Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 29 (2026), No. 7, pp. 2885–2895
DOI : 10.47974/JDMSC-2686

Quotient rings and polynomial structures in the context of p-adic integers

Boubakeur Bahri [‡]
Department of Mathematics
University of Abbes Laghrour
Khenchela
Algeria

Yassine Guerboussa [†]
Department of Computer Science
Kasdi Merbah University
Ouargla
Algeria

Souad Ayadi [§]
Department of Physics
Acoustics and Civil Engineering Laboratory
Faculty of Materials Sciences and Computer Science
Khemis Miliana University
Thniet El Had Street
Khemis Miliana 44225
Algeria

Abdelkader Benali *
Department of Mathematics
Laboratory of Mathematics and Applications (LMA)
Faculty of Exact Sciences and Informatics
Hassiba Benbouali University
Chlef 02000
Algeria

[‡] *ORCID-ID:* **0000-0001-1311-0512**
[†] *ORCID-ID:* **0000-0001-5518-0513**
[§] *ORCID-ID:* **0000-0001-7011-5389**
* *ORCID-ID:* **0009-0006-9772-2799**

[‡] *E-mail:* **bahri.boubakeur@univ-khenchela.dz**
[†] *E-mail:* **yassine guer@hotmail.fr**
[§] *E-mail:* **souad.ayadi@univ-dbkm.dz**
* *E-mail:* **benali4848@gmail.com (Corresponding Author)**

Abstract

This work provides a comprehensive description of the quotient ring A/m^n, where $A = \mathbb{Z}[\zeta]$ and $m = (1 - \zeta)$ is a maximal ideal corresponding to a primitive p-th root of unity ζ. where [1] p is prime number . We explore the structure of A/m^n for various values of n, highlighting its properties as a finite Artin local ring [2] and its connection to the p-adic integer ring $\mathbb{Z}_p$. By employing techniques from algebraic number theory, we explicitly describe the elements of A/m^n, which facilitates the computation of sums and products of any two elements within this ring. This exposition not only elucidates the arithmetic structure of A/m^n but also provides valuable insights into its relationship with cyclotomic fields and p-adic analysis [3].

Subject Classification: *13B30, 12E05, 11R18.*

Keywords: *p-adic integer ring, Polynomial Structures, Cyclotomic rings.*

1. Introduction; the main results

Let $A = \mathbb{Z}[\zeta]$, where ζ is a primitive p-th root of unity. The ideal $m = (1 - \zeta)$ is a maximal ideal, and a direct computation shows that $(1 - \zeta)^{p-1}$ is equal to a unit in A times p. Consequently, m^{p-1} corresponds to the ideal pA generated by p in A.

When considering the ring A/m^n, for $n \leq p - 1$, we find that

$$A/m^n \cong \mathbb{Z}/(p\mathbb{Z})[y]/(y^n$$

which is the polynomial ring in one variable over $\mathbb{Z}/p\mathbb{Z}$ mod the ideal generated by y^n. This structure reveals that A/m^n is a finite Artin local ring with exactly p^n elements, where all ideals are principal. The residue field, obtained by taking the quotient over the unique maximal ideal, is isomorphic to $\mathbb{Z}/p\mathbb{Z}$.

However, when $n > p - 1$, the situation changes; A/m^n contains a copy of $\mathbb{Z}/(p^d\mathbb{Z})$ for $d > 1$, and thus it no longer contains a copy of $\mathbb{Z}/p\mathbb{Z}$. Specifically, for $(d - 1)(p - 1) < n \leq d(p - 1)$, A/m^n will include $\mathbb{Z}/(p^d\mathbb{Z})$. As n increases, so does the value of d, indicating that in the limit as $n \to \infty$, the inverse limit would yield the p-adic integers $\mathbb{Z}_p$ [4], suggesting it aligns with the m-adic completion of the ring A as discussed in Chapter 10 of Atiyah and Macdonald. [5]

Furthermore, I conjectured that A/m^n might be isomorphic to $\mathbb{Z}/(p^d\mathbb{Z})[y]/(y^n)$ for appropriately chosen d, echoing the case for $n \leq p - 1$ where $d = 1$. However, for $d > 1$, these rings turn out to be larger, containing p^{dn} elements compared to the p^n elements of A/m^n.

In general, A/m^n is always a finite Artin local ring with p^n elements, and every ideal in A/m^n is principal. One can also view A/m^n as a factor ring of $\mathbb{Z}[x]$, specifically isomorphic to

$$\mathbb{Z}[x]/((x - 1)^n, \Phi_p(x)),$$

where $\Phi_p(x)$ is the p-th cyclotomic polynomial. While this representation accurately describes the ring, it may obscure its underlying arithmetic structure. By changing variables to $y = x - 1$, we can rewrite this as

$$A/m^n \cong \mathbb{Z}[y]/(y^n, \Phi_p(y+1)).$$

Defining $I = (y^n, \Phi_p(y+1))$ leads to

$$A/m^n \cong \mathbb{Z}[y]/I.$$

My aim was to provide a clear description of A/m^n as a familiar factor ring, allowing us to discern the multiplication rule. We can further express this factor ring as

$$\mathbb{Z}[y]/(y^n, y^{p-1} - u \cdot p),$$

where u is a unit modulo y^n. In this context, y^{p-1} is identified with a unit times p in the quotient, and y^n corresponds to 0.

By interpreting y as mapping to $\zeta - 1$ in A, we maintain consistency with the observation that

$$(\zeta - 1)^{p-1} = -(1-\zeta)^{p-1},$$

which equals a unit times p in A. This framework allows us to explicitly describe the elements of A/m^n, facilitating the computation of sums and products of any two elements.

2. Explanation of the Theorem

In our work we give The theorem states that for a given integer n and a prime p, the structure of the quotient ring A/m^n can be characterized based on the relationship between n and $p-1$. [7, 8]

- $A = \mathbb{Z}[\zeta]$ is the ring of integers adjoined with a primitive p-th root of unity ζ.
- $m = (1-\zeta)$ is a maximal ideal in A.
- The integer d is defined as the smallest positive integer such that $d \leq \frac{n}{p-1}$.

2.1 *Cases:*

Case 1: If n is less than or equal to $p-1$, then the quotient ring can be expressed as:

$$A/m^n \cong (\mathbb{Z}/p\mathbb{Z})[y]/(y^n).$$

This indicates that for small n, the structure resembles that of a polynomial ring over a finite field.

Case 2: If $n > p-1$, then the quotient ring has a more complex structure:

$$A/m^n \cong \begin{cases} \mathbb{Z}[y]/(y^n, y^{p-1} - u) \\ \mathbb{Z}/p^d\mathbb{Z}[y]/(y^n, y^{p-1} - u) \end{cases}$$

Here, u is a unit modulo y^n, and the ring can either be a polynomial ring or a polynomial ring over $\mathbb{Z}/p^d\mathbb{Z}$.

3. Definition of the p-adic Integer Ring

The p-adic integer ring, denoted $\mathbb{Z}_p$, is defined as the set of all formal series of the form:

$$\mathbb{Z}_p = \{a_0 + a_1 p + a_2 p^2 + \cdots | a_i \in \{0,1,\ldots,p-1\}\}$$

This ring can also be characterized as the inverse limit of the rings of integers modulo powers of p:

$$\mathbb{Z}_p = \overset{\lim}{\longrightarrow} \mathbb{Z}/p^n\mathbb{Z}$$

As a complete local ring, $\mathbb{Z}_p$ is an Artin local ring, meaning that every ideal is a principal ideal and the residue field is finite. Specifically, the residue field $\mathbb{Z}_p/(p)$ is isomorphic to $\mathbb{F}_p$, the finite field with p elements. Thus, $\mathbb{Z}_p$ has a rich arithmetic structure that mirrors that of $\mathbb{Q}_p$, the field of p-adic numbers.[9]

4. Proposition

Let ζ denote a pth root of unity, let $A = \mathbb{Z}[\zeta]$, and let $m = (1-\zeta)$ denote the maximal ideal in A generated by $1-\zeta$. Then $|A/m^n| = p^n$.

Proof: **Step 1:** First, argue that $A/m \cong \mathbb{Z}/p\mathbb{Z}$, and hence $|A/m| = p$. You seem to know this fact, but there are also several easy proofs. [6] For example, one could look at the composite map ϕ obtained by first embedding $\mathbb{Z}$ in A in the canonical way, and then reducing A modulo m:

$$\mathbb{Z} \overset{\text{embed}}{\longrightarrow} A \overset{\text{reduce}}{\longrightarrow} A/m.$$

Since $m = (1-\zeta)$, it is clear that $\zeta \equiv 1 \bmod m$, and hence any element of $A = \{a_0 + a_1\zeta + a_2\zeta^2 + \cdots + a_{p-1}\zeta^{p-2} | a_i \in \mathbb{Z}\}$ will be congruent to an element of $\mathbb{Z} \bmod m$. This means that every coset in A/m can be chosen to have a representative in $\mathbb{Z}$, which implies that the composite homomorphism ϕ maps $\mathbb{Z}$ onto A/m.

Then it follows from the First Isomorphism Theorem that

$$\mathbb{Z}/\text{Kernel}(\phi) \cong A/m.$$

Since ϕ is onto, we have $\text{Image}(\phi) = A/m$. Moreover, it is easy to see that $\text{Kernel}(\phi) = p\mathbb{Z}$ since clearly $p\mathbb{Z} \subseteq \text{Kernel}(\phi)$ (as one can plug $x = 1$ into both sides of the equation

$$(x-\zeta)(x-\zeta^2)(x-\zeta^3)\cdots(x-\zeta^{p-1}) = x^p - 1 \equiv x - 1 \bmod m$$

to deduce that $(1-\zeta)(1-\zeta^2)(1-\zeta^3)\cdots(1-\zeta^{p-1}) = p$, which says that p is divisible by $1-\zeta$ in A, hence $p \equiv 0 \bmod m$).

But ϕ is not the trivial homomorphism (as $1 \notin m$), and hence its kernel cannot equal all of $\mathbb{Z}$. Thus, the fact that $p\mathbb{Z}$ is a maximal ideal in $\mathbb{Z}$ combined with the fact that $p\mathbb{Z} \subseteq \text{Kernel}(\phi)$ implies that $\text{Kernel}(\phi) = p\mathbb{Z}$, and hence by the equation (1), we have $\mathbb{Z}/p\mathbb{Z} \cong A/m$.

Step 2: Show $A/m \cong m_i/m_{i+1}$ as an abelian group, and hence by Step 1, $|m/m_i| = p$ for all i. This follows easily from the First Isomorphism Theorem,

since the map $\psi: A \to m_i/m_{i+1}$ given by $a \mapsto a(1-\zeta)^i$ is clearly a group homomorphism, and the fact that $m_i = (1-\zeta)^i$ easily implies that ψ is onto, whereas the fact that $m_{i+1} = (1-\zeta)^{i+1}$ easily implies that $\text{Kernel}(\psi) = (1-\zeta)$, which is just another way of saying that $\text{Kernel}(\psi) = m$.

Step 3: The Proposition immediately follows from Step 2 once we note that

$$|A/m^n| = |A/m| \times |m/m^2| \times |m^2/m^3| \times \cdots \times |m^{n-1}/m^n|$$

and this follows easily using basic group theory and induction from the fact that $A \supseteq m \supseteq m^2 \supseteq m^3 \supseteq \cdots \supseteq m^n$.

The only other thing I wanted to point out is that your argument in

Example 4.1: As Example $(\mathbb{Z}/5\mathbb{Z})[x]/(x^3)$ has cardinality 125 is incomplete (although you might have known how to complete it). The conclusion follows easily from the fact that even though $(\mathbb{Z}/5\mathbb{Z})[x]/(x^3)$ is not a field, it is easily seen to be a 3-dimensional vector space over $\mathbb{Z}/p\mathbb{Z}$ with basis $\{1, x, x^2\}$, which says that any element of $(\mathbb{Z}/5\mathbb{Z})[x]/(x^3)$ can be uniquely written as a linear combination $a_0 + a_1x + a_2x^2$ with $a_i \in \mathbb{Z}/p\mathbb{Z}$. Using reasoning similar to that used in your proof of Theorem 0.1, one argues that there are p choices for each of a_0, a_1, and a_2, hence a total of p^3 elements in $(\mathbb{Z}/5\mathbb{Z})[x]/(x^3)$.

Theorem 4.2: *Let d as above be the smallest positive integer such that $d \leq n/(p-1)$. Then*

$$A/m^n \cong \begin{cases} \mathbb{Z}[y]/(y^n, y^{p-1} - u) \\ \mathbb{Z}/p^d\mathbb{Z}[y]/(y^n, y^{p-1} - u) \end{cases} \quad \text{or}$$

where u is a particular unit mod y^n (i.e., u corresponds to a unit in $\mathbb{Z}[y]/(y^n)$ or in $\mathbb{Z}/p^d\mathbb{Z}[y]/(y^n)$ respectively). In the special case where $n \leq p-1$, this implies that

$$A/m^n \cong (\mathbb{Z}/p\mathbb{Z})[y]/(y^n).$$

Remark 4.3: We use this result in Corollary 2.3 to explicitly describe all of the elements in A/m^n in a way that allows one to compute the sum or product of any two elements, [3] and also allows us to show that $|A/m^n| = p^n$ (there are also other elementary ways to count the number of elements in A/m that do not rely on the isomorphism in the above Theorem).

5. Examples

5.1 *Example 1: $n = 2$ and $p = 5$*

In this case, we have $n \leq p-1$ since $p - 1 = 4$. According to the theorem:

$$A/m^2 \cong (\mathbb{Z}/5\mathbb{Z})[y]/(y^2).$$

This implies that the quotient ring consists of polynomials in y of degree less than 2, with coefficients from $\mathbb{Z}/5\mathbb{Z}$. Thus, elements in this ring can be expressed as:

$$a_0 + a_1 y \text{ where } a_0, a_1 \in \{0, 1, 2, 3, 4\}.$$

The total number of elements in this ring is $5^2 = 25$.

5.2 *Example 2:* $n = 6$ *and* $p = 5$

Here, $n > p - 1$ because $p - 1 = 4$. We need to find d:

$$d = \left\lfloor \frac{6}{4} \right\rfloor = 1.$$

Thus, we can write:

$$A/m^6 \cong \mathbb{Z}[y]/(y^6, y^4 - u).$$

Assuming u is a particular unit in $\mathbb{Z}[y]/(y^6)$, we can express elements of this quotient as:

$$f(y) = a_0 + a_1 y + a_2 y^2 + a_3 y^3 + a_4 y^4 + a_5 y^5,$$

where $a_i \in \mathbb{Z}$. The structure of this ring is more complex due to the additional relation $y^4 - u$, which constrains the polynomials further. The exact nature of u will determine how this polynomial behaves.

5.3 *Example 3:* $n = 8$ *and* $p = 7$

In this scenario, we have $n > p - 1$ since $p - 1 = 6$. We need to calculate d:

$$d = \left\lfloor \frac{8}{6} \right\rfloor = 1.$$

Since $d = 1$, we can express the structure of the quotient ring as follows:

$$A/m^8 \cong \mathbb{Z}[y]/(y^8, y^6 - u),$$

where u is a unit in $\mathbb{Z}[y]/(y^8)$.

Elements of the Ring

In this case, the elements of the ring can be represented as:

$$f(y) = a_0 + a_1 y + a_2 y^2 + a_3 y^3 + a_4 y^4 + a_5 y^5 + a_6 y^6 + a_7 y^7,$$

where $a_i \in \mathbb{Z}$. The relation $y^6 - u$ means that we can express y^6 in terms of lower powers of y modulo u.

Understanding the Structure

The structure of this ring indicates that y^6 can be replaced by u in any polynomial of degree greater than or equal to 6. Thus, any polynomial in A/m^8 can effectively be reduced to a degree less than 6:

$$f(y) \equiv a_0 + a_1 y + a_2 y^2 + a_3 y^3 + a_4 y^4 + a_5 y^5 \pmod{(y^6 - u)}.$$

Number of Elements [1]

Since the coefficients a_i can take any integer value, the total number of distinct elements in A/m^8 is infinite. However, if we consider the coefficients modulo some integer p, such as in $\mathbb{Z}/7\mathbb{Z}$, the number of distinct elements becomes:

$$7^6,$$

which accounts for all combinations of the coefficients $a_0, a_1, a_2, a_3, a_4, a_5$ taken from $\{0, 1, 2, 3, 4, 5, 6\}$.

Proof: We look at the composition of maps $g_2 \circ g_1$, (where we are writing functions on the left, so that $g_2 \circ g_1$ means that one first applies g_1 followed by g_2)

$$\mathbb{Z}[x] \overset{g_1}{\to} A \overset{g_2}{\to} A/m^n = \mathbb{Z}[\theta]/(1-\theta).$$

where g_1 is the evaluation homomorphism that sends the variable x to the element $\theta \in A$ (so that it sends the polynomial $f(x) \in \mathbb{Z}[x]$ to the element $f(\theta) \in A$), and g_2 is the canonical surjective homomorphism from A to its factor ring. It is then easy to see that the kernel of $g_2 \circ g_1$ equals the ideal $((x-1)^n, \Phi_p(x))$, where $\Phi_p(x)$ denotes the p-th cyclotomic polynomial. Note that $g_2 \circ g_1$ is surjective.

This implies that

$$A/m^n \cong \mathbb{Z}[x]/((x-1)^n, \Phi_p(x)) \tag{1}$$

but this tells us little about what the ring $\mathbb{Z}[\theta]/(1-\theta)^n$ actually looks like or how multiplication in this ring behaves (addition is more transparent).

To get a better idea about the arithmetic structure of this ring, we make the change of variables $y = x - 1$ (or equivalently $x = y + 1$). This implies that

$$A/m^n \cong \mathbb{Z}[y]/(y^n, \Phi_p(y+1)) \tag{2}$$

Moreover, since $\Phi_p(x) = x^p - 1$, we have

$$\Phi_p(y+1) = (y+1)^p - 1.$$

A standard computation using the binomial expansion formula shows that

$$\Phi_p(y+1) = y^{p-1} + p \cdot y^{p-2} + \frac{p(p-1)}{2} y^{p-3} + \cdots + \frac{p(p-1)}{2} y + 1. \tag{3}$$

Equations (2) and (3) then imply that

$$A/m^n \cong \mathbb{Z}[y]/\left(y^n, y^{p-1} + p \cdot y^{p-2} + \frac{p(p-1)}{2} y^{p-3} + \cdots + \frac{p(p-1)}{2} y + 1\right). \tag{4}$$

This means that $A/m^n \cong \mathbb{Z}[y]/I$, where

$$I = \left(y^n, y^{p-1} + p \cdot y^{p-2} + \frac{p(p-1)}{2} y^{p-3} + \cdots + \frac{p(p-1)}{2} y + 1\right). \tag{5}$$

Now note that $y^{p-2} + \frac{p-1}{2} y^{p-3} + \cdots + \frac{p-1}{2} y + 1$ is a unit mod y^n. By this, I mean that if we consider it as an element in the ring $\mathbb{Z}[y]/(y^n)$, it is a unit. This follows from the fact that the constant term is 1 and all of the other terms are nilpotent mod y^n. Since the sum of nilpotent elements is easily seen to be nilpotent, the fact that this polynomial is a unit in $\mathbb{Z}[y]/(y^n)$ follows, for example, from Exercise 1 at the end of Chapter 1 in Atiyah and Macdonald, which states that a unit plus a nilpotent element is always a unit.

This indicates that the ideal I spelled out in Equation (5) equals

$$I = (y^n, y^{p-1} + u_0 p)$$

where u_0 is a unit mod y^n. Thus, if we let $u = -u_0$, we can rewrite this as

$$I = (y^n, y^{p-1} - up)$$

where u is a unit mod y^n. (Note that u is a polynomial in y of degree $p-2$, and we will use this fact in our proof of Corollary 2 below.)

This gives us

$$A/m^n \cong \mathbb{Z}[y]/I = \mathbb{Z}[y]/(y^n, y^{p-1} - up) \tag{6}$$

where u is a unit mod y^n.

This indicates that to obtain A/m^n, we take polynomials in the variable y up to degree n (or more precisely, up to arbitrary degree, but we "pretend" that y^n and higher powers of y equal 0), and then we identify y^{p-1} with a unit multiple of p.

Note that you can check directly that

$$\mathbb{Z}[y]/(y^n, y^{p-1} - up)$$

is a local ring, with maximal ideal equal to the image of (y, p). Clearly, both y^n and $y^{p-1} - up$ are contained in (y, p), which is a maximal ideal in $\mathbb{Z}[y]$. Any maximal ideal containing both y^n and $y^{p-1} - up$ must also contain y, hence also contain up. Since u is a unit mod y^n, it must also contain p. The residue field in all cases is $\mathbb{Z}/p\mathbb{Z}$, which is isomorphic to A/m.

Moreover, since we have seen above that $m^n \cap \mathbb{Z} = p^d$, it is not hard to deduce from the description of A/m^n contained in Equation (6) that we also have

$$A/m^n \cong (\mathbb{Z}/p^d\mathbb{Z})[y]/(y^n, y^{p-1} - up).$$

Finally, note that the last sentence of the Theorem follows since in the special case where $n \leq p-1$, y^{p-1} is divisible by y^n. Thus, the ideal

$$I = (y^n, y^{p-1} - up)$$

can be rewritten as

$$I = (y^n, up),$$

which, since u is a unit mod y^n, is the same as the ideal

$$I = (y^n, p).$$

From this, it immediately follows that

$$\mathbb{Z}[y]/(y^n, y^{p-1} - up) \cong \mathbb{Z}[y]/(y^n, p) \cong (\mathbb{Z}/p\mathbb{Z})[y]/(y^n).$$

Remark 5.1: Recall that d was defined to be the smallest integer such that $d(p-1) \geq n$. Equivalently, $d-1$ is the largest integer such that $(d-1)(p-1) < n$. This means we can write

$$n = (d-1)(p-1) + r \text{ with } 1 \leq r < p-1,$$

where it is important to note that if $p-1$ divides n, then r does not represent the remainder from the long division of n by $p-1$.

Then, we have

$$y_n = y^{(d-1)(p-1)+r} = (y^{p-1})^{d-1} y^r.$$

In particular, the fact that y^{p-1} gets identified with u_p in the ring $A/m_n = Z[y]/(y_n, y^{p-1} - u_p)$ implies that

$$y_n \text{can be identified with } u^{d-1}p^{d-1}y^r,$$

where u^{d-1} is also a unit mod y_n. This in turn means that

$$u^{d-1}p^{d-1}y^r \equiv 0 \text{ in } A/m_n,$$

which since u^{d-1} corresponds to a unit mod y_n implies that

$$p^{d-1}y^r \equiv 0 \text{ in } A/m_n.$$

Then the description of A/m_n found in Theorem 1 allows us to explicitly list all of the elements of the ring in a way that enables us to completely understand the underlying arithmetic structure. More precisely, we have

Corollary 5.2: *Let r be as in the above Remark. Then, when we identify A/m^n with*

$$\mathbb{Z}[y]/(y^n, y^{p-1} - up),$$

it consists of all

$$\sum_{i=0}^{r} c_i y^i + \sum_{j=0}^{p-r-2} c_j y^j$$

for $0 \le c_i < p^d - 1$ and $0 \le c_j < p^{d-1} - 1$ (meaning these polynomials constitute a complete set of coset representatives, so that any element of $\mathbb{Z}[y]$ can be uniquely identified in the factor ring with a polynomial of the above form). Note that by definition,

$$\sum_{j=0}^{p-r-2} c_j y^j = 0$$

in the case where $r = p - 1$.

This implies that $|A/m^n| = p^n$, and this also allows one to work out the arithmetic structure of the ring A/m^n.

Proof: Note first that any term ay^i can be rewritten as $(bp^d + c)y^i$, for $0 \le c < p^d - 1$, which, since we established above that p^d is 0 in A/m^n, can be rewritten as cy^i for such c.

Also note that we can do even better if $i \ge r$, since any term ay^i with $i \ge r$ can be rewritten as

$$(bp^{d-1} + c)y^r y^{i-r},$$

for $0 \le c < p^{d-1} - 1$, which can be rewritten as cy^i for such c, since we established in the above Remark that $p^{d-1}y^r$ is 0 in A/m^n.

It follows that any polynomial of degree $\le p - 2$ (you will see why I picked the cutoff point of $p - 2$ in a moment) can be written as

$$\sum_{i=0}^{r} c_i y^i + \sum_{j=0}^{p-r-2} c_j y^j$$

with $0 \le c_i < p^{d-1}$ and $0 \le c_j < p^{d-1} - 1$, where one can check that no two such polynomials can be equal in $\mathbb{Z}[y]/(y^n, y^{p-1} - up)$ (note that this requires an argument, so I am skipping a nontrivial step here, but it should be possible to fill in the details).

Since we have r choices for i with p^d choices for each c_i and $p-1-r$ choices for j with p^{d-1} choices for each c_j, this gives us a total of

$$(p^d)^r(p^{d-1})^{p-1-r} = p^{dr}(p^{d-1})^{p-1-r} = p^{(d-1)(p-1)+r} = p^n$$

polynomials of degree $\leq p-2$ (keep in mind that by choice of r, $(d-1)(p-1)+r=n$).

It remains to show that this gives us all of the elements in the ring $\mathbb{Z}[y]/(y^n, y^{p-1}-up)$. In other words, we must show that any polynomial is equivalent to a polynomial of degree $\leq p-2$ in $\mathbb{Z}[y]/(y^n, y^{p-1}-up)$.

We first note that since y^{p-1} can be identified with up, where u was shown in the proof of Theorem 1 above to be a polynomial of degree $p-2$, this is certainly true for polynomials of degree $\leq p-1$.

Moreover, since $y^i = y \cdot y^{i-1}$, the result follows by induction for all larger i. In this way, we obtain a "list of names" for all of the elements of $\mathbb{Z}[y]/(y^n, y^{p-1}-up)$, and one can then use the definition of the unit $u=-u_0$ spelled out in the proof of Theorem 1 to write the sum or product of any two given elements in this ring in terms of one of the elements appearing in this list.

Acknowledgment

We are grateful to Dr. Yassine Guerboussa from University of Ouargla, Algeria and Naomi Jochnowitz for their interest and for several invaluable discussions. We would like to thank the referee for carefully reading the paper and for his suggestions.

References

[1] B. Bahri and Y. Guerboussa, "Discrete Valuation Rings, Partitions and p-groups I," *J. Pure Appl. Algebra*, vol. 228, no. 3, p. 107490 (2023), doi: 10.1016/j.jpaa.2023.107490.

[2] A. Abdollahi, "Cohomologically trivial modules over finite groups of prime power order," *J. Algebra*, vol. 342, pp. 154-160 (2011).

[3] M. F. Atiyah and I. G. Macdonald, Introduction to Commutative Algebra. Reading, MA, USA: Addison-Wesley (1969).

[4] M. F. Atiyah and I. G. Macdonald, Introduction to Commutative Algebra. Reading, MA, USA: Addison-Wesley, Prop. 1.6 (1969).

[5] M. F. Atiyah and I. G. Macdonald, Introduction to Commutative Algebra. Reading, MA, USA: Addison-Wesley, Th. 8.5 (1969).

[6] V. D. Mazurov and E. I. Khukhro, The Kourovka Notebook: Unsolved Problems in Group Theory, 18th ed. Novosibirsk, Russia: Russian Academy of Sciences, Siberian Division, Institute of Mathematics (2014).

[7] R. J. Miech, "The metabelian p-groups of maximal class," *Trans. Amer. Math. Soc*., vol. 236, pp. 93-119 (1978).

[8] R. J. Miech, "The metabelian p-groups of maximal class II," *Trans. Amer. Math. Soc*., vol. 272, pp. 465-474 (1982).

[9] J.-P. Serre, Local Fields, Graduate Texts in Mathematics, vol. 67. New York, NY, USA: Springer-Verlag (1979).

Received November, 2025