A More Reduced Inventory

Nir Elber

January 14, 2022

Abstract

We show that the classical reduced inventory for $\mathbb{Z}$ is equivalent to the statement that $\mathbb{Z}$ is initial in Ring.

Contents

0 Review of the Reduced Inventory

In the discussion that follows, all rings are commutative with identity, as God intended.

To review, in first-year number theory, one builds the following reduced inventory which suffices to characterize $\mathbb{Z}$.

Inventory 1 (Reduced inventory, I)**.** We have that $\mathbb{Z}$ is a ring with the following properties.

1. There is a nonempty subset $\mathbb{N} \subseteq \mathbb{Z}$ with the following properties.
   - Closure: the set $\mathbb{N}$ is closed under the operations $+$ and $\times$.
   - Trichotomy: for each integer $n \in \mathbb{Z}$, exactly one of the statements $\{-n \in \mathbb{N}, n = 0, n \in \mathbb{N}\}$ is true. Equivalently, $\mathbb{Z} = -\mathbb{N} \sqcup \{0\} \sqcup \mathbb{N}$.
2. Well-ordering: each nonempty subset $S \subseteq \mathbb{N}$ has a least element.

Observe that well-ordering requires an ordering on $\mathbb{N}$, which one usually defines by saying

$$a < b \iff b - a \in \mathbb{N}$$

for $a, b \in \mathbb{Z}$. This defines an assymetric relation roughly because $0 \notin \mathbb{N}$ by trichotomy; it is transitive because $\mathbb{N}$ is closed under $+$. So indeed, $<$ provides a strict total ordering of $\mathbb{Z}$.

We are interested in showing that the single following statement is sufficient in characterizing the set of integers $\mathbb{Z}$.

Inventory 2 (Reduced inventory, II)**.** We have that $\mathbb{Z}$ is initial in the category Ring.

Formally, our goal is to show the equivalence of Inventory 2 and Inventory 1. Work done during the number theory course can show that Inventory 1 implies that $\mathbb{Z}$ is initial without too much work, so we will be focusing on trying to show Inventory 2 implies Inventory 1. Nevertheless, we will show that Inventory 1 implies Inventory 2 in our work later anyways.

Before continuing, we issue the following warning.

Warning 3. Many of the proofs in this article were made quite rigorous because one must be careful in foundations. As such, the reader is encouraged to merely read the statements of results and only read the proofs which interest the reader.

1 Constructing Naturals

Anyways, we see that the main feature of $\mathbb{Z}$ according to Inventory 1 is that it has a very special subset $\mathbb{N} \subseteq \mathbb{Z}$, so to make Inventory 2 work, we will need to construct this subset $\mathbb{N}$. Here is the idea.

Idea 4. The subset $\mathbb{N} \subseteq \mathbb{Z}$ is the subset of $\mathbb{Z}$ generated by 1 under addition (as a monoid).

Formalizing this requires some care. We take a moment to note that there is no reason to restrict ourselves to $\mathbb{Z}$ for the moment, for the above idea ought to apply to general rings.

Lemma 5. Fix a ring R. Then the collection

$$\mathcal{S}(R) := \{S \subseteq R : 1 \in S \quad \text{and} \quad a \in S \implies a + 1 \in S\}$$

has a unique minimum set, orderded by inclusion.

Proof. The main point is that $\mathcal{S}(R)$ is closed under intersection. Namely, we simply define

$$N := \bigcap_{S\in\mathcal{S}(R)} S.$$

Note that $1 \in N$ because $1 \in S$ for each $S \in S(R)$. Additionally, $a \in N$ implies that $a \in S$ for each $S \in \mathcal{S}(R)$ implies that $a+1 \in S$ for each $S \in \mathcal{S}(R)$ implies that $a+1 \in N$. So indeed, the intersection $N \in \mathcal{S}(R)$.

Now, to show that N is a minimum of $\mathcal{S}(R)$, we note that any $S \in \mathcal{S}(R)$ has $N \subseteq S$ by construction. The uniqueness of N as a minimum element is simply because $\subseteq$ defines a partial order. So we are done. ∎

The above lemma justifies the following definition.

Definition 6 ($N(R)$)**.** Fix a ring R. Then we define the set $N(R) \subseteq R$ as the minimum of the collection

$$\{S \subseteq R : 1 \in S \quad \text{and} \quad a \in S \implies a+1 \in S\}.$$

For the purposes of our examples, we will ignore the fact we have not defined the objects in the examples.

Example 7. We have that $N(\mathbb{C}) = \mathbb{N}$.

Example 8. We have that $N(\mathbb{Z}/6\mathbb{Z}) = \mathbb{Z}/6\mathbb{Z}$. Importantly, it is possible for $0 \in N(\mathbb{Z}/6\mathbb{Z})$.

This condition on $N(R)$ might feel awkward, but it can be essentially rephrased as induction.

Corollary 9 (Induction)**.** Fix a ring R. Then the set $N(R)$ satisfies

$$(S \subseteq R \quad \text{and} \quad 1 \in S \quad \text{and} \quad a \in S \implies a+1 \in S) \implies N(R) \subseteq S.$$

Proof. The condition on S given above is simply asserting that $S \in \mathcal{S}(R)$, as defined in Lemma 5. So $N(R) \subseteq S$ follows because $N(R)$ is the minimum of $\mathcal{S}(R)$. ∎

While we're here, we pick up some facts about $N(R)$.

Proposition 10. Fix R a ring. Then $N(R)$ is closed under the operations $+$ and $\times$ of R.

Proof. We take the operations one at a time.

- We show that $N(R)$ is closed under addition. This means we want to show that, for any $a, b \in N(R)$, we have $a + b \in N(R)$. Equivalently, we show that $N(R)$ is a subset of

  $$S_+ := \{b \in R : a + b \in N(R) \text{ for each } a \in N(R)\}.$$

  We apply induction. Observe that $a \in N(R)$ implies that $a+1 \in N(R)$, so $1 \in S_+$. Additionally, $b \in S_+$ and $a \in N(R)$ implies that $a+b \in N(R)$, so $(a+b)+1 \in N(R)$, so $a+(b+1) \in N(R)$. Thus, $b+1 \in S_+$ follows.

- We show that $N(R)$ is closed under multiplication. This means we want to show that, for any $a, b \in N(R)$, we have $ab \in N(R)$. Equivalently, we show that $N(R)$ is a subset of

  $$S_\times := \{b \in R : ab \in N(R) \text{ for each } a \in N(R)\}.$$

  We apply induction. Observe that $a \in N(R)$ implies that $a \cdot 1 = a \in N(R)$, so $1 \in S_\times$. Additionally, $b \in S_+$ and $a \in N(R)$ implies that $ab \in N(R)$, so $ab + a \in N(R)$, so $a(b+1) \in N(R)$. Thus, $b+1 \in S_\times$ follows. ∎

At this point, we may say that $N(R)$ is more or less the minimal subset of R which contains 1 and is closed under addition. Namely, the definition asserts minimality under $+1$, but this implies closure under addition as shown above anyways.

However, Idea 4 asserted that $N(R)$ should be generated by 1. While our work provides one interpretation of this, viewing "generated" as a minimality condition, another way to view "generated" is to say that every element should be a sum of 1s. Here is a formalization of this idea.

Proposition 11. Fix a ring R. Then any $n \in N(R)$ has at least one of the following true.

- We have $n = 1$.
- There exists $m \in N(R)$ such that $n = m + 1$. Equivalently, $n - 1 \in N(R)$.

Proof. We proceed by contraposition: suppose that $x \in R$ has $x \neq 1$ and $x - 1 \notin N(R)$. Then we show that $x \notin N(R)$.

For this, we show that $N(R) \subseteq N(R) \setminus \{x\}$, from which $x \notin N(R)$ will follow. We show this by induction.

- Observe that $1 \in N(R)$ and $x \neq 1$ implies that $1 \in N(R) \setminus \{x\}$.
- Additionally, $a \in N(R)$ implies that $a + 1 \in N(R)$ as well as $a \neq x - 1$, so $a + 1 \neq x$, so in fact, $a + 1 \in N(R) \setminus \{x\}$. ■

Remark 12. The above proposition does not assert that the two conditions are mutually exclusive. For example, $R = \mathbb{Z}/2\mathbb{Z}$ has $N(R) = R$, in which case 1 does have $1 = 0 + 1$, where $0 \in N(R)$.

To close out this section, we note that we acn verify our construction of the naturals is the "correct" one in the sense of Inventory 1.

Proposition 13. Suppose that $\mathbb{Z}$ satisfies Inventory 1. Then $N(\mathbb{Z}) = \mathbb{N}$.

Proof. We proceed by double-inclusion. As some warning, we will have to do some number theory with Inventory 1 during this proof.

- We show that $N(\mathbb{Z}) \subseteq \mathbb{N}$ by induciton.

  Showing that $1 \in \mathbb{N}$ is somewhat subtle. By trichotomy, we have three cases.

  - If $1 \in \mathbb{N}$, we are done.
  - If $1 = 0$, then $\mathbb{Z} = \{0\}$ is the zero ring, so $\mathbb{N}$, being nonempty, must have $\mathbb{N} = \mathbb{Z}$, so $1 \in \mathbb{N}$ still.
  - Lastly, if $-1 \in \mathbb{N}$, then $(-1)(-1) = 1 \in \mathbb{N}$.

  To finish the induction, we note that $a \in \mathbb{N}$ implies $a + 1 \in \mathbb{N}$ by closure of $\mathbb{N}$ under addition.

- We show that $\mathbb{N} \subseteq N(\mathbb{Z})$ by well-ordering. Before doing anything, we show, along the lines of Proposition 11, that $a \in \mathbb{N}$ implies $a = 1$ or $a - 1 \in \mathbb{N}$. By trichotomy, it suffices to show that $a \not< 1$.

  Well, suppose for the sake of contradiction there exists counterexample $a \in \mathbb{N}$ such that $a < 1$; let m be the smallest such. Then $m < 1$ promises $n \in \mathbb{N}$ such that $m + n = 1$. But then

  $$m^2 + mn = m < 1$$

  implies that $m^2 < 1$ is a smaller counterexample as well by closure of $\mathbb{N}$ under multiplication. This is our contradiction.

  We now sho wthat $\mathbb{N} \subseteq N(\mathbb{Z})$. Indeed, suppose for the sake of contradiction $\mathbb{N} \setminus N(\mathbb{Z}) \subseteq \mathbb{N}$ is nonempty. Then well-ordering gives us a least element, which we call a.

  Surely, $a \neq 1$ because $1 \in N(\mathbb{Z})$. But then we note that $a - 1 \in \mathbb{N}$ and is not in $\mathbb{N} \setminus N(\mathbb{Z})$ because a is the smallest element. So $a - 1 \in N(\mathbb{Z})$. But then $a = a - 1 + a \in N(\mathbb{Z})$, which is a contradiction. ■

2 Achieving Well-Ordering

One might expect us to prove trichotomy for our specific ring $\mathbb{Z}$ roughly about now, but this turns out to be surprisingly subtle, as we will discuss later. For now we will content ourselves with proving well-ordering from induction and trichotomy.

Definition 14 (Satisfies trichotomy)**.** Fix R a ring. We say that R *satistfies trichotomy* if and only if, for each $r \in R$, exactly one of $\{-r \in N(R), r = 0, r \in N(R)\}$ is true. Equivalently, $R = -N(R) \sqcup \{0\} \sqcup N(R)$.

Like last time, we will ignore the fact we have not defined the objects in our examples while giving the examples.

Example 15. The ring $\mathbb{Z}$ should satisfy trichotomy.

Non-Example 16. The ring $\mathbb{C}$ does not satisfy trichotomy because $i \neq 0$ and $\pm i \notin \mathbb{N}$.

Non-Example 17. The ring $\mathbb{Z}/6\mathbb{Z}$ does not satisfy trichotomy because $0 \in N(\mathbb{Z}/6\mathbb{Z}) = \mathbb{Z}/6\mathbb{Z}$.

In fact, it turns out we expect $\mathbb{Z}$ to be the only ring (up to canonical isomorphism) which satisfies trichotomy because trichtomy will imply well-ordering, which then completes Inventory 1.

As discussed before, well-ordering requires an ordering. It turns out trichotomy is just a fancy way to define our ordering.

Lemma 18. Fix R a ring. Define the relation $<$ by $a < b$ if and only if $b - a \in N(R)$. The relation $<$ is a strict total order on R if and only if R satisfies trichotomy.

Proof. We show the directions one at a time.

- Suppose that R satisfies trichotomy, and we show that $<$ is a total order.
  - Irreflexive: note that $a - a = 0 \notin N(R)$ by trichotomy, so $a \not< a$.
  - Transitive: note that $a < b$ and $b < c$ implies $b - a \in N(R)$ and $c - b \in N(R)$, so adding gives $c - a \in N(R)$, so $a < c$.
  - Connected: fix $a \neq b$ so that $b - a \neq 0$. Then $b - a \in N(R)$ or $b - a \in -N(R)$. The former gives $a < b$, and the latter gives $b < a$.
- Suppose that $<$ is a total order, and we show that R has trichotomy. Fix $r \in R$. Note that $r = 0$ implies that $0 \not< r$ and $r \not< 0$. Additionally, $r < 0$ cannot have $r = 0$ or $0 < r$ because $0 \not< 0$; similarly, $0 < r$ cannot have $r = 0$ or $r < 0$.

  Thus, the conditions $\{r < 0, r = 0, 0 < r\}$ are mutually exclusive. Only now that we note $r < 0$ is equivalent to $-r \in N(R)$, and $0 < r$ is equivalent to $r \in N(R)$. So we indeed have trichotomy. ∎

And now we prove well-ordering.

Proposition 19. Fix R a ring satisfying trichotomy. Then any nonempty subset $S \subseteq N(R)$ has a minimal element, using the ordering of Lemma 18.

Proof. We start by using induction to show the result for subsets S which are strictly upper-bounded. Formally, define

$$T := \{n \in N(R) : \text{each nonempty } S \subseteq N(R) \text{ strictly upper-bounded by } n \text{ has a minimal}\}.$$

We show that $N(R) \subseteq T$ by induction.

- Any $m \in N(R)$ has $m = 1$ or $m - 1 \in N(R)$ by Proposition 11, so $m = 1$ or $1 < m$. In particular, $m \not< 1$ is forced, so there is no nonempty subset $S \subseteq N(R)$ which is strictly upper-bounded by 1. So $1 \in T$ vacuously.
- Suppose that $a \in T$, and we show that $a + 1 \in T$. Well, pick up any nonempty subset $S \subseteq N(R)$ which is strictly upper-bounded by $a + 1$. We have two cases.
  - If $S = \{a\}$, then a is a minimal element for S.
  - Otherwise $S \setminus \{a\}$ is a nonempty subset of $N(R)$. We would like to show that $S \setminus \{a\}$ is upper-bounded by a, which will give it a minimal element $m \in S \setminus \{a\}$ by induction, which will also be a minimal element for S because adding in the large element a doesn't matter.
    So pick up some $b \in S \setminus \{a\}$. We know $b \neq a$ and $b < a + 1$. From this we get $a - b + 1 \in N(R)$ while $a - b \neq 0$ so that $a - b + 1 \neq 1$, so it follows $a - b \in N(R)$ by Proposition 11 So indeed $b < a$.

To finish, pick up a generic nonempty subset $S \subseteq N(R)$. Now, pick any $n \in S$ and define

$$S' := \{s \in S : s = n \text{ or } s < n\}.$$

Now, $S' \subseteq N(R)$ has a strict upper bound (e.g., $n + 1$) and is nonempty because $n \in S'$, so by the discussion above, S' has a minimal element. Beacuse S will only add larger elements to S', we see that S and S' share a minimal element, so S has a minimal element. This finishes. ■

Thus, having more or less verified well-ordering, we have reduced checking that Inventory 2 implies Inventory 1 to merely showing that our initial ring $\mathbb{Z}$ satisfies trichotomy. We can codify this thinking into the following result.

Proposition 20. Fix $\mathbb{Z}$ a ring. Then $\mathbb{Z}$ satisfies Inventory 1 if and only if $\mathbb{Z}$ satisfies trichotomy.

Proof. If $\mathbb{Z}$ satisfies Inventory 1, then Proposition 13 implies that the promised subset $\mathbb{N}$ is $N(\mathbb{Z})$. Then the trichotomy of Inventory 1 becomes the needed trichotomy for R to satisfy trichotomy.

In the other direction, suppose that $\mathbb{Z}$ satisfies trichotomy. Then, setting $\mathbb{N} := N(\mathbb{Z})$, we can check through the conditions of Inventory 1 to see that a ring $\mathbb{Z}$ satisfying trichotomy will satisfy each condition of Inventory 1.

- We see $\mathbb{N}$ is closed under $+$ and $\times$ by Proposition 10.
- We see that $\mathbb{Z}$ has the needed trichotomy directly from satisfying trichotomy.
- We see $\mathbb{N}$ satisfies well-ordering by Proposition 19. ■

3 Constructing Integers

Trichotomy turns out to be somewhat subtle. To begin our discussion, we will get a handle on things by creating an object with weaker trichotomy.

Definition 21 ($Z(R)$)**.** Fix R a ring. Then we define $Z(R) := -N(R) \cup \{0\} \cup N(R)$. Observe that we are not requiring these sets to be disjoint.

Example 22. We have that $Z(\mathbb{C}) = \mathbb{Z}$.

Example 23. We have that $Z(\mathbb{Z}/6\mathbb{Z}) = \mathbb{Z}/6\mathbb{Z}$.

The point of introducing $Z(R)$ is to hope that we can reduce our study of trichotmoy from general rings to the more controlled $N(R)$ by way of $Z(R)$. To this end, we quickly check that $Z(R)$ is a ring.

Proposition 24. Fix R a ring. Then $Z(R) \subseteq R$ is a subring.

Proof. This proof is boring, and there is no reason to read it, but we will write out the checks simply to show that there is nothing clever involved. Of course, $0 \in Z(R)$ and $1 \in N(R) \subseteq Z(R)$, so it remains to check that $Z(R)$ is closed under $+$ and $\times$. We take these one at a time.

- We show that $Z(R)$ is closed under $\times$. Well, fix $a, b \in Z(R)$, and we have to show that $ab \in Z(R)$. We have the following cases.
  - If either $a = 0$ or $b = 0$, then $ab = 0 \in Z(R)$.
  - If $a, b \in N(R)$, then $ab \in N(R)$.
  - If $a, b \in -N(R)$, then $ab = (-a)(-b) \in N(R)$.
  - If one of $\{a, b\}$ is in $N(R)$ and the other is in $-N(R)$, then without loss of generality $a \in N(R)$ and $b \in -N(R)$ so that $-(ab) = a(-b) \in N(R)$, so $ab \in -N(R)$.
- We show that $Z(R)$ is closed under $+$. Well, fix $a, b \in Z(R)$, and we have to show that $a + b \in Z(R)$. We have the following cases.
  - If either $a = 0$, then $a + b = b \in Z(R)$. Similar works for $b = 0$.
  - If $a, b \in N(R)$, then $a + b \in N(R)$.
  - If $a, b \in -N(R)$, then $-(a + b) = -a + -b \in N(R)$, so $a + b \in -N(R)$.
  - Otherwise, as before, without loss of generality take $a \in N(R)$ and $-b \in -N(R)$ so that we want $a - b \in Z(R)$. We proceed by induction on b. In particular, it suffices to show that

    $$N(R) \overset{?}{\subseteq} S_+ := \{b \in N(R) : a - b \in Z(R) \text{ for each } a \in N(R)\}.$$

    To see that $1 \in S_+$, we note that Proposition 11 means $a \in N(R)$ implies that $a = 1$ (so that $a - b = 0 \in Z(R)$) or $a - 1 \in N(R)$.

    Then suppose that $b \in S_+$ and fix any $a \in N(R)$. We know that $a - b \in Z(R)$. If $a - b \in -N(R)$, then $a - (b + 1) \in -N(R)$ still; if $a - b = 0$, then $a - (b + 1) = -1 \in -N(R)$ as well.

    Otherwise $a - b \in N(R)$, and the argument above tells us that $a - (b + 1) = (a - b) - 1 \in Z(R)$. So we have verified that $b + 1 \in S_+$, as needed. ■

Remark 25. In fact, $Z(R)$ can be shown to be the smallest subring of R. Indeed, we already know that $Z(R)$ is a subring. On the other hand, fix R' a subring. Note $0 \in R'$. Additionally, we need $1 \in R'$, and closure under addition forces $a \in R'$ to imply $a + 1 \in R'$, so $N(R) \subseteq R'$. Lastly, closure under negation forces each $n \in N(R)$ to have $-n \in R'$. So indeed, $Z(R) \subseteq R'$.

In fact, given the addition on $N(R)$, there is exactly one multiplication we can supply for $Z(R)$ which satisfies the distributive law, provided that the generator of $N(R)$ is the multiplicative identity. We will not show this here, but it follows from an induction.

4 Removing Trichotomy

Anyways, as promised trichotomy for $Z(R)$ is easier than for general rings.

Proposition 26. Fix R a ring. Then $0 \notin N(R)$ if and only if $Z(R)$ satisfies trichotomy. Thus, $0 \notin N(R)$ if and only if $Z(R)$ satisfies Inventory 1.

Proof. Technically the condition that $Z(R)$ satisfies trichotomy is that $Z(R) = -N(Z(R)) \sqcup \{0\} \sqcup N(Z(R))$, which is a bit annoying to work with, so we pick up the following coherence result.

Lemma 27. Fix R a ring. Then $N(Z(R)) = N(R)$.

Proof. Note that $1_{Z(R)} = 1_R \in N(R)$ and $a \in N(R)$ implies $a+1_{Z(R)} = a+1_R \in N(R)$, so $N(Z(R)) \subseteq N(R)$ by induction. Similarly, $1_R = 1_{Z(R)} \in N(Z(R))$ and $a \in N(Z(R))$ implies $a + 1_R = a + 1_{Z(R)} \in N(Z(R))$, so $N(R) \subseteq N(Z(R))$. This finishes. ■

While we are here, we also pick up the following, for cuteness reasons. (We will not use it anywhere.)

Corollary 28. Fix R a ring. Then $Z(Z(R)) = Z(R)$.

Proof. We have that $Z(Z(R)) = -N(Z(R)) \cup \{0\} \cup N(Z(R))$ by definition, but Lemma 27 implies that this is $Z(Z(R)) = -N(R) \cup \{0\} \cup N(R) = Z(R)$. ■

Thus, $Z(R)$ satisfies trichotomy if and only if $Z(R) = -N(R) \sqcup \{0\} \sqcup N(R)$. Now, in the reverse direction, we see that $Z(R)$ satisfies trichotomy implies $0 \notin N(R)$ by the nature of the disjoint union.

The forward direction is more interesting. Suppose that $0 \notin N(R)$. Now pick up any $a \in Z(R)$, and we have to show that exactly one of $\{a \in -N(R), a = 0, a \in N(R)\}$ is true. Certainly one of them is true by construction of $Z(R)$. So we have the following cases.

- If $a = 0$, then we note $0 = -0 \notin N(R)$.
- If $a \in N(R)$, then $a \neq 0$. Additionally, $-a \in N(R)$ would imply $a + -a = 0 \in N(R)$, whihch is false.
- If $a \in -N(R)$, then $a \neq -0 = 0$. Additionally, $a \in N(R)$ would imply that $a + -a = 0 \in N(R)$, which is false. ■

Because a ring satisfying trichotomy should be $\mathbb{Z}$, at this point we see that $0 \notin N(R)$ is our condition of interest. For example, we can show that such rings will satisfy Inventory 2.

Lemma 29. Fix R, R' rings. Then there is at most one ring homomorphism $Z(R) \to R'$.

Note that it is possible for there to be no such map: take $R = \mathbb{Z}/6\mathbb{Z}$ and $R' = \mathbb{Z}$.

Proof. Fix two ring homomorphisms $\varphi_1, \varphi_2 : Z(R) \to R'$. We want to show that $\varphi_1(a) = \varphi_2(a)$ for each $a \in Z(R)$. We have three cases.

- Note that $\varphi_1(0) = 0 = \varphi_2(0)$.
- We deal with the case $a \in N(R)$ by indution. Set

  $$S := \{a \in R : \varphi_1(a) - \varphi_2(a)\}.$$

  Note $1 \in S$ because $\varphi_1(1) = 1 = \varphi_2(1)$. Further, if $a \in S$, then

  $$\varphi_1(a+1) = \varphi_1(a) + 1 = \varphi_2(a) + 1 = \varphi_2(a+1),$$

  so $a + 1 \in S$. So it follows $N(R) \subseteq S$, as needed.
- For any $a \in -N(R)$, the previous case tells us that $\varphi_1(a) = -\varphi_1(-a) = -\varphi_2(-a) = \varphi_2(a)$. ■

Proposition 30. Fix R a ring. Suppose that $0 \notin N(R)$. Then $Z(R)$ is initial in Ring.

Proof. By Lemma 29, it suffices to show that, for any ring R', there exists a ring homomorphism $\varphi : Z(R) \to R'$. The main idea here is that sums of 1s should go to sums of 1s, which uniquely describes the morphism. Doing this formally requires some technical care.

Fix our second ring R', and note that $0 \notin N(R)$ implies that R satisfies trichotomy by Proposition 26, so we may give R the ordering described in Lemma 18. Given $n \in N(R)$, we define

$$R_n := \{a \in N(R) : a \leq n\}.$$

Observe that, by Proposition 11, each $a \in N(R)$ has $a = 1$ or $a - 1 \in N(R)$, so in either case $a \geq 1$. In particular, if $a < n+1$, then $n + 1 - a \in N(R)$, so $n + 1 - a \geq 1$, so $a \leq n$. It follows that

$$R_{n+1} = \{a \in N(R) : a < n+1 \text{ or } a = n+1\} = R_n \cup \{n+1\}.$$

Now, most of the construction will be done in the following lemma.

Lemma 31. Fix any $n \in N(R)$. There is exaclty one function $\varphi : R_n \to R'$ such that $\varphi(1) = 1$ and $\varphi(a+1) = \varphi(a) + 1$ whenever $a, a+1 \in R_n$.

Proof. We induct on n; we would like to show that each $n \in N(R)$ satisfies the conclusion of the lemma.

For $n = 1$, we note that $R_1 = \{1\}$: now that we know $Z(R)$ satisfies Inventory 1, we see from the proof of Proposition 13 that each $a \in N(R)$ has $a \geq 1$, so $a \in R_1$ forces $a = 1$. Thus, $\varphi(1) = 1$ forces our hand for R_1, and this preserves addition (vacuously) and multiplication because $\varphi(1)\varphi(1) = 1 = \varphi(1)$.

Now suppose that $n \in N(R)$ satisfies the conclusion of the lemma. For $n+1$, we note that any function $\varphi : R_{n+1} \to R'$ satisfying $\varphi(a+1) = \varphi(a) + 1$ with $\varphi(1) = 1$ will have $\varphi|_{R_n} : R_n \to R'$ do the same, so $\varphi|_{R_n}$ is forced. But now

$$\varphi(n+1) = \varphi(n) + 1$$

is forced by hypothesis on φ, so φ is forced entirely. In fact, the above discussion gives a construction of φ which satisfies $\varphi(a+1) = \varphi(a) + 1$ whenever $a, a+1 \in R_n$, and then we get this also when $a, a+1 \in R_{n+1}$ by noting the only extra condition to check is $a + 1 = n + 1$, which is $\varphi(n+1) = \varphi(n) + 1$. ■

By the construction of the proof, we note that $\varphi_{n+1}|_{R_n} = \varphi_n$ for each $n \in N(R)$. One can also show this more directly by using the uniqueness of the lemma.

To finish, we let $\varphi_n : R_n \to R'$ be the functions promiseed by the lemma, and we define $\varphi : Z(R) \to R'$ by

$$\varphi(x) := \begin{cases} \varphi_x(x) & x \in N(R), \\ 0 & x = 0, \\ -\varphi_{-x}(-x) & x \in -N(R). \end{cases}$$

Note that these cases are in fact disjiont because $Z(R)$ satisfies trichotomy. (Here is where we crucially use that $Z(R)$ satisfies trichotomy!) We now do casework to verify that $\varphi(a+1) = \varphi(a) + 1$ for each $a \in Z(R)$.

- If $a \in N(R)$, then $a + 1 \in N(R)$ as well, so

  $$\varphi(a+1) = \varphi_{a+1}(a+1) = \varphi_{a+1}(a) + 1.$$

  It remains to show that $\varphi_{a+1}(a) = \varphi_a(a)$. But we know $\varphi_{a+1}|_{R_a} = \varphi_a$, so we are done.

- If $a = 0$, then $\varphi(a+1) = 1 = 0 + 1 = \varphi(a) + 1$.

- If $a = -1$, then $\varphi(a) + 1 = -1 + 1 = 0 = \varphi(a+1)$.

- Otherwise, $-a \in N(R)$ and $-a \neq 1$. Thus, $-a - 1 \in N(R)$ by Proposition 11 and in particular is nonzero, so

  $$\varphi(a) = -\varphi_{-a}(-a) \stackrel{*}{=} -(\varphi_{-a-1}(-a-1) + 1) = \varphi(a+1) - 1,$$

  where we have used the first case in $\stackrel{*}{=}$. This finishes.

From here, one can show that φ preserves $+$ and $\times$ by hand using a few inductions and more casework, which finishes. We will not be more explicit than this because these checks are somewhat painful, and they are essentially the same as the ones in Proposition 24. ■

Remark 32. The condition that $0 \notin N(R)$ is very important here. For example, $\mathbb{Z}/4\mathbb{Z}$ is initial in the category of rings such that $1+1+1+1=0$.

While we're here, we note that the machinery we've built is now sufficient to show that Inventory 1 implies Inventory 2.

Theorem 33. Suppose that a ring $\mathbb{Z}$ satisfies Inventory 1. Then $\mathbb{Z}$ satisfies Inventory 2; i.e., $\mathbb{Z}$ is initial in Ring.

Proof. By Proposition 13, we have that $N(\mathbb{Z}) = \mathbb{N}$. Additionally, by trichotomy on $\mathbb{Z}$, we see that $\mathbb{Z} = -N(\mathbb{Z}) \cup \{0\} \cup N(\mathbb{Z}) = Z(\mathbb{Z})$. Lastly, trichotomy on $\mathbb{Z}$ (again) implies that $0 \notin \mathbb{N} = N(\mathbb{Z})$, so $\mathbb{Z} = Z(\mathbb{Z})$ is initial in Ring by Proposition 30. ■

5 Setting Up

We now return to showing that Inventory 2 implies Inventory 1. We pick up the following technical result.

Proposition 34. Fix R, R' rings. For any ring homomorphism $\varphi : R \to R'$, we have that $\varphi(N(R)) = N(R')$.

Proof. Intuitively, sums of ones should go to sums of ones. Formally, we show this in two parts.

- We show that $\varphi(N(R)) \supseteq N(R')$ by induction. Well, note that $1 = \varphi(1) \in \varphi(N(R))$. Additionally, $a' \in \varphi(N(R))$ promises $a \in N(R)$ such that $\varphi(a) = a'$. Then $a+1 \in N(R)$, so
$$a'+1 = \varphi(a+1) \in \varphi(N(R)).$$
So indeed, $N(R') \subseteq \varphi(N(R))$ by induction.
- We show that $\varphi(N(R)) \subseteq N(R')$. It suffices to show that $N(R) \subseteq \varphi^{-1}(N(R'))$, which we do by induction. Well, $\varphi(1) = 1 \in N(R')$, so $1 \in \varphi^{-1}(N(R'))$. Additionally, $a \in \varphi^{-1}(N(R'))$ implies $\varphi(a) \in N(R')$, so
$$\varphi(a+1) = \varphi(a) + 1 \in N(R'),$$
so $a+1 \in \varphi^{-1}(N(R'))$ as well. So indeed, $N(R) \subseteq \varphi^{-1}(N(R'))$ by induction. ■

The main point of this result is that we can carry around the $0 \in N(R)$ condition between rings. To be explicit, we have the following.

Corollary 35. Suppose $\mathbb{Z}$ is a ring satisfying Inventory 2; i.e., $\mathbb{Z}$ is initial in Ring. Then $0 \in N(\mathbb{Z})$ if and only if $0 \in N(R)$ for all rings R.

Proof. Fix R a ring. By hypothesis on $\mathbb{Z}$, there is a ring homomorphism $\varphi : \mathbb{Z} \to R$, and by Proposition 34, we see that $0 = \varphi(0) \in \varphi(N(\mathbb{Z})) = \varphi(N(R))$. ■

This gives the following test.

Proposition 36. Suppose there exists a ring R such that $0 \notin N(R)$. Then any ring $\mathbb{Z}$ satisfying Inventory 2 will also satisfy Inventory 1.

Proof. By Corollary 35, we have that $0 \notin N(\mathbb{Z})$, which implies that $Z(\mathbb{Z})$ satisfies Inventory 1 by Proposition 26.

So it remains to show that $\mathbb{Z} = Z(\mathbb{Z})$. Note that $0 \notin N(\mathbb{Z})$ impies that $Z(\mathbb{Z})$ is intial in Ring by Proposition 30, so there are unique morphisms between $\mathbb{Z}$ and $Z(\mathbb{Z})$, so these must be isomorphisms. But there is an embedding

$$Z(\mathbb{Z}) \subseteq \mathbb{Z},$$

so this must be the isomorphism $Z(\mathbb{Z}) \to \mathbb{Z}$, so $Z(\mathbb{Z}) = \mathbb{Z}$ follows. ∎

Remark 37. In order to meaningfully use the condition that $\mathbb{Z}$ is intial in Ring, one is going to need access to a large supply of rings. For example, as in Remark 32, one would not be able to distinguish $\mathbb{Z}$ from $\mathbb{Z}/4\mathbb{Z}$ if the only rings we had access to satisfied $1+1+1+1=0$. More generally, one needs to show that no fixed finite sum of 1s yields 0 for all rings.

What is amazing about the Proposition 36 is that it says the above is the only obstruction, and in particular one only needs access to a single ring R with $0 \notin N(R)$ in order to pin down $\mathbb{Z}$.

6 Construction of a Ring

By Proposition 36, we see that showing Inventory 2 implies that Inventory 1 comes down to construcing a ring R such that $0 \notin N(R)$. I am not aware of any clean way to do this.