

An Application of Topology to Number Theory

Nathan Carlson
University of Arizona

In this discussion we aim towards a proof of a celebrated result in number theory, the Finite Sum Theorem. Originally proven by Neil Hindman with number theoretic techniques, we give a proof that involves a unique synthesis of topology and algebra. We state the theorem:

Finite Sum Theorem (Hindman). *Let $\{A_i\}_{i=1}^k$ be a finite partition of the natural numbers \mathbb{N} . There exists an A_i that contains an infinite sequence whose finite, nonrepeating sums remain in A_i .*

We will need the very useful concept of an **ultrafilter** from set-theoretic topology:

Definition. *Let X be a set. A nonempty family $\mathcal{F} \subseteq \mathcal{P}(X)$ is a **filter** provided*

- (1) $F \in \mathcal{F}$ implies $F \neq \emptyset$,
- (2) $F, G \in \mathcal{F}$ implies there exists $H \in \mathcal{F}$ such that $H \subseteq F \cap G$, and
- (3) $F \in \mathcal{F}, G \in \mathcal{P}(X)$, and $G \supseteq F$ imply $G \in \mathcal{F}$. This is the superset property.

Definition. *A filter \mathcal{F} on a set X is an **ultrafilter** if it is a maximal element in the set of all filters on X , partially ordered by inclusion. I.e, \mathcal{F} is not contained in any strictly larger filter on X .*

If \mathcal{U} is an ultrafilter then it contains so many subsets of X that for all $A \subseteq X$ either $A \in \mathcal{U}$ or $X \setminus A \in \mathcal{U}$.

Let $\beta\mathbb{N} = \{\mathcal{U} : \mathcal{U} \text{ is an ultrafilter on } \mathbb{N}\}$. We give a few examples and non-examples of elements of $\beta\mathbb{N}$:

- (1) For a given $n \in \mathbb{N}$, $\mathcal{U} = \{A \subseteq \mathbb{N} : n \in A\}$ is an ultrafilter on \mathbb{N} . These are *principle* ultrafilters.
- (2) Suppose $A \subseteq \mathbb{N}$ contains more than one element. Then the set $\mathcal{F} = \{B \subseteq \mathbb{N} : A \subseteq B\}$ is a filter, but is not an ultrafilter. For a fixed $a \in A$, $\mathcal{G} = \{B \subseteq \mathbb{N} : a \in B\}$ is a filter such that $\mathcal{F} \subsetneq \mathcal{G}$.
- (3) Non-principle ultrafilters (or *free* ultrafilters) on \mathbb{N} exist, since it can be shown that $|\beta\mathbb{N}| = 2^{\mathfrak{c}}$, yet there are only ω many principle ultrafilters. But I have yet to actually see an explicit construction of a non-principle element of $\beta\mathbb{N}$!

A Topological Structure on $\beta\mathbb{N}$:

For $A \subseteq \mathbb{N}$, set $A^* = \{\mathcal{U} \in \beta\mathbb{N} : A \in \mathcal{U}\}$. Then the set $\{A^* : A \subseteq \mathbb{N}\}$ forms a basis for a compact Hausdorff topology on $\beta\mathbb{N}$. Next, we would like to identify the elements of \mathbb{N} with certain elements of $\beta\mathbb{N}$, so that we can think of \mathbb{N} as being contained in $\beta\mathbb{N}$. We do this using the principle ultrafilters. We note that for $n \in \mathbb{N}$, $\{n\}^*$ consists of one ultrafilter. [Suppose there exist \mathcal{U} and \mathcal{V} in $\{n\}^*$. If $A \in \mathcal{U}$, then $n \in A$. As $\{n\} \in \mathcal{V}$, we have $A \in \mathcal{V}$ by the superset property of \mathcal{V} . This shows $\mathcal{U} \subseteq \mathcal{V}$. Similarly, $\mathcal{V} \subseteq \mathcal{U}$. So $\mathcal{U} = \mathcal{V}$.] Let n^* be the unique element of $\{n\}^*$. We then identify $n \in \mathbb{N}$ with $n^* \in \beta\mathbb{N}$. With this identification, it turns out \mathbb{N} is dense in $\beta\mathbb{N}$ and that $\beta\mathbb{N}$ is the Stone-Cech compactification of \mathbb{N} .

An Algebraic Structure on $\beta\mathbb{N}$:

We now define an algebraic operation $(+)$ on $\beta\mathbb{N}$ that extends the ordinary sum on \mathbb{N} , i.e. $n^* + m^* = (n + m)^*$. For $A \subseteq \mathbb{N}$, define $A - n = \{k \in \mathbb{N} : k + n \in A\}$. This is simply the elements of A shifted to the left n units. For $\mathcal{U}, \mathcal{V} \in \beta\mathbb{N}$, define

$$\mathcal{U} + \mathcal{V} = \{A \subseteq \mathbb{N} : \{n \in \mathbb{N} : A - n \in \mathcal{U}\} \in \mathcal{V}\}.$$

Theorem. $n^* + m^* = (n + m)^*$ for all $n, m \in \mathbb{N}$.

Proof.

$$\begin{aligned} n^* + m^* &= \{A \subseteq \mathbb{N} : \{k \in \mathbb{N} : A - k \in n^*\} \in m^*\} \\ &= \{A \subseteq \mathbb{N} : \{k \in \mathbb{N} : n \in A - k\} \in m^*\} \\ &= \{A \subseteq \mathbb{N} : \{k \in \mathbb{N} : n + k \in A\} \in m^*\} \\ &= \{A \subseteq \mathbb{N} : A - n \in m^*\} \\ &= \{A \subseteq \mathbb{N} : m \in A - n\} \\ &= \{A \subseteq \mathbb{N} : n + m \in A\} \\ &= (n + m)^* \end{aligned}$$

□

It can be shown that $(+)$ defined above is closed and associative, making $(\beta\mathbb{N}, +)$ a semi-group. Furthermore, the topological and algebraic structures on $\beta\mathbb{N}$ interact well: for a fixed $\mathcal{U} \in \beta\mathbb{N}$, the left-translation map $L_{\mathcal{U}} : \beta\mathbb{N} \rightarrow \beta\mathbb{N}$ defined by $L_{\mathcal{U}}(\mathcal{V}) = \mathcal{U} + \mathcal{V}$ is continuous. Finally, then, we have the necessary structure on $\beta\mathbb{N}$ for the proof of the Finite Sum Theorem: $(\beta\mathbb{N}, +)$ is a *compact, left-topological semigroup*.

A very important theorem is known about such structures:

Theorem (Auslander-Ellis). *Every compact left-topological semi-group has an idempotent element, i.e. an element a such that $a + a = a$.*

As $(\beta\mathbb{N}, +)$ is such a structure, the following is an immediate corollary:

Glazer's Theorem. *There exists $\mathcal{U} \in \beta\mathbb{N}$ such that $\mathcal{U} + \mathcal{U} = \mathcal{U}$.*

So, what's the connection between all this and the Finite Sum Theorem? It turns out in the 1970's KU math professor Fred Galvin had a construction that showed that the Finite Sum Theorem was true if there existed an idempotent element in $(\beta\mathbb{N}, +)$. However, Galvin did not know of the Auslander-Ellis Theorem, that is until he talked to Steve Glazer in 1975 when Glazer was speaking KU. It was this conversation that established the final link in the proof.

Lemma (Galvin). *Let \mathcal{U} be an idempotent element of $\beta\mathbb{N}$. Then for all $A \in \mathcal{U}$ there exists a infinite sequence $B \subseteq A$ such that all nonempty finite sums of elements in B remain in A .*

Proof of Finite Sum Theorem. Consider the partition $\mathbb{N} = \bigcup_{i=1}^k A_k$, and let \mathcal{U} be an idempotent ultrafilter on \mathbb{N} . There exists some $i \in \{1, \dots, k\}$ such that $A_i \in \mathcal{U}$. By Galvin's Lemma there exists an infinite sequence $B \subseteq A_i$ such that all nonempty finite sums of elements of B remain in A_i . \square

As a final remark, we note that techniques similar to the above can be used to prove other results in number theory, notably Van der Waerden's Theorem and the Hales-Jewett Theorem.