This paper was published in *Topology and Its Applications*, **131** (2003), 149-176.
To the best of my knowledge this is the final version as it was submitted to the publisher. – NH

Multiplications in Additive Compactifications of $\mathbb{N}$ and $\mathbb{Z}$

Neil Hindman[1], **John Pym** and **Dona Strauss**

ABSTRACT. There is a natural action $(n, x) \mapsto nx$ of $(\mathbb{N}, \cdot\,)$ on any semigroup $(S, +\,)$. When S is compact, there is always an extension to a map $\beta\mathbb{N} \times S \to S$. When S has additional properties, there are extensions to other familiar semigroup compactifications of $\mathbb{N}$, for example wap$\mathbb{N}$, ap$\mathbb{N}$ and sap$\mathbb{N} \cong$ b$\mathbb{Z}$ (the Bohr compactification of $\mathbb{Z}$). Special cases of these extensions yield multiplications $*$ on these compactifications. The properties of multiplication, and its relationships with the natural addition, in each compactification are discussed. In particular, (b$\mathbb{Z}, +, *\,$) is a ring and its properties can often be pulled back to the other structures. The final section is devoted to the enveloping semigroups (which are in fact rings) of the actions of $\mathbb{Z}$ on compact groups. There turn out to be few possibilities: for example, if the group is not totally disconnected, then the enveloping ring for the action $n \mapsto nx$ is just (b$\mathbb{Z}, +, *\,$).

1. Introduction.

The theory of compactifications of the semigroup $(\mathbb{N}, +)$ has produced several important compact semigroups, including $\beta\mathbb{N}$, wap$\mathbb{N}$, ap$\mathbb{N}$ and sap$\mathbb{N}$ (definitions will be given below); we shall denote the operation in each of these semigroups by $+$ in the customary fashion. There are corresponding compactifications of $\mathbb{Z}$; the first two, $\beta\mathbb{Z}$ and wap$\mathbb{Z}$, will be of little concern to us in this paper. The compactifications ap$\mathbb{Z}$ and sap$\mathbb{Z}$ both coincide with the Bohr compactification b$\mathbb{Z}$ of $\mathbb{Z}$, and in fact b$\mathbb{Z}$ is also identical with sap$\mathbb{N}$.

The purpose of our paper is to investigate a binary operation $*$ defined on these compact semigroups which is a natural extension of the operation of multiplication on $\mathbb{N}$. Multiplication, $\cdot$, on $\mathbb{N}$ can also be extended to a different binary operation on $\beta\mathbb{N}$, where it provides a semigroup operation. A determining property of $p \cdot q$ for $p, q \in \beta\mathbb{N}$ is

$$p \cdot q = \lim_{m\to p} \lim_{n\to q} m \cdot n$$

(where m and n are restricted to lie in $\mathbb{N}$ and the order in which the limit operations are taken is important). The algebraic structure $(\beta\mathbb{N}, +, \cdot\,)$ is difficult but interesting, and does have important combinatorial applications [8]. However, the multiplication of $\mathbb{N}$ does not seem to have been extended to the other compactifications. Indeed the formula just given for the product in $\beta\mathbb{N}$ cannot be used to define a binary operation on wap$\mathbb{N}$, as we shall see in Theorem 5.4.

[1]This author acknowledges support received from the National Science Foundation (USA) via grant DMS-0070593

However, multiplication can be extended in another way. We could say that the product mn of integers m and n simply means a sum of m copies of n:

$$m * n = n + n + \ldots + n$$

(where we have used a different notation, $*$, as the operations $*$ and $\cdot$ will not always coincide in our compactifications). Below we shall show how the approach using the operation $*$ does provide extensions of multiplication to all the above compactifications of $\mathbb{N}$ and to $\mathrm{b}\mathbb{Z}$. In $\beta\mathbb{N}$ this new operation $*$ is different from $\cdot$, but its relationship with $+$ is hardly any more satisfactory. In $\mathrm{wap}\mathbb{N}$ the situation is a little better in that the associative law and one distributive law hold. In $\mathrm{ap}\mathbb{N}$ and $\mathrm{b}\mathbb{Z}$ the operation $*$ coincides with $\cdot$ and $(\mathrm{b}\mathbb{Z}, +, *)$ is even a ring. We provide a detailed description of this ring and use it to deduce properties of $\beta\mathbb{N}$ and $\mathrm{wap}\mathbb{N}$. Although $\mathrm{b}\mathbb{Z}$ is very extensively studied we know of no papers on its ring structure. This may be because topologically the multiplication $*$ is not so satisfactory. We shall point out the extent to which it is continuous.

The overall context of our work is a little more general than we have so far admitted. We begin with any semigroup $(S, +)$; as is often the case in this field, the use of the $+$ sign is not intended to imply that the operation is commutative, and we shall adhere to this convention even when S is a non-commutative group. We consider the action of $\mathbb{N}$ on S by

$$n * x = x + x + \ldots + x$$

for $n \in \mathbb{N}$, $x \in S$, where there are n occurrences of x on the right. Of course, $n * x$ would usually be denoted by nx. If $(S, +)$ is a group, $x \mapsto n * x$ is well-defined for $n \in \mathbb{Z}$ and determines an action of $\mathbb{Z}$ on S.

When S has a compact topology, for each $x \in S$ the map

$$n \mapsto n * x$$

must have a continuous extension

$$q \mapsto q * x$$

from $\beta\mathbb{N}$ to S. In particular we can take $(S, +) = (\beta\mathbb{N}, +)$ and so produce a binary operation $*$ on $\beta\mathbb{N}$. In Theorem 2.1 we show how the properties of the 'action' $*$ of $\beta\mathbb{N}$ on S depend on the continuity properties of the multiplication in S. We have put inverted commas around the word action since the normal associative property $(p*q)*x = p*(q*x)$ does not always hold. In addition, for a given $q \in \beta\mathbb{N}$, the map $x \mapsto q * x$ from S to itself can be discontinuous. This is even so when $q = 2$. Examples of situations where this occurs are given in Theorems 6.1 and 5.1. Later theorems in §2 show that other compactifications of $\mathbb{N}$ provide more satisfactory actions on S.

This approach to our topic suggests that we should look at the enveloping semigroups for our actions of $\mathbb{N}$ on S, that is the pointwise closure in the set of all mappings from S to itself of $\{x \mapsto n * x : n \in \mathbb{N}\}$. Two answers are particularly interesting. When S is a compact topological group, the enveloping semigroup is always a ring. It is the ring $(\mathrm{b}\mathbb{Z}, +, *)$ if S is not totally disconnected. So $(\mathrm{b}\mathbb{Z}, *)$ arises naturally in this case as the enveloping semigroup of the action of $(\mathbb{N}, \cdot\ )$ (or of $(\mathbb{Z}, \cdot\ )$) on S defined by the maps $x \mapsto n * x$. The enveloping rings associated in this way with compact topological groups which are totally disconnected, are precisely the quotients of the ring $\prod_{p \text{ prime}} A_p$, where A_p denotes the ring of p-adic integers.

Our semigroups will usually be *right topological*, that is, multiplication xy is continuous in x for every fixed y. A few of our results do not require this hypothesis, and we shall then refer to S as having a compact topology, with no continuity of multiplication implied. We shall assume that all hypothesized topological spaces are Hausdorff. If X is a topological space, X_d will denote X with the discrete topology.

We shall find it useful to use some of the terminology of semigroup theory for a binary operation which is not assumed to be associative. Let $\diamond$ be a binary operation on a topological space S. We shall say that $\diamond$ is *right topological* if the map $x \mapsto x \diamond y$ is continuous for each $y \in S$. In this case, we define the *topological centre* $\Lambda(S, \diamond)$ to be the set of elements $x \in S$ for which the map $y \mapsto x \diamond y$ is a continuous map from S to itself. If $\diamond$ and $\diamond'$ are binary operations on the sets S and S' respectively, we shall say that $h : S \to S'$ is a *homomorphism* from $(S, \diamond)$ to $(S', \diamond')$ if $h(x \diamond y) = h(x) \diamond' h(y)$ for every $x, y \in S$.

We regard $\beta\mathbb{N}$ as the set of ultrafilters on $\mathbb{N}$, with the topology defined by taking the sets of the form $\overline{A} = \{p \in \beta\mathbb{N} : A \in p\}$, where $A \subseteq \mathbb{N}$, as a base for the open sets. Then $\overline{A} = \mathrm{cl}_{\beta\mathbb{N}}(A)$. It is well known that the operations of addition and multiplication on $\mathbb{N}$ extend to binary operations on $\beta\mathbb{N}$, denoted by $+$ and $\cdot$ respectively, for which $(\beta\mathbb{N}, +)$ and $(\beta\mathbb{N}, \cdot\,)$ are right topological semigroups. (The extension of $\cdot$ is described by the iterated limit formula above; see [8] for formal definitions of these operations.)

The organisation of this paper is as follows. We begin, in §2, and end, in §8, by considering actions of $\mathbb{N}$ and $\mathbb{Z}$ on compact semigroups S. §2 is concerned with general results about how the extension of these actions to compactifications depends on the continuity properties of S. It ends with a 'simultaneous idempotent theorem', giving conditions under which a compact set with two semigroup operations has an element which is an idempotent for both (2.15). §8 develops the special theory when S is a group; here the enveloping semigroups turn out to be rings of particular forms. Between come a series of sections which discuss the properties of the multiplication $*$ in the various compactifications. In §3, b$\mathbb{Z}$ is studied, and some detail is given about its ring structure. The short §4 looks at ap$\mathbb{N}$. We know least about wap$\mathbb{N}$; mainly negative results are given in §5. §6 is devoted to $\beta\mathbb{N}$. In §7 the properties of b$\mathbb{Z}$ are used to obtain corresponding properties for most of the other compactifications.

2. Extending $*$.

2.1 Theorem. *Let $(S, +)$ be a semigroup with a compact topology. Let $(n, x) \mapsto n * x$, $\mathbb{N} \times S \to S$ be the action of $\mathbb{N}$ on S defined above.*

(i) *The action extends to a map $*$: $\beta\mathbb{N} \times S \to S$*

(a) *which is continuous in the left-hand (i.e. the $\beta\mathbb{N}$) variable,*

(b) *and for which $1 * x = x$ for all $x \in S$.*

In particular, $\beta\mathbb{N}$ itself has a unique binary operation $*$ which is continuous in the left-hand variable and extends the operation $(n, q) \mapsto n * q$ for $n \in \mathbb{N}$, $q \in \beta\mathbb{N}$. $(\beta\mathbb{N}, *)$ has the two-sided identity 1.

(ii) *In addition, let $(S, +)$ be separately continuous. Then also*

(c) $*$ *is distributive over* $+$ *from the right (that is, for* $p, q \in \beta\mathbb{N}$ *and* $x \in S$ *we have* $(p+q)*x = p*x + q*x$*),*

(d) $\beta\mathbb{N} \times S \to S$ *is an action in the sense that* $(p*q)*x = p*(q*x)$ *for* $p, q \in \beta\mathbb{N}$ *and* $x \in S$*.*

(iii) *In addition, let* $(S, +)$ *be jointly continuous and abelian. Then also*

(e) $*$ *is distributive over* $+$ *from the left (that is, for* $p \in \beta\mathbb{N}$ *and* $x, y \in S$ *we have* $p*(x+y) = p*x + p*y$*).*

Proof (i) is essentially in our introduction above, except for the fact that 1 is a right identity for $(\beta\mathbb{N}, *)$. But this is easy, since for $n \in \mathbb{N}$ we have $n*1 = 1+1+\ldots+1 = n$, and continuity gives the result. For (ii)(c) first observe that

$$(m+n)*x = x + x + \ldots + x = m*x + n*x$$

for $m, n \in \mathbb{N}$ and $x \in S$ where there are $m+n$ x's in the middle term. Now let n converge to q and subsequently m converge to p; we get the required result on using continuity of $q' \mapsto m' + q'$ and of $p' \mapsto p' + q'$ in $(\beta\mathbb{N}, +)$ and separate continuity in S. To prove (d) begin by taking $m \in \mathbb{N}$, $q \in \beta\mathbb{N}$ and $x \in S$. Then, using the distributive law we have just established,

$$(m*q)*x = (q+q+\ldots+q)*x = q*x + q*x + \ldots + q*x = m*(q*x).$$

(d) follows on letting $m \to p$. For (iii)(e) we notice that for $n \in \mathbb{N}$ and $x, y \in S$,

$$n*(x+y) = x+y+x+y+\ldots+x+y = x+x+\ldots+x+y+y+\ldots+y = n*x+n*y,$$

since S is now commutative. Our result follows on letting n converge to p, using joint continuity in S. □

The question of whether we have the *right* conditions in the above theorem arises. What this means – for example, in the case of (c) – is, do we actually need S to be separately continuous in order that the distributivity property should hold? In fact, looking at this particular proof, we need only separate continuity of $+$ in the subset $\beta\mathbb{N} * x$ for each $x \in S$. This condition does not seem in any way natural and it is not obvious that it has a nice interpretation in terms of familiar theories.

2.2 Corollary. *Let* $(S, +)$ *be a semigroup with a compact topology. A subset of* S *is an invariant subset for the '$*$-action' of* $\beta\mathbb{N}$ *if it is a union of closed subsemigroups of* $(S, +)$*. If* $(S, +)$ *is separately continuous, the converse holds.*

In particular, idempotents of $(S, +)$ *are minimal invariant subsets.*

Proof. If x is in a closed subsemigroup T then $n*x \in T$ for all $n \in \mathbb{N}$ and so also $\beta\mathbb{N}*x \subseteq T$. Any union of invariant subsets is invariant. If $(S, +)$ is separately continuous then for any $x \in S$ the subset $\beta\mathbb{N}*x$ is a semigroup from (ii)(c) of the Theorem, and it is evidently closed. The conclusion follows. □

We say that a compact right topological semigroup $(\kappa\Sigma, +)$ is a semigroup compactification of a semigroup $(\Sigma, +)$ with a topology if there is a continuous homomorphism from

Σ to $\kappa\Sigma$ for which the image of Σ is dense in $\kappa\Sigma$ and contained in its topological centre. (Notice that the continuous homomorphism is not required to be an embedding, so a semigroup compactification need not be a compactification in the topological sense.) We shall say that a compactification $\kappa_1\Sigma$ is larger than another $\kappa_2\Sigma$ if there is a continuous homomorphism $\pi : \kappa_1\Sigma \to \kappa_2\Sigma$ such that the composite $\Sigma \to \kappa_1\Sigma \to \kappa_2\Sigma$ is just the map $\Sigma \to \kappa_2\Sigma$.

If $(\kappa\mathbb{N}, +)$ is a compactification of $(\mathbb{N}, +)$ and the canonical homomorphism $\mathbb{N} \to \kappa\mathbb{N}$ is not injective, easy algebraic arguments show that the image, and so also $\kappa\mathbb{N}$ itself, is finite. Including such cases leads to complications in proofs, though our results, in so far as they are relevant in this situation, hold for reasons which are usually trivial. We shall therefore consider only compactifications $\kappa\mathbb{N}$ for which $\mathbb{N} \to \kappa\mathbb{N}$ is injective. We shall then make the simplifying assumption that $\mathbb{N} \subseteq \kappa\mathbb{N}$. The reader should be warned however that in one of the compactifications that we consider, namely $\kappa\mathbb{N} = \mathrm{sap}\mathbb{N}$, the copy of $\mathbb{N}$ is not discrete in $\kappa\mathbb{N}$.

We shall be considering several different compactifications of the semigroup $(\mathbb{N}, +)$. The first, $\beta\mathbb{N}$, we have already looked at in Theorem 2.1. The second, $(\mathrm{wap}\mathbb{N}, +)$, is the largest in which the operation $+$ is separately continuous. The third, $(\mathrm{ap}\mathbb{N}, +)$ is the largest for which the operation $+$ is jointly continuous, and the fourth, $(\mathrm{sap}\mathbb{N}, +)$, is the largest which is a compact topological group. Each of these compactifications is larger than the succeeding one; we shall denote the natural surjective homomorphism between the compactifications $\kappa_1\mathbb{N}$ and $\kappa_2\mathbb{N}$ by π_{κ_1,κ_2}. The canonical map $\mathbb{N} \to \mathrm{sap}\mathbb{N}$ is injective (and therefore the canonical maps into the other compactifications are injective) because there is an injective homomorphism from $\mathbb{N}$ into the circle group $\mathbb{T}$. $(\beta\mathbb{N}, +)$ is not commutative, but $(\mathrm{wap}\mathbb{N}, +)$ is, and so are all the others. For the existence of these compactifications and the relationships between them, see [1] or [8].

In fact, $(\mathrm{sap}\mathbb{N}, +)$ is identical with the Bohr compactification $(\mathrm{b}\mathbb{Z}, +)$ (which can be defined either as the largest compactification $\mathrm{ap}\mathbb{Z}$ of $(\mathbb{Z}, +)$ in which $+$ is jointly continuous, or as the largest compactification $\mathrm{sap}\mathbb{Z}$ of $(\mathbb{Z}, +)$ which is a topological group; these are easily seen to be the same). To prove this, recall the easy result that the closure of a semigroup in a compact topological group is a subgroup. Then (i) $(\mathrm{b}\mathbb{Z}, +)$ is larger than $(\mathrm{sap}\mathbb{N}, +)$ because $(\mathrm{sap}\mathbb{N}, +)$ is a group compactification of $\mathbb{N}$ and is therefore a topological group compactification of the group $\mathbb{Z}$ generated by $\mathbb{N}$, and (ii) that $(\mathrm{sap}\mathbb{N}, +)$ is larger than $(\mathrm{b}\mathbb{Z}, +)$ because the closure of the image of the map $\mathbb{N} \to \mathbb{Z} \to \mathrm{b}\mathbb{Z}$ is a compact subgroup of $(\mathrm{b}\mathbb{Z}, +)$ containing $\mathbb{Z}$ and is therefore equal to $\mathrm{b}\mathbb{Z}$, which is thus a topological group compactification of $\mathbb{N}$. The canonical homomorphism $\kappa\mathbb{N} \to \mathrm{b}\mathbb{Z}$ will be denoted by $\pi_{\kappa,\mathrm{b}}$.

2.3 Definition. Let $(S, +)$ be a compact right topological semigroup. Let $(\kappa\mathbb{N}, +)$ be a semigroup compactification of $(\mathbb{N}, +)$. We say that $*$ *extends to* $\kappa\mathbb{N} \times S$ if for each $x \in S$, the function $n \mapsto n * x$ from $\mathbb{N}$ to S extends to a continuous function from $\kappa\mathbb{N}$ to S. In this case, if $p \in \kappa\mathbb{N}$, then $p * x$ will denote the value of this function at p. If $(S, +)$ is taken to be $(\kappa\mathbb{N}, +)$ we say that *the multiplication* $*$ *extends to* $\kappa\mathbb{N}$.

Both extensions exist (for all S) when $\kappa\mathbb{N} = \beta\mathbb{N}$ as we saw above. We shall use this fact in discussing extensions to other compactifications.

2.4 Proposition. (i) *Let* $p \in \beta\mathbb{N}$, $x \in S$, *and suppose* $*$ *extends to* $\kappa\mathbb{N} \times S$. *Then*

$p * x = \pi_{\beta,\kappa}(p) * x$.

(ii) *If the multiplication $*$ extends to $\kappa\mathbb{N}$ then $\pi_{\beta,\kappa}$ is a $*$-homomorphism.*

Proof. (i) Take $m \in \mathbb{N}$. The limit of $m * x \in S$ as $m \to p$ in $\beta\mathbb{N}$ is $p * x$. But when $m \to p$, also $m \to \pi_{\beta,\kappa}(p)$ in $\kappa\mathbb{N}$. Since $*$ extends to $\kappa\mathbb{N} \times S$ the limit of $m * p$ is also $\pi_{\beta,\kappa}(p) * x$. Thus (i) is proved.

(ii) Observe that for $q \in \kappa\mathbb{N}$,

$$\pi_{\beta,\kappa}(m * q) = \pi_{\beta,\kappa}(q + q + \ldots + q) = \pi_{\beta,\kappa}(q) + \pi_{\beta,\kappa}(q) + \ldots + \pi_{\beta,\kappa}(q) = m * \pi_{\beta,\kappa}(q),$$

and then let $m \to p$, using (i). □

We now investigate how the operation $*$ behaves in each of our compactifications. We deal with these semigroups separately.

2.5 Theorem. *If $(S, +)$ is a compact separately continuous semigroup the action $(n, x) \mapsto n * x$ of $\mathbb{N}$ on S extends to an action of* $\mathrm{wap}\mathbb{N}$ *on S. By taking $S = \mathrm{wap}\mathbb{N}$ we obtain a structure* $(\mathrm{wap}\mathbb{N}, +, *)$ *in which the operation $*$ is associative, distributes over addition from the right, has an identity* 1*, is continuous in the left-hand variable (so that* $(\mathrm{wap}\mathbb{N}, *)$ *is a right topological semigroup), and* $1 \in \Lambda(\mathrm{wap}\mathbb{N}, *)$.

Proof. We first show that $*$ extends to $\mathrm{wap}\mathbb{N} \times S \to S$. For each $x \in S$ the map $n \mapsto n * x$ is a homomorphism from $(\mathbb{N}, +)$ to $(S, +)$ because

$$(m + n) * x = x + x + \ldots + x = m * x + n * x$$

where there are $m+n$ x's in the middle term, and the extension of this map to a continuous homomorphism from $\mathrm{wap}\mathbb{N}$ to S exists by the defining property of $\mathrm{wap}\mathbb{N}$. The properties of this extension now follow from Theorem 2.1 and Proposition 2.4 because $\pi_{\beta,\mathrm{wap}}$ is surjective (for example the distributive law follows directly from $(p+q)*x = p*x+q*x$ for $p, q \in \beta\mathbb{N}$ and $x \in \mathrm{wap}\mathbb{N}$ on applying 2.4(i) to $\pi_{\beta,\mathrm{wap}}$). That $1 \in \Lambda(\mathrm{wap}\mathbb{N}, *)$ is trivial because 1 is a left identity. □

There is a parallel result for $\mathrm{ap}\mathbb{N}$.

2.6 Theorem. *If $(S, +)$ is a compact jointly continuous semigroup the action $(n, x) \mapsto n*x$ of $\mathbb{N}$ on S extends to an action of* $\mathrm{ap}\mathbb{N}$ *on S. By taking $S = \mathrm{ap}\mathbb{N}$ we obtain a structure* $(\mathrm{ap}\mathbb{N}, +, *)$ *in which* $(\mathrm{ap}\mathbb{N}, *)$ *is a right topological semigroup with identity, $*$ distributes over $+$ on both sides, and* $\mathbb{N} \subseteq \Lambda(\mathrm{ap}\mathbb{N}, *)$.

Proof. The proof is exactly like that of Theorem 2.5, except that for the final part we need to observe that since addition is jointly continuous in $\mathrm{ap}\mathbb{N}$, the map

$$x \mapsto n * x = x + x + \ldots + x$$

is continuous for any $n \in \mathbb{N}$. □

There is a minor subtlety in the next theorem. When $(S, +)$ is a group, besides the action $*$ of $\mathbb{N}$ on S there is a natural action $*$ of $\mathbb{Z}$ on S, which we again denote by $(n, x) \mapsto n * x$. This action will of course extend to $\beta\mathbb{Z} \times S$ and the analogue of Theorem 2.1 holds, though (ii) is redundant since a separately continuous compact group is a topological group. Our theorem asserts not only that $*$ extends to a multiplication on $\mathrm{b}\mathbb{Z}$, but that the structure $(\mathrm{b}\mathbb{Z}, +, *)$ is the same as that obtained by extending $*$ to $(\mathrm{sap}\mathbb{N}, +)$.

2.7 Theorem. *If $(S, +)$ is a compact jointly continuous group the action $(n, x) \mapsto n*x$ of $\mathbb{N}$ on S (resp. of $\mathbb{Z}$ on S) extends to an action of* $\mathrm{sap}\mathbb{N}$ *on S (resp of* $\mathrm{b}\mathbb{Z}$ *on S). By taking $S = \mathrm{sap}\mathbb{N}$ and $S = \mathrm{b}\mathbb{Z}$ we obtain rings $(\mathrm{sap}\mathbb{N}, +, *)$ and $(\mathrm{b}\mathbb{Z}, +, *)$; these are isomorphic. $(\mathrm{b}\mathbb{Z}, *)$ is right topological and $\mathbb{Z} \subseteq \Lambda(\mathrm{b}\mathbb{Z}, *)$.*

Proof. The proof that $(\mathrm{sap}\mathbb{N}, +, *)$ and $(\mathrm{b}\mathbb{Z}, +, *)$ are well-defined and algebraically rings is just like that of Theorem 2.5. We have already observed that the natural map $\psi : (\mathrm{sap}\mathbb{N}, +) \to (\mathrm{b}\mathbb{Z}, +)$ is an isomorphism of topological groups, and therefore for $m \in \mathbb{N}$, $x \in \mathrm{sap}\mathbb{N}$ we have $\psi(m * x) = m * \psi(x)$. The right continuity of $*$ shows that ψ is a $*$-homomorphism.

To get the topological centre result we must add to the conclusion of 2.6 the remark that in the topological group $(\mathrm{b}\mathbb{Z}, +)$ the operation $x \mapsto -x$ is continuous. □

Later we shall determine the topological centres of our semigroups. For the moment we observe that this topological problem is sometimes the same as an algebraic one. We give the proof of the next (well-known) lemma because we do not know of a convenient reference.

2.8 Lemma. *Let S be a compact right topological semigroup in which the topological centre $\Lambda(S)$ contains a commutative subset Z which is dense in S. Then $\Lambda(S)$ coincides with the algebraic centre $Z(S)$.*

Proof. We first show that $Z \subseteq Z(S)$. Let $z \in Z$. Take any $s \in S$ and then $s_i \in Z$ with $s_i \to s$. Then, since $z \in \Lambda(S)$, $zs = \lim zs_i = \lim s_i z = sz$, as required.

Now obviously $Z(S) \subseteq \Lambda(S)$. Take $s \in \Lambda(S)$. Given any $t \in S$, choose $t_i \in Z$ with $t_i \to t$. Then $t_i s \to ts$ by right continuity. But since $t_i \in Z(S)$ we find $t_i s = st_i \to st$ because $s \in \Lambda(S)$. Thus $ts = st$ and $s \in Z(S)$. □

Next we give another lemma which has uses in determining topological centres.

2.9 Lemma. *Let X, Y be compact spaces and let $\pi : X \to Y$ be a continuous* surjective *map. Let $\varphi : X \to X$ and $\psi : Y \to Y$ be such that $\pi \circ \varphi = \psi \circ \pi$. If φ is continuous, then so is ψ.*

Proof. All that needs to be done to prove this is to observe that if $K \subseteq Y$ is closed and so compact, $\psi^{-1}(K) = \pi\big(\varphi^{-1}(\pi^{-1}(K))\big)$ is compact and therefore closed. □

This lemma has the immediate consequence that if X and Y are compact right topological semigroups and π is a surjective homomorphism then $p \in \Lambda(X)$ implies $\pi(p) \in \Lambda(Y)$.

2.10 Definition. We say that the operation $\cdot$ *is defined on the compactification* $\kappa\mathbb{N}$ if the formula

$$p \cdot q = \lim_{m \to p} \lim_{n \to q} m \cdot n$$

defines a binary operation on $\kappa\mathbb{N}$. (It is to be understood that in the above formula, the variables m and n range over $\mathbb{N}$.)

As we saw in the introduction, $\cdot$ is always defined on $\beta\mathbb{N}$. We omit the proof of the following lemma; the conclusions involving continuity of the multiplication follow from

Lemma 2.9 (recall that $\mathbb{N} = \Lambda(\beta\mathbb{N})$).

2.11 Lemma. *Let $(\kappa\mathbb{N}, +)$ be a semigroup compactification of $(\mathbb{N}, +)$. If the operation $\cdot$ is defined on $\kappa\mathbb{N}$, then $(\kappa\mathbb{N}, \cdot\,)$ is a compact right topological semigroup and the projection $\pi_{\beta,\kappa}$ is a homomorphism from $(\beta\mathbb{N}, \cdot\,)$ onto $(\kappa\mathbb{N}, \cdot\,)$. Moreover, $\mathbb{N} \subseteq \Lambda(\kappa\mathbb{N}, \cdot\,)$.* □

We now give a relationship between the multiplications $*$ and $\cdot$ and topological centres.

2.12 Theorem. *Let $(\kappa\mathbb{N}, +)$ be a semigroup compactification of $(\mathbb{N}, +)$ to which the operation $*$ extends. Then $\mathbb{N} \subseteq \Lambda(\kappa\mathbb{N}, *)$ if and only if $\cdot$ is defined on $\kappa\mathbb{N}$ and $* = \cdot$ on $\kappa\mathbb{N}$. In particular $* = \cdot$ in* apℕ *and* bℤ.

Proof. If $* = \cdot$ in $\kappa\mathbb{N}$ then from Lemma 2.11, $\mathbb{N} \subseteq \Lambda(\kappa\mathbb{N}, \cdot\,) = \Lambda(\kappa\mathbb{N}, *)$.

Conversely, when $m, n \in \mathbb{N}$ we have $m \cdot n = m * n$. Since $m \in \Lambda(\kappa\mathbb{N}, *)$, for any $q \in \kappa\mathbb{N}$, we have $m * q = \lim_{n\to q} m * n = \lim_{n\to q} m \cdot n$. Then, from the continuity of $p \mapsto p * q$ we find $p * q = \lim_{m\to p} m * q = \lim_{m\to p}\lim_{n\to q} m \cdot n$.

The "in particular" conclusions follow from Theorems 2.6 and 2.7. □

Theorem 2.12 says that both apℕ and bℤ are compactifications of ℕ in which $* = \cdot$. The question arises, is apℕ the largest compactification for which this is true? There is a little evidence that this might be the case, since $\cdot$ does not extend to wapℕ (Theorem 5.4).

We now show that the ring bℤ has a universal property.

2.13 Definition. We say that $(R, +, \cdot\,)$ is a *compact right topological ring* if $(R, +, \cdot\,)$ is a ring, $(R, +)$ is a compact topological group, and $(R, \cdot\,)$ is a right topological semigroup.

2.14 Theorem. *Let $(R, +, \cdot\,)$ be a compact right topological ring. Any ring homomorphism $h : (\mathbb{N}, +, \cdot\,) \to (R, +, \cdot\,)$ for which $h(\mathbb{N}) \subseteq \Lambda(R, \cdot\,)$ has a unique continuous extension to a ring homomorphism $\widetilde{h} : (\mathrm{b}\mathbb{Z}, +, *) \to (R, +, \cdot\,)$.*

Proof. By the universal property of the compact group $(\mathrm{b}\mathbb{Z}, +)$, there is a unique continuous group homomorphism $\widetilde{h} : (\mathrm{b}\mathbb{Z}, +) \to (R, +)$ extending h. Because h is a ring homomorphism, $h(m \cdot n) = h(m) \cdot h(n)$. If we take $p, q \in \mathrm{b}\mathbb{Z}$ and let $n \to q$ and afterwards $m \to p$ using $h(m) \in \Lambda(R, \cdot\,)$ and the continuity of $\widetilde{h}$, we find $\widetilde{h}(p \cdot q) = \widetilde{h}(p) \cdot \widetilde{h}(q)$ as required. □

The additional condition involving the topological centre in the last theorem is common in the theory of right topological semigroups (see [1]).

The existence of idempotents has played an important role in applications of the algebra of βS. We close this section by recording a simple observation about the existence of joint idempotents if addition and multiplication are both defined and possess certain properties.

2.15 Theorem. *Let $(X, +)$ and $(X, \cdot)$ be compact right topological semigroups such that $\cdot$ distributes over $+$ from the right. There exists $x \in X$ such that $x = x + x = x \cdot x$.*

Proof. (This is a simple adaptation of a proof of Ellis – Corollary 2.10 in [4].) By Zorn's Lemma, let $D \subseteq X$ be minimal subject to being non-empty, compact and closed for both $+$ and $\cdot$. By Corollary 2.10 of [4], we can choose $x \in D$ such that $x = x + x$. We note that $D \cdot x$ is non-empty, compact and closed for both $+$ and $\cdot$. (The fact that $D \cdot x + D \cdot x \subseteq D \cdot x$ follows from the right distributivity.) Thus, since $D \cdot x \subseteq D$, in fact $D \cdot x = D$. In particular, $y \cdot x = x$ for some $y \in D$. Let $E = \{y \in D : y \cdot x = x\}$. Since E is non-empty, compact, closed for $+$ (again using right distributivity), and closed for $\cdot$, it follows that $E = D$ and hence that $x \cdot x = x$. □

It is an immediate consequence of Theorems 2.5 and 2.7 that each of wap$\mathbb{N}$, ap$\mathbb{N}$, and b$\mathbb{Z}$ have points x satisfying $x = x + x = x * x$. However, this conclusion is actually trivial because every x such that $x + x = x$ automatically satisfies $y * x = x$ for every y.

3. b$\mathbb{Z}$.

We have seen that $*$ and $\cdot$ coincide in b$\mathbb{Z}$ and that $(\mathrm{b}\mathbb{Z}, +, *)$ is a ring. However a useful way to view $(\mathrm{b}\mathbb{Z}, +)$ is not as a universal compactification but using the fact from the duality theory of locally compact groups that

$$(\mathrm{b}\mathbb{Z}, +) \cong (\mathrm{ap}\mathbb{Z}, +) \cong (\widehat{\widehat{\mathbb{Z}}_{\mathrm{d}}}),$$

where $\widehat{}$ denotes the Pontryagin dual group and the suffix d means taking the discrete topology (see [7] Theorem 26.12). Since $\widehat{\mathbb{Z}} = \mathbb{T}$, the circle group, b$\mathbb{Z}$ can be identified with the dual group of $\mathbb{T}_{\mathrm{d}}$, that is the group of all characters, or homomorphisms, from $\mathbb{T}_{\mathrm{d}}$ to $\mathbb{T}$. But $\mathbb{T}$ is isomorphic with $(\mathbb{R}/\mathbb{Z}, +)$, and therefore $(\mathrm{b}\mathbb{Z}, +)$ can be identified with all group homomorphisms from $(\mathbb{R}/\mathbb{Z}, +)$ to itself, or in other words with the $\mathbb{Z}$-module endomorphisms of the abelian group $(\mathbb{R}/\mathbb{Z}, +)$. We shall denote this object by $\mathrm{End}(\mathbb{R}/\mathbb{Z}, +)$.

Observe that the Pontryagin topology on $\mathrm{b}\mathbb{Z} = \widehat{\mathbb{T}_{\mathrm{d}}}$ is the topology of pointwise convergence for functions from $\mathbb{T}_{\mathrm{d}}$ to the circle $\mathbb{T}$ with its usual topology. This translates to the topology of pointwise convergence of functions from $\mathbb{R}/\mathbb{Z}$ to $\mathbb{R}/\mathbb{Z}$ when the latter has its usual topology as a quotient of the real line.

3.1 Theorem. $(\mathrm{b}\mathbb{Z}, +, *)$ *is algebraically naturally isomorphic with the endomorphism ring* $\mathrm{End}(\mathbb{R}/\mathbb{Z}, +)$ *(the multiplication in this ring is of course composition of endomorphisms).*

Proof. Under the isomorphism which identifies $(\mathrm{b}\mathbb{Z}, +)$ and $\mathrm{End}(\mathbb{R}/\mathbb{Z}, +)$, the integer $n \in \mathrm{b}\mathbb{Z}$ corresponds to the endomorphism χ_n determined by $\chi_n(x) = nx$ $(x \in \mathbb{R}/\mathbb{Z})$. Thus for any $\chi \in (\mathrm{b}\mathbb{Z}, +) \cong \mathrm{End}(\mathbb{R}/\mathbb{Z}, +)$ we have for $x \in \mathbb{R}/\mathbb{Z}$

$$n * \chi(x) = \chi(x) + \chi(x) + \ldots + \chi(x) = (\chi_n \circ \chi)(x),$$

whence $n * \chi = \chi_n \circ \chi$. Since $*$ is right continuous in b$\mathbb{Z}$ and convergence in $\mathrm{End}(\mathbb{R}/\mathbb{Z}, +)$ is pointwise, we can take limits to see that for any $\psi \in \mathrm{b}\mathbb{Z}$ we have $\psi * \chi = \psi \circ \chi$. □

We now consider ways of representing the algebraic structure of $\mathrm{End}(\mathbb{R}/\mathbb{Z}, +)$. The abelian group $\mathbb{R}/\mathbb{Z}$ is the direct sum of its torsion part $\mathbb{Q}/\mathbb{Z}$ and its vector space part $\mathbb{Q}^{(\mathfrak{c})}$, which is a direct sum of $\mathfrak{c}$ copies of the field $\mathbb{Q}$. The isomorphism can be realized by taking a Hamel basis $(b_\alpha)_{\alpha<\mathfrak{c}}$ for $\mathbb{R}$ with b_0 chosen to be 1, and sending $y = (y_\alpha)_{\alpha<\mathfrak{c}}$ with $y_0 \in \mathbb{Q}/\mathbb{Z}$, $y_\alpha \in \mathbb{Q}$ for $\alpha \geq 1$, to $\sum_\alpha y_\alpha b_\alpha (\mathrm{mod}\ \mathbb{Z})$. Duality theory now tells us that b$\mathbb{Z}$ is the direct product $\widehat{\mathbb{Q}/\mathbb{Z}} \times \widehat{\mathbb{Q}}^{\mathfrak{c}}$ ([7], Theorem 23.22). $\widehat{\mathbb{Q}/\mathbb{Z}}$ is the compact totally disconnected group $\prod_{p \text{ prime}} A_p$ of all groups of p-adic integers (see [7] section 25.4 or [9], Example 1.38). $\widehat{\mathbb{Q}}^{\mathfrak{c}}$ is a compact connected group ([7] Theorem 24.25 or [9] Corollary 7.70). In fact, because $\mathbb{R}$ itself is algebraically isomorphic to the direct sum $\mathbb{Q}^{(\mathfrak{c})}$, the compact group $\widehat{\mathbb{Q}}^{\mathfrak{c}}$ is isomorphic with $\widehat{\mathbb{R}_d}$, and this is just the Bohr compactification b$\mathbb{R}$ of the additive real line $\mathbb{R}$. Thus we can write

$$\mathrm{b}\mathbb{Z} \cong \left(\prod_{p \text{ prime}} A_p \right) \times \mathrm{b}\mathbb{R},$$

with the first factor totally disconnected and the second connected; moreover b$\mathbb{R}$ is monothetic with weight $\mathfrak{w}(\mathrm{b}\mathbb{R}) = \mathfrak{c}$ (see [7], (25.14) and (25.18)).

Our alternative way of considering b$\mathbb{Z}$ is as the $\mathbb{Z}$-module or abelian group homomorphisms from $\mathbb{Q}/\mathbb{Z} \oplus \mathbb{Q}^{(\mathfrak{c})}$ to itself. If we regard elements of this group as column vectors, these homomorphisms can be considered to be matrices $\begin{pmatrix} J & H \\ K & L \end{pmatrix}$ where $J : \mathbb{Q}/\mathbb{Z} \to \mathbb{Q}/\mathbb{Z}$, $H : \mathbb{Q}^{(\mathfrak{c})} \to \mathbb{Q}/\mathbb{Z}$, $K : \mathbb{Q}/\mathbb{Z} \to \mathbb{Q}^{(\mathfrak{c})}$ and $L : \mathbb{Q}^{(\mathfrak{c})} \to \mathbb{Q}^{(\mathfrak{c})}$. Since all elements of $\mathbb{Q}/\mathbb{Z}$ have finite order, but no elements of $\mathbb{Q}^{(\mathfrak{c})}$ do, K must be 0. L is not only $\mathbb{Z}$-linear but $\mathbb{Q}$-linear, and so is given by a $\mathfrak{c} \times \mathfrak{c}$ matrix with entries from $\mathbb{Q}$; since the image of L is in the direct sum $\mathbb{Q}^{(\mathfrak{c})}$, the columns of L can have only a finite number of non-zero entries. H is a row matrix whose entries are homomorphisms from $\mathbb{Q}$ to $\mathbb{Q}/\mathbb{Z}$. The multiplication $*$ in b$\mathbb{Z}$ is, of course, just ordinary matrix multiplication. We should also draw attention to the fact that the inclusion $\mathbb{Z} \subset \mathrm{b}\mathbb{Z}$ is obtained by sending the integer n to the diagonal matrix all of whose entries are n, that is, nI where I is the identity matrix.

Sometimes it will be convenient for us to spell out the matrix formulation. Let $1 \leq \alpha, \beta < \mathfrak{c}$. We denote by $\delta_{\alpha\beta}$ the homomorphism from $\mathbb{R}/\mathbb{Z}$ to itself given by $\delta_{\alpha\beta}(b_\gamma) = b_\alpha$ if $\gamma = \beta$ and 0 otherwise, and $\delta_{\alpha\beta}(\mathbb{Q}/\mathbb{Z}) = 0$. We can then write a general homomorphism $\varphi : \mathrm{b}\mathbb{Z} \to \mathrm{b}\mathbb{Z}$ in the form

$$\varphi = \varphi_{00} + \sum_{1 \leq \beta < \mathfrak{c}} \varphi_{0\beta} + \sum_{1 \leq \alpha, \beta < \mathfrak{c}} \varphi_{\alpha\beta}\delta_{\alpha\beta}$$

where φ_{00} is a homomorphism from $\mathbb{Q}/\mathbb{Z}$ to itself and zero on $\mathbb{Q}^{\mathfrak{c}}$, $\varphi_{0\beta}$ is a homomorphism from $\mathbb{Q}b_\beta$ to $\mathbb{Q}/\mathbb{Z}$ and is zero on the rest of $\mathbb{R}/\mathbb{Z}$, and for $\alpha, \beta \geq 1$, $\varphi_{\alpha\beta}$ are rational numbers with $\varphi_{\alpha\beta} \neq 0$ for only finitely many α for any given β. If ψ is a second such homomorphism we can write the product $\varphi * \psi$ as

$$\varphi * \psi = \varphi_{00} * \psi_{00} + \sum_{\beta} \varphi_{00} * \psi_{0\beta} + \sum_{\beta} \sum_{\gamma} \varphi_{0\gamma} * \psi_{\gamma\beta}\delta_{\gamma\beta} + \sum_{\alpha,\beta} \sum_{\gamma} \varphi_{\alpha\gamma}\psi_{\gamma\beta}\delta_{\alpha\beta}.$$

It is now easy to determine the topological centre of b$\mathbb{Z}$.

3.2 Theorem. *The topological and algebraic centres of* $(\mathrm{b}\mathbb{Z}, *)$ *are both* $\mathbb{Z}$.

Proof. From Theorem 2.7 the topological centre contains $\mathbb{Z}$, which is dense. Since $\mathbb{Z}$ is commutative, from Lemma 2.8, the two centres are the same. We shall give two different proofs our theorem; the first shows that the topological centre is a subset of $\mathbb{Z}$, and the other (using the algebraic structure described above) shows that the algebraic centre is a subset of $\mathbb{Z}$.

Here is the topological proof. Consider $(\mathrm{b}\mathbb{Z}, +)$ as $\mathrm{End}(\mathbb{R}/\mathbb{Z}, +)$ and take $p \in \Lambda(\mathrm{b}\mathbb{Z}, +)$. We shall show the endomorphism p is continuous on $\mathbb{R}/\mathbb{Z}$ with its usual topology; this gives the result since the continuous characters of $\mathbb{R}/\mathbb{Z}$ are in $\mathbb{Z}$.

Fix an irrational $u \in \mathbb{R}/\mathbb{Z}$. The map $\pi : \mathrm{b}\mathbb{Z} \to \mathbb{R}/\mathbb{Z}$, $q \mapsto q(u)$ is continuous and contains $\mathbb{Z}(u)$, so is surjective. The relationship $(pq)(u) = p(q(u))$ shows that left multiplication by p in $\mathrm{b}\mathbb{Z}$ composed with π is the same as π composed with the action of p on $\mathbb{R}/\mathbb{Z}$. Thus the conditions of Lemma 2.9 are satisfied when $p \in \Lambda(\mathbb{R}/\mathbb{Z}, *)$, whence p is continuous on $\mathbb{R}/\mathbb{Z}$.

Now we give the algebraic proof. Take $\varphi \in Z(\mathrm{b}\mathbb{Z})$. For all λ, μ with $1 \leq \lambda, \mu < \mathfrak{c}$ we have $\varphi * \delta_{\lambda\mu} = \delta_{\lambda\mu} * \varphi$, that is

$$\varphi_{0\mu} + \sum_{1 \leq \alpha < \mathfrak{c}} \varphi_{\alpha\lambda}\delta_{\alpha\mu} = \sum_{1 \leq \beta < \mathfrak{c}} \varphi_{\mu\beta}\delta_{\lambda\beta}.$$

Immediately we see that $\varphi_{0\mu} = 0$ for all μ. Evaluating both sides of this equation at b_μ gives us that $\varphi_{\alpha\lambda} = 0$ if $\alpha \neq \lambda$, and $\varphi_{\lambda\lambda} = \varphi_{\mu\mu}$ (or in other words, $H = 0$ and L is a multiple of the identity matrix). Now for $\mu \geq 1$ and $q \in \mathbb{Q}$ put $\delta_{0\mu}(qb_\gamma) = q (\mathrm{mod}\ \mathbb{Z}) \in \mathbb{Q}/\mathbb{Z}$ if $\mu = \gamma$ and $= 0$ if $\mu \neq \gamma$. Then

$$\varphi * \delta_{0\mu}(qb_\mu) = \varphi_{00}(q)(\mathrm{mod}\ \mathbb{Z}), \qquad \delta_{0\mu} * \varphi(qb_\mu) = (\varphi_{\mu\mu}q)(\mathrm{mod}\ \mathbb{Z}).$$

These two must be equal, and taking $q = 1$ shows that $\varphi_{\mu\mu}$ is an integer, and then we see that φ_{00} is just multiplication by the integer $\varphi_{\mu\mu}$. Thus φ is just multiplication by an element of $\mathbb{Z}$. □

The formula for the product shows immediately

3.3 Theorem.

(i) *If* $A, B \subseteq [1, \mathfrak{c})$ *and* $A \cap B = \emptyset$ *then* $\left(\sum_{\alpha \in A,\, \beta \in B} \varphi_{\alpha\beta}\delta_{\alpha\beta}\right)^2 = 0$.

(ii) *If* $A, B \subseteq [1, \mathfrak{c})$ *and* $A \cap B = \emptyset$ *then* $\sum_{\alpha \in A} \delta_{\alpha\alpha} + \sum_{\alpha \in A,\, \beta \in B} \varphi_{\alpha\beta}\delta_{\alpha\beta}$ *is idempotent.*

□

By fixing A and allowing B to vary in $[1, \mathfrak{c})$ we see from this theorem that the $\mathbb{Q}$-vector space $\widehat{\mathbb{Q}}^{\mathfrak{c}}$ contains subspaces of dimension $2^{\mathfrak{c}}$ consisting entirely of idempotents or of elements of square zero. The idempotents in $(\beta\mathbb{N}, +)$, and those in $(\beta N, \cdot)$, are key elements in applications to number theory and they can be pulled back from $\mathrm{b}\mathbb{Z}$ using the continuous homomorphism $\pi_{\beta,\mathrm{b}}$.

Since any finite matrix can be embedded in a matrix L, we see immediately that

3.4 Theorem. $(\mathrm{b}\mathbb{Z}, *)$ *contains* $n \times n$ *matrix groups over* $\mathbb{Q}$ *for all* n*, and indeed matrix groups of size* $\mathfrak{c} \times \mathfrak{c}$. □

The topology of $\mathrm{b}\mathbb{Z}$ is determined by the requirement that $\varphi_i \to \varphi$ if and only if $\varphi_i(x) \to \varphi(x)$ for each $x \in \mathbb{R}/\mathbb{Z}$. This is the same as saying that $\varphi_i(q) \to \varphi(q)$ for each $q \in \mathbb{Q}/\mathbb{Z}$ and $\varphi_i(b_\gamma) \to \varphi(b_\gamma)$ for each $\gamma \geq 1$, since elements of $\mathrm{b}\mathbb{Z}$ are $\mathbb{Q}$-linear.

In particular then, $\{\varphi : \varphi(b_\gamma) = 0 \text{ for all } \gamma \geq 1\}$ is closed. This set is just $\widehat{\mathbb{Q}/\mathbb{Z}}$ (which we have already observed is compact) or equivalently the set of all matrices of the form

$\begin{pmatrix} J & 0 \\ 0 & 0 \end{pmatrix}$. The matrix viewpoint shows that this is obviously a left ideal, but not a right ideal.

The set $\{\varphi : \varphi(q) = 0 \text{ for all } q \in \mathbb{Q}/\mathbb{Z}\}$ is also closed. It is the set $\widehat{\mathbb{Q}}^{\mathfrak{c}}$ (which as we observed early in this section is isomorphic with $\mathrm{b}\mathbb{R}$), or the set of matrices of the form $\begin{pmatrix} 0 & H \\ 0 & L \end{pmatrix}$. This is a two-sided ideal (thus the group $\mathrm{b}\mathbb{R}$ also has a ring structure), and the quotient of $\mathrm{b}\mathbb{Z}$ by this ideal is $\widehat{\mathbb{Q}/\mathbb{Z}}$.

We have already remarked that $\widehat{\mathbb{Q}}^{\mathfrak{c}}$ is connected and that $\widehat{\mathbb{Q}/\mathbb{Z}}$ is totally disconnected. Therefore $\widehat{\mathbb{Q}}^{\mathfrak{c}}$ is the connected component containing 0 in the compact group $(\mathrm{b}\mathbb{Z}, +)$.

3.5 Theorem. (i) *The elements of* $\widehat{\mathbb{Q}}^{\mathfrak{c}}$ *with* $*$*-square* 0 *are dense in* $\widehat{\mathbb{Q}}^{\mathfrak{c}}$.
(ii) *The* $*$*-idempotents in* $\widehat{\mathbb{Q}}^{\mathfrak{c}}$ *are dense in* $\widehat{\mathbb{Q}}^{\mathfrak{c}}$.

Proof. (i) Elements of $\widehat{\mathbb{Q}}^{\mathfrak{c}}$ are completely determined by their values on the elements b_γ with $\gamma \geq 1$. Take any elements $a_\gamma \in \mathbb{R}/\mathbb{Z}$. For any finite set $F \subset [1, \mathfrak{c})$ and any $\varepsilon > 0$ we shall find $\varphi_{F,\varepsilon} \in \widehat{\mathbb{Q}}^{\mathfrak{c}}$ such that $\varphi^2_{F,\varepsilon} = 0$ and $|\varphi_{F,\varepsilon}(b_\gamma) - a_\gamma| < \varepsilon$. The net $(\varphi_{F,\varepsilon})$ then converges to the (arbitrary) endomorphism φ with $\varphi(b_\gamma) = a_\gamma$ for all $\gamma \geq 1$.

So let F, ε be given. Take β with $\beta \geq 1$ and $\beta \notin F$. Define $\varphi_{F,\varepsilon}$ for $\gamma \in F$ by $\varphi_{F,\varepsilon} = \sum_{\gamma \in F} q_\gamma \delta_{\beta\gamma}$ where q_γ is chosen so that $|q_\gamma b_\beta - a_\gamma| < \varepsilon$. Thus $\varphi_{F,\varepsilon}(b_\gamma) = q_\gamma b_\beta$. Then $\varphi^2_{F,\varepsilon} = 0$ by Theorem 3.3 and $\varphi_{F,\varepsilon}$ satisfies our other conditions.

(ii) is proved in a similar way. □

We can determine all closed right ideals in $(\mathrm{b}\mathbb{Z}, *)$.

3.6 Theorem. *Every closed, non-trivial right* $*$*-ideal in* $\mathrm{b}\mathbb{Z}$ *is a two-sided ring ideal which contains* $\widehat{\mathbb{Q}}^{\mathfrak{c}}$. *If* $\pi : \mathrm{b}\mathbb{Z} \to \widehat{\mathbb{Q}/\mathbb{Z}}$ *denotes the natural quotient map, each such ideal is of the form* $\pi^{-1}(I)$ *where* I *is a ring ideal in* $\widehat{\mathbb{Q}/\mathbb{Z}}$.

Proof. Let R be a closed right $*$-ideal. Take $\varphi \in R$. Then $\varphi * \mathrm{b}\mathbb{Z} \subseteq R$. Now $\varphi * \mathrm{b}\mathbb{Z}$ is a right ideal which is also an additive subgroup. Its closure is firstly a right $*$-ideal, and secondly an additive subgroup and therefore, from Corollary 2.2, also a left $*$-ideal. Thus $\overline{\varphi * \mathrm{b}\mathbb{Z}}$ is a ring ideal.

Now suppose the ideal $\overline{\varphi * \mathrm{b}\mathbb{Z}}$ contains a non-zero element

$$\psi = \psi_{00} + \sum_{1 \leq \beta < \mathfrak{c}} \psi_{0\beta} + \sum_{1 \leq \alpha, \beta < \mathfrak{c}} \psi_{\alpha\beta}\delta_{\alpha\beta}.$$

If not all scalars $\psi_{\alpha\beta}$ are zero, say $\psi_{\gamma\xi} \neq 0$, then $\overline{\varphi * \mathrm{b}\mathbb{Z}}$ also contains $\delta_{\alpha\gamma} * \psi * \delta_{\xi\beta}$ and so all $\delta_{\alpha\delta}$ with $\alpha, \beta \geq 1$. Since it is closed it contains the whole of $\widehat{\mathbb{Q}}^{\mathfrak{c}}$.

If all these $\psi_{\alpha\beta}$ are zero, but $\psi_{0\beta} \neq 0$ for some $\beta \geq 1$, then for each $\gamma \geq 1$ the homomorphism $\psi'_{0\gamma} = \psi * \delta_{\beta\gamma}$ is non-zero. Since $\psi'_{0\gamma} \neq 0$, the set

$$\{\psi'_{0\gamma}(qb_\gamma) : q \in \mathbb{Q}\}$$

is dense in $\mathbb{R}/\mathbb{Z}$. A proof on the lines of Theorem 3.5 (i) shows that $\overline{\varphi * \mathrm{b}\mathbb{Z}}$ contains $\widehat{\mathbb{Q}}^{\mathfrak{c}}$.

The final possibility is that ψ is of the form ψ_{00} with $\psi_{00} \neq 0$. In that case, for each $\gamma \geq 1$, $\psi'_{0\gamma} = \psi_{00} * \delta_{0\gamma}$ is non-zero, and as in the last pragraph we see that $\overline{\varphi * \mathrm{b}\mathbb{Z}}$ contains $\widehat{\mathbb{Q}}^{\mathfrak{c}}$. Our first assertion is proved.

Take $\varphi \in R$. Then we know $\varphi \in \varphi * \mathrm{b}\mathbb{Z}$ and also that $\widehat{\mathbb{Q}}^{\mathfrak{c}} \subseteq \overline{\varphi * \mathrm{b}\mathbb{Z}}$. Since $\overline{\varphi * \mathrm{b}\mathbb{Z}}$ is an additive subgroup, $\varphi + \widehat{\mathbb{Q}}^{\mathfrak{c}} \subseteq \overline{\varphi * \mathrm{b}\mathbb{Z}} \subseteq R$. Therefore $R = \pi^{-1}(\pi(R))$, where π is the quotient map. Since $\pi(R)$ is a multiplicative right ideal in the commutative ring $\widehat{\mathbb{Q}/\mathbb{Z}}$, R is in fact a two-sided ideal in $(\mathrm{b}\mathbb{Z}, *)$.

It remains to show that R is an additive subgroup of $\mathrm{b}\mathbb{Z}$, or equivalently that any $*$-ideal in $\widehat{\mathbb{Q}/\mathbb{Z}}$ is an additive subgroup. We use the fact that $\widehat{\mathbb{Q}/\mathbb{Z}} = \prod_{p \text{ prime}} A_p$, where A_p denotes the ring of p-adic integers. Each element $x \in A_p$ can be expressed in the form $x = x_0 + x_1 p + x_2 p^2 + \cdots$, where each $x_i \in \{0, 1, 2, \cdots, p-1\}$. The only proper non-zero multiplicative ideals in A_p are the ideals I_n defined by the condition $x_0 = x_1 = x_2 = \cdots = x_n = 0$, where $n \in \omega$. (This follows easily from the fact that x is invertible in A_p unless $x_0 = 0$.) Each I_n is an additive subgroup and therefore an ideal in the ring A_p.

Conversely, each ring ideal I in $\widehat{\mathbb{Q}/\mathbb{Z}}$ is closed, so that $\pi^{-1}(I)$ is a closed right ideal in $(\mathrm{b}\mathbb{Z}, +, *)$. $\square$.

Remark. It follows from Theorem 3.6 that $(\mathrm{b}\mathbb{Z}, *)$ has exactly $\mathfrak{c}$ closed right ideals. On the other hand, it is easy to see that there are closed left ideals of $(\mathrm{b}\mathbb{Z}, *)$ which are not right ideals. In fact, $(\mathrm{b}\mathbb{Z}, *)$ has at least $2^{\mathfrak{c}}$ closed left ideals. To see this, let $(b_\alpha)_{\alpha<\mathfrak{c}}$ denote the Hamel basis described in the discussion following Theorem 3.1. For each set X of of ordinals in $[1, \mathfrak{c})$, $L_X = \{\varphi \in \mathrm{b}\mathbb{Z} : \varphi(b_\alpha) = 0 \text{ for } \alpha \in X\}$ is a closed left ideal, and different sets X determine different ideals.

Other algebraic questions can be decided quite easily. For example, we can determine when an element of $(\mathrm{b}\mathbb{Z}, *)$ is left invertible. This question is significant because an element of $\mathrm{b}\mathbb{Z}$ is left invertible in $(\mathrm{b}\mathbb{Z}, *)$ if and only if it is a topological generator of the compact group $(\mathrm{b}\mathbb{Z}, +)$ (notice that $x \in \mathrm{b}\mathbb{Z}$ is a generator if and only if $\{n * x : n \in \mathbb{N}\}$ is dense). Represent the left invertible element φ as the matrix $\varphi = \begin{pmatrix} J & H \\ 0 & L \end{pmatrix}$ and its left inverse as $\begin{pmatrix} J' & H' \\ 0 & L' \end{pmatrix}$. The image $\pi(\varphi)$ must be invertible in the commutative semigroup $\mathrm{b}\mathbb{Z}/\widehat{\mathbb{Q}}^{\mathfrak{c}}$, and this means J is invertible with $J' = J^{-1}$. Also, the $\mathbb{Q}$-linear L has the left inverse L', and this is equivalent to the requirement that L should be injective. Finally we need $J'H + H'L = 0$ Thus $H' = -J^{-1}HL'$ on the $\mathbb{Q}$-subspace $L(\widehat{\mathbb{Q}}^{\mathfrak{c}})$; we can take H' to be any group homomorphism which extends this map to the whole of $\mathbb{Q}^{(\mathfrak{c})}$ (see [7] Theorem A7 or [9] Proposition A1.35; the image group is commutative and divisible). Thus φ is left invertible if and only if J is invertible and L is injective.

A slight extension of the argument shows that φ is invertible if and only if J and L are invertible.

We can also see that the set of left invertible elements is small in two senses: it is not dense in $\mathrm{b}\mathbb{Z}$ nor does it have positive Haar measure in the group $(\mathrm{b}\mathbb{Z}, +)$. These assertions follow because they hold in the quotient space $\widehat{\mathbb{Q}/\mathbb{Z}}$.

4. apℕ.

As is well known, apℕ can be written as the disjoint union of ℕ and sapℕ = bℤ (see for example [6]). To be more precise, there is a continuous injective homomorphism $\varphi : \mathrm{b}\mathbb{Z} \to \mathrm{ap}\mathbb{N}$ such that $\mathrm{ap}\mathbb{N} = \mathbb{N} \cup \varphi(\mathrm{b}\mathbb{Z})$. The group $(\varphi(\mathrm{b}\mathbb{Z}), +)$ is the smallest ideal of $(\mathrm{ap}\mathbb{N}, +)$ and for $n \in \mathbb{N}$, $x \in \mathrm{b}\mathbb{Z}$ we have $n + \varphi(x) = \varphi(n + x)$. The topology of apℕ is determined by the properties that ℕ is a discrete subspace and a base of neighbourhoods of $\varphi(x) \in \varphi(\mathrm{ap}\mathbb{N})$ is formed by the sets $\{n \in \mathbb{N} : \varphi(n) \in \varphi(V)\} \cup \varphi(V)$ when V runs through a neighbourhood base of x in bℤ.

The operation $*$ on apℕ is easily described. Both $(\mathbb{N}, *)$ and $(\mathrm{b}\mathbb{Z}, *)$ are substructures of $(\mathrm{ap}\mathbb{N}, *)$, and for $n \in \mathbb{N}$, $\varphi(x) \in \mathrm{b}\mathbb{Z}$ we have $n * \varphi(x) = \varphi(x) * n = \varphi(n * x)$.

We can now read the properties of apℕ from those of bℤ. For example, from Theorem 3.2 we find easily

4.1 Theorem. *The topological and algebraic centres of* $(\mathrm{ap}\mathbb{N}, *)$ *are both* $\mathbb{N} \cup \varphi(\mathbb{Z})$. □

5. wapℕ.

The first point to make about wapℕ is that the multiplication · does *not* extend to it. We prove this in Theorem 5.4. We begin by showing that the topological centre of $(\mathrm{wap}\mathbb{N}, *)$ is surprisingly small.

5.1 Theorem. $\Lambda(\mathrm{wap}\mathbb{N}, *) = Z(\mathrm{wap}\mathbb{N}, *) = \{1\}$.

Proof. Of course, the identity 1 is always in the algebraic centre, and the algebraic centre is a subset of the topological centre.

To prove that no elements other than 1 are in $\Lambda(\mathrm{wap}\mathbb{N}, *)$, we need a result slightly stronger than the assertion that the set of idempotents in $(\mathrm{wap}\mathbb{N}, +)$ is not closed. There are two ways of obtaining what we need from the literature. First we consider the approach of Bouziad, Lemańczyk and Mentzen [3]. They show that the unit ball B_1 of $L^\infty[0,1]$, which is a compact separately continuous semigroup in its weak* topology when given the pointwise multiplication of functions (in fact they use $L^2[0,1]$ but that makes no difference here), actually contains a dense homomorphic image of $(\mathbb{N}, +)$. We let $g : \mathbb{N} \to B_1$ be that homomorphism and note that it extends to a continuous homomorphism $g : \mathrm{wap}\mathbb{N} \to B_1$. Since the image is compact, $g(\mathrm{wap}\mathbb{N}) = B_1$. In [3] it is also shown that the closure of the set of multiplicative idempotents in $L^\infty[0,1]$ – these are just the characteristic functions of measurable sets – contains the constant function $\frac{1}{2}$.

We now take a family (e_i) of additive idempotents in wapℕ such that $g(e_i) \to \frac{1}{2}$. Let x be a cluster point in wapℕ of the net (e_i), so that $g(x) = \frac{1}{2}$. By replacing (e_i) by a subnet we may assume $e_i \to x$. We show first that if $m \in \mathbb{N}$ and $m > 1$ then $m \notin \Lambda(\mathrm{wap}\mathbb{N}, *)$ by proving that $m * e_i \not\to m * x$. Indeed, $g(m * e_i) = g(e_i + \ldots + e_i) = g(e_i) \to \frac{1}{2}$, but $g(m * x) = g(x + \ldots + x) = g(x)^m = (\frac{1}{2})^m$. The argument that $q \in \mathrm{wap}\mathbb{N} \setminus \mathbb{N}$ does not belong to $\Lambda(\mathrm{wap}\mathbb{N}, *)$ is now easy. $g(q * e_i) = \lim_{m \to q} g(m * e_i) = g(e_i)$ for every i, and $g(e_i) \to \frac{1}{2}$, but $g(q * x) = \lim_{m \to q} g(m * x) = \lim_{m \to q} (\frac{1}{2})^m = 0$.

The alternative is to use the more elementary – but harder – approach to idempotents in wapℕ in [2]. There a continuous function $g : \mathrm{wap}\mathbb{N} \to [0, \infty]$ is produced together with a sequence (e_i) of additive idempotents for which $g(e_{i_1} + \ldots + e_{i_m}) = m$ for any distinct suffices $i_1, \ldots, i_m$. Then if x is any cluster point of (e_i) we have $g(m * x) = m$

for each integer m, and so for $q \in \mathrm{wap}\mathbb{N} \setminus \mathbb{N}$ we have $g(q * x) = \infty$. But of course $g(m * e_i) = g(e_i) = 1$ for each i. Thus $m \notin \Lambda(\mathrm{wap}\mathbb{N}, *)$ when $m > 1$ and $q \notin \Lambda(\mathrm{wap}\mathbb{N}, *)$. □

5.2 Corollary. *In* $(\mathrm{wap}\mathbb{N}, +, *)$, $*$ *does not distribute over* $+$ *from the left.*

Proof. Since $2 \notin Z(\mathrm{wap}\mathbb{N}, *)$, there is $x \in \mathrm{wap}\mathbb{N}$ such that $x + x = 2 * x \neq x * 2 = x * (1 + 1)$. □

In Definition 2.10 we said that $\cdot$ is defined on $\kappa\mathbb{N}$ if $p \cdot q = \lim_{m \to p} \lim_{n \to q} m \cdot n$ is well-defined. We next show that this is not true of $\mathrm{wap}\mathbb{N}$. Notice that for any $m \in \mathbb{N}$, $m \cdot q = \lim_{n \to q} m \cdot n$ exists. To see this observe that the function $n \mapsto m \cdot n$ is a homomorphism hence has a continuous extension to $\mathrm{wap}\mathbb{N}$.

5.3 Lemma. *Write* $A = \{2^{m+r} + 2^{n+r} : m, n, r \in \mathbb{N}, m < n < r\}$. *Let* $g : \mathbb{N} \to \mathbb{R}$ *be any function which is bounded on* A *and is* 0 *off* A. *Then* g *is weakly almost periodic and thus has a unique continuous extension to* $\mathrm{wap}\mathbb{N}$.

Proof. Recall that a bounded function $g : \mathbb{N} \to \mathbb{R}$ is weakly almost periodic if it satisfies the iterated limit condition: if (x_i), (y_j) are any sequences in $\mathbb{N}$ with the property that the limits

$$\lim_i \lim_j g(x_i + y_j), \quad \lim_j \lim_i g(x_i + y_j)$$

both exist, then they are equal (see [1] or [8]). Here we may suppose that $x_i \to \infty$ and $y_j \to \infty$ (the other cases are trivial). Suppose that the left-hand limit exists and

$$\lim_i \lim_j g(x_i + y_j) \neq 0.$$

Then for large i there is J_i such that when $j > J_i$ we have $x_i + y_j \in A$. Fix such an i_1. Take $j, j' > J_{i_1}$ with $j' > j$. Then

$$\begin{aligned} x_{i_1} + y_j &= 2^{m_1 + r_1} + 2^{n_1 + r_1} \qquad (m_1 < n_1 < r_1) \\ x_{i_1} + y_{j'} &= 2^{m'_1 + r'_1} + 2^{n'_1 + r'_1} \qquad (m'_1 < n'_1 < r'_1) \end{aligned}$$

By taking j' sufficiently large we can ensure that $r'_1 > 2r_1 + 1$ so that

$$2^{m_1 + r_1} + 2^{n_1 + r_1} < 2^{r_1 + r_1} + 2^{r_1 + r_1} = 2^{2r_1 + 1} < 2^{r'_1}.$$

Now take $i_2 > i_1$. We get similar expressions involving m_2, m'_2 and so on. If we take $j > \max\{J_{i_1}, J_{i_2}\}$, then $j' > j$ and sufficiently large, and subtract the expressions obtained we find

$$\begin{aligned} y_{j'} - y_j &= 2^{m'_1 + r'_1} + 2^{n'_1 + r'_1} - 2^{m_1 + r_1} - 2^{n_1 + r_1} \\ &= 2^{m'_2 + r'_2} + 2^{n'_2 + r'_2} - 2^{m_2 + r_2} - 2^{n_2 + r_2}. \end{aligned}$$

In each of these two lines, no two of the exponents are equal. The uniqueness of binary expansions of integers shows that

$$m'_1 + r'_1 = m'_2 + r'_2, \quad n'_1 + r'_1 = n'_2 + r'_2, \quad m_1 + r_1 = m_2 + r_2, \quad n_1 + r_1 = n_2 + r_2$$

Therefore $x_{i_1} + y_j = x_{i_2} + y_j$, and so $x_{i_1} = x_{i_2}$. This means that for $i \geq i_1$, the sequence (x_i) is constant, contradicting $x_i \to \infty$. Thus the iterated limit we began with cannot be non-zero. We conclude that if the two iterated limits exist they must both be zero, and thus equal. □

Notice that as a consequence of Lemma 5.3, we have that the restriction of $\pi_{\beta,\mathrm{wap}}$ to $\mathrm{cls}_{\beta\mathbb{N}}(A)$ is a bijection onto $\mathrm{cls}_{\mathrm{wap}\mathbb{N}}(A)$. (It is trivially surjective. Given $p \neq q \in \mathrm{cls}_{\beta\mathbb{N}}(A)$, pick $B \in p \backslash q$ and let $g = \chi_{A\cap B}$, the characteristic function of $A\cap B$. Let $\widetilde{g} : \mathrm{wap}\mathbb{N} \to \{0,1\}$ be the continuous extension of g. Then $\widetilde{g} \circ \pi_{\beta,\mathrm{wap}}(p) = 1$ and $\widetilde{g} \circ \pi_{\beta,\mathrm{wap}}(q) = 0$.)

5.4 Theorem. *The multiplication $\cdot$ is not defined on* wap$\mathbb{N}$.

Proof. Pick $q \in \mathrm{cls}_{\mathrm{wap}\mathbb{N}}(A) \setminus A$. Now observe that

$$\mathrm{cls}_{\mathrm{wap}\mathbb{N}}\{2^{2n} + 2^{2m+1} : n, m \in \mathbb{N}, n < m\} \cap \mathrm{cls}_{\mathrm{wap}\mathbb{N}}\{2^{2n} + 2^{2m+1} : n, m \in \mathbb{N}, n > m\} \neq \emptyset\,.$$

(If the intersection were empty, there would be, by Urysohn's Lemma, a function $h : \mathrm{wap}\mathbb{N} \to [0,1]$ such that $h(\mathrm{cls}_{\mathrm{wap}\mathbb{N}}\{2^{2n} + 2^{2m+1} : n, m \in \mathbb{N}, n < m\}) = \{0\}$ and $h(\mathrm{cls}_{\mathrm{wap}\mathbb{N}}\{2^{2n}+2^{2m+1} : n, m \in \mathbb{N}, n > m\}) = \{1\}$. But then $\lim\limits_m \lim\limits_n h(2^{2n}+2^{2m+1}) = 1$ and $\lim\limits_n \lim\limits_m h(2^{2n}+2^{2m+1}) = 0$ so the restriction of h to $\mathbb{N}$ would not be weakly almost periodic.) Pick $p \in \mathrm{cls}_{\mathrm{wap}\mathbb{N}}\{2^{2n}+2^{2m+1} : n, m \in \mathbb{N}, n < m\} \cap \mathrm{cls}_{\mathrm{wap}\mathbb{N}}\{2^{2n}+2^{2m+1} : n, m \in \mathbb{N}, n > m\}$.

Suppose that $p \cdot q$ is defined. Then

$$\begin{aligned} p \cdot q \in\ & \mathrm{cls}_{\mathrm{wap}\mathbb{N}}\{(2^{2n} + 2^{2m+1})2^{2r} : n, m, r \in \mathbb{N}, n < m < r\} \cap \\ & \mathrm{cls}_{\mathrm{wap}\mathbb{N}}\{(2^{2n} + 2^{2m+1})2^{2r} : n, m, r \in \mathbb{N}, m < n < r\}\,. \end{aligned}$$

But this is a contradiction because, if $B = \{(2^{2n} + 2^{2m+1})2^{2r} : n, m, r \in \mathbb{N}, n < m < r\}$, we have by Lemma 5.3 that χ_B is weakly almost periodic. □

6. $\beta\mathbb{N}$.

In this section as usual we write $\mathbb{N}^* = \beta\mathbb{N} \setminus \mathbb{N}$. We begin by looking at the topological centre of $\beta\mathbb{N}$ with the operation $*$.

6.1 Theorem. $\Lambda(\beta\mathbb{N}, *) = Z(\beta\mathbb{N}, *) = \{1\}$.

Proof. If $q \in \beta\mathbb{N}$ is in the topological centre then $\pi_{\beta,\mathrm{wap}}(q)$ is in the topological centre of wap$\mathbb{N}$ by Lemma 2.9. If $q \in \mathbb{N}^* = \beta\mathbb{N} \setminus \mathbb{N}$ then $\pi_{\beta,\mathrm{wap}}(q) \in \mathrm{wap}\mathbb{N} \setminus \mathbb{N}$, so in this case $q \notin \Lambda(\beta\mathbb{N}, *)$ from Theorem 5.1. If $m \in \mathbb{N}$ and $m \neq 1$ then $\pi_{\beta,\mathrm{wap}}(m) = m \notin \Lambda(\mathrm{wap}\mathbb{N}, *)$ so $m \notin \Lambda(\beta\mathbb{N}, *)$. □

In just the same way as Corollary 5.2 followed from Theorem 5.1 we can obtain from Theorem 6.1

6.2 Corollary. *In $\beta\mathbb{N}$, $*$ does not distribute over $+$ from the left.* □

However this conclusion is also immediate from Corollary 5.2 and the fact that $\pi_{\beta,\mathrm{wap}}$ is a surjective 'homomorphism' for both $*$ and $+$. More important is the failure of the other distributive law. We could simply quote [8] which contains much stronger results than this, but we shall give a proof which allows us to show at the same time that $*$ is not associative on $\beta\mathbb{N}$.

Any $m \in \mathbb{N}$ has a unique expression in the form $m = \sum_{i=0}^{\infty} a_i 2^i$ with each a_i either 0 or 1. We write $\text{supp}(m) = \{i : a_i \neq 0\}$, a finite set, and $\gamma(m) = |\text{supp}(m)|$. Let $\overline{\gamma} : \beta\mathbb{N} \to \beta\mathbb{N}$ denote the continuous extension of γ.

Let $\mathbb{H} = \bigcap_{n\in\mathbb{N}} \text{cl}_{\beta\mathbb{N}}(2^n\mathbb{N})$. We observe that $\mathbb{H}$ is a closed subsemigroup of $\beta\mathbb{N}$ (see Lemma 6.8 in [8]). For $m, n \in \mathbb{N}$ we have the simple result that, if $\max\{\text{supp}(m)\} < \min\{\text{supp}(n)\}$, then $\gamma(m + n) = \gamma(m) + \gamma(n)$. It is easy to deduce that $\overline{\gamma}(x + y) = \overline{\gamma}(x) + \overline{\gamma}(y)$ for every $x \in \beta\mathbb{N}$ and every $y \in \mathbb{H}$, by first letting n tend to y and then letting m tend to x in this equation.

Now take $p \in \overline{\{2^k : k \in \mathbb{N}\}} \cap \mathbb{N}^*$. Then $\overline{\gamma}(p) = 1$. Moreover if $r \in \mathbb{N}$ then for any integer M, $r * p = p + p + \ldots + p$ is in the closure of

$$\{2^{k_1} + 2^{k_2} + \ldots + 2^{k_r} : M \leq k_1 < k_2 \ldots < k_r\},$$

showing that $\overline{\gamma}(r * p) = r$. It follows by continuity that $\overline{\gamma}(x * p) = x$ for every $x \in \beta\mathbb{N}$.

We note that $p \in \mathbb{H}$ and hence that $\beta\mathbb{N} * p \subseteq \mathbb{H}$, because $\beta\mathbb{N} * p$ is the closed subsemigroup of $(\beta\mathbb{N}, +)$ generated by p.

We use these observations in our next proof.

6.3 Proposition. *Let $p \in \overline{\{2^k : k \in \mathbb{N}\}} \cap \mathbb{N}^*$. Then*

$$(\beta\mathbb{N} * p) \cap (\beta\mathbb{N} + \mathbb{N}^* * p) = \emptyset.$$

Proof. Suppose there is $t \in \mathbb{N}^*$ with $(\beta\mathbb{N} * p) \cap (\beta\mathbb{N} + t * p) \neq \emptyset$. We note that $\beta\mathbb{N} * p = \text{cl}_{\beta\mathbb{N}}(\mathbb{N} * p)$ and $\beta\mathbb{N} + t * p = \text{cl}_{\beta\mathbb{N}}(\mathbb{N} + t * p)$. It follows from Theorem 3.40 in [8] that either

(a) there are $n \in \mathbb{N}$, $q \in \beta\mathbb{N}$ with $n * p = q + t * p$, or

(b) there are $n \in \mathbb{N}$, $q \in \beta\mathbb{N}$ with $q * p = n + t * p$.

From the properties of $\overline{\gamma}$ above we find that if (a) holds then

$$n = \overline{\gamma}(n * p) = \overline{\gamma}(q + t * p) = \overline{\gamma}(q) + \overline{\gamma}(t * p) = \overline{\gamma}(q) + t \in \mathbb{N}^*,$$

which is impossible. However, (b) cannot hold because $q * p \in \mathbb{H}$ and $n + t * p \notin \mathbb{H}$. $\square$

6.4 Theorem. *In $\beta\mathbb{N}$, $*$ is not associative, nor is it distributive over addition from the right.*

Proof. For $q, p \in \beta\mathbb{N}$ we have $(2 * q) * p = (q + q) * p$ and $2 * (q * p) = q * p + q * p$; we can therefore establish both parts of our assertion by showing that these two elements are sometimes different. If we take $q \in \mathbb{N}^*$ and p as in Proposition 6.3, we see that $(2 * q) * p \in \beta\mathbb{N} * p$ and $q * p + q * p \in \beta\mathbb{N} + \mathbb{N}^* * p$ must be distinct. $\square$

There is yet another proof of the failure of distributivity which provides more information. If $q \in \mathbb{N}^*$ and if $(x + y) * q = x * q + y * q$ for every $x, y \in \beta\mathbb{N}$, then the continuous map $p \mapsto p * q$ from $(\beta\mathbb{N}, +)$ to itself is a semigroup homomorphism. So the image of $\beta\mathbb{N}$ is finite and the image of $\mathbb{N}^*$ under this map is a singleton $\{e\}$ for some idempotent e in $(\beta\mathbb{N}, +)$ (see Theorem 10.18 in [8]). So q must generate a finite subsemigroup of $(\beta\mathbb{N}, +)$.

It is easy to give one example of an element q which generates an infinite semigroup, since $\pi_{\beta,\mathrm{b}}(\mathbb{N}^*) = \mathrm{b}\mathbb{Z}$ contains elements of infinite (additive) order (see §3) (and it is conjectured that the only case in which the semigroup is finite is when q is an idempotent for $+$).

Our next result provides yet another confirmation that $*$ is neither associative nor right distributive over addition (it has the consequence that $2 * (x * p) = x * p + x * p$ differs from $(2 * x) * p$).

6.5 Theorem. *If $p \in \mathbb{N}^* = \beta\mathbb{N} \setminus \mathbb{N}$ is right cancellable in $(\mathbb{N}^*, +)$ then $\{x * p : x \in \mathbb{N}^*\}$ generates algebraically a free subsemigroup in $(\beta\mathbb{N}, +)$.*

Proof. This conclusion is an immediate consequence of Theorem 4.3 of [5]. □.

For any $p \in \mathbb{N}^*$ the elements $n * p$ $(n \in \mathbb{N})$ are also usually distinct.

6.6 Theorem. *If $p \in \beta\mathbb{N}$ and there are distinct positive integers m, n such that $m * p = n * p$ then there is $r \in \mathbb{N}$ such that $r * p$ is idempotent and $x * p = r * p$ when $x \in \mathbb{N}^*$ or $x \in \mathbb{N}$ and $x \geq r$.*

Proof. The hypothesis guarantees that the additive subsemigroup $\{n * p : n \in \mathbb{N}\}$ is finite. Since $(\beta\mathbb{N}, +)$ has only trivial finite subgroups (Zelenjuk's Theorem, 7.17 in [8]), there is $r \in \mathbb{N}$ with $n * p = r * p$ for all $n \geq r$. The conclusion now follows easily. □

We next look at a relationship between $\mathrm{b}\mathbb{Z}$ and $\beta\mathbb{N}$. There are large parts of these two compact spaces which are topologically the same. This fact was shown by Ruppert [10]; we shall give a proof in a slightly more general form.

6.7 Theorem. *Let $(b_n)_{n=1}^{\infty}$ be an increasing sequence in $\mathbb{N}$ with the property that b_{n+1} is a multiple of b_n for every $n \in \mathbb{N}$. Let $B = \{b_n : n \in \mathbb{N}\}$ and $B^* = \overline{B} \setminus B$, with the closure being taken in $\beta\mathbb{N}$. Then $\pi_{\beta,\mathrm{b}} : \beta\mathbb{N} \to \mathrm{b}\mathbb{Z}$ is a homeomorphism on B^*.*

Proof. Since B^* is compact all we need do is prove that $\pi_{\beta,\mathrm{b}}$ is injective on B^*. We do this by considering the $*$-actions of $\beta\mathbb{N}$ and $\mathrm{b}\mathbb{Z}$ on the group $\mathbb{R}/\mathbb{Z}$. Proposition 2.4(i) tells us that for $q \in \beta\mathbb{N}$ and $s \in \mathbb{R}/\mathbb{Z}$ we have $\pi_{\beta,\mathrm{b}}(q) * s = q * s$. In other words, the action of $\beta\mathbb{N}$ factors through the action of $\mathrm{b}\mathbb{Z}$. So to prove that $\pi_{\beta,\mathrm{b}}$ is injective on B^*, it is enough to show that if $p \neq q$ are elements of B^* then there is $s \in \mathbb{R}/\mathbb{Z}$ such that $p * s \neq q * s$.

Since $p \neq q$ we can find disjoint subsets B_p, B_q of B such that $p \in \overline{B_p}$, $q \in \overline{B_q}$. We also note that if $S_p = \{r : b_r \in B_p\}$ then $S_p \cap 3\mathbb{N}$, $S_p \cap (3\mathbb{N}+1)$ and $S_p \cap (3\mathbb{N}+2)$ produce a partition of $B_p \setminus \{1, 2\}$, so by replacing B_p by a subset if necessary we may assume that $S_p \subseteq (3\mathbb{N} + i)$ for just one i. Then S_p, $S_p + 1$ and $S_p + 2$ are disjoint sets.

We now write $a_{r+1} = b_{r+1}/b_r \in \mathbb{N}$ and

$$s_r = \frac{\lfloor a_{r+1}/2 \rfloor}{b_{r+1}} \ \text{ if } r \in S_p, \quad s_r = 0 \text{ otherwise}$$

and put

$$s = \sum_{r \in S_p} s_r.$$

The series converges in $\mathbb{R}/\mathbb{Z}$ because $s_r \le \dfrac{1}{2b_r}$ and $b_r \ge 2^{r-1}$ for each r. Notice also that

$$\frac{1}{3} \le \frac{\lfloor a_{r+1}/2 \rfloor}{a_{r+1}} = b_r s_r \le \frac{1}{2}.$$

and that

$$b_r s_{r+k} = \frac{b_r}{b_{r+k}} b_{r+k} s_{r+k} \le \frac{1}{2^{k+1}}.$$

Now take $m \in S_p$. Since $b_m s_r = 0$ in $\mathbb{R}/\mathbb{Z}$ if $m > r$, and $S_p \subseteq 3\mathbb{N} + i$, the relevant values of r in the following sums are contained in $\{m, m+3, m+6, \ldots\}$, so that

$$\frac{1}{3} \le b_m s_m \le \sum_{r \in S_p} b_m s_r = b_m * s \le \frac{1}{2} + \frac{1}{2^4} + \frac{1}{2^7} + \ldots = \frac{4}{7}.$$

Since this holds for each $m \in S_p$ we can take limits to find that $p * s \in [\frac{1}{3}, \frac{4}{7}]$. On the other hand, if we take $m \notin S_p$ then $s_m = 0$ and

$$0 \le \sum_{r \in S_p} b_m s_r \le \frac{1}{2^2} + \frac{1}{2^5} + + \frac{1}{2^8} + \ldots = \frac{2}{7}.$$

As before we see that $q * s \in [0, \frac{2}{7}]$ and since $\frac{2}{7} < \frac{1}{3}$, $p * s \ne q * s$. □

This way of looking at the problem allows us to see one of the main results of [10] from a new perspective.

6.8 Corollary. *The enveloping semigroup of the action of* $\mathbb{N}$ *on* $\mathbb{R}/\mathbb{Z}$ *given for* $n \in \mathbb{N}$ *by*

$$s \mapsto 2^n * s$$

is $(\beta\mathbb{N}, +)$*. The closure of* $\{2^n : n \in \mathbb{N}\}$ *in* $(\mathrm{b}\mathbb{Z}, *)$ *is a subsemigroup of* $(\mathrm{b}\mathbb{Z}, *)$ *isomorphic with* $(\beta\mathbb{N}, +)$*.*

Proof. The semigroup $(\mathrm{b}\mathbb{Z}, *)$ has $\mathbb{Z}$ as its topological centre (Theorem 3.2). $\mathbb{Z}$ contains the elements 2^n with $n \in \mathbb{N}$ and therefore the closure of $\{2^n : n \in \mathbb{N}\}$ in $\mathrm{b}\mathbb{Z}$ is a subsemigroup of $(\mathrm{b}\mathbb{Z}, *)$. But from our theorem, the map $n \mapsto 2^n$ extends to a continuous isomorphism from $(\beta\mathbb{N}, +)$ onto this subsemigroup of $(\mathrm{b}\mathbb{Z}, *)$. □

Remark. This innocent looking corollary might have some worthwhile consequences when combined with §3. There we saw that $(\mathrm{b}\mathbb{Z}, *)$ is representable as a semigroup of matrices, so the corollary gives us a way of looking at $(\beta\mathbb{N}, +)$ as a semigroup of matrices.

7. $\kappa\mathbb{N}$.

Now we shall consider some properties which pertain to all our compactifications. Let $(\kappa\mathbb{N}, +, *)$ denote any one of them. Except in the case $\kappa\mathbb{N} = \beta\mathbb{N}$, $(\kappa\mathbb{N}, *)$ is a compact right topological semigroup and so it has all the general structure these semigroups enjoy [1], [8]. For example, it has minimal left and right ideals, a smallest two-sided ideal and it contains idempotents. We can already say much about these. In this section we shall denote the smallest two sided ideal of the semigroup S by $\mathcal{K}(S)$.

7.1 Proposition. *Assume that $\kappa \neq \beta$.* (i) *Every closed additive subsemigroup of $\kappa\mathbb{N}$ is a $*$-left ideal. In particular the minimal $*$-left ideals are the additive idempotents of $\kappa\mathbb{N}$.*
(ii) *The set of additive idempotents is a $*$-right-zero semigroup.*
(iii) *There is a unique minimal right ideal in $(\kappa\mathbb{N}, *)$, namely the set of all additive idempotents of $\kappa\mathbb{N}$. It is also the smallest $*$-two-sided ideal.*

Proof. (i) follows from the observation that closed additive subsemigroups are $*$-invariant (Corollary 2.2) and the fact that all minimal left ideals are algebraically isomorphic.

(ii) is a consequence of (i).

(iii) The argument uses some basic structure theory for compact right topological semigroups. The union of all minimal left ideals is well known to be the smallest ideal. As this set is a right-zero semigroup it must be the only minimal right ideal. □

Every additive idempotent in $\kappa\mathbb{N}$ is also a $*$-idempotent. We shall next show that there are many $*$-idempotents which are not additive idempotents.

7.2 Theorem. *$\mathcal{K}(\kappa\mathbb{N}, +)$ contains $2^{\mathfrak{c}}$ $*$-idempotents which are not additive idempotents. $\overline{\mathcal{K}(\beta\mathbb{N}, +)}$ contains $2^{\mathfrak{c}}$ $\cdot$-idempotents which are not additive idempotents. These sets of idempotents are not closed.*

Proof. First exclude the case $\kappa = \beta$. If q denotes the minimum idempotent of $\kappa\mathbb{N}$ (there is a unique one), $\pi_{\kappa,\mathrm{b}}(\kappa\mathbb{N} + q) = \pi_{\kappa,\mathrm{b}}(\kappa\mathbb{N}) = \mathrm{b}\mathbb{Z}$. Then if $e \in \mathrm{b}\mathbb{Z}$ is a $*$-idempotent, $\pi_{\kappa,\mathrm{b}}^{-1}(\{e\}) \cap (\kappa\mathbb{N} + q)$ is a compact $*$-subsemigroup of $\kappa\mathbb{N}$ and so contains a $*$-idempotent, which is not an additive idempotent unless $e = 0$. Since $(\mathrm{b}\mathbb{Z}, *)$ has $2^{\mathfrak{c}}$ $*$-idempotents (see §3), we immediately conclude that there are $2^{\mathfrak{c}}$ $*$-idempotents in $\kappa\mathbb{N} + q = \mathcal{K}(\kappa\mathbb{N}, +)$ which are not additive idempotents.

The same argument works when $\kappa = \beta$ if we replace $*$ by $\cdot$. From Proposition 2.4(ii), $\pi_{\beta,\mathrm{b}}$ is a homomorphism from $(\beta\mathbb{N}, \cdot\ )$ to $(\mathrm{b}\mathbb{Z}, \cdot\ )$, and on $\mathrm{b}\mathbb{Z}$ the operations $*$ and $\cdot$ coincide. So we can pull back $*$-idempotents of $\mathrm{b}\mathbb{Z}$ to $\cdot$-idempotents of $\beta\mathbb{N}$. However the smallest ideal of $(\beta\mathbb{N}, +)$ is not closed, so we can only assert that these $\cdot$-idempotents lie in the closure of $\mathcal{K}(\beta\mathbb{N}, +)$. (Indeed, we can see that if $p \in \beta\mathbb{N}$ is a $\cdot$-idempotent for which $\pi_{\kappa,\mathrm{b}}(p)$ is in the component of $\mathrm{b}\mathbb{Z}$ which contains 0, then $n\mathbb{N} \in p$ for every $n \in \mathbb{N}$ and so $p \notin \mathcal{K}(\beta\mathbb{N}, +)$ (see Theorem 13.14 in [8])).

We show that $\mathcal{K}(\beta\mathbb{N}, +)$ contains $2^{\mathfrak{c}}$ $*$-idempotents by giving, for any κ, a more explicit demonstration of the existence of $*$-idempotents in $\kappa\mathbb{N}$ which are not additive idempotents (though this method only produces one idempotent in $\mathrm{b}\mathbb{Z}$, namely the integer 1). For any additive idempotent $p \in \kappa\mathbb{N}$, for any $x \in \kappa\mathbb{N}$, we have

$$x * (1 + p) = \lim_{n \to x} n * (1 + p) = \lim_{n \to x} (n + p) = x + p.$$

Taking $x \in \kappa\mathbb{N} + p$ shows that $1 + p$ is a right identity in $(\kappa\mathbb{N} + p, *)$ so that $1 + p$ is a $*$-idempotent. It is obviously not an additive idempotent. This argument works even for $\beta\mathbb{N}$, in which the distributive laws do not hold.

The only point remaining is to show that the these sets of idempotents are not closed. If they were, then their continuous image in $\mathrm{b}\mathbb{Z}$ under the map $\pi_{\kappa,\mathrm{b}}$ would be closed, that is, the set of $*$-idempotents in $b\mathbb{Z}$ would be closed. But this is not the case since $(b\mathbb{Z}, *)$ contains a copy of $(\beta\mathbb{N}, +)$ (see Corollary 6.8). $\square$

Can we pull back $*$-group structures from $b\mathbb{Z}$ in the same way? The answer is given in the following lemma.

7.3 Lemma. *Let $\pi : S \to T$ be a continuous surjective homomorphism between compact right topological semigroups. Let G be a subgroup of T. Then $G = \pi(H)$ for some subgroup H of S.*

Proof. Let e denote the identity of G and let G_e be the maximal group in T with identity e. Then $\pi^{-1}(\{e\})$ is a compact subsemigroup of S; we take f to be an idempotent in the smallest ideal of $\pi^{-1}(\{e\})$. Then $f \cdot \pi^{-1}(\{e\}) \cdot f = \pi^{-1}(\{e\}) \cap fSf$ is a group. (See [8, Theorem 1.48] or [1, Theorem I.2.12].)

Consider the semigroups fSf and eTe, noting that $G_e \subseteq eTe$. We have $\pi(fSf) = eTe$ and so π is a continuous surjective homomorphism between these semigroups too.

Let G_f be the maximal group in fSf with identity f. If $x \in G_f$, then x is invertible with respect to f and therefore $\pi(x)$ is invertible with respect to e. Thus $\pi(G_f) \subseteq G_e$.

Now we claim that $fSf \cap \pi^{-1}(G_e)$ is a group. To see this, let $y \in fSf \cap \pi^{-1}(G_e)$. We produce $v \in fSf \cap \pi^{-1}(G_e)$ such that $vy = f$. Since $\pi(y) \in G_e$, pick $w \in G_e$ such that $w\pi(y) = e$ and pick $z \in fSf$ such that $\pi(z) = w$. Let u be an idempotent in the left ideal $\pi^{-1}(\{e\})zy$ of $\pi^{-1}(\{e\})$. Pick $x \in \pi^{-1}(\{e\})$ such that $u = xzy$ and let $v = fxzf$. Then $v \in fSf \cap \pi^{-1}(G_e)$. Also, $u \in Sy \subseteq Sf$ so $uf = u$ and thus fu is an idempotent. Also $fu \in fSf \cap \pi^{-1}(\{e\})$ which we have observed is a group with identity f. Since f is the only idempotent in $fSf \cap \pi^{-1}(\{e\})$, we must have that $fu = f$. Thus $vy = fxzfy = fxzy = fu = f$ as required and so $fSf \cap \pi^{-1}(G_e)$ is a group with identity f. Therefore $fSf \cap \pi^{-1}(G_e) \subseteq G_f$ and so $G_e \subseteq \pi(G_f)$, and thus $\pi(G_f) = G_e$.

It follows that if $H = \pi^{-1}(G) \cap G_f$, then H is a subgroup of S and $\pi(H) = G$. $\square$

7.4 Theorem. *If $\kappa \neq \beta$, $\mathcal{K}(\kappa\mathbb{N}, +)$ contains $*$-subgroups with homomorphic images which are matrix groups of any size appearing in $(b\mathbb{Z}, *)$. Also, $\overline{\mathcal{K}(\beta\mathbb{N}, +)}$ contains $\cdot$-subgroups of the same kind.* $\square$

We give another application of these ideas to the algebra of $\beta\mathbb{N}$. By [8, Remark 16.23 and Theorem 16.24] there are left ideals in $(\beta\mathbb{N}, \cdot)$ contained in $\overline{\mathcal{K}(\beta\mathbb{N}, +)}$. We now show that there are $2^{\mathfrak{c}}$ left ideals in $(\beta\mathbb{N}, \cdot)$ which are disjoint from $\overline{\mathcal{K}(\beta\mathbb{N}, +)}$. This is a consequence of the following theorem and the fact that wap$\mathbb{N}$ contains $2^{\mathfrak{c}}$ additive idempotents.

7.5 Theorem. *If p is an idempotent in $(\beta\mathbb{N}, +)$ for which $\pi_{\beta,\text{wap}}(p)$ is not equal to the minimum idempotent in $(\text{wap}\mathbb{N}, +)$, $\beta\mathbb{N} \cdot p$ does not meet $\overline{\mathcal{K}(\beta\mathbb{N}, +)}$.*

Proof. For every $x \in \beta\mathbb{N}$, we have

$$\begin{aligned}
\pi_{\beta,\text{wap}}(x \cdot p + p) &= \lim_{m\to x} \lim_{n\to p} \pi_{\beta,\text{wap}}(m \cdot n + p) \\
&= \lim_{m\to x} \lim_{n\to p} \pi_{\beta,\text{wap}}\big((n+p) + (n+p) + \cdots (n+p)\big) \\
&\qquad\qquad\qquad\qquad \text{(with } m \text{ terms in the sum)} \\
&= \lim_{m\to x} \pi_{\beta,\text{wap}}(p) \text{ (by Theorem 2.38 in [8])} \\
&= \pi_{\beta,\text{wap}}(p).
\end{aligned}$$

Since $\pi_{\beta,\mathrm{wap}}(p) \notin \mathcal{K}(\mathrm{wap}\mathbb{N}, +)$, it follows that $x \cdot p \notin \overline{\mathcal{K}(\beta\mathbb{N}, +)}$. □

8. Enveloping rings.

Let $(G, +)$ be a (not necessarily commutative) compact topological group. Then G^G, the set of all maps from G to itself, has a compact topological group operation $+$ as a product of the compact groups G (or equivalently as functions with values in G and the pointwise operations and topology), and a semigroup operation $\circ$, composition of functions. Generally these two operations have little to do with each other, However, we shall be concerned with the subset determined by the set of maps $\{\sigma_n : n \in \mathbb{Z}\}$ where $\sigma_n(g) = n * g$ for $g \in G$. For these maps

$$\sigma_{m+n} = \sigma_m + \sigma_n, \quad \sigma_{m*n} = \sigma_m \circ \sigma_n$$

for $m, n \in \mathbb{Z}$. We shall write

$$\mathrm{Env}_G(\mathbb{Z}) = \overline{\{\sigma_n : n \in \mathbb{Z}\}},$$

where the closure is taken in G^G, and call this the enveloping semigroup of $\mathbb{Z}$ on G. It is, in fact, the enveloping semigroup for the natural action of $(\mathbb{Z}, \cdot)$ on G. $\mathrm{Env}_G(\mathbb{Z})$ is also an abelian subgroup of G^G. If we use $+$ for the operation on $\mathrm{Env}_G(\mathbb{Z})$ induced by the group operation of G^G, we now see that $(\mathrm{Env}_G(\mathbb{Z}), +, \circ)$ is a right topological ring.

8.1 Theorem. *For any compact topological group G, $\mathrm{Env}_G(\mathbb{Z})$ is a compact right topological ring.*

Proof. $(\mathrm{Env}_G(\mathbb{Z}), +)$ is of course a compact abelian topological group and $(\mathrm{Env}_G(\mathbb{Z}), \circ)$ is obviously a right topological semigroup as it is the enveloping semigroup for an action on G. So we only need to show that $\circ$ distributes over $+$.

Let $\rho, \gamma, \tau \in \mathrm{Env}_G(\mathbb{Z})$ and let $x \in G$. Then

$$(\rho \circ (\gamma + \tau))(x) = \lim_{\sigma_n \to \rho} (\sigma_n \circ (\gamma + \tau))(x) = \lim_{\sigma_n \to \rho} (\sigma_n \circ \gamma + \sigma_n \circ \tau)(x) = (\rho \circ \gamma + \rho \circ \tau)(x).$$

Also

$$((\gamma+\tau)\circ\rho)(x) = \lim_{\sigma_m \to \gamma} \lim_{\sigma_n \to \tau} ((\sigma_m+\sigma_n)\circ\rho)(x) = \lim_{\sigma_m \to \gamma} \lim_{\sigma_n \to \tau} (\sigma_m\circ\rho+\sigma_n\circ\rho)(x) = (\gamma\circ\rho+\tau\circ\rho)(x).$$

□

Let G be a compact topological group. We observe that $\sigma_n \in \Lambda(\mathrm{Env}_G(\mathbb{Z}), \circ)$ for every $n \in \mathbb{Z}$, because σ_n is a continuous function from G to itself.

8.2 Definition. $\sigma : \mathrm{b}\mathbb{Z} \to \mathrm{Env}_G(\mathbb{Z})$ is the continuous surjective ring homomorphism for which $\sigma(n) = \sigma_n$ for every $n \in \mathbb{Z}$. For $p \in \mathrm{b}\mathbb{Z}$ and $x \in G$, we put $p * x = \sigma(p)(x)$.

The existence of σ follows from Theorem 2.14. We also see that

$$p * x = \lim_{n \to p} \sigma_n(x) = \lim_{n \to p} n * x.$$

8.3 Theorem. *If G is a totally disconnected compact topological group, the ring* $\mathrm{Env}_G(\mathbb{Z})$ *is a commutative totally disconnected topological ring. It is, in fact, a quotient of* $\prod_{p \text{ prime}} A_p$*, where* A_p *denotes the ring of* p*-adic integers.*

Proof. There is a continuous ring homomorphism σ from $\mathrm{b}\mathbb{Z}$ onto $\mathrm{Env}_G(\mathbb{Z})$. Since $\mathrm{Env}_G(\mathbb{Z})$ is a subgroup of G^G, it is totally disconnected. So, with the notation of §3, $\sigma(\{0\} \times \widehat{\mathbb{Q}}^{\mathfrak{c}}) = \{0\}$ and therefore $\mathrm{Env}_G(\mathbb{Z})$ is a homomorphic image of $\widehat{\mathbb{Q}/\mathbb{Z}}$. Since $\widehat{\mathbb{Q}/\mathbb{Z}} = \prod_{p \text{ prime}} A_p$ is a commutative topological ring, our claim follows. □

Our next result is that the ring $\mathrm{Env}_{\mathbb{R}/\mathbb{Z}}(\mathbb{Z})$ is easy to determine.

8.4 Theorem. $(\mathrm{Env}_{\mathbb{R}/\mathbb{Z}}(\mathbb{Z}), +, \circ) \cong (\mathrm{b}\mathbb{Z}, +, *)$.

Proof. As we remarked at the beginning of Section 3, the Pontryagin duality theory tells us that $\mathrm{b}\mathbb{Z}$ can be identified with all group homomorphisms from $(\mathbb{R}/\mathbb{Z}, +)$ to itself with the topology of pointwise convergence when the target space $\mathbb{R}/\mathbb{Z}$ is given its usual compact topology. Under this identification, the element $n \in \mathbb{Z}$ goes to the homomorphism $x \mapsto n * x$, that is to σ_n, and the Pontryagin theory tells us that $\mathbb{Z}$ is dense in $\mathrm{b}\mathbb{Z}$. Thus $\mathrm{b}\mathbb{Z} \cong \mathrm{Env}_{\mathbb{R}/\mathbb{Z}}(\mathbb{N})$. □

This result will be used to obtain the following much more general theorem.

8.5 Theorem. *Let G be any compact group which is not totally disconnected. Then* $(\mathrm{Env}_G(\mathbb{Z}), +, \circ) \cong (\mathrm{b}\mathbb{Z}, +, *)$*. In fact, the mapping which takes $p \in \mathrm{b}\mathbb{Z}$ to the element $x \mapsto p * x$ of* $\mathrm{Env}_G(\mathbb{Z})$ *is a continuous ring isomorphism.*

In our proof we require the following simple lemma.

8.6 Lemma. *Let G and H be compact topological groups and let $h : G \to H$ be a continuous homomorphism. For every $p \in \mathrm{b}\mathbb{Z}$, we have $h(p * x) = p * h(x)$.*

Proof. This follows by continuity from the fact $h(n * x) = n * h(x)$ for every $n \in \mathbb{Z}$. □

Proof of Theorem 8.5. By Theorem 2.7, $\mathrm{b}\mathbb{Z}$ acts on G. We shall show that the ring homomorphism σ described in Definition 8.2 is injective by showing that, for any $q \in \mathrm{b}\mathbb{Z}$ different from the identity, there exists $x \in G$ with $q * x \neq 0$. We use the fact that this holds for G if it holds for any closed subgroup of G, by applying Lemma 8.6 with h as an inclusion map. Furthermore, by applying Lemma 8.6 again, it holds for G if it holds for the image of G under a continuous homomorphism.

Because the connected component C of G containing the identity is a closed subgroup, it is enough to prove the result when G is replaced by C. Then C has a quotient C_L which is a connected non-trivial Lie group; C_L has a closed non-trivial connected abelian subgroup C_{LA} (see for example [9], Lemma 6.20); finally C_{LA} has $\mathbb{R}/\mathbb{Z}$ as a quotient since there is a complex homomorphism from any non-trivial connected compact abelian group onto the circle group. So it is enough to find $x \in \mathbb{R}/\mathbb{Z}$ with $q * x \neq 0$. This is always possible by Theorem 8.4. □

We can now extend Corollary 6.8.

8.7 Corollary. *Let G be a compact topological group which is not totally disconnected. Then $(\beta\mathbb{N}, +)$ is the enveloping semigroup for the action of $(\mathbb{N}, +)$ on G defined by the maps $x \mapsto 2^n * x$.*

Proof. By Theorems 6.7 and 8.5, for any two distinct elements p and q in $\mathrm{cl}_{\beta\mathbb{N}}\{2^n : n \in \mathbb{N}\}$, there exists $x \in G$ for which $p * x \neq q * x$. □

If S is a semigroup with a compact topology, X is a compact space and $(s, x) \mapsto s \diamond x$ is a mapping from $S \times X$ to X which is continuous in the S-variable, we write

$$\Lambda(S, \diamond, X) = \{s \in S : x \mapsto s \diamond x \text{ is continuous }\}.$$

This is an obvious generalisation of the topological centre of a semigroup.

8.8 Theorem. *Let G be a compact topological group.*

(i) *If G is totally disconnected,* $\Lambda(\mathrm{b}\mathbb{Z}, *, G) = \mathrm{b}\mathbb{Z}$.

(ii) *If G is not totally disconnected,* $\Lambda(\mathrm{b}\mathbb{Z}, *, G) = \mathbb{Z}$.

Proof. (i) If G is totally disconnected, it is the projective limit of finite groups. Since the action of $\mathrm{b}\mathbb{Z}$ commutes with taking quotients (Lemma 8.6) and since the action of $\mathrm{b}\mathbb{Z}$ on finite groups is obviously continuous, the projective limit maps are also continuous.

(ii) If G is not totally disconnected, $\mathrm{Env}_G(\mathbb{N}) \cong (\mathrm{b}\mathbb{Z}, *) \subseteq G^G$ (Theorem 8.5). Let $p \in \Lambda(\mathrm{b}\mathbb{Z}, *, G)$ and let $q_i \to q$ in $\mathrm{b}\mathbb{Z}$. Then for any $x \in G$, $(p * q_i) * x = p * (q_i * x) \to p * (q * x) = (p * q) * x$, and therefore $p * q_i \to p * q$. Thus $p \in \Lambda(\mathrm{b}\mathbb{Z}, *) = \mathbb{Z}$, by Theorem 3.2. □

8.9 Corollary. *Let G be a totally disconnected compact topological group. Every element of* $\mathrm{Env}_G(\mathbb{Z})$ *is a continuous map from G to itself.*

Proof. Let $q \in \mathrm{Env}_G(\mathbb{Z})$. Then $q = \sigma(p)$ for some $p \in \mathrm{b}\mathbb{Z}$, where σ is the mapping described in Definition 8.2. Since $q(x) = p * x$ for every $x \in G$, our claim follows from Theorem 8.8. □

8.10 Theorem. *If G is a singly-generated compact group and totally disconnected then* $(\mathrm{Env}_G(\mathbb{Z}), +) = G$.

Proof. Let g be a generator of G. The map $h : q \mapsto q(g)$, $\mathrm{Env}_G(\mathbb{Z}) \to G$, is an additive homomorphism. We show it is bijective. First its image is a compact additive subgroup of G containing g and is therefore equal to G. So h is surjective. Let $q \in \mathrm{Ker}(h)$; so $q(g) = 0$, the identity of G. It follows that $q(ng) = 0$ for every $n \in \mathbb{Z}$. Taking limits and applying Corollary 8.9, shows that $q(x) = 0$ for every $x \in G$. Thus q is the identity of $(\mathrm{Env}_G(\mathbb{Z}), +)$ and h is injective. □

We prove several results about compact monothetic topological groups. We observe that these include all compact connected abelian topological groups of weight at most $\mathfrak{c}$ ([7] Theorem 25.14).

8.11 Theorem. *Let C be a compact monothetic topological group. Then C is isomorphic to a group of the form* $(\mathrm{Env}_G(\mathbb{Z}), +)$ *if and only if C satisfies one of the two following conditions:*

(i) *C is totally disconnected;*

(ii) $C \cong (\mathrm{b}\mathbb{Z}, +)$.

Proof. This is immediate from Theorems 8.5 and 8.10. □

We now see that the rings $\mathrm{Env}_G(\mathbb{Z})$ are precisely the compact right topological rings which have a multiplicative identity as a generator. Among these $\mathrm{b}\mathbb{Z}$ has several unique properties. It is the only one which is not totally disconnected, the only one which is not a topological ring and the only one with more than $\mathfrak{c}$ points.

8.12 Theorem. *Let $(R, +, \cdot\,)$ be a compact right topological ring with a generator u which is an identity for $\cdot$. Then R is topologically isomorphic to the ring* $(\mathrm{Env}_R(\mathbb{Z}), +, \circ)$.

Proof. We note that the mapping $n \mapsto n * u$ is a ring homomorphism from $\mathbb{Z}$ to R. Since $n * u \in \Lambda(R, \cdot)$ for every $n \in \mathbb{Z}$, it follows from Theorem 2.14 that there is a continuous ring homomorphism $\rho : \mathrm{b}\mathbb{Z} \to R$ such that $\rho(n) = n * u$ for every $n \in \mathbb{Z}$. It follows by continuity that $\rho(p) = p * u$ for every $p \in \mathrm{b}\mathbb{Z}$.

Let $\sigma : \mathrm{b}\mathbb{Z} \to \mathrm{Env}_R(\mathbb{Z})$ be the mapping described in Definition 8.2. Clearly, for any $p, q \in \mathrm{b}\mathbb{Z}$, $\sigma(p) = \sigma(q)$ implies that $\rho(p) = \rho(q)$. Conversely, suppose that $\rho(p) = \rho(q)$. For any $r \in \mathrm{b}\mathbb{Z}$, we have $\rho(p * r) = \rho(p) \cdot \rho(r) = \rho(q) \cdot \rho(r) = \rho(q * r)$. So $p * \rho(r) = \rho(p * r) = \rho(q * r) = q * \rho(r)$, by Lemma 8.6. Since ρ is surjective, $p * x = q * x$ for every $x \in R$ and so $\sigma(p) = \sigma(q)$. □

8.13 Corollary. *Let $(R, +)$ be a compact monothetic topological group. Then R admits a multiplication $\cdot$ such that $(R, +, \cdot\,)$ is a ring satisfying the hypotheses of Theorem 8.12 if and only if one of the two following conditions holds:*

(i) *R is totally disconnected;*

(ii) $R \cong (\mathrm{ap}\mathbb{Z}, +)$.

Proof. This is a consequence of Theorems 8.11 and 8.12. □

The following simple theorem seems worth noting.

8.14 Theorem. *Let κ be any cardinal. $\mathbb{T}^\kappa$ does not admit a non-trivial binary operation $\cdot$ which is right topological and distributive over addition.*

Proof. Let $\cdot$ be a binary operation on $\mathbb{T}^\kappa$ such that $(\mathbb{T}^\kappa, \cdot)$ is right topological and $\cdot$ distributes over addition. We show that $x \cdot y = 0$ for all x and y in $\mathbb{T}^\kappa$. For each $\alpha < \kappa$, let $\pi_\alpha : \mathbb{T}^\kappa \to \mathbb{T}$ denote the projection map. Let $h : \mathbb{T} \to \mathbb{T}^\kappa$ be an arbitrary homomorphism. Given $\alpha < \kappa$ and $x \in \mathbb{T}^\kappa$ the map $t \mapsto \pi_\alpha\big(x \cdot h(t)\big)$ from $\mathbb{T}$ to itself defines an element of $\widehat{\mathbb{T}_d} \cong \mathrm{b}\mathbb{Z}$. Since $\mathrm{b}\mathbb{Z}$ has no non-trivial elements of additive finite order (this is immediate from the matrix description of $\mathrm{b}\mathbb{Z}$) $\pi_\alpha\big(x \cdot h(t)\big) = 0$ for every $t \in \mathbb{T}$ if x has finite order. The set of elements of finite order is dense in $\mathbb{T}^\kappa$ and so $\pi_\alpha\big(x \cdot h(t)\big) = 0$ for every $x \in \mathbb{T}^\kappa$ and every $t \in \mathbb{T}$. Thus $x \cdot h(t) = 0$ for every $x \in \mathbb{T}^\kappa$ and every $t \in \mathbb{T}$.

To complete the proof, we observe that, for every $y \in \mathbb{T}^\kappa$, we can define a homomorphism $h : \mathbb{T} \to \mathbb{T}^\kappa$ for which $y \in h(\mathbb{T})$. To see this, choose any irrational $t \in \mathbb{T}$ and define $h(nt) = ny$ for every $n \in \mathbb{Z}$. We can then extend h to a homomorphism defined on $\mathbb{T}$ (see [7] Theorem A7 or [9] Proposition A1.35; the image group is commutative and divisible). □

We now, in part (ii) of our final theorem, give an application of these ideas. Part (i) is a simpler result, offered for comparison. We recall that for any sequence (x_i) in a semigroup the set $FP(x_i)$ consists of all finite products $x_{i_1} x_{i_2} \ldots x_{i_k}$ with $i_1 < i_2 < \ldots < i_k$.

8.15 Theorem. *Let $(C,+)$ be a compact topological group with identity 0.*

(i) *For every $x \in C$ and every neighbourhood U of x in C, there is an infinite sequence (n_i) in $\mathbb{N}$ such that $nx \in U$ whenever $n \in FP(n_i)$.*

(ii) *Let (a_i) be an increasing sequence in $\mathbb{N}$ for which $\prod_{i=1}^{n} a_i$ divides a_{n+1} for every n. If C is not totally disconnected, there exists $x \in C \setminus \{0\}$ such that, for every neighbourhood U of x, there is an infinite subsequence (n_i) of $FP(a_i)$ with the property that $nx \in U$ whenever $n \in FP(n_i)$.*

Proof. (i) Since $\sigma_1(x) = x$, it follows that $V = \{p \in \mathrm{Env}_C(\mathbb{Z}) : p(x) \in U\}$ is a neighbourhood of σ_1 in $\mathrm{Env}_C(\mathbb{Z})$. If $\mathrm{Env}_C(\mathbb{Z})$ is finite, there exists $k \in \mathbb{N}$ such that $kx = 0$. In this case, we simply choose an infinite sequence (n_i) in $\mathbb{N}$ such that $n_i \equiv 1 \bmod(k)$ for every i. So we may suppose that $\mathrm{Env}_C(\mathbb{Z})$ is infinite. Let $h : \beta\mathbb{N} \to \mathrm{Env}_C(\mathbb{Z})$ be the continuous surjective homomorphism from $(\beta\mathbb{N}, \cdot)$ to $(\mathrm{Env}_C(\mathbb{Z}), \circ)$ extending $h(n) = \sigma_n$ $(n \in \mathbb{N})$. Since σ_1 is not isolated in $\mathrm{Env}_C(\mathbb{Z})$, $\sigma_1 \in h(\beta\mathbb{N} \setminus \mathbb{N})$. By applying Lemma 2.10 in [4] to $(\beta\mathbb{N} \setminus \mathbb{N}) \cap h^{-1}(\sigma_1)$, we see that there exists $q \in \beta\mathbb{N} \setminus \mathbb{N}$ for which $q \cdot q = q$ and $h(q) = \sigma_1$. Since $h^{-1}(V)$ is a neighbourhood of q in $\beta\mathbb{N}$, our claim follows from Theorem 5.8 in [8].

(ii) Let $X = \bigcap_{m \in \mathbb{N}} \mathrm{cl}_{\beta\mathbb{N}} FP(a_n)_{n=m}^{\infty}$. Note that for any $x, y \in X$ with $x < y$, x is a factor of y. By Lemma 5.11 and Corollary 6.33 in [8], X contains $2^{\mathfrak{c}}$ idempotents of $(\beta\mathbb{N}, \cdot)$. If $p, q \in X$ are distinct idempotents of $(\beta\mathbb{N}, \cdot)$, then $\pi_{\beta,\mathrm{b}}(p) \neq \pi_{\beta,\mathrm{b}}(q)$, by Theorem 6.7. So there exists $y \in C$ such that $\pi_{\beta,\mathrm{b}}(p) * y \neq \pi_{\beta,\mathrm{b}}(q) * y$ by Theorem 8.5. We may suppose that $\pi_{\beta,\mathrm{b}}(p) * y \neq 1$. If $x = \pi_{\beta,\mathrm{b}}(p) * y$, then $\pi_{\beta,\mathrm{b}}(p) * x = x$. Since $\{r \in \beta\mathbb{N} : \pi_{\beta,\mathrm{b}}(r) * x \in U\}$ is a neighbourhood of p in $\beta\mathbb{N}$, our claim follows from Theorem 5.14 in [8]. □

Remark. We observe that (ii) of Theorem 8.15 does not hold if C is totally disconnected. In this case, C is a subgroup of a product of finite groups. If we define (a_n) inductively by putting $a_1 = 1$ and $a_n = n a_1 a_2 \cdots a_{n-1}$, then $x^{a_n} \to 1$ as $n \to \infty$ for every $x \in C$.

References.

[1] J. Berglund, H. Junghenn, and P. Milnes, *Analysis on semigroups*, Wiley, N.Y., 1989.

[2] B. Bordbar and J. Pym, *The set of idempotents in the weakly almost periodic compactification of the integers is not closed*, Trans. Amer. Math. Soc. 352 (2000) 823–842.

[3] A. Bouziad, M. Lemańczyk and M. Mentzen, *A compact monothetic semitopological semigroup whose set of idempotents is not closed*, Semigroup Forum, 62 (2001) 98–102.

[4] R. Ellis, *Lectures on topological dynamics*, Benjamin, New York, 1969.

[5] A. El-Mabhouh, J. Pym and D. Strauss, *Subsemigroups of* $\beta\mathbb{N}$, Topology Applic., 60 (1994) 87–100.

[6] E. Hewitt, *Compact monothetic semigroups*, Duke Math. J. **23** (1956), 447-457.

[7] E. Hewitt and K. A. Ross, *Abstract harmonic analysis I*, Springer-Verlag, Berlin, 1979.

[8] N. Hindman and D. Strauss, *Algebra in the Stone-Čech compactification: theory and applications*, de Gruyter, Berlin, 1998.

[9] K. H. Hofmann and S. A. Morris, *The structure of compact groups*, de Gruyter, Berlin, 1998.

[10] W. Ruppert, *Endomorphic actions of* $\beta\mathbb{N}$ *on the torus group*, Semigroup Forum **43** (1991), 202-217.

Neil Hindman
Department of Mathematics
Howard University
Washington, DC 20059
USA
nhindman@aol.com
http://members.aol.com/nhindman/

John Pym
School of Mathematics and Statistics
University of Sheffield
Sheffield S3 7RH
UK
j.pym@sheffield.ac.uk

Dona Strauss
Department of Pure Mathematics
University of Hull
Hull HU6 7RX
UK
d.strauss@hull.ac.uk