mathbb{F}_p[x]$. Note that $Q_{[1]}$ is a proper ideal of Q since otherwise, $Q = R$ by lemma 2.9(iv).

Let $BC \subseteq Q_{[1]}$ for $B, C \unlhd \mathbb{F}_p[x]$. One can see that $uB(C + uC) \subseteq Q$. So $uB \subseteq Q$ or $(C + uC)^n \subseteq Q$ for some $n \in \mathbb{N}$, since Q is primary and $uB, C + uC \unlhd R$. If $(C + uC)^n \subseteq Q$ for some $n \in \mathbb{N}$, then $C^n \in Q_{[1]}$. If $uB \subseteq Q$, then $< u >< B >\subseteq \langle vB \rangle \subseteq Q$. So $u \in Q$ or $< B >^m \subseteq Q$ for some $m \in \mathbb{N}$, which implies that $B^m \subseteq Q_{[1]}$. So we have proved that $u \in Q$ or $B^n \subseteq Q_{[1]}$ or $C^m \subseteq Q_{[1]}$. Now, we show that $u \in Q$ leads to $B \subseteq \sqrt{Q_{[1]}}$ or $C \subseteq \sqrt{Q_{[1]}}$. Let $u \in Q$. Suppose that $k \in BC \subseteq Q_{[1]}$. So there exist $k' \in Q_{[2]}$ such that $k + uk' \in Q$. Since $uk' \in Q$, $k \in Q$. That is, $BC \subseteq Q$. Now $(B + uB)(C + uC) \subseteq Q$. Hence $B + uB \subseteq Q$ or $(C + uC)^n \subseteq Q$ for some $n \in \mathbb{N}$. Thus $B \subseteq Q_{[1]} \subseteq \sqrt{Q_{[1]}}$ or $C \subseteq \sqrt{Q_{[1]}}$ as required.

Therefore, we have shown that if $BC \subseteq Q_{[1]}$ for $B, C \unlhd \mathbb{F}_p[x]$, then $B \subseteq \sqrt{Q_{[1]}}$ or $C \subseteq \sqrt{Q_{[1]}}$. Since $\mathbb{F}_p[x]$ is a PID, lemma 2.22 shows that $Q_{[1]}$ is a primary ideal of $\mathbb{F}_p[x]$. Hence $\sqrt{Q_{[1]}} = P$ is a prime and hence maximal or zero by Theorem 2.19. Thus $Q_{[1]} = P^a$ or $Q_{[1]} = 0$ for some positive integer a and a non-zero prime ideal $P \unlhd \mathbb{F}_p[x]$, by Note 2.

First, suppose that $Q_{[1]} = P^a$. Since $Q_{[1]} \subseteq Q_{[2]}$, so $Q_{[2]} = P^b$ for some $b \leq a$. If $b = 0$, then (ii) does hold. Let $b > 0$. We show that if $P' + P = \mathbb{F}_p[x]$, where P' is the partaker of P, then Q is not primary. So let $P + P' = \mathbb{F}_p[x]$, and $P = \langle \pi \rangle$, where π is an irreducible polynomial in $\mathbb{F}_p[x]$. Let $k \neq \pi$ be another irreducible polynomial in $\mathbb{F}_p[x]$. Then

$$(uk\mathbb{F}_p[x])(\pi^a\mathbb{F}_p[x] + u\mathbb{F}_p[x]) = uk\pi^a\mathbb{F}_p[x] \subseteq u\pi^a\mathbb{F}_p[x] \subseteq uP^a = uQ_{[1]} \subseteq Q. \tag{2.9}$$

However, $uk\mathbb{F}_p[x] \nsubseteq Q$. So let $(\pi^a\mathbb{F}_p[x] + u\mathbb{F}_p[x])^r \subseteq Q$ for some $r \in \mathbb{N}$. Hence $(\pi^a + u)^r \in Q$ for some $r \in \mathbb{N}$. Thus

$$(\pi^a + u)^r = \pi^{ar} + u\pi^{a(r-1)} + u\pi^{a(r-2)}(\pi')^a + \cdots + u(\pi')^{a(r-1)} \in Q \tag{2.10}$$

where π' is the partaker of π. So $(\pi')^{a(r-1)} \in P^b$, since $u\pi^{a(r-i)}(\pi')^{ai} \in P^b = Q_{[1]}$. But P and P' are coprime, and hence $(\pi', \pi) = 1$. So $\pi'^{a(r-1)} \in P^b$ would be impossible. Hence $P' \subseteq P$ (otherwise, $P + P' = \mathbb{F}_p[x]$ since P is maximal in $\mathbb{F}_p[x]$).

Now, suppose that $Q_{[1]} = 0$. Then $Q = Q_{[1]} + uQ_{[2]} = uQ_{[2]}$. So

$$uQ_{[2]} = u\mathbb{F}_p[x](Q_{[2]} + uQ_{[2]}) \subseteq uQ_{[2]} = Q. \tag{2.11}$$

Hence $u\mathbb{F}_p[x] \subseteq Q$ or $(Q_{[2]} + uQ_{[2]})^n \subseteq Q$ for some $n \in \mathbb{N}$. Thus $\mathbb{F}_p[x] \subseteq Q_{[2]}$ or $(Q_{[2]} + uQ_{[2]})^n \subseteq Q$. If $\mathbb{F}_p[x] \subseteq Q_{[2]}$, then $Q_{[2]} = \mathbb{F}_p[x]$ and (iii) is satisfied. However, if $(Q_{[2]} + uQ_{[2]})^n \subseteq Q$, then $Q_{[2]}^n \subseteq Q_{[1]} = 0$. So $Q_{[2]} = 0$. Therefore, $Q = 0$ and (iv) is satisfied. □

Now, we prove the converse of Theorem 2.23.

Theorem 2.24. *Any proper first type ideal Q of R which satisfies each one of the following cases, is primary.*

i) $Q = P^a + u\mathbb{F}_p[x]$ for some prime ideal P of $\mathbb{F}_p[x]$ and some positive integer a.

ii) $Q = P^a + uP^b$ for some non-zero prime ideal P which contains its partiner P' and for some positive integer a, b such that $a > b$.

iii) $Q = u\mathbb{F}_p[x]$

iv) $Q = 0$.

Proof. i) Suppose that $Q = P^a + u\mathbb{F}_p[x]$, where P is a prime ideal of $\mathbb{F}_p[x]$ and $a \in \mathbb{N}$. Let $BC \subseteq Q$. Then $B_{[1]}C_{[1]} \subseteq Q_{[1]} = P^a$. Since P^a is primary, $B_{[1]} \subseteq P^a$ or $C_{[1]} \subseteq \sqrt{P^a} = P$. If $B_{[1]} \subseteq P^a$, then

$$B \subseteq B_{[1]} + uB_{[2]} \subseteq P^a + u\mathbb{F}_p[x] = Q. \tag{2.12}$$

However, if $C_{[1]} \subseteq P$, we show that $(P + u\mathbb{F}_p[x])^a \subseteq Q$ for some $a \in \mathbb{N}$. Let $f_i \in P + u\mathbb{F}_p[x]$ for $i \leq a$. Then $\prod_i f_i \in P^a + u\mathbb{F}_p[x] = Q$. Hence, $(P + u\mathbb{F}_p[x])^a \subseteq Q$. We assumed that $C_{[1]} \subseteq P$. So $C^a \subseteq (C_{[1]} + uC_{[2]})^a \subseteq (P + u\mathbb{F}_p[x])^a \subseteq Q$. Thus Q is primary in this case.

ii) Let $Q = P^a + uP^b$ for some prime P which contains its partaker P' and for some $a, b \in \mathbb{N}$ with $a > b$. Let $AB \subseteq Q = P^a + uP^b$, for some $A, B \trianglelefteq R$. So $(AB)_{[1]} = A_{[1]}B_{[1]} \subseteq P^a$. Hence $A_{[1]} \subseteq P^a$ or $B_{[1]} \subseteq P$. Suppose that $B_{[1]} \subseteq P$ and let $y_i = b_{1,i}\pi + ub_{2,i} \in B$, where $b_{1,i}\pi \in B_{[1]} \subseteq P$ and $b_{2,i} \in B_{[2]}$.

$$\begin{aligned}\prod_{i \leq a} y_i &= \prod_{i \leq a} (b_{1,i}\pi + ub_{2,i}) \\ &= \prod_{i \leq a} b_{1,i}\pi^a + \prod_{i \leq a} b_{1,i}\pi^{a-1}ub_{2,i} + \prod_{i \leq a} b_{1,i}\pi^{a-2}ub_{1,i}\pi b_{2,i} + \cdots + \prod_{i \leq a} u(b_{1,i}\pi)^{a-1}b_{2,i}\end{aligned}$$

Since $P' \subseteq P$, there exists $t \in \mathbb{F}_p[x]$ such that $\pi' = t\pi$. So there exists $b' \in \mathbb{F}_p[x]$ such that

$$\prod_{i \leq a} y_i = \prod_{i \leq a} b_{1,i}\pi^a + ub't^a\pi^a \in \pi^a\mathbb{F}_p[x] + u\pi^b\mathbb{F}_p[x] = P^a + uP^b = Q.$$

Hence $\prod_{i \leq a} y_i \in Q$. That is, $B^a \subseteq Q$.

Now, let $A_{[1]} \subseteq P^a$. If $A_{[2]} \subseteq P^b$, then $A \subseteq P^a + uP^b = Q$, which is done. So let $A_{[2]} \nsubseteq P^2$. Hence there exists $s \in \mathbb{N} \cup \{0\}$ such that $s < b$, $\pi^s h \in A_{[2]}$ with $gcd(\pi, h) = 1$. So there exists $r \in \mathbb{F}_p[x]$ such that $r\pi^a + u\pi^s h \in A$.

Let $y = b_1 + ub_2 \in B$. Then

$$(r\pi^a + u\pi^s h)y = r\pi^a b_1 + r\pi^a ub_2 + u\pi^s hb_1 \in AB \subseteq Q = P^a + uP^b.$$

Now, there exists $l \in \mathbb{F}_p[x]$ such that $r\pi^a ub_2 = ul\pi^a b_2$. Hence

$$(r\pi^a + u\pi^s h)y = r\pi^a b_1 + ul\pi^a b_2 + u\pi^s hb_1 \in P^a + uP^b.$$

So $u\pi^s h b_1 \in vP^b$, which does hold provided that $b_1 \in P$. But, this implies that $B_{[1]} \subseteq P$, which we get that $B^n \subseteq Q$ for some $n \in \mathbb{N}$, as required.

Let $Q = u\mathbb{F}_p[x]$, then by lemma 2.18, Q is prime, and hence primary.

Let $Q = 0$. suppose that $AB \subseteq Q$. Then $A_{[1]}B_{[1]} \subseteq 0$. Hence $A_{[1]} = 0$ or $B_{[1]} = 0$. Thus $A = uA_{[2]}$ or $B = uB_{[2]}$. Let $A = uA_{[2]}$. Then $uA_{[2]}B_{[1]} = AB \subseteq 0$. So $A_{[2]} = 0$ or $B_{[1]} = 0$. If $A_{[2]} = 0$, then $A = 0$. Else, $B = uB_{[2]}$. So $B^2 = uB_{[2]}uB_{[2]} = 0$. □

Note: Let $f \in \mathbb{F}_p[x]$. Then it can easily be proved that there exists $h \in \mathbb{F}_p[x]$ such that $ug = hu$. We note h by $\widehat{f}$ and call it inverse partaker of f.

Lemma 2.25. *Let $A \trianglelefteq R$ and A is second type. Then, there exists a first type ideal $B \trianglelefteq R$ such that $B \subseteq A$. In particular, if $A_{[1]} = \langle f\rangle$, $A_{[2]} = \langle g\rangle$, then $\langle f\hat{f}\rangle + u\langle f\rangle \subseteq A$.*

Proof. Let $f+uh \in A$ for some $s \in \mathbb{F}_p[x]$. So $uf \in A$. Also, $\hat{f}(f+uh) \in A$. Hence, $\hat{f}f+ufh \in A$ and this results in $f\hat{f} \in A$. So $\langle f\hat{f}\rangle + u\langle f\rangle \subseteq A$. □

Lemma 2.26. *Let $<\pi>$ be a prime ideal of $\mathbb{F}_p[x]$. Then, $(\pi, \hat{\pi}) = 1$.*

Proof. Let $\pi|\hat{\pi}$. Then, $\pi h = \hat{\pi}$. Let $\pi = \sum_{i=0}^{m} p_i x^i$, $\hat{\pi} = \sum_{i=0}^{m} \hat{p}_i x^i$ and $h = \sum_{i=0}^{r} h_i x^i$. So for $m+1 \leq r \leq r+m$, $\sum_{i=0}^{r} p_i \alpha^i h_{r-i} = 0$.

We have r equations and r undetermined, and equations are independent. This results in $h = 0$. So $\hat{\pi} = 0$ which means that $\pi u = u\hat{\pi} = 0$. So $\pi = 0$, which is impossible. □

Theorem 2.27. *There is not a second type primary ideal in R.*

Proof. Let $BC \subseteq Q_{[1]}$. One can prove that $B^m \subseteq Q$ or $C^{m'} \subseteq Q$ or $u \in Q$ for some $m, m' \in \mathbb{N}$ in similar to Lemma 2.22.

If $u \in Q$ and $Q_{[1]} = \langle f\rangle$, $f \in Q$ by the fact that $f + uq \in Q$ for some $g \in Q_{[2]}$. Hence, Q must be of the first type ideal. So $Q_{[1]}$ is in the form of $P^l = \langle\pi\rangle^l$ for some irreducible polynomial in $\mathbb{F}_p[x]$. Let $Q_{[2]} = \langle\pi\rangle^{l-s} = P^{l-s}$. Also one can see that

$$(\langle\pi\hat{\pi}\rangle^l + u\langle\pi\rangle^{l-s})(\langle\pi\rangle^s + u\mathbb{F}_p) \subseteq \langle\pi^{l+s}\hat{\pi}^l\rangle + u\langle\pi\rangle^l + u\langle\pi'\pi\rangle^l \subseteq \langle\pi\hat{\pi}\rangle^l + u\langle\pi\rangle^l \subseteq Q. \tag{2.13}$$

So $\langle\pi\hat{\pi}\rangle^l + u\langle\pi\rangle^{l-s} \subseteq Q$ or $(\langle\pi\rangle^s + u\mathbb{F}_p[x])^m \subseteq Q$. If $\langle\pi\hat{\pi}\rangle^l + u\langle\pi\rangle^{l-s} \subseteq Q$, then $u\pi^{l-s} \in Q$ and so $\pi^l \in Q$. Thus Q becomes a first type ideal of R, which is impossible. So $(\pi^s + u)^m \in Q$ which results in $(\pi')^{s(m-1)} + \pi w \in Q_{[2]}$ for some $w \in \mathbb{F}_p[x]$. Hence, there exists some $k \in \mathbb{F}_p[x]$ such that $(\pi')^{s(m-1)} + \pi w_1 = \pi^{l-s}k$. So $\pi|\pi'$ or $l - s = 0$. $\pi|\pi'$ is not possible by previous lemma. Thus, $Q_{[2]} = \mathbb{F}_p[x]$.

Let $L \in \mathbb{F}_p[x]$. So for each $c, d \in \mathbb{F}_p[x]$, there exists $w_2 \in \mathbb{F}_p[x]$ such that $(\pi^{l-1}\hat{\pi}^l + u\pi')(c + ud)(\pi + uL) = \pi^l c\hat{\pi}^l + u\pi^l w_2 \in Q$. One can see that $\hat{\pi}^l\pi^{l-1} \notin Q_{[1]}$, so $\hat{\pi}^l\pi^{l-1} + u\pi^l \notin Q$. So $(\pi + uL)^m \in Q$ for some $m \in \mathbb{N}$. So there exists $m_1, m_2 \in \mathbb{N}$ such that $(\pi + u)^{m_1}, (\pi + 2u)^{m_2} \in Q$. Let $m = \max\{m_1, m_2\}$. Hence, $(\pi + 2u)^m - (\pi + u)^m \in Q$. Thus

$$\pi^m + 2u(\sum_{i=0}^{m-1} \pi^i(\pi')^{m-1-i}) - \pi^m - u(\sum_{i=0}^{m-1} \pi^i(\pi')^{m-1-i}) = u\sum_{i=0}^{m-1} \pi^i(\pi')^{m-i-1} \in Q. \tag{2.14}$$

Let $r = min\{\alpha | u\pi^\beta \in Q \quad for \quad \beta \geq \alpha\}$. So $\hat{\pi}^{r-1}u\sum_{i=0}^{m-1} \pi^i(\pi')^{m-i-1} \in Q$. Considering $u\pi^r \in Q$, we have $u\pi^{r-1}(\pi')^{m-1} \in Q$.

Since $(\pi, \pi') = 1$, there exists $z_1, z_2 \in \mathbb{F}_p[x]$ such that $(\pi')^{m-1}z_1 + \pi z_2 = 1$. We know that $u\pi^r \in Q$, so $\hat{z_2}u\pi^r \in Q$. Thus,

$$u\pi^{r-1} = u\pi^{r-1}(z_1(\pi')^{m-1} + \pi z_2) = u(z_1\pi^{r-1}(\pi')^{m-1} + z_2\pi^r) = \hat{z_1}u\pi^{r-1}(\pi')^{m-1} + \hat{z_2}u\pi^r \in Q.$$

This is a contradiction by definition of r. □

According to the above results, we could characterize first type primary ideals. We will study more about the role of the first and the second type primary ideals in primary decomposition as follows. First we prove the following lemma.

Theorem 2.28. *If $A \trianglelefteq R$ is a second type ideal and has a primary decomposition, then at least one of its components in primary decomposition of A must be of second type.*

Proof. Let there exists m primary ideals in decomposition of A. We prove the case $m = 2$. The general case is followed by induction. Let $A = Q \cap T$ for some primary ideals Q and T of R. If both of Q and T are of the first type, then by lemma 2.15

$$A = Q \cap T = (Q_{[1]} + uQ_{[2]}) \cap (T_{[1]} + uT_{[2]}) = (Q_{[1]} \cap T_{[1]}) + u(Q_{[2]} \cap T_{[2]})$$

Which is a first type ideal. So A is a first type ideal which is a contradiction by assumption. □

Corollary 2.29. *The second type ideals of R do not have primary decomposition. In another word, the ring R is not Laskerian.*

Proof. According to the Theorem 2.28, if a second type ideal has a primary decomposition, one of its components should be second type. But there is not any second type primary ideal by Theorem 2.27. □

3 Over the ring $(\mathbb{F}_p + u\mathbb{F}_p)[\mathbb{Z}_n]$

Our goal in this section is to show the equivalence of ideals of R_n (or the skew cyclic codes over $F_p + uF_p$) and the ideals of T_n. In the first step, we prove that θ' is well-defined. We know

$$\theta' : \frac{F_p[x]}{< x^n - 1 >} \longrightarrow \frac{F_p[x]}{< x^n - 1 >}, \qquad \theta'(\overline{1}) = \overline{1}, \theta'(\overline{x}) = \alpha^{-1}\overline{x}, \qquad \alpha \in F_p$$

Also, $O(\alpha) = O(\theta')$ (i.e. $O(\alpha)|n$). Let $h, g \in F_p[x]$ such that $\overline{h} = \overline{g}$. So $x^n - 1|h - g$. Moreover, $\theta'(\overline{h}) = \theta'(\sum_i \overline{h_i}\overline{x}^i) = \sum_i \overline{h_i}\theta'(\overline{x})^i = \sum_i \overline{h_i}\alpha^{-i}\overline{x}^i$ and $\theta'(\overline{g}) = \theta'(\sum_i \overline{g_i}\overline{x}^i) = \sum_i \overline{g_i}\theta'(\overline{x})^i = \sum_i \overline{g_i}\alpha^{-i}\overline{x}^i$.

We know $x^n - 1|\sum_i(h_i - g_i)x^i$, so $(\alpha^{-1}x)^n - 1|\sum_i(h_i - g_i)(\alpha^{-1}x)^i$. Since $\alpha^n = 1$, $x^n - 1|\sum_i(h_i - g_i)\alpha^{-i}x^i$. So $\sum_i \overline{h_i}\alpha^{-i}\overline{x}^i = \sum_i \overline{g_i}\alpha^{-i}\overline{x}^i$. So $\theta'(\overline{h}) = \theta'(\overline{g})$. Thus θ' is well-defined.

Furthemore, θ' is a ring homomorphism. Suppose that $\overline{f}, \overline{g} \in \frac{F_p[x]}{<x^n-1>}$. Then, if $f = \sum_i \overline{f_i}\overline{x}^i$, $g = \sum_i \overline{g_i}\overline{x}^i$,

$$\begin{aligned}\theta'(\overline{f}\overline{g}) =& \theta'((\sum_i \overline{f_i}\overline{x}^i)(\sum_i \overline{g_i}\overline{x}^i)) = \theta'(\sum_i\sum_j \overline{f_i}\overline{g_i}\overline{x}^{i+j}) \\ =& \sum_i\sum_j \overline{f_i}\overline{g_i}\theta'(\overline{x})^{i+j} = \sum_i\sum_j \overline{f_i}\overline{g_i}\alpha^{-i-j}\overline{x}^{i+j}\end{aligned}$$

$$=(\sum_i \overline{f}_i\alpha^{-i}\overline{x}^i)(\sum_i \overline{g_i}\alpha^{-i}\overline{x}^i) = \theta'(\overline{f})\theta(\overline{g}).$$

Hence, the ring T_n is well-defined by the definition of θ'. Now, it is turn to prove the isomorphism between T_n, R_n.

Theorem 3.1. *$T_n \simeq R_n$.*

Proof. Let $\psi : R_n \longrightarrow T_n$ be as follows

$$\psi(\sum_i(f_i + ul_ix^i) + R(x^n-1)) = (\sum_i(f_ix^i) + F_p[x](x^n-1)) + (\sum_i l_ix^i + F_p[x](x^n-1))v + < u^2 > .$$

First, we prove that ψ is well-defined. Let $\sum_i(f_i+ul_ix^i)+R(x^n-1) = \sum_i(g_i+uk^ix^i)+R(x^n-1)$. So $x^n-1|\sum_i((f_i-g_i)+u(l_i-k_i))x^i$. Hence, there exists $v, w \in \frac{F_p[x]}{<x^n-1>}$, such that

$$(x^n-1)v + u(x^n-1)w = \sum_i(f_i-g_i)x^i + u\sum_i(l_i-k_i))x^i$$

Thus, $x^n-1|\sum_i(f_i-g_i)x^i$ and $x^n-1|\sum_i(l_i-k_i)x^i$. So $\sum_i f_ix^i + F_p[x](x^n-1) = \sum_i g_ix^i + F_p[x](x^n-1)$ and $\sum_i l_ix^i + F_p[x](x^n-1) = \sum_i k_ix^i + F_p[x](x^n-1)$. So $\psi(\sum_i(f_i+ul_i)x^i + R(x^n-1)) = \psi(\sum_i(g_i+uk_i)x^i + R(x^n-1))$. This proves that ψ is well-defined.

Second, we prove that ψ is a ring homomorphism. Let $s(x) = (f+ul)+R(x^n-1) \in R_n$ and $v(x) = (g+uk)+R(x^n-1) \in R_n$. One can see

$$\overline{s}(x)\overline{v}(x) = \big((f+ul)+R(x^n-1)\big)\big((g+uk)+R(x^n-1)\big) = (fg+ulg+uf'k)+R(x^n-1).$$

So

$$\begin{aligned}
&\psi(\overline{s}(x))\psi(\overline{v}(x))\\
=&\big((f+F_p[x](x^n-1)) + (l+F_p[x](x^n-1))u + < u^2 > \big)\\
&\times\big((g+F_p[x](x^n-1)) + (k+F_p[x](x^n-1))u + < u^2 > \big)\\
=&\big(fg+F_p[x](x^n-1)\big) + \big(f'k+F_p[x](x^n-1)\big)u + (lg+F_p[x](x^n-1))u + < u^2 > .
\end{aligned}$$

Hence, $\psi(\overline{sv}) = \psi(\overline{s})\psi(\overline{v})$. Also, $\psi(\overline{s}+\overline{v}) = \psi(\overline{s})+\psi(\overline{v})$ is easy to prove.

Third, we prove that psi is an injective map. Let $\psi(\sum_i(f_i+ul_i)x^i + R(x^n-1)) = \overline{0}$. So

$$\big(\sum_i f_ix^i + F_p[x](x^n-1)\big) + u\big(\sum_i l_ix^i + F_p[x](x^n-1)\big) + < u^2 >= \overline{0}.$$

Thus, $s(x)(x^n-1) = \sum_i f_ix^i$, $w(x)(x^n-1) = \sum_i l_ix^i$ for some $s, w \in F_p[x]$. Hence, $(s(x)+uw(x))(x^n-1) = \sum_i(f_i+ul_i)x^i$. So $\sum_i(f_i+ul_i)x^i + R(x^n-1) = 0 + R(x^n-1)$.

Finally, we prove that ψ is surjective. Let $s(x) = h(x) + F_p[x](x^n-1) + (l(x)+F_p[x])u + < u^2 > \in T_n$. It is easy to see that

$$\psi(h(x) + ul(x) + R(x^n-1)) = s(x).$$

□

3.1 Prime ideals of T_n

Let $A \trianglelefteq R$, $x^n-1 \in A$. So $\frac{A}{<x^n-1>} \trianglelefteq R_n$. Thus, $\widehat{A} = \psi(\frac{A}{<x^n-1>}) \trianglelefteq T_n$. Let $\overline{f} = \big(g + F_p[x](x^n - 1)\big) + \big(h + F_p[x](x^n-1)\big)v+ < u^2 >$. Now, define

$$\overline{A}_{[1]} = \{g + F_p[x](x^n-1) | \exists h + F_p[x](x^n-1) \in \frac{F_p[x]}{< x^n - 1 >},$$
$$\psi^{-1}\big(g + F_p[x](x^n-1) + u(h + F_p[x](x^n-1)) + < u^2 > \big) \in \frac{A}{< x^n-1 >}\}$$
$$\overline{A}_{[2]} = \{h + F_p[x](x^n-1) | \exists g + F_p[x](x^n-1) \in \frac{F_p[x]}{< x^n - 1 >},$$
$$\psi^{-1}\big(g + F_p[x](x^n-1) + u(h + F_p[x](x^n-1)) + < u^2 > \big) \in \frac{A}{< x^n-1 >}\}$$

Theorem 3.2. *If $A \trianglelefteq R$ is a first type ideal, and $x^n - 1 \in A$, then $\psi(\frac{A}{<x^n-1>}) = \overline{A}_{[1]} + \overline{A}_{[2]}v+ < u^2 >$ (Consider $\overline{A}_{[1]}, \overline{A}_{[2]}$ as subrings of T_n).*

Proof. Let $A_{[1]} =< f >$ and $A_{[2]} =< g >$. So $f + ug \in A$. Hence, $\psi(f + ug + R(x^n - 1)) \in \psi(\frac{A}{<x^n-1>}) = \widehat{A}$. So

$$(f + F_p[x](x^n-1)) + (g + F_p[x](x^n-1))u+ < u^2 > \in \widehat{A}.$$

It is enough to show that $\overline{A}_{[1]} =< \overline{f} >, \overline{A}_{[2]} =< \overline{g} >$. Let $k \in \widehat{A}$ and $k = (h + F_p[x](x^n-1)) + (l + F_p[x](x^n-1))u+ < u^2 >$. Hence, $\psi^{-1}(k) = h + ul + R(x^n-1)$. Thus, there exists $v, w \in F_p[x]$ such that

$$h + ul + (x^n-1)(v + uw) \in A.$$

So $h(x) + u(x)(x^n-1) \in A_{[1]}$ and $l(x) + w(x)(x^n-1) \in A_{[2]}$. This means that $f(x)|h(x) + u(x)(x^n-1)$ and $g(x)|l(x) + w(x)(x^n-1)$. Considering the fact that $f|x^n-1, g|x^n-1$, $f|h, g|l$. So $h = fh_1$ and $l = gl_1$.

Hence, $k = (fh_1 + F_p[x](x^n-1)) + u(gl_1 + F_p[x](x^n-1))+ < u^2 >$. Thus, $\overline{A}_{[1]} =< f + F_p[x](x^n-1) >$, $\overline{A}_{[2]} =< g + F_p[x](x^n-1) >$. Considering the fact that $(f + F_p[x](x^n-1)) + u(g + F_p[x](x^n-1))+ < u^2 > \in \widehat{A}$, $\widehat{A} = \overline{A}_{[1]} + u\overline{A}_{[2]}+ < u^2 >$. □

Theorem 3.3. *Let $A \trianglelefteq R$, $x^n - 1 \in A$ and $\widehat{A} = \overline{A}_{[1]} + u\overline{A}_{[2]}+ < u^2 >$. Then A is a first type ideal of R.*

Proof. Let $A_{[1]} =< f >$ and $A_{[2]} =< g >$. Suppose that $(h + F_p[x](x^n-1)) + (k + F_p[x](x^n-1))u+ < u^2 > \in \widehat{A}$. So $h + uk + R(x^n-1) \in \frac{A}{<x^n-1>}$. Hence, there exists $l_1, l_2 \in R$ such that $f|h + l_1(x^n-1)$ and $g|k + l_2(x^n-1)$. Thus $f|h$ and $g|k$. If $h = h_1 f, k = k_1 g$, $(h_1 + F_p[x](x^n-1))(f + F_p[x](x^n-1)) + (k_1 + F_p[x](x^n-1))(g + F_p[x](x^n-1))u+ < u^2 > \in \widehat{A}$. So $\overline{A}_{[1]} =< f + F_p[x](x^n-1) >$, $A_{[2]} =< g + F_p[x](x^n-1) >$. This means that $(f + F_p[x](x^n-1)) + (g + F_p[x](x^n-1))u+ < u^2 > \in \widehat{A}$ (Otherwise, $\widehat{A} \neq \overline{A}_{[1]} + \overline{A}_{[2]}u+ < u^2 >$). Hence, $f + ug + R(x^n-1) = \psi^{-1}((f + F_p[x](x^n-1)) + (g + F_p[x](x^n-1))u+ < u^2 >) \in \frac{A}{<x^n-1>}$. So there exists $l_1 \in R$ such that $f + ug + l_1(x^n-1) \in A$. Considering the fact that $x^n - 1 \in A$, $f + ug \in A$. So $A = A_{[1]} + A_{[2]}u$. Hence, A is first type. □

We call $\widehat{A}$ is a first type ideal of T_n, if A is a first type ideal of R. Hence, $\widehat{A}$ is first type, if and only if $\widehat{A} = \overline{A}_{[1]} + \overline{A}_{[2]}u + < u^2 >$. We show it by $\widehat{A} = \overline{A}_{[1]} + \overline{A}_{[2]}u$ for simplicity reasons.

Theorem 3.4. *Let $A \trianglelefteq R$, $x^n - 1 \in A$. Then $\overline{A}_{[1]}, \overline{A}_{[2]}$ are ideals of $\frac{F_p[x]}{<x^n-1>}$.*

Proof. Let $f + F_p[x](x^n - 1) \in \overline{A}_{[1]}$ and $g + F_p[x](x^n - 1) \in \frac{F_p[x]}{<x^n-1>}$, So there exists $k + F_p[x](x^n - 1) \in \frac{F_p[x]}{<x^n-1>}$ such that

$$\psi^{-1}\big((f + F_p[x](x^n - 1)) + u(k + F_p[x](x^n - 1)) + < u^2 > \big) \in \frac{A}{< x^n - 1 >}.$$

Hence, $f + uk + R(x^n - 1) \in \frac{A}{<x^n-1>}$. So $\big((g + R(x^n - 1))(f + uk + R(x^n - 1))\big) \in \frac{A}{<x^n-1>}$. So $fg + ukg + R(x^n - 1) \in \frac{A}{<x^n-1>}$. Thus

$$\psi\big(fg + ukg + R(x^n - 1)\big) \in \widehat{A}.$$

Hence, $fg + F_p[x](x^n - 1) \in \overline{A}_{[1]}$ which means that $(f + F_p[x](x^n - 1))(g + F_p[x](x^n - 1)) \in \overline{A}_{[1]}$. Thus $\overline{A}_{[1]}$ is an ideal of $\frac{F_p[x]}{<x^n-1>}$. In similar way, one can see that $\overline{A}_{[2]}$ is an ideal of $\frac{F_p[x]}{<x^n-1>}$. □

Theorem 3.5. *Let $A \trianglelefteq R$, $x^n - 1 \in A$. Then $\psi(u\overline{A}_{[1]}) = \frac{\overline{A}_{[1]}[u,\theta']u}{<u^2>} \trianglelefteq T_n$. Moreover, $\frac{\overline{A}_{[1]}[u,\theta']u}{<u^2>} \subseteq \widehat{A}$.*

Proof. Let $f + F_p[x](x^n - 1) \in \overline{A}_{[1]}$ and $\overline{u} = (g + F_p[x](x^n - 1)) + (k + F_p[x](x^n - 1))u + < u^2 > \in T_n$. It is enough to show that $\overline{u}\big((f + F_p[x](x^n - 1))u + < u^2 > \big) \in \frac{\overline{A}_{[1]}[u,\theta']u}{<u^2>}$. Since, $\overline{A}_{[1]} \trianglelefteq \frac{F_p[x]}{<x^n-1>}$ and $f + F_p[x](x^n - 1) \in \overline{A}_{[1]}$, $fg \in \overline{A}_{[1]}$. So $(g'f + F_p[x](x^n - 1))u + < u^2 > \in \frac{u\overline{A}_{[1]}[u,\theta']}{<u^2>}$. Hence,

$$\begin{aligned}&\big((f + F_p[x](x^n - 1))u + < u^2 > \big)\big((g + F_p[x](x^n - 1)) + (k + F_p[x](x^n - 1))u + < u^2 > \big)\\ &= \big((fg + F_p[x](x^n - 1))u + < u^2 > \big) \in \frac{\overline{A}_{[1]}[u, \theta']u}{< u^2 >}.\end{aligned}$$

So $\frac{\overline{A}_{[1]}[u,\theta']u}{<u^2>} \trianglelefteq T_n$. Also, let $f + F_p[x](x^n - 1) \in \overline{A}_{[1]}$. So there exists $h + F_p[x](x^n - 1) \in \frac{F_p[x]}{<x^n-1>}$ such that $\psi^{-1}\big((f + F_p[x](x^n - 1)) + (h + F_p[x](x^n - 1))u + < u^2 > \big) \in \frac{A}{<x^n-1>}$. Thus $f + uh + R(x^n - 1) \in \frac{A}{<x^n-1>}$. Hence, $(u + R(x^n - 1))(f + uh + R(x^n - 1)) \in \frac{A}{<x^n-1>}$. So $uf + R(x^n - 1) \in \frac{A}{<x^n-1>}$. So $(f + F_p[x](x^n - 1))u + < u^2 > \in \widehat{A}$. Thus $\frac{\overline{A}_{[1]}[v,\theta']v}{<u^2>} \subseteq \widehat{A}$. □

Theorem 3.6. *Let $A \trianglelefteq R$, $x^n - 1 \in A$. Then $\overline{A}_{[1]} \subseteq \overline{A}_{[2]}$.*

Proof. Let $f + F_p[x](x^n - 1) \trianglelefteq \overline{A}_{[1]}$. So there exists $h + F_p[x](x^n - 1) \in \frac{F_p[x]}{<x^n-1>}$ such that $\psi^{-1}\big((f + F_p[x](x^n - 1)) + (h + F_p[x](x^n - 1))u + < u^2 > \big) \in \frac{A}{<x^n-1>}$. Thus $f + uh + R(x^n - 1) \in \frac{A}{<x^n-1>}$. So

$$(u + R(x^n - 1))(f + uh + R(x^n - 1)) = uf + R(x^n - 1) \in \frac{A}{< x^n - 1 >}$$

Thus $\psi(uf + R(x^n - 1)) \in \widehat{A}$. This means that $(f + F_p[x](x^n - 1))u + < u^2 > \in \widehat{A}$. So $f + F_p[x](x^n - 1) \in \overline{A}_{[2]}$. Hence, $\overline{A}_{[1]} \subseteq \overline{A}_{[2]}$. □

Theorem 3.7. *If $P \trianglelefteq R$ is a prime ideal and $x^n - 1 \in P$, then $\widehat{P}$ is a prime in T_n.*

Proof. Let $\widehat{A}\widehat{B} \subseteq \widehat{P}$ and $\widehat{A}, \widehat{B}$ are two arbitrary ideal of T_n. Hence, $\psi^{-1}(\widehat{A}\widehat{B}) \subseteq \psi^{-1}(\widehat{P})$. Since ψ is isomorphism, $\psi^{-1}(\widehat{A})\psi^{-1}(\widehat{B}) \subseteq \psi^{-1}(\widehat{A}\widehat{B})$. So $\psi^{-1}(\widehat{A})\psi(\widehat{B}) \subseteq \frac{P}{<x^n-1>}$. Thus, $\frac{A}{<x^n-1>}\frac{B}{x^n-1} \subseteq \frac{P}{x^n-1}$. So $AB \subseteq P$. This implies $A \subseteq P$ or $B \subseteq P$ (Since $x^n - 1 \in A, B$). So $\psi(\frac{A}{<x^n-1>}) \subseteq \widehat{P}$ or $\psi(\frac{B}{<x^n-1>}) \subseteq \widehat{P}$. Hence, $\widehat{A} \subseteq \widehat{P}$ or $\widehat{B} \subseteq \widehat{P}$. □

Theorem 3.8. *Let $\widehat{P}$ is a prime ideal of T_n, then P is a prime ideal of R.*

Proof. Let $AB \subseteq P, A, B \trianglelefteq R$. Suppose that $A^* =< A, x^n - 1 >$ and $B^* =< B, x^n - 1 >$. Since $x^n - 1 \in P$, $A^*B^* \subseteq P$. So $\frac{A^*}{<x^n-1>}\frac{B^*}{<x^n-1>} \subseteq \frac{P}{<x^n-1>}$. So $\widehat{A^*}\widehat{B^*} \subseteq \widehat{P}$. This implies that $\widehat{A^*} \subseteq \widehat{P}$ or $\widehat{B^*} \subseteq \widehat{P}$. So $\frac{A^*}{<x^n-1>} \subseteq \frac{P}{<x^n-1>}$ or $\frac{B^*}{<x^n-1>} \subseteq \frac{P}{<x^n-1>}$. Hence, $A^* \subseteq P$ or $B^* \subseteq P$. This means that $A \subseteq P$ or $B \subseteq P$. So P is a prime ideal of R. □

Corollary 3.9. *Let $P \trianglelefteq R$, $x^n - 1 \in P$. Then P is a prime ideal of R, iff $\widehat{P}$ is a prime ideal of T_n.*

Corollary 3.10. *Let $\widehat{P} \trianglelefteq T_n$ be a prime ideal. Then there are two cases.*
i) $P = \psi(\frac{F_p[x]f+uF_p[x]}{<x^n-1>})$ where $f \in F_p[x]$ is an irreducible polynomial such that $f|x^n - 1$.
ii) $P = \psi(\frac{F_p[x](x^n-1)+uF_p[x]}{<x^n-1>})$.

Proof. The proof follows from Corollary 3.9 and Theorem 2.19 □

Proposition 3.11. *$J(R_n) =< \prod_{f:irreducible} f > +u\mathbb{F}_p[x]$.*

Proof. According to correspondence theorem for PID, the maximal ideals of $\frac{\mathbb{F}_p[x]}{<x^n-1>}$ are correspondent to the maximal ideals of $\mathbb{F}_p[x]$ which contains $x^n - 1$. So

$$J(R_n) = \bigcap_{\overline{m} \trianglelefteq_m R_n} \overline{m} = \bigcap_{\substack{m \trianglelefteq_m R \\ x^n-1 \in m}} \frac{m}{< x^n - 1 >}.$$

According to Theorem 2.14, every maximal ideals of R are in the form of $< f > +u\mathbb{F}_p[x]$ where f is irreducible. Since $x^n - 1 \in m$, $f|x^n - 1$. On the other hand, $x^n - 1$ does not have any repeated root, so

$$J(R_n) = \bigcap_{\substack{m \trianglelefteq_m R \\ x^n-1 \in m}} \frac{m}{< x^n - 1 >} = \frac{< \prod_{\substack{f:irreducible \\ f|x^n-1}} f > +u\mathbb{F}_p[x]}{< x^n - 1 >}.$$

□

Proposition 3.12. *$Nil(R_n) = \frac{\mathbb{F}_p[x](x^n-1)+u\mathbb{F}_p[x]}{<x^n-1>}$*

Proof. Let $f+ < x^n - 1 >\in Nil(R_n)$. So there exists $m \in \mathbb{N}$ such that $(f+ < x^n - 1)^m = 0$. Thus $f^m \in< x^n - 1 >$. Hence $x^n - 1|f_1^m$. Since $x^n - 1$ does not have any repeated root in its split field, $x^n - 1|f_1$. So $f_1+ < x^n - 1 >=< x^n - 1 >$. This means that $f = uf_2+ < x^n - 1 >$. Hence $Nil(R) \subseteq \frac{\mathbb{F}_p[x](x^n-1)+u\mathbb{F}_p[x]}{<x^n-1>}$. The converse is easy. □

Corollary 3.13. *$Nil_*(R_n) = Nil(R_n) = Nil^*(R_n)$.*

Proof. According to Corollary 3.10, we have

$$
\begin{aligned}
Nil_*(R_n) &= \bigcap_{P\in Spec(R_n)} P\\
&=\Big(\bigcap_{f:irreducible}(\frac{F_p[x]f+uF_p[x]}{<x^n-1>})\Big)\cap(\frac{F_p[x](x^n-1)+uF_p[x]}{<x^n-1>})=\frac{F_p[x](x^n-1)+uF_p[x]}{<x^n-1>}
\end{aligned}
$$

Since $Nil(R_n)$ is an ideal, $Nil(R_n) = Nil^*(R_n)$. This and Proposition 3.12 completes the proof. □

3.2 The primary ideals of T_n

First, we start with some lemma to find an equivalence theorem between primary ideals of T_n and some of primary ideals in R.

Lemma 3.14. *Let $A \trianglelefteq R, x^n-1 \in A$. Then $(\psi^{-1}(\widehat{A}))^m \subseteq \psi^{-1}(\widehat{A}^m)$.*

Proof. Since ψ is an isomorphism, $\psi^{-1}(B)\psi^{-1}(C) \subseteq \psi^{-1}(BC)$ for each ideals of T_n like B, C. So $\psi^{-1}(\widehat{A})^m \subseteq \psi^{-1}(\widehat{A}^m)$. □

Also, one can prove that easily that $\frac{A^m}{<x^n-1>} = (\frac{A}{<x^n-1>})^m$.

Theorem 3.15. *Let $Q \trianglelefteq R$, $x^n-1 \in Q$. If $\widehat{Q}$ is a primary ideal of T_n, then Q is a primary ideal of R.*

Proof. Let $AB \subseteq Q$. Suppose that $A^* =< A, x^n-1 >, B^* =< B, x^n-1 >$. So $A^*B^* \subseteq Q$ and this results in $\frac{A^*}{<x^n-1>}\frac{B^*}{<x^n-1>} \subseteq \frac{Q}{<x^n-1>}$. Hence, $\psi(\frac{A^*}{<x^n-1>})\psi(\frac{B^*}{<x^n-1>}) \subseteq \psi(\frac{Q}{<x^n-1>})$. Thus $\widehat{A^*}\widehat{B^*} \subseteq \widehat{Q}$. This means that $\widehat{A^*} \subseteq \widehat{Q}$ or $(\widehat{B^*})^m \subseteq \widehat{Q}$ for some $m \in \mathbb{N}$. Hence, $\psi^{-1}(\widehat{A^*}) \subseteq \psi^{-1}(\widehat{Q})$ or $\psi^{-1}(\widehat{B^*}^m) \subseteq \psi^{-1}(\widehat{Q})$. So $\frac{A^*}{<x^n-1>} \subseteq \frac{Q}{<x^n-1>}$ or $(\frac{B^*}{<x^n-1>})^m \subseteq \frac{Q}{<x^n-1>}$ for some $m \in \mathbb{N}$ by lemma 3.14. So $A^* \subseteq Q$ or $(B^*)^m \subseteq Q$ for some $m \in \mathbb{N}$. So Q is primary. □

Theorem 3.16. *Let $Q \trianglelefteq R, x^n-1 \in Q$ be a primary ideal of R. Then $\widehat{Q}$ is a primary ideal of T_n.*

Proof. Let $\widehat{A}\widehat{B} \subseteq \widehat{Q}$. So $\psi^{-1}(\widehat{A})\psi^{-1}(\widehat{B}) \subseteq \psi^{-1}(\widehat{A}\widehat{B}) \subseteq \psi(\widehat{Q})$. So $\frac{AB,x^n-1}{<x^n-1>} \subseteq \frac{Q}{<x^n-1>}$. Hence, $< AB, x^n-1 >\subseteq Q$. Thus $AB \subseteq Q$ which results in $A \subseteq Q$ or $B^m \subseteq Q$ fr some $m \in \mathbb{N}$. So $\psi(\frac{A}{<x^n-1>}) \subseteq \psi(\frac{Q}{<x^n-1>})$ or $\psi(\frac{B^m,x^n-1}{<x^n-1>}) = \big(\psi(\frac{B}{<x^n-1>})\big)^m \subseteq \psi(\frac{Q}{<x^n-1>})$ for some $m \in \mathbb{N}$. Hence, $\widehat{A} \subseteq \widehat{Q}$ or $\widehat{B}^m \subseteq \widehat{Q}$ for some $m \in \mathbb{N}$. Thus $\widehat{Q}$ is a primary ideal. □

Corollary 3.17. *Let $Q \trianglelefteq R, x^n-1 \in Q$. Then Q is a primary ideal of Q, iff $\widehat{Q}$ is a primary ideal of T_n. In particular, every primary ideal $\widehat{Q}$ in T_n is the first type ideal and exactly in one of the following forms.*

i) $\psi(\frac{F_p[x]f^a+uF_p[x]}{<x^n-1>})$ *where $f \in F_p[x]$ is an irreducible polynomial such that $f^a|x^n-1$ and $a \geq 0$.*

ii) $\psi(\frac{F_p[x]f^a+uF_p[x]f^b}{<x^n-1>})$ *where $f \in F_p[x]$ is an irreducible polynomial such that $f^b|x^n-1$ and $a > b \geq 0$.*

iii) $\widehat{0}$.

Theorem 3.18. *Let $A \trianglelefteq R, x^n-1 \in A$. If $\widehat{A}$ has a primary decomposition such that all of its primary coefficients in decomposition are first type, then $\widehat{A}$ is a first type ideal.*

Proof. Let $\widehat{A}$ be a second type ideal. Also $\widehat{A} = \widehat{Q}_1 \cap \widehat{Q}_2 \cap \cdots \cap \widehat{Q}_t$ for some primary ideals $\widehat{Q}_i$. Then $\psi^{-1}(\widehat{A}) = \psi^{-1}(\widehat{Q}_1) \cap \cdots \cap \psi^{-1}\widehat{Q}_t$. So $\frac{A}{<x^n-1>} = \frac{Q_1}{<x^n-1>} \cap \cdots \cap \frac{Q_t}{<x^n-1>}$. As$x^n - 1 \in Q_i$ for some $1 \leq i \leq t$, $x^n - 1 \in \bigcap_{i=1}^t Q_i$. So $\frac{A}{<x^n-1>} = \frac{\bigcap_{i=1}^t Q_i}{<x^n-1>}$. Hence, $A = Q_1 \cap \cdots \cap Q_t$. Thus A should be a first type ideal by lemma 2.28. So $\widehat{A}$ is a first type ideal by lemma 3.2. □

So if $\widehat{A}$ is a second type ideal and has a primary decomposition, then there exists at least one second type primary coefficient in its decomposition. But finding a second type ideal is not easy and from the computation view, it seems demanding.

Assume a first type ideal $\widehat{A}$. So $\widehat{A} = \overline{A}_{[1]} + u\overline{A}_{[2]}$. Since $\frac{F_p[x]}{<x^n-1>}$ is a Notherian commutative ring, the unique primary decomposition exists for $\overline{A}_{[1]}, \overline{A}_{[2]}$.So

$$\widehat{A} = (\bigcap_i Z_i) + u(\bigcap_i Y_i) \tag{3.1}$$

where Z_i, Y_i are primary ideals of $\frac{F_p[x]}{<x^n-1>}$. So there is a characterization for first type ideals of T_n.

Proposition 3.19. *There is no second type primary ideal in R_n.*

Proof. According to the Theorem 3.15 and Theorem 3.16, $A \trianglelefteq R, x^n - 1 \in A$ is primary, if and only if $\widehat{A} \trianglelefteq R_n$. Let $\widehat{A}$ be a second type primary ideal in R_n. Then A should be a second type primary ideal according to Theorems 3.2,3.3. This is impossible according to Theorem 2.27. So there is not any second type primary ideal in R_n. □

Corollary 3.20. *The second type ideals of R_n do not have primary decomposition. In particular, R_n is not Laskerian.*

Proof. The proof follows by the Proposition 3.19 and Theorem 3.18. □

References

[1] Zariski, Oscar, and Pierre Samuel. Commutative algebra. **2**. *Springer Science , Business Media*, 2013.

[2] Calderbank, A. Robert, and Neil JA Sloane. Modular and p-adic cyclic codes. Designs, Codes and Cryptography **6**.1 (1995): 21-35.

[3] Kanwar, Pramod, and Sergio R. Lopez-Permouth. Cyclic Codes over the Integers Modulo p_m. Finite Fields and Their Applications **3**.4 (1997): 334-352.

[4] Bonnecaze, Alexis, and Parampalli Udaya. Cyclic codes and self-dual codes over $\mathbb{F}_2 + u\mathbb{F}_2$. IEEE Transactions on Information Theory. **45**.4 (1999): 1250-1255.

[5] Wolfmann, Binary Images of Cyclic Codes over $\mathbb{Z}_4$, IEEE Transactions on Information Theory. **47**, No. 5, 2001, 1773.

[6] Blackford, Thomas. Negacyclic codes over $\mathbb{Z}_4$ of even length. IEEE Transactions on Information Theory. **49**.6 (2003): 1417-1424.

[7] Wood, Jay. The structure of linear codes of constant weight. Transactions of the American Mathematical Society **354**.3 (2002): 1007-1026.

[8] Dougherty, Steven T., and Keisuke Shiromoto. Maximum distance codes over rings of order 4. IEEE Transactions on Information Theory **47**.1 (2001): 400-404.

[9] Dinh, Hai Quang, and Sergio R. Lopez-Permouth. Cyclic and negacyclic codes over finite chain rings. IEEE Transactions on Information Theory, **50**.8 (2004): 1728-1744.

[10] Boucher, Delphine, Willi Geiselmann, and Flix Ulmer. Skew-cyclic codes. Applicable Algebra in Engineering, Communication and Computing **18**.4 (2007): 379-389.

[11] Boucher, D. Sole, P. Ulmer, F. Skew constacyclic codes over galois rings. Advances in Mathematics of Communications, **2**, 273-292 (2008).

[12] Abualrub, Taher, et al. On the construction of skew quasi-cyclic codes. IEEE Transactions on Information Theory, 56.5 (2010): 2081-2090.

[13] Siap, Irfan, et al. Skew cyclic codes of arbitrary length. International Journal of Information and Coding Theory 2.1 (2011): 10-20.

[14] Gao, Jian. Skew cyclic codes over $\mathbb{F}_p + v\mathbb{F}_p$. J. Appl. Math. Inform 31.3-4 (2013): 337-342.

[15] Chatzidakis, Zo, and Peter Pappas. ”Von Neumann regular group rings not representable as rings of continuous functions.” Algebra Universalis 29.3 (1992): 332-337.

[16] Karpilovsky, G. ”The Jacobson radical of commutative group rings.” Archiv der Mathematik 39.5 (1982): 428-430.

[17] Zhou, Yiqiang. ”On clean group rings.” Advances in Ring Theory. Birkhuser Basel, 2010. 335-345.

[18] Li, Yuanlin, M. M. Parmenter, and Pingzhi Yuan. ”On*-clean group rings.”Journal of Algebra and Its Applications 14.01 (2015): 1550004.

[19] Fisher, Joe. ”The primary decomposition theory for modules.” Pacific Journal of Mathematics 35.2 (1970): 359-367.

[20] Hutchinson, John J., and Maureen H. Fenrick. ”Primary decompositions and morita contexts.” Communications in Algebra 6.13 (1978): 1359-1368.

[21] Jahan, Ali Soleyman. ”Prime filtrations and primary decompositions of modules.” Communications in Algebra 39.1 (2010): 116-124.

[22] Smith, P F. ”Uniqueness of primary decompositions.” Turkish Journal of Mathematics 27.3 (2003): 425-434.

[23] Ayoub, Christine W. ”The decomposition theorem for ideals in polynomial rings over a domain.” Journal of Algebra 76.1 (1982): 99-110.

[24] Gianni, Patrizia, Barry Trager, and Gail Zacharias. ”Grobner bases and primary decomposition of polynomial ideals.” Journal of Symbolic Computation 6.2 (1988): 149-167.

[25] Grbe, Hans-Gert. "Minimal primary decomposition and factorized Grobner bases." Applicable Algebra in Engineering, Communication and Computing8.4 (1997): 265-278.

[26] Monico, Chris. "Computing the primary decomposition of zero-dimensional ideals." Journal of Symbolic Computation 34.5 (2002): 451-459.

[27] Sausse, Alain. "A new approach to primary decomposition." Journal of Symbolic Computation 31.1 (2001):243-257.

[28] Shimoyama, Takeshi, and Kazuhiro Yokoyama. "Localization and primary decomposition of polynomial ideals." Journal of Symbolic Computation 22.3 (1996): 247-277.

[29] Dinh, Trung T. "Growth of primary decompositions of Frobenius powers of ideals." Journal of Algebra 321.3 (2009): 829-846.

[30] Gordon, Robert. "Primary decomposition in right noetherian rings."Communications in Algebra 2.6 (1974): 491-524.

[31] Yao, Yongwei. "Primary decomposition II: Primary components and linear growth." Journal of Pure and Applied Algebra 205.1 (2006): 226-242.

[32] Ceken, Seil, and Mustafa Alkan. "ON Prime submodules and primary decompositions in two-generated free modules." Taiwanese Journal of Mathematics 17.1 (2013): pp-133.

[33] Perling, Markus, and Shiv Datt Kumar. "Primary decomposition over rings graded by finitely generated Abelian groups." Journal of Algebra 318.2 (2007): 553-561.

[34] Lescot, Paul. "Prime and primary ideals in characteristic one." arXiv preprint arXiv:1310.8400 (2013).

[35] Brookfield, Gary. "Noetherian generalized power series rings." (2004): 919-926.