Structure of Non-Nilpotent Elements of Some $\mathbb{Z}$-Modules

David Ssevviiri
Department of Mathematics
Makerere University, P.O Box 7062, Kampala, Uganda
ssevviiri@math.mak.ac.ug

Abstract

We characterize non-nilpotent elements of the $\mathbb{Z}$-module $\mathbb{Z}/(p_{k_1}^{k_1} \times p_{k_2}^{k_2} \times \cdots \times p_{k_n}^{k_n})\mathbb{Z}$. If $B_k$ is a set of non-nilpotent elements of $\mathbb{Z}/p^k\mathbb{Z}$, $B^0_k = B_k \cup \{0\}$ is a non-unital ring. When considered as a $\mathbb{Z}$-module, $B^0_k$ is isomorphic to $\mathbb{Z}/p\mathbb{Z}$ and $N_p = \varprojlim B^0_k$ is a compact topological ideal of the ring $\mathbb{Z}_p$ of $p$-adic integers.

Keywords: Nilpotent elements of modules

1 Introduction

All modules considered are left modules which are not necessarily unital. The rings are associative. We write $A \triangleleft R$ to mean $A$ is an ideal of $R$ and $N \leq M$ to mean $N$ is a submodule of $M$. A nonzero element $m$ of an $R$-module $M$ is nilpotent [2] of degree $k$ if there exists $a \in R$ and $k \in \mathbb{N}$ such that $a^k m = 0$ and $am \neq 0$. We take every zero element of a module to be nilpotent. The non-nilpotent elements [2, Proposition 2.1] of the $\mathbb{Z}$-module $A_k = \mathbb{Z}/p^k\mathbb{Z}$ where $1 \neq k \in \mathbb{Z}^+$ are \{\(p^{k-1}, 2p^{k-1}, 3p^{k-1}, \ldots, (p-1)p^{k-1}\)\}, i.e., they are $p - 1$ in number and are all multiples of $p^{k-1}$. The table below gives examples of non-nilpotent elements of the $\mathbb{Z}$-module $\mathbb{Z}/p^k\mathbb{Z}$.

\(^1\)This research forms part of the work leading to award of a PhD degree at Nelson Mandela Metropolitan University (NMMU) under the supervision of Prof. N. J. Groenewald. It was supported by both NRF and NMMU.
This note aims at characterizing non-nilpotent elements of the $\mathbb{Z}$-modules $\mathbb{Z}/(p_1^{k_1} \times p_2^{k_2} \times \cdots \times p_n^{k_n}) \mathbb{Z}$.

## 2 Main results

**Theorem 2.1** The non-nilpotent elements of the $\mathbb{Z}$-module $\mathbb{Z}/(\prod_{i=1}^{n} p_i^{k_i}) \mathbb{Z}$ are $\#(N^c) = \left(\prod_{i=1}^{n} p_i\right) - 1$ in number and are all multiples of $\prod_{i=1}^{n} (p_i^{k_i} - 1)$.

**Proof:** We know by Chinese remainder theorem that $\mathbb{Z}/(\prod_{i=1}^{n} p_i^{k_i}) \mathbb{Z} \cong \prod_{i=1}^{n} (\mathbb{Z}/p_i^{k_i} \mathbb{Z})$. Since by [2, Example 2.3], the non-nilpotent elements of $\mathbb{Z}/p_i^{k_i} \mathbb{Z}$ are multiples of $p_i^{k_i} - 1$ for all $i \in \{2, 3, 4, \ldots\}$ and are $p_i - 1$ in number; the non-nilpotent elements of $\mathbb{Z}/(\prod_{i=1}^{n} p_i^{k_i}) \mathbb{Z}$ must be the multiples of $p_1^{k_1-1} \times p_2^{k_2-1} \times \cdots \times p_n^{k_n-1}$ modulo $(p_1^{k_1} \times p_2^{k_2} \times \cdots \times p_n^{k_n})$. Hence, they are $(p_1 \times p_2 \times \cdots \times p_n) - 1$ in number.

**Corollary 2.1** For any $\mathbb{Z}$-module $\mathbb{Z}/(\prod_{i=1}^{n} p_i^{k_i}) \mathbb{Z}$,

1. the number $\#(N)$ of nilpotent elements is $\left(\prod_{i=1}^{n} p_i^{k_i}\right) - \left(\prod_{i=1}^{n} p_i\right) + 1$,
2. $\#(N_M^c) < \#(N_M)$,
3. \( \lim_{n \to \infty} \sharp(N_M^n) = \infty \) and \( \lim_{n \to \infty} \sharp(N_M) = \infty. \)

**Proposition 2.1** Let \( B_k = \{np^{k-1}\}_{n=1}^{p-1} \) for \( k \in \{2, 3, 4, \ldots\},^2 \) then

1. for a given prime \( p \), \( |B_k| = |B_{k+1}| \) for all \( k \in \{2, 3, 4, \ldots\}; \)

2. \( \sum_{n=1}^{p-1} np^{k-1} = \begin{cases} 2^{k-1} & \text{if } p = 2; \\ 0 \pmod{p^k} & \text{if } p \neq 2. \end{cases} \)

**Proof:**

1. 1 is evident from how \( B_k \) is defined, i.e., each \( B_k \) for a given prime \( p \) consists of \( p - 1 \) elements.

2. If \( p = 2 \), then \( B_k \) has only one element \( 2^{k-1} \). Suppose \( p \neq 2 \), \( \sum_{n=1}^{p-1} np^{k-1} = p^{k-1}p(\frac{p-1}{2}) = p^k(\frac{p-1}{2}) = 0 \pmod{p^k}. \)

**Proposition 2.2** Define \( B_k^0 \) as \( B_k^0 = B_k \cup \{0\} \). Then, \( B_k^0 \) is a ring (without unity) under addition modulo \( p \) and multiplication modulo \( p \).

**Proof:** If \( a, b \in B_k^0 \), then \( a = np^{k-1} \) and \( b = mp^{k-1} \) for some \( m, n \in \mathbb{Z}^+ \). \( a + b = np^{k-1} + mp^{k-1} = (n+m)p^{k-1} \). If \( n+m \leq p \), \( (n+m)p^{k-1} \in B_k^0 \) otherwise by division algorithm \( n+m = rp+s \) for some \( r, s \in \mathbb{Z}^+ \) and \( 0 < s < p \). So, in this case, \( (n+m)p^{k-1} = (rp+s)p^{k-1} \equiv sp^{k-1} \pmod{p} \). Therefore, in both cases \( a + b \in B_k^0 \). The identity element is 0, the additive inverse of \( np^{k-1} \) is \( (p-n)p^{k-1} \) for \( n \in \{1, 2, 3, \ldots, p-1\} \). Associativity is inherited from \( \mathbb{Z} \). If \( a, b \in B_k^0 \), then \( ab = (np^{k-1})(mp^{k-1}) \) for some \( n, m \in \{1, 2, 3, \ldots, p-1\} \). This implies \( ab = np^{2(k-1)} \equiv 0 \pmod{p} \) since \( 2(k-1) > 1 \) for all \( k \geq 2 \).

Although the rings \( \mathbb{Z}/p\mathbb{Z} \) and \( B_k^0 \) have the same number of elements and elements of \( B_k^0 \) are got by multiplying those of \( \mathbb{Z}/p\mathbb{Z} \) by \( p^{k-1} \), the two rings are not isomorphic. The former is unital but the latter is non-unital. However, the two rings coincide if \( k = 1 \).

**Proposition 2.3** Define \( \psi_k : B_{k+1}^0 \to B_k^0 \) by \( \psi_k(np^k) = np^{k-1} \). \( \psi_k \) is a ring isomorphism from \( B_{k+1}^0 \) to \( B_k^0 \).

**Proof:** \( \psi_k \) is well defined, for if \( np^k = mp^k \), then \( n \equiv m \pmod{p} \). This implies \( np^{k-1} \equiv mp^{k-1} \pmod{p} \) and so \( \psi_k(np^{k-1}) = \psi_k(mp^{k-1}) = \psi_k(\frac{[n+m]p^k}{p^k}) = (n+m)p^{k-1} = np^{k-1} + mp^{k-1} = \psi_k(np^k) + \psi_k(mp^k) \).

\( \psi_k([np^k][mp^k]) = \psi_k(\frac{np^{(k-1)}mp^k}{p^k}) = \psi_k(0p^k) = 0 = nmp^{2(k-1)} = (np^{k-1})(mp^{k-1}) = \psi_k(np^k)\psi_k(mp^k) \).

\( \psi_k \) has kernel \( pB_k^0 \equiv 0 \pmod{p} \), hence \( \psi_k \) is injective. Lastly, for all \( np^{k-1} \in B_k^0 \) there is \( np^k \in B_{k+1}^0 \) such that \( \psi_k(np^k) = np^{k-1} \). Thus, \( \psi_k \) is surjective.

---

^2Note that \( B_k \) is the set of all non-nilpotent elements of the \( \mathbb{Z} \)-module \( \mathbb{Z}/p^k \mathbb{Z} \).
For an indexed set $I$, the collection $\{R_i : i \in I\}$ of rings together with ring homomorphisms, $\psi_i : R_i \to R_{i-1}$ is called a projective system (inverse system) if whenever $i < j$, we have a homomorphism $f_{ij}$ from $R_j$ to $R_i$ and if $i \leq j \leq k$, then $f_{ij} \circ f_{jk} = f_{ik}$. A sequence $(x_i)$ in the direct product $\prod R_i$ is said to be coherent if it respects the maps $\psi_i$ in the sense that for every $i$ we have $\psi_{i+1}(x_{i+1}) = x_i$. The collection of all coherent sequences is called the inverse limit of the inverse system. The inverse limit is denoted by $\lim_{\leftarrow} R_i$, or just $\lim R_i$ if no confusion is likely to arise.

$$\cdots \xrightarrow{\psi_k} B_k \xrightarrow{\psi_{k-1}} B_{k-1} \cdots \xrightarrow{\psi_3} B_3 \xrightarrow{\psi_2} B_2$$

is a projective system indexed by integers greater than 1. As an example, consider $B_k^0$ with $p = 5$:

$$\cdots \to B_4^0 \xrightarrow{\psi_3} B_3^0 \xrightarrow{\psi_2} B_2^0 \xrightarrow{\psi_1} B_1^0 \xrightarrow{\psi_0} B_0^0 \xrightarrow{\psi_1} B_1^0 \to \cdots$$

In general, we have sequences defined by $\psi(np^m) = np^{m-1}$ across $B_m$'s with an infinite number of elements but convergent to $np$. We also have sequences defined by $f(np^m) = (n-1)p^m$ within $B_m$ with a finite number of elements (equal to $p-1$) and convergent to $p^m$.

**Lemma 2.1** If $a_1, a_2, \ldots, a_m$ is a complete system of residues modulo $m$, and if $r$ is a positive integer with $(r, m) = 1$, (i.e., $r$ is relatively prime to $m$) then $ra_1 + s, ra_2 + s, \ldots, ra_m + s$ is also a complete system of residues modulo $m$ for any $s \in \mathbb{Z}$.

**Theorem 2.2** Let $N_p = \lim_{\leftarrow}(B_k^0, \psi_k)$, then $N_p$ is a compact topological ideal of the ring $\mathbb{Z}_p$ of $p$-adic integers. Furthermore, $N_p$ consists of sequences of the form $(\cdots, np^k, \cdots, np^3, np^2, np, 0)$, where $n \in \mathbb{Z}/p\mathbb{Z}$.

**Proof:** Let $A_k = \{0, 1, 2, \ldots, p^k-1\}$ and $B_k^0 = \{0, p^k-1, 2p^k-1, \ldots, (p-1)p^k-1\}$. Since $p^k - 1 \geq (p-1)p^k - 1$ for all $k \in \mathbb{Z}^+$ and every $a \in B_k^0$ is a positive integer less than or equal to $p^k - 1$, and hence $a \in A_k$, we have $B_k^0 \subseteq A_k$ for all $k$. Therefore, $N_p = \lim_{\leftarrow}(B_k^0, \psi_k) \subseteq \lim_{\leftarrow}(A_k, \phi_k) = \mathbb{Z}_p$, where $A_k = \mathbb{Z}/p^k\mathbb{Z}$ and $\phi_k$ is a homomorphism from $A_k$ to $A_{k-1}$. To show that $N_p \triangleleft \mathbb{Z}_p$, it is enough
to show that $B^0_k \triangleleft A_k$ for each $k$. Since $\{0,1,2,\ldots,(p-1)\}$ is a complete system of residues modulo $p$ and for any $r \in A_k$, $(r,p) = 1$, by Lemma 2.1, $\{0,r,2r,\ldots,(p-1)r\}$ is also a complete system of residues modulo $p$. So, $B^0_k r - rB^0_k \equiv B^0_k$ (mod $p$) for all $r \in A_k$. Since $B^0_k$ are rings, their inverse limit $N_p$ is also a ring. If we give $\prod_{k \geq 2} B_k$ the product topology and $B_k$ the discrete topology, the ring $N_p$ inherits a topology which turns it into a compact space since it is closed in a product of compact spaces.

**Corollary 2.2** The ideal $N_p$ (of the ring $\mathbb{Z}_p$) has no invertible elements.

**Proof:** Follows from [1, Chap II, Proposition 2(a)] and the fact that every element of $N_p$ is of the form $(\cdots, np^k, \cdots, np^3, np^2, np, 0)$, $n \in \mathbb{Z}/p\mathbb{Z}$.

**Corollary 2.3** $N_p$ is an integral domain and a complete metric space.

**Proof:** Since $\mathbb{Z}_p$ is an integral domain, cf., [1, p.12], its ideal $N_p$ is also an integral domain. For the rest we follow the proof in [1, p.12, Proposition 3]. Every element $x$ of $N_p$ is of the form $x = p^ny$ where $y \in A_k$ and $n$ is the $p$-adic valuation of $x$ denoted by $v_p(x)$. The ideals $p^nN_p$ form a basis of neighborhoods of 0; since $x \in p^nN_p$ implies $v_p(x) \geq n$, the topology on $N_p$ is defined by the distance $d(x, y) = e^{-v_p(x-y)}$. Since $N_p$ is compact [cf. Theorem 2.2], it is complete.

**Proposition 2.4** $B^0_k$ and $\mathbb{Z}/p\mathbb{Z}$ are isomorphic $\mathbb{Z}$-modules.

**Proof:** Since $B^0_k$ and $A_k$ are abelian groups, they are $\mathbb{Z}$-modules and $\varphi_k(np^{k-1}) = n \pmod{p}$ is a module isomorphism from $B^0_k$ to $A_k$. $\varphi$ is well defined, for if $np^{k-1}, mp^{k-1} \in B^0_k$ and $np^{k-1} = mp^{k-1}$, then $n \equiv m \pmod{p}$ and hence $n \pmod{p} = m \pmod{p}$ which implies $\varphi_k(np^{k-1}) = \varphi_k(mp^{k-1})$. $\varphi_k(np^{k-1} + mp^{k-1}) = \varphi_k([n + m]p^{k-1}) = (n + m) \pmod{p} = n \pmod{p} + m \pmod{p} = \varphi_k(np^{k-1}) + \varphi_k(mp^{k-1})$. For all $a \in \mathbb{Z}$, $\varphi_k(a[np^{k-1}]) = \varphi_k([an]p^{k-1}) = an \pmod{p} = a\varphi_k(np^{k-1})$. $\varphi_k(np^{k-1}) = 0 \iff n \pmod{p} = 0 \iff n = 0$. Thus, Ker $\varphi_k = 0$ and $\varphi_k$ is injective. Since the $\mathbb{Z}$-modules $B^0_k$ and $A_k$ are of the same size and $\varphi_k$ is injective, by the pigeon hole principal $\varphi_k$ is surjective.

**Question 2.1** Can one characterize the structure $C_k = \{np_1^{k_1-1} \times p_2^{k_2-1} \times \cdots \times p_n^{k_n-1}\}_{n=p_1 \times p_2 \times \cdots \times p_n}$ adjoined with 0 like we did for $B_k$?

**References**


Received: December, 2011