A TORSION-FREE ABELIAN GROUP EXISTS WHOSE QUOTIENT GROUP MODULO THE SQUARE SUBGROUP IS NOT A NIL-GROUP

R. R. ANDRUSZKIEWICZ and M. WORONOWICZ

(Received 12 April 2016; accepted 30 April 2016; first published online 30 August 2016)

Abstract

The first example of a torsion-free abelian group \((A, +, 0)\) such that the quotient group of \(A\) modulo the square subgroup is not a nil-group is indicated (for both associative and general rings). In particular, the answer to the question posed by Stratton and Webb ['Abelian groups, nil modulo a subgroup, need not have nil quotient group', *Publ. Math. Debrecen* 27 (1980), 127–130] is given for torsion-free groups. A new method of constructing indecomposable nil-groups of any rank from 2 to \(2^{\aleph_0}\) is presented. Ring multiplications on \(p\)-pure subgroups of the additive group of the ring of \(p\)-adic integers are investigated using only elementary methods.


Keywords and phrases: nil-groups, square subgroups, abelian groups.

1. Introduction

In this paper, we continue the research on the square subgroup of an abelian group. It can be understood as follows. Given an abelian group \((A, +, 0)\), the square subgroup \(\Box A\) of \(A\) is the smallest subgroup \(B\) of \(A\) satisfying the condition that if \(R\) is any ring (not necessarily associative) with the additive group \(A\), then \(R^2 \subseteq B\). The notion was partially investigated by Aghdam in [1] and it is closely connected with the paper [16] by Stratton and Webb. Aghdam continued his research on the square subgroup together with Najafizadeh in [2–4]. Nevertheless, the basic question related to the topic remained unanswered. Namely, it was not known whether the quotient group of any abelian group \(A\) modulo the square subgroup \(\Box A\) is a nil-group (see [1, 16]). The first (negative) answer with an example of a mixed abelian group was given recently by Najafizadeh in [15]. Previously, it was known that the answer is positive for torsion abelian groups (see [16, Theorem 2.4]). In his proof, Najafizadeh used advanced tools such as the tensor product of abelian groups and theorems for splitting modules. Therefore he could not assume the associativity of rings, which is important for many algebraists. Our much more elementary proof in [6] allows the conclusion...
that Najafizadeh’s result remains true also for the case of associative rings. It is a well-known fact that there exists a torsion-free nil-group $A$ such that $A/nA$ is not a nil-group for some positive integer $n$ and, consequently, any ring $R$ defined on $A$ satisfies $R^2 \subseteq nA$ (see [16]). However, the square subgroup of a torsion-free abelian group was investigated only in some special cases: for example, Aghdam and Najafizadeh have indicated some classes of torsion-free abelian groups $A$ of rank two for which $A/\Box A$ is a nil-group (see [4]).

The main result of this paper is a construction of a torsion-free abelian group $A$ such that $A/\Box A$ is not a nil-group in both cases of associative and general rings. Moreover, we give a new method of constructing indecomposable nil-groups of any rank from 2 to $2^{\aleph_0}$. We also present various effects concerning ring multiplications on $p$-pure subgroups of the additive group of the ring of $p$-adic integers. In particular, we show, using only elementary methods, that any ring multiplication on a $p$-pure subgroup of the additive group of the ring of $p$-adic integers is associative and commutative. Furthermore, we characterise, in an elementary way, subgroups of the additive group of that ring which are not nil.

This topic has a long history in algebra and is generating renewed interest. In addition to the work cited above, there are developments in recent papers of Feigelstock [9], Pham Thi Thu Thuy [17, 18] and Kompantseva [13, 14].

2. Preliminaries

Throughout the paper, the letter $p$ stands for an arbitrary fixed prime. Symbols $\mathbb{Q}$, $\mathbb{Q}_p$, $\mathbb{Z}_p$, $\mathbb{Z}$, $\mathbb{P}$, $\mathbb{N}$, $\mathbb{N}_0$ stand for the fields of rationals, $p$-adic numbers and integers modulo $p$, the rings of integers and $p$-adic integers, and the sets of all prime numbers, positive integers and nonnegative integers, respectively. In this paper, only abelian groups with the traditional additive notation will be considered. Every abelian group $(A, +, 0)$ can be provided with a ring structure in a trivial way by defining $a \cdot b = 0$ for all $a, b \in A$. An abelian group $A$ is called a nil-group (nil$_a$-group) if, on $A$, there does not exist any nonzero (associative) ring multiplication. It follows, from [5, Remark 2.6] and [8, Conjecture 2.1.4], that if the concepts of nil$_a$-group and nil-group are not equivalent, then there exists a torsion-free nil$_a$-group of rank more than one which is not a nil-group. Obviously, $A$ is a nil-group exactly if $\Box A = \{0\}$, so the notion of square subgroup generalises the concept of nil-group. The following formula greatly simplifies the considerations related to the topic: that is,

$$\Box A = \sum_{\ast \in \text{Mult}(A)} A \ast A,$$

where Mult($A$) means the set of all ring multiplications on the group $A$. If we restrict our consideration to associative rings $R$ with the additive group $A$, then the square subgroup of $A$ is denoted by $\Box_a A$. It follows, from [6, Corollary 2.6], that if there exists an abelian group $A$ which satisfies $\Box_a A \subsetneq \Box A$, then $A$ is reduced and nontorsion. More basic information about square subgroups and their generalisations is available in [1, 3, 6].
The additive group of a ring $R$ is denoted by $R^+$. The notation $I < R$ means that $I$ is an ideal of $R$. If $R$ is a unital ring, then its group of units is denoted by $R^*$.

It is a well-known fact that any $p$-adic integer $\alpha$ is determined by a sequence $(x_n)_{n=0}^{\infty}$ of integers satisfying $x_n \equiv x_{n-1} \mod p^n$ for each $n \in \mathbb{N}$. We shall write the above expression as $(x_n)_{n=0}^{\infty} \rightarrow \alpha$. Moreover, $(x_n)_{n=0}^{\infty} \rightarrow \alpha$ and $(y_n)_{n=0}^{\infty} \rightarrow \alpha$ if and only if $x_n \equiv y_n \mod p^{n+1}$ for each $n \in \mathbb{N}_0$. For more preliminary knowledge of $p$-adic integers we refer the reader to [7].

All other designations are consistent with generally accepted standards (see, for example, [11]).

3. A simple characterisation of ring multiplications on $p$-pure subgroups of $\mathbb{Z}_p^+$

**Lemma 3.1.** For every nontrivial subgroup $A$ of $\mathbb{Z}_p^+$ the following conditions are equivalent:

(i) $A = M \cap \mathbb{Z}_p$ for some nontrivial $\mathbb{Z}[p^{-1}]$-submodule $M$ of the field $\mathbb{Q}_p$;

(ii) $A$ is $p$-pure in $\mathbb{Z}_p^*$; and

(iii) $A = \langle \varepsilon \rangle + pA$ for some $\varepsilon \in A \cap \mathbb{Z}_p^*$.

**Proof.** (i) $\Rightarrow$ (ii). Take any $x \in \mathbb{Z}_p$. If $px \in A$, then $px \in M$ and, consequently, $x = p^{-1}(px) \in M$. Thus $x \in M \cap \mathbb{Z}_p$, that is, $x \in A$. Moreover, $\mathbb{Z}_p^+$ is a torsion-free group, so $A$ is a $p$-pure subgroup of $\mathbb{Z}_p^+$.

(ii) $\Rightarrow$ (iii). Take any $a \in A \setminus \{0\}$. Then $a = p^m\varepsilon$ for some uniquely determined $m \in \mathbb{N}_0$ and $\varepsilon \in \mathbb{Z}_p^*$ (compare with [7, Theorem 2]). Hence, by the $p$-purity of $A$ in $\mathbb{Z}_p^+$, we obtain $\varepsilon \in A$. Moreover, $\varepsilon \notin p\mathbb{Z}_p$, so $\varepsilon \notin A \cap p\mathbb{A}$. Next, $(A + p\mathbb{Z}_p) \cdot \mathbb{Z}_p = A \cdot \mathbb{Z}_p + p\mathbb{Z}_p = A \cdot (\mathbb{Z} + p\mathbb{Z}_p) + p\mathbb{Z}_p = A \cdot \mathbb{Z} + p\mathbb{Z}_p = A + p\mathbb{Z}_p$, and hence $A + p\mathbb{Z}_p < \mathbb{Z}_p$. But $\varepsilon \in A \cap \mathbb{Z}_p^*$, so $1 \in A + p\mathbb{Z}_p$ and, consequently, $A + p\mathbb{Z}_p = \mathbb{Z}_p$. As $A$ is a $p$-pure subgroup of $\mathbb{Z}_p^*$, $A \cap p\mathbb{Z}_p = pA$. Thus $A/pA = A/(A \cap p\mathbb{Z}_p^*) \cong (A + p\mathbb{Z}_p^*)/p\mathbb{Z}_p^* = (\mathbb{Z}_p/p\mathbb{Z}_p^*)^\alpha \cong \mathbb{Z}_p^\alpha$. Furthermore, $\varepsilon + pA \neq pA$ in $A/pA$, so $A = \langle \varepsilon \rangle + pA$.

(iii) $\Rightarrow$ (i). An easy computation shows that $M = \{ap^{-n} : a \in A, n \in \mathbb{N}_0\}$ is a nontrivial $\mathbb{Z}[p^{-1}]$-submodule of $\mathbb{Q}_p$. Directly from the definition of $M$, it follows that $A \subseteq M \cap \mathbb{Z}_p$. To prove the opposite inclusion, take any $x \in M \cap \mathbb{Z}_p$. Then $x = ap^{-s}$ for some $a \in A$ and $s \in \mathbb{N}_0$. Moreover, by a simple induction argument, $a = kc + p^{s+k}c$ for some $k \in \mathbb{Z}$ and $c \in A$. Thus $p^s x = k\varepsilon + p^{s+1}c$, and hence $k\varepsilon = p^s(x - pc)$. It follows, from [7, Theorem 2], that $k = p^k\varepsilon$ for some $k \in \mathbb{Z}$, so $k\varepsilon = x - pc$. Hence $x = k\varepsilon + pc \in A$. Thus $M \cap \mathbb{Z}_p \subseteq A$ and, finally, $A = M \cap \mathbb{Z}_p$. \(\square\)

We get the following result directly from the proof of Lemma 3.1.

**Corollary 3.2.** For every nontrivial $p$-pure subgroup $A$ of $\mathbb{Z}_p^+$, $A/pA \cong \mathbb{Z}_p^\alpha$. In particular, $A = \langle a \rangle + p^nA$ for all $a \in A \setminus p\mathbb{A}$ and $n \in \mathbb{N}$.

**Lemma 3.3.** If $A$ and $B$ are nontrivial $p$-pure subgroups of $\mathbb{Z}_p^+$, then so is $AB$.

**Proof.** Take any $x \in \mathbb{Z}_p$. If $px \in AB$, then $px = \sum_{i=1}^{n} a_i b_i$ for some $n \in \mathbb{N}, a_1, \ldots, a_n \in A$ and $b_1, \ldots, b_n \in B$. First, suppose that $a_1, \ldots, a_n \in pA$. Then, for each $a_i$, there
exists $x_i \in A$ such that $a_i = px_i$. Hence $p(x - \sum_{i=1}^{n} x_ib_i) = 0$ and, consequently, $x = \sum_{i=1}^{n} x_ib_i \in AB$. If $b_1, \ldots, b_n \in pB$, then we proceed analogously. Now suppose that $a_j \notin pA$ and $b_s \notin pB$ for some $j, s \in \{1, \ldots, n\}$. The $p$-purity of $A$ and $B$ in $Z_p^+$, together with [7, Theorem 2], implies that $a_j, b_s \in Z_p^+$. Moreover, it follows, from Lemma 3.1, that $A = \langle a_j \rangle + pA$ and $B = \langle b_s \rangle + pB$. Thus, for each $i \in \{1, 2, \ldots, n\}$, there exist $a_i' \in A$, $b_i' \in B$ and $k_i, l_i \in \mathbb{Z}$ such that $a_i = k_ia_j + pa_i'$ and $b_i = l_ib_s + pb_i'$. Hence $px = (\sum_{i=1}^{n} k_ia_j b_i + p \sum_{i=1}^{n} k_i a_i b_i') + p \sum_{i=1}^{n} l_ia_i' b_i + p^2 \sum_{i=1}^{n} a_i' b_i' \in A \cap pA$. In particular, every ring $R$ with $R^+ = A$ is associative and commutative.

**Lemma 3.4.** If $*$ is a ring multiplication on a nontrivial $p$-pure subgroup $A$ of $Z_p^+$, then there exists $c \in Z_p$ such that $a * b = a \cdot c \cdot b$ for all $a, b \in A$. In particular, every ring $R$ with $R^+ = A$ is associative and commutative.

**Proof.** It follows, from Lemma 3.1 and Corollary 3.2, that there exists $e \in A \cap Z_p^+$ such that, for every $n \in \mathbb{N}$, $A = \langle e \rangle + p^n A$. Take any $a, b \in A$, $n \in \mathbb{N}$ and define $e = e * e$. Then $a = knea + p^n a_n$, $b = l_ne + p^n b_n$ and $a * b = (k_n l_n)e + p^n x_n$ for some $k_n, l_n \in \mathbb{Z}$, $a_n, b_n, x_n \in A$. Therefore, for $c = e^{-2} \cdot e$, we get $a * c \cdot b = (k_n l_n)e + p^n y_n$, where $y_n$ is some element of $A$. Hence $a * b = a \cdot c \cdot b$ for all $a, b \in A$. Thus, for $c = e^{-2} \cdot e$, we get $a * c \cdot b = (k_n l_n)e + p^n y_n$, where $y_n$ is some element of $A$. Hence $a * b = a \cdot c \cdot b$. Thus the multiplication $*$ is associative and commutative.

**Proposition 3.5.** Let $A$ be a nontrivial $p$-pure subgroup of $Z_p^+$. Then $A$ is not a nil-group if and only if $A$ is isomorphic to the additive group of some subring of $Z_p$.

**Proof.** Suppose that $\square A \neq \{0\}$. It follows, from Lemma 3.1, that $A = \langle e \rangle + pA$ for some $e \in A \cap Z_p^+$. Since $Z_p$ is an integral domain, the function $x \mapsto x \cdot e^{-1}$ is an automorphism of $Z_p$. Hence $B = A \cdot e^{-1}$ is a subgroup of $Z_p^+$ such that $B \cong A$ and $1 \in B$. Thus $B$ is a $p$-pure subgroup of $Z_p^+$, with $\square B \neq \{0\}$. Hence, by Lemma 3.1 and Corollary 3.2, we get $B = \langle 1 \rangle + pB$. Moreover, Lemma 3.4 implies the existence of a nonzero element $c$ of $Z_p$ such that $a \cdot c \cdot b \in B$ for all $a, b \in B$. Therefore, $c = 1 \cdot c \cdot 1 \in B$. Furthermore, $c = p^m \eta$ for some uniquely determined $\alpha \in \mathbb{N}_0$ and $\eta \in Z_p^+$ (compare with [7, Theorem 2]). Thus $p^m (a \cdot \eta \cdot b) \in B$ for all $a, b \in B$. Hence, by the $p$-purity of $B$ in $Z_p^+$, we obtain $\eta \in B$ and $a \cdot \eta \cdot b \in B$ for all $a, b \in B$. Define $S = B \cdot \eta$. Then $S$ is a subgroup of $Z_p^+$ satisfying $S \cong B$ and $S \cdot S = (B \cdot \eta \cdot B) \cdot \eta \subseteq S$. Consequently, $S$ is a subring of $Z_p^+$ with $S^+ \cong A$. The opposite implication is obvious.

The next result follows directly from the proof of the above proposition.

**Corollary 3.6.** Let $A$ be a nontrivial $p$-pure subgroup of $Z_p^+$. Then $A$ is not a nil-group exactly if $A = S \cdot \omega$ for some subring $S$ of $Z_p$ and $\omega \in Z_p^+$.

**Proposition 3.7.** For every subgroup $A$ of $Z_p^+$, the following conditions are equivalent:

(i) $A = \langle a_0 \rangle + pA$ for some $a_0 \in A \cap pA$; and
(ii) \( A = p^\alpha B \) for some nonnegative integer \( \alpha \) and nontrivial \( p \)-pure subgroup \( B \) of \( Z_p^+ \).

**Proof.** (i) \( \Rightarrow \) (ii). Since \( a_0 \neq 0 \), it follows, from [7, Theorem 2], that \( a_0 = p^m \epsilon \) for some uniquely determined \( m \in \mathbb{N}_0 \) and \( \epsilon \in Z_p^+ \). If \( m = 0 \), then Lemma 3.1 implies that \( A \) is a \( p \)-pure subgroup of \( Z_p^+ \) and it is sufficient to put \( \alpha = 0 \). Now suppose that \( m > 0 \) and define \( B = \langle \epsilon \rangle + pA \). Then \( A = \langle a_0 \rangle + p^{m+1}A = \langle p^m \epsilon \rangle + p^{m+1}A = p^mB \). Thus \( B = \langle \epsilon \rangle + pB \). We apply Lemma 3.1 again to infer that \( B \) is a \( p \)-pure subgroup of \( Z_p^+ \).

(ii) \( \Rightarrow \) (i). It follows, from Lemma 3.1, that there exists \( \epsilon \in B \cap Z_p^+ \) such that \( B = \langle \epsilon \rangle + pB \). Hence \( A = p^\alpha B = \langle p^\alpha \epsilon \rangle + p^{\alpha+1}B = \langle p^\alpha \epsilon \rangle + pA \). Notice that \( pA = \langle p^{\alpha+1} \epsilon \rangle + p^2A = \langle p^{\alpha+1} \epsilon \rangle + p^{\alpha+2}B \subseteq p^{\alpha+1}Z_p^+ \). Therefore, if \( p^\alpha \epsilon \in pA \), then \( \epsilon \in pZ_p^+ \) and, consequently, \( \epsilon \notin Z_p^+ \), which is a contradiction. Thus it suffices to put \( a_0 = p^\alpha \epsilon \). \( \Box \)

**Remark 3.8.** It is a well-known fact that there exist indecomposable nil-groups of any rank up to \( 2^{\aleph_0} \) (see [10, page 292, Exercise 25]). For groups of rank one, the result is obvious. Notice that Lemmas 3.1 and 3.4 are useful for constructing an indecomposable nil-group of any rank \( r \) satisfying \( 1 < r \leq 2^{\aleph_0} \). There exists a subset \( Y \) of \( Z_p^+ \) of cardinality \( 2^{\aleph_0} \) that is algebraically independent over \( Q \). Let \( X \) be a nonempty subset of \( Y \). An easy computation shows that \( M = \mathbb{Z}[p^{-1}] + \sum_{x \in X} \mathbb{Z}[p^{-1}]x \) is a \( \mathbb{Z}[p^{-1}] \)-submodule of \( Q_p \). Hence, by Lemma 3.1, we infer that \( A = M \cap Z_p^+ \) is a \( p \)-pure subgroup of \( Z_p^+ \). Suppose, contrary to our claim, that \( \square A \neq \{0\} \). It follows, from Lemma 3.4, that there exists \( c \in Z_p^+ \setminus \{0\} \) such that, for all \( a, b \in A \), \( a \cdot c \cdot b \in A \). As \( 1 \in A \), we obtain \( c = 1 \cdot c \cdot 1 \in A \). Hence there exist \( s \in \mathbb{N}, a_0, a_1, a_2, \ldots, a_s \in \mathbb{Z}[p^{-1}] \), not all equal to zero, and pairwise distinct \( x_1, x_2, \ldots, x_s \in X \) such that \( c = a_0 + \sum_{i=1}^s a_ix_i \). Thus \( x_i^2 \cdot c \in A \) and, consequently, \( x_i^2 \cdot (a_0 + \sum_{i=1}^s a_ix_i) \in M \), which contradicts the algebraic independence of \( X \) over \( Q \). Therefore \( A \) is a nil-group. The indecomposability of \( A \) follows from [12, Theorem 88.1]. If \( 1 < |X| < \aleph_0 \), then \( A \) is a group of rank \( |X| + 1 \). If \( \aleph_0 \leq |X| \leq 2^{\aleph_0} \), then \( A \) is a group of rank \( |X| \).

4. Main results

**Proposition 4.1.** If \( M \) and \( N \) are nontrivial \( \mathbb{Z}[p^{-1}] \)-submodules of the field \( Q_p \), then \( (M \cap Z_p^+) \cdot (N \cap Z_p^+) = (MN) \cap Z_p^+ \).

**Proof.** Since \( M \cap Z_p^+ \subseteq M \) and \( N \cap Z_p^+ \subseteq N \), we see that \( (M \cap Z_p^+) \cdot (N \cap Z_p^+) \subseteq MN \). Moreover, \( M \cap Z_p^+, N \cap Z_p^+ \subseteq Z_p^+ \), so \( (M \cap Z_p^+) \cdot (N \cap Z_p^+) \subseteq (MN) \cap Z_p^+ \). To prove the opposite inclusion, take any \( x \in (MN) \cap Z_p^+ \). Then \( x = \sum_{i=1}^n a_ib_i \) for some \( n \in \mathbb{N}, a_1, a_2, \ldots, a_n \in M \) and \( b_1, b_2, \ldots, b_n \in N \). Furthermore, it follows, from [7, Theorem 4], that there exists \( s \in \mathbb{N} \) such that, for each \( i \in \{1, 2, \ldots, n\}, p^s a_i, p^s b_i \in Z_p^+ \). Thus \( p^{2s}x \in (M \cap Z_p^+) \cdot (N \cap Z_p^+) \). Hence, by Lemmas 3.1 and 3.3, \( x \in (M \cap Z_p^+) \cdot (N \cap Z_p^+) \). \( \Box \)

**Remark 4.2.** Let \( \alpha, \beta \) be elements of \( Z_p^+ \) that are algebraically independent over \( Q \). Let \( R \) be the subring of \( Q_p \) generated by \( p^{-1}, \alpha, \beta \) and let \( S \) be the subring of \( Z_p^+ \) generated by \( \alpha, \beta \). The polynomial ring \( (\mathbb{Z}[p^{-1}])[x, y] \) can be treated as a subring of the polynomial ring \( Q_p[x, y] \). Similarly, the polynomial ring \( \mathbb{Z}[x, y] \) can be treated
as a subring of the polynomial ring $\mathbb{Z}[x,y]$. Moreover, the algebraic independence implies that $R \cong (\mathbb{Z}[p^{-1}])[x,y]$, $S \cong \mathbb{Z}[x,y]$ and

$$R = \{ f(\alpha, \beta) : f \in (\mathbb{Z}[p^{-1}])[x,y], \quad S = \{ g(\alpha, \beta) : g \in \mathbb{Z}[x,y] \}. \quad (4.1)$$

Let $(a_n)_{n=0}^{\infty} \to \alpha$ and $(b_n)_{n=0}^{\infty} \to \beta$. From the basic properties of $p$-adic integers (see [7]) it follows that, for all $\gamma, \delta \in \mathbb{Z}_p$ and $g \in \mathbb{Z}[x,y]$, 

$$((c_n)_{n=0}^{\infty} \to \gamma, (d_n)_{n=0}^{\infty} \to \delta) \Rightarrow (g(c_n, d_n))_{n=0}^{\infty} \to g(\gamma, \delta). \quad (4.2)$$

Furthermore, if $(c_n)_{n=0}^{\infty} \to \gamma$ and $k \in \mathbb{N}$, then it follows, from [7, Corollary 1 and (3.4)], that $p^k$ divides $\gamma$ in $\mathbb{Z}_p$ exactly if $p^k$ divides $c_{k-1}$ in $\mathbb{Z}$. Moreover, $\mathbb{Z}_p \cap R = \{ \omega p^{-k} : \omega \in S, k \in \mathbb{N}, p^k | \omega \}$, so (4.2) implies that

$$\mathbb{Z}_p \cap R = \{ f(\alpha, \beta)p^{-k} : f \in \mathbb{Z}[x,y], k \in \mathbb{N}, p^k | f(a_{k-1}, b_{k-1}) \}. \quad (4.3)$$

**Theorem 4.3.** There exists a torsion-free abelian group $A$ such that $A/\square A$ is not a nil$_a$-group and $\square A = \square A = A \oplus A$ for some $\oplus \in \text{Mult}(A)$. 

**Proof.** We retain all designations of Remark 4.2 under the additional assumption that $\alpha, \beta \in \mathbb{Z}_p$. Define $I = \alpha \cdot R + \beta \cdot R$ and $A = \mathbb{Z}_p \cap I$. Then $I \triangleleft R$ and $I$ is a $\mathbb{Z}[p^{-1}]$-submodule of $Q_p$. Hence $A$ is a subring of $\mathbb{Z}_p$ and Lemma 3.1 implies that $A$ is a $p$-pure subgroup of $\mathbb{Z}_p^\times$. 

Take any $* \in \text{Mult}(A)$. It follows, from Lemma 3.4, that there exists $c \in \mathbb{Z}_p$ such that $a*b = a \cdot c \cdot b$ for all $a, b \in A$. Define $s_1 = \alpha \cdot \alpha$ and $s_2 = \beta \cdot \beta$. Then $s_1 = c \cdot \alpha^2$ and $s_2 = c \cdot \beta^2$, and hence $s_1/\alpha^2 = s_2/\beta^2$. Thus $s_1\beta^2 = s_2\alpha^2$. Moreover, $\mathbb{Z}[p^{-1}]$ is a unique factorisation domain, and so is $R$, by Gauss’s lemma and Remark 4.2. Furthermore, $\alpha$ and $\beta$ are nonassociate prime elements of $R$, so $\alpha^2 \mid s_1$ in $R$. Hence $c = s_1/\alpha^2 \in R$ and, consequently, $c \in R \cap \mathbb{Z}_p$. Since $A \subseteq I$, $c \in R$ and $I \triangleleft R$, we obtain $A \cdot c \subseteq I$. Moreover, $A \cdot c \subseteq \mathbb{Z}_p$ because $A \subseteq \mathbb{Z}_p$ and $c \in \mathbb{Z}_p$. Thus $A \cdot c \subseteq A$, and hence $A * A = A \cdot c \cdot A \subseteq A \cdot A = A^2$. As $*$ has been chosen arbitrarily, we get $\square A \subseteq A^2$. Observe also that $A^2 \subseteq \square A \subseteq A$ so $\square A = \square A = A^2$. 

Notice that $I^2 = \alpha^2 \cdot R + (\alpha \cdot \beta) \cdot R + \beta^2 \cdot R$. Moreover, it follows, from Proposition 4.1, that $A^2 = \mathbb{Z}_p \cap I^2$. Take any $\Psi \in A/A^2$. Then $\Psi = \alpha \cdot \xi + \beta \cdot \zeta + A^2$ for some $\xi, \zeta \in \mathbb{Z}_p$. Moreover, (4.1) implies the existence of $g, h \in \mathbb{Z}[x,y]$ and $k \in \mathbb{N}$ such that $\alpha \cdot \xi + \beta \cdot \zeta = (\alpha \cdot g(\alpha, \beta) + \beta \cdot h(\alpha, \beta))p^{-k}$. As $\alpha \cdot \xi + \beta \cdot \zeta \in \mathbb{Z}_p$, $p^k | \alpha \cdot g(\alpha, \beta) + \beta \cdot h(\alpha, \beta)$. Let $a$ and $b$ denote the constant terms of polynomials $g$ and $h$, respectively. We will show that there exists $c \in \mathbb{Z}$ for which $\Psi = (a\alpha + b\beta + ca^2)p^{-k} + A^2$. This equation holds if and only if $(g(\alpha, \beta) - a)\alpha + (h(\alpha, \beta) - b) \beta - ca^2)p^{-k} \in A^2$, which is equivalent to $(g(\alpha, \beta) - a)\alpha + (h(\alpha, \beta) - b) \beta - ca^2)p^{-k} \in \mathbb{Z}_p$. It is true exactly if $p^k | (g(\alpha, \beta) - a)\alpha + (h(\alpha, \beta) - b) \beta - ca^2$.

It follows, from (4.3), that it holds if and only if $p^k | (g(a_{k-1}, b_{k-1} - a)a_{k-1} + (h(a_{k-1}, b_{k-1} - b)b_{k-1} - ca_{k-1}^2a_{k-1})$, which is equivalent to $ca_{k-1}^2a_{k-1} \equiv (g(a_{k-1}, b_{k-1} - a)a_{k-1} + (h(a_{k-1}, b_{k-1} - b)b_{k-1} - ca_{k-1}^2)a_{k-1} \mod p^k)$. Since $\alpha \in \mathbb{Z}_p^\times$, it follows, from [7, Theorem 1 and (3.4)], that $p \nmid a_{k-1}$. Thus the claimed element $c$ exists. Obviously, for any $a, b, c \in \mathbb{Z}$ and $k \in \mathbb{N}$ satisfying $p^k | a\alpha + b\beta + ca^2$, $a\alpha + b\beta + ca^2)p^{-k} \in A$, so

$$A/A^2 = \{(a\alpha + b\beta + ca^2)p^{-k} + A^2 : k \in \mathbb{N}, a, b, c \in \mathbb{Z}, p^k | a\alpha + b\beta + ca^2 \}.$$
Consider the function \( \varphi : (A/A^2)^+ \to (\mathbb{Z}[p^{-1}] \times \mathbb{Z}[p^{-1}])^+ \) given by
\[
\varphi((a\alpha + b\beta + ca^2)p^{-k} + A^2) = (ap^{-k}, bp^{-k}).
\]
Take any \( a, b, c, d, e, f \in \mathbb{Z}, k, l \in \mathbb{N} \) such that \( p^k | a\alpha + b\beta + ca^2, p^l | da + eb + fa^2 \) and \((a\alpha + b\beta + ca^2)p^{-k} + A^2 = (da + eb + fa^2)p^{-l} + A^2\). Then
\[
((p^l a - p^k d)\alpha + (p^l b - p^k e)\beta + (p^l c - p^k f)\alpha^2)p^{-(k+l)} = (a\alpha + b\beta + ca^2)p^{-k} - (da + eb + fa^2)p^{-l}
\]
is in \( A^2 \), so \((p^l a - p^k d)\alpha + (p^l b - p^k e)\beta + (p^l c - p^k f)\alpha^2 \in A^2\). Hence \((p^l a - p^k d)\alpha + (p^l b - p^k e)\beta \in A^2\). For abbreviation, define \( U = p^l a - p^k d \) and \( V = p^l b - p^k e \). Since \( U\alpha + V\beta \in I^2 \), (4.1) implies that there exist \( f_1, f_2, f_3 \in (\mathbb{Z}[p^{-1}])[x, y] \) such that \( U\alpha + V\beta = a^2 f_1(\alpha, \beta) + a\beta f_2(\alpha, \beta) + \beta^2 f_3(\alpha, \beta) \). We apply (4.1) again to obtain \( Ux = x^2 f_1(x, 0) \) and, consequently, \( U = 0 \). Similarly, \( V = 0 \), and hence \( p^l a = p^k d \) and \( p^l b = p^k e \). Thus \( ap^{-k} = dp^{-l} \) and \( bp^{-k} = ep^{-l} \). Therefore the definition of \( \varphi \) is correct. A straightforward verification shows that \( \varphi \) is an additive homomorphism. If \((a\alpha + b\beta + ca^2)p^{-k} + A^2 \in \ker \varphi \), then \((ap^{-k}, bp^{-k}) = (0, 0)\) and, consequently, \( a = b = 0 \). Hence \((a\alpha + b\beta + ca^2)p^{-k} + A^2 = ca^2p^{-k} + A^2\). Moreover, \( p^k | ca^2_1 \), so \( cp^{-k} \in \mathbb{Z} \). Therefore \( p^k | ca^2 \), and hence \( ca^2p^{-k} \in \mathbb{Z}_p \cap I^2 = A^2 \). Thus \( \varphi \) is a monomorphism. Take any \( z \in (\mathbb{Z}[p^{-1}] \times \mathbb{Z}[p^{-1}])^+ \). Then \( z = (up^{-s}, vp^{-s}) \) for some \( u, v \in \mathbb{Z} \) and \( s \in \mathbb{N} \). Since \( p \nmid a_{s-1} \), there exists \( r \in \mathbb{Z} \) satisfying \( -ra_{s-1}^2 \equiv uas_{-1} + vb_{s-1} \pmod{p^s} \). Hence, by Remark 4.2, we get \( p^k | u\alpha + v\beta + ra^2 \). Thus \((u\alpha + v\beta + ra^2)p^{-s} \in A \) and \( z = \varphi((u\alpha + v\beta + ra^2)p^{-s} + A^2) \). Therefore \( \varphi \) is an isomorphism and, consequently, \( A/\Box A \cong (\mathbb{Z}[p^{-1}] \times \mathbb{Z}[p^{-1}])^+ \). Finally, \( A/\Box A \) is not a nil\(_a\)-group. □

References


R. R. ANDRUSZKIEWICZ, Institute of Mathematics,
University of Białystok, 15-267 Białystok, K. Ciołkowskiego 1M, Poland
e-mail: randrusz@math.uwb.edu.pl

M. WORONOWICZ, Institute of Mathematics,
University of Białystok, 15-267 Białystok, K. Ciołkowskiego 1M, Poland
e-mail: mworonowicz@math.uwb.edu.pl