Finitely Generated Congruences in Semirings and Canonical Positive Models

Snehinh Sen*

November 18, 2025

Abstract

In this paper, we inspect a relatively unexplored notion of finite generation in semirings, namely semirings in which all congruences are finitely generated. Such semirings are dubbed *Congruence Noetherian*. After developing sufficient background and examples, we focus on the canonical positive models of a real order and show that this obvious choice, though not finitely generated as an $\mathbb{N}$-module, is both Congruence Noetherian and flat over $\mathbb{N}$.

Keywords: Semirings, Noetherian, Hilbert Basis Theorem, Flatness, Congruences, Positive Models

MSC 2020: Primary: 16Y60 , 13F20.

1 Introduction

A *semiring* is, essentially, a ring in which some elements might not have additive inverses. Finding interesting general properties for semirings is difficult because of their versatility. Nevertheless, one is often tempted to consider the most obvious generalizations of the usual definitions from the world of rings. For example, one may define a semiring to be *Noetherian* if every ideal is finitely generated. This notion has been explored, though not extensively (see, for instance, [3], [5], [7], [9]). Interestingly, for semirings, there is another obvious generalization of Noetherianness. More precisely, we can look at semirings for which every congruence is finitely generated. Such semirings will be called *Congruence Noetherian* or *c-Noetherian*. Similarly, a semiring is said to be *Congruence Principal* or *c-principal* if every congruence is generated by a single relation.

*Mathematical Sciences Institute
The Australian National University
Canberra, ACT, Australia - 2601
E-mail: snehinh.sen@anu.edu.au

The first part of this article studies the properties of c-Noetherian semirings and provides ample examples. One of the main results which we prove is the following.

Theorem 1. *Let R be a semiring. The following are equivalent.*

(i) *$R[X]$ is c-Noetherian.*
(ii) *Every finitely generated semialgebra over R is c-Noetherian.*
(iii) *Every finitely generated semialgebra over R is finitely presented.*
(iv) *R is a Noetherian ring.*

Even though attempts to generalize Hilbert Basis Theorem exist in the literature on semirings (see, for instance, [9]), to the best of our knowledge, the above result and the constructions presented here have not been explored.

In the second part of this article, we shift our focus to subgroups and subrings of real numbers and their positive models. In this setting, a positive model is a corresponding object defined over $\mathbb{N}$ (instead of $\mathbb{Z}$) which recovers the initial object upon base change. The most natural positive model would be the set of all non-negative elements $S = R_{\geq 0}$ of a subgroup R. As this model is independent of choice of basis, it will be called the *canonical positive model* of R. After verifying functoriality, we prove a few fascinating properties of S. Recall that a *k-ideal* of a semiring R is a cancellative ideal. We say that a semiring is *k-Noetherian* if its k-ideals satisfy the ascending chain condition.

Theorem 2. *Let R be a subgroup of $\mathbb{R}$ and $S = R_{\geq 0}$. Then S is flat over $\mathbb{N}$. Furthermore, if R is a subring, then*

(i) *S is c-Noetherian if and only if S is k-Noetherian, which is if and only if R is Noetherian.*
(ii) *S is c-principal if and only if R is a PID.*
(iii) *If R is a real order, then every non-trivial quotient is finite.*

These are, in some sense, the best that one could hope for (as, for instance, S is not finitely generated as an $\mathbb{N}$-module, nor is S free, even if R is free).

Regarding the structure of the article, Section 2 describes some preliminaries and known results from the theory of semirings. Section 3 studies c-principal and c-Noetherian semirings. Section 4 gives a somewhat universal example of a semiring which is not c-Noetherian, and we prove Theorem 1 in Section 5. Shifting our focus, we consider positive models in Section 6, prove their finiteness properties in Section 7 and their flatness in Section 8.

2 Basics

Let R be a semiring and $\mathcal{C} \subseteq R \times R$ be an equivalence relation denoted by $\sim$, that is, $a \sim b$ if $(a, b) \in \mathcal{C}$. We say that $\mathcal{C}$ is a *congruence* if $a \sim b$, $c \sim d$ implies $a+c \sim c+d$ and $ac \sim bd$. As $\mathcal{C}$ is also reflexive, this includes the cases of $ar \sim br$

and $a + r \sim b + r$ for any $r \in R$. In other words, it is a subsemiring of $R \times R$ which is also an equivalence relation.

It is clear that the intersection of congruences is a congruence, so we may talk about the congruence generated by a subset $B \subseteq R \times R$ denoted by $\sim$. If B is empty, let this be the trivial diagonal congruence. We say that a congruence is *finitely generated* if it can be generated by a finite set B.

Essentially, all examples of congruences come from the following construction.

Example 2.1. Let $f : R \to S$ be a surjective semiring homomorphism. Then the *Congruence Kernel of* f, denoted by $\mathcal{C}_f$ is defined as $\{(a, b) : f(a) = f(b)\}$. It is easy to verify that this is indeed a congruence. Conversely, given a congruence $\mathcal{C}$ of R, the equivalence classes $R/\mathcal{C}$ of $\mathcal{C}$ form a semiring under the operations induced from R. Furthermore, $\mathcal{C}_{\pi:R\to R/\mathcal{C}} = \mathcal{C}$.

We now recall the definition of finitely generated and finitely presented algebras over a semiring and prove a general result.

Definition 3. Let R be a semiring and S be an R-algebra.

(i) We say S is *finitely generated as an R-algebra* if there is a surjective map from a polynomial ring $R[X_1, \ldots, X_n]$ of finitely many variables to S.
(ii) We say S is *finitely presented as an R-algebra* if there is a surjective map as described above with a finitely generated congruence kernel.

Just as in the case of rings, we have the following invariance result.

Proposition 4. *Suppose R is a semiring, T is a finitely presented R-algebra,and $f : R[Y_1, Y_2, \ldots, Y_k] \to T$ is a surjective map. Then C_f is finitely generated.*

Proof. Let $R[X_1, \ldots X_l]/C' \xrightarrow{\sim} T$ be a finite presentation of T induced by a map g. Let $x_i \in T, y_j \in T$ be the images of X_i and Y_j with respect to g and f respectively. Let h_j be some lifts of y_j's in $R[\underline{X}] := R[X_1, \ldots, X_l]$ and g_i be some lifts of X_i in $R[\underline{Y}] := R[Y_1, \ldots, Y_k]$. Consider the map $R[\underline{X}, \underline{Y}] \to R[\underline{Y}]$ taking X_i to g_i. Then, $R[\underline{X}, \underline{Y}]/C'' \cong R$ where C'' is the congruence generated by C' and $X_i \sim g_i$. Clearly, it is a finite congruence.

In a similar spirit, we get quotient maps $R[\underline{X}, \underline{Y}] \xrightarrow{\pi} R[\underline{X}] \to R$ with congruence kernel of $f \circ \pi$ generated by $Y_j \sim h_j$ and C_f. We observe that $C_f = \{\pi(u) \sim \pi(v) : (u, v) \in C''\}$, from which it follows that C_f is finitely generated. □

The following elegant result can be used to determine when a semiring is a rings. Let $\mathbb{B}$ the semifield of Booleans.

Theorem 5 (Borger – Grinberg Theorem)**.** *Let R be a semiring. Then the following are equivalent.*

(i) R *is a ring.*
(ii) $R \otimes_{\mathbb{N}} \mathbb{B} = 0$
(iii) R *does not admit* $\mathbb{B}$ *as a quotient.*

Proof. Proposition 7.9 of [10]. □

Before concluding the section, we shift our focus to the flatness of modules over semirings and recall a few properties from [1]. Let R be a semiring and let M be an R-module. Recall that $\mathrm{Hom}_R(M, -)$ has a left adjoint $- \otimes_R M$ in the category of R-modules that has many properties analogous to the usual tensor product over rings. For more details, see [8] and [1].

Definition 6. We say M is *mono-flat* if $F_M = - \otimes_R M : \mathbf{Mod}_R \to \mathbf{Mod}_R$ preserves monomorphisms. We say M is *flat* if F_M preserves finite limits.

While all flat modules are mono-flat, it is still not known if there are mono-flat modules which are not flat. The conditions are equivalent whenever R is a ring. Theorem 3.5 of [1] beautifully characterizes flat modules by giving multiple equivalent conditions. For the purpose of this talk, we will only need the following result.

Corollary 6.1. *An R-module M is flat if it is a directed union of its finite, free submodules.*

Proof. Tensor product commutes with filtered colimits. A directed union is a filtered colimit. □

Remark 2.1. Note that the converse is not true for a general R. For instance, $\mathbb{B}_2$ is flat over $\mathbb{B}_4$ as it is isomorphic to the localization $\mathbb{B}_4[1/2]$. However, it is clear that $\mathbb{B}_2$ does not contain any free $\mathbb{B}_4$-submodule for cardinality constraint. For a modified converse, see Theorem 3.5 of [1].

3 Principal and Congruence Noetherian Semirings

Definition 7. (i) We say that a congruence is *principal* if it can be generated by a single relation of the form $a \sim b$.
(ii) We say that a semiring is *congruence principal* or *c-principal* if every congruence is principal.
(iii) We say that a semiring is *congruence Noetherian* or *c-Noetherian* if every congruence is finitely generated.

Let us describe a few examples.

Example 3.1. (i) A ring is c-Noetherian if and only if it is Noetherian, and it is c-principal if and only if it is principal.
(ii) As a monoid, the only congruences of $(\mathbb{N}, +)$ are principal and look like $n \sim n + k$ for some $n, k \geq 0$. This would imply that both $\mathbb{N}_{usual}$ and $\mathbb{N}_{trop}$ are principal. We will soon generalize this significantly.
(iii) $\mathbb{N}_{\min,\max}$ is not c-Noetherian.
(iv) Every finite semiring is trivially c-Noetherian.

(v) Let $\mathcal{M}_b$ be the minmax semiring with b elements. Then $\mathcal{M}_b$ is principal if and only if $b \leq 3$.
(vi) Quotients, localizations, and products of principal (resp. c-Noetherian) semirings are principal (resp. c-Noetherian).

As an increasing union of congruences is still a congruence, we get the following result. The proof, being identical to the classical case of rings, is omitted.

Proposition 8. *Let R be a semiring. The following are equivalent.*

(i) R is c-Noetherian.
(ii) Any chain $C_1 \subseteq C_2 \subseteq \ldots \subseteq C_n \subseteq C_{n+1} \subseteq \ldots$ of congruences stabilizes (that is, $C_n = C_{n+1}$ for every $n \gg 1$).
(iii) Any non-empty collection of congruences in R has a maximal element.

The following proposition produces some new examples of c-Noetherian semirings. The proof only uses the monoid structure and has been known for a while.

Proposition 9. *Let S be a finite $\mathbb{N}$-algebra . Then S is c-Noetherian.*

Proof. Suppose S is not c-Noetherian, that is, there is an infinite chain $C_1 \subsetneq C_2 \subsetneq C_3 \ldots$ of congruences on S. For a monoid U, let $\mathbb{Z}[U]$ be the free $\mathbb{Z}$-algebra generated by it. For example, if $U = \mathbb{N}$, then $\mathbb{Z}[U] \cong \mathbb{Z}[T]$, the polynomial ring in one variable over $\mathbb{Z}$. Let $S_i = S/C_{i-1}$ for $i \geq 2$ and $S_1 = S$ and S_0 be a free finitely generated $\mathbb{N}$-module surjecting on to S_1. Then the non-isomorphic surjections $S_0 \twoheadrightarrow S_1 \twoheadrightarrow S_2 \ldots$ yield non-isomorphic surjections $\mathbb{Z}[S_0] \twoheadrightarrow \mathbb{Z}[S_1] \twoheadrightarrow \mathbb{Z}[S_2] \ldots$. But the first ring in this sequence is isomorphic to a finite polynomial ring over $\mathbb{Z}$, and is therefore Noetherian in the classical sense. This contradicts the existence of such a chain of surjections. □

At the time of writing, it was still not known whether any finite algebra over a c-Noetherian semiring S is c-Noetherian again. Finitely generated algebras definitely fail, see Theorem 1

It is natural to ask when a semiring being c-Noetherian would imply that it is Noetherian, in the sense that every ideal is finitely generated. Unfortunately, there is no direct correspondence between arbitrary ideals and congruences of semirings. Instead, we look at a more restrictive class, the class of k-ideals, following [3]. We will see how they relate to the c-Noetherian condition later on.

Definition 10. Let R be a semiring. We say that an ideal I is a *k-ideal* if $\ker(R \twoheadrightarrow R/\mathcal{C}_I) = I$, where $\mathcal{C}_I = \langle x \sim 0 : x \in I \rangle$ is the Rees congruence corresponding to I. In other words, if $x, y \in R, x, x + y \in I$, then $y \in I$.

Given any subset $S \subseteq R$, the *k-ideal generated by S* is defined to be the smallest k-ideal containing S. We say R is *k-Noetherian* if every k-ideal is finitely generated (as a k-ideal).

The following proposition is immediate, and hence the proof is omitted.

Proposition 11. *Let R be a semiring.*

(i) The k-ideal generated by an ideal I is the kernel of the map $R \twoheadrightarrow R/\mathcal{C}_I$.
(ii) The following are equivalent.
  (a) R is k-Noetherian.
  (b) The k-ideals satisfy the ascending chain condition.
  (c) Any non-empty collection of k-ideals has a maximal element.

The following proposition says that k-ideals behave somewhat better than arbitrary ideals in semirings of a special kind.

Proposition 12. *Let R be a totally ordered ring and $S = R_{\geq 0}$. Then there is a bijective correspondence*

$$\{Ideals\ of\ R\} \longleftrightarrow \{k - ideals\ of\ S\}$$

given by

$$I \subseteq R \mapsto I_{\geq 0} \subseteq S$$

and

$$J \subseteq S \mapsto J \cup (-J) \subseteq R.$$

Finally, if I is generated by $\mathcal{D}$, then $I_{\geq 0}$ is generated, as a k-ideal, by $\{|x| : x \in \mathcal{D}\}$. Thus, if R is Noetherian, then S is k-Noetherian.

Proof. These maps are inverses of each other and map to the correct domains. Now, if $I = R\langle S\rangle$ and $x \in \mathcal{D}$. Then $|x| \in I_{\geq 0}$. Now, let J be the k-ideal generated by $|\mathcal{D}| = \{|x| : x \in \mathcal{D}\}$. Then $J \cup (-J) = R\langle|\mathcal{D}|\rangle = R\langle\mathcal{D}\rangle = I$, proving that $I_{\geq 0} = J$ and the claim about generation. k-Noetherianness follows either from the order preservation of the above correspondence or by using the previous line. □

4 A Non-c-Noetherian Semiring

In this section, we explicitly construct a somewhat universal example of a Non-c-Noetherian semiring.

Theorem 13. *Let $R = \mathbb{B}[X]$. Then the congruence $\mathcal{C} = \langle X^n + 1 \sim X^m + 1 : n, m \geq 1\rangle$ is not finitely generated.*

Proof. Suppose, for the sake of contradiction, that it was finitely generated. Say $\mathcal{C} = \langle a_1 \sim b_1, \ldots, a_k \sim b_k\rangle$ with each $a_i \neq b_i$. Call the set of these relations S. Let N be greater than the degree of these finitely many a_i, b_i.

Suppose $X^N + 1$ is related to some element u of R. Then we can find a sequence of relations $u \sim u_1, u_1 \sim u_2, \ldots, u_l \sim X^N + 1$ where each of these are elementary polynomial congruences. Thus, $X^N + 1 = P(f_1, \ldots, f_u, a_1, \ldots, a_k, b_1, \ldots b_k)$ and $u_l = P(f_1, \ldots, f_u, b_1, \ldots, b_k, a_1, \ldots a_k)$ for some polynomial P and $f_i \in R$.

So, each summand of the sum described by the polynomial should be equal to one of $1, X^N, X^N + 1$. Assuming that the polynomial is non-trivial, we realize

that it is independent of the a_i and b_i factors. For instance, say some a_i occurred in the expression for F. Then we would get $a_i | X^N + 1$ or $a_i | X^N$. The former is impossible because $X^N + 1$ is irreducible and a_i is a non-constant polynomial of a smaller degree, while the latter is impossible because the only divisors X^N are powers of X which, by definition of $\mathcal{C}$, are only related reflexively, while $a_i \sim b_i$ and $b_i \neq a_i$. The same argument is applicable to show that b_i's do not occur in the expression for P.

Thus, the polynomial only involves the f_i's, whence it follows that $u_l = X^N + 1$. By induction, this implies $u \sim X^N + 1$ and thus $X^N + 1$ should only be related to itself in $\mathcal{C}$. This contradicts the fact that, say $X^N + 1 \sim X^{N+1} + 1$. □

Corollary 13.1. *The semiring $\mathbb{B}[X]/\mathcal{C}$ described above is finitely generated over N but not finitely presented.*

Proof. Immediate from Theorem 13 and Proposition 4. □

Remark 4.1. It must be noted that $\mathbb{B}[X]$ is not even Noetherian in the sense that there are ideals of $\mathbb{B}[X]$ that cannot be finitely generated. For instance, consider the ideal generated by $\{X^n + 1 : n \geq 1\}$. An argument similar to the one given above would prove that this ideal is not finitely generated. However, it is k-Noetherian. Indeed, let I be a nonzero k-ideal. Let $n \geq 0$ be the least such that I has an element of the form $f(X) = X^n +$ (higher degree terms). Then $X^n + f(X), f(X) \in I \implies X^n \in I$. Also, as for any other term in I. every monomial has degree at least n, we get that $I = (X^n)$, showing that every k-ideal is actually principal (as an ideal, not just a k-ideal).

5 The Hilbert Basis Criterion

In this section, we prove the Hilbert Basis Criterion described in Theorem 1.

Theorem 1. *Let R be a semiring. The following are equivalent.*

(i) *$R[X]$ is c-Noetherian.*
(ii) *Every finitely generated semialgebra over R is c-Noetherian.*
(iii) *Every finitely generated semialgebra over R is finitely presented.*
(iv) *R is a Noetherian ring.*

Proof. The implications $(i) \implies (iv) \implies (iii) \implies (ii)$ are immediate. Now suppose (ii) holds. For the sake of contradiction, suppose that R is not a ring. Then R admits $\mathbb{B}$ as a homomorphic image by Theorem 5. Then we have a surjective map $\phi : R[X] \to \mathbb{B}[X] \to \mathbb{B}[X]/\mathcal{C}$, where $\mathcal{C}$ is the congruence described in Theorem 13. But then the congruence kernel $\mathcal{C}_\phi$ is not finitely generated as $\mathcal{C}$ is not finitely generated. This contradicts our assumption that $R[X]$ is c-Noetherian. Thus, R must be a ring to start with. It follows that $R[X]$, hence R, is a Noetherian ring □

6 Positive Models

In this section, we briefly consider positive models in generality.

Definition 14. Let R be a ring. A *positivity* or *trichotomy function* is a function $p : R \to \{0, \pm 1\}$ such that

(i) $p(0) = 0, p(1) = 1$.
(ii) $p(xy) = p(x)p(y)$.
(iii) $p(x + y) = -1 \implies p(x) = -1$ or $p(y) = -1$.

In such a case, the set $R_p = \{x \in R : p(x) \geq 0\}$ is a subsemiring of R.

The most common examples of trichotomy functions are the *signum* function $sgn : \mathbb{R} \to \{0, \pm 1\}$ and the zero divisor function $p(x) = \delta\{x \text{ is a nonzerodivisor}\}$.

Definition 15. Let R be a ring endowed with a positivity function p and let $S = R_p$. Let $\mathcal{C}$ be a subcategory of $\mathbf{Mod}_R$. A *positive model construction* on $\mathcal{C}$ is a functor $F : \mathcal{C} \to \mathbf{Mod}_S$ with a natural isomorphism $R \otimes_S F \xrightarrow{\sim} Id$.

The following would be the most important construction for a positive model for the sake of our considerations.

Example 6.1. Let $R = \mathbb{Z}$, $p = sgn$. Let $\mathcal{C}$ be the category of all $\mathbb{Z}$-subalgebras of $\mathbb{R}$, with the morphisms being sign-preserving ring homomorphisms. Define $F(R) = R_{\geq 0}$. Then one may easily verify that F is a positive model construction. As no choice of a basis is involved, this positive model is called the *canonical positive model* of real $\mathbb{Z}$-algebras. Similar constructions can be given for any totally ordered ring.

We may generalize the construction of positive models to algebras, schemes, and other algebraic and geometric objects in a similar way. Positive models may or may not retain the properties of the initial object. However, as one may expect, if a positive model has some nice properties, it is almost always the case that the initial object had those properties.

Theorem 16. *Let R be a ring equipped with a positivity function p. Let $S = R_p$, $\mathcal{C}$ be a subcategory of $\mathbf{Mod}_R$ and $F : \mathcal{C} \to \mathbf{Mod}_S$ be a positive model construction. If $F(M)$ is free/projective/flat, then so is M.*

Furthermore, assume that $p(-1) = -1$, and let $\mathcal{C}'$ be the subcategory of $\mathbf{Ring}_R$ and $F' : \mathcal{C}' \to \mathbf{Ring}_S$ be a positive model construction. Then $F'(U)$ is c-Noetherian/c-principal only if U is a Noetherian/principal ring.

Proof. For freeness, one uses $R \otimes_S S^I \cong R^I$ for each indexed sum R^I. For projectivity, one realizes that sections (resp. retracts) go to sections (resp. retracts). For flatness, one uses the fact that the tensor product commutes with filtered colimits and that every flat module is a filtered colimit of free modules.

Now, let us shift our focus to the ring conditions. The condition $R \otimes_S F'(U) \cong U$ along with $p(-1) = 1$ implies that for each $r \in R$, there are $x, y \in S$ such that

$r = 1 \otimes x + (-1) \otimes y$. Suppose $F'(U)$ is c-Noetherian. Let I be an ideal of U. Define the congruence $\mathcal{D}$ on $F'(U)$ as $x \sim y$ if $1 \otimes x + (-1) \otimes y \in I$. One immediately verifies that this is a congruence. Indeed, if $x \sim y, z \sim w$, then

$$1 \otimes xz + (-1) \otimes yw = (1 \otimes xz + (-1) \otimes yz + 1 \otimes yz + (-1) \otimes yw) \in I.$$

The rest of the properties are established similarly. Now, every congruence on $F'(U)$ is finitely generated. Thus, there are finitely many elements $r_i, s_i \in F'(U)$ such that $\mathcal{D} = \langle r_i \sim s_i \rangle$. Then we claim that $I = R\langle 1 \otimes r_i + (-1) \otimes s_i \rangle$. Indeed, let $\alpha = 1 \otimes r + (-1) \otimes s \in I$, then $r \sim s$, which implies that there is a sequence of relations $r = a_0 \sim a_1 \sim \ldots \sim a_n = s$ where each $a_i \sim a_{i+1}$ looks like $a_i = P_i(u_1, \ldots, u_l, r_1, \ldots, r_k, s_1, \ldots, s_k)$ and $a_{i+1} = P_i(u_1, \ldots, u_l, s_1, \ldots, s_k, r_1, \ldots, r_k)$, where $P_i \in \mathbb{N}[\underline{X}]$. But then $1 \otimes a_i + (-1) \otimes a_{i+1} \in R\langle 1 \otimes r_i + (-1) \otimes s_i \rangle$ implies

$$\alpha = 1 \otimes r + (-1) \otimes s = \sum_{i=1}^{n} 1 \otimes a_{i-1} + (-1) \otimes a_i \in R\langle 1 \otimes r_i + (-1) \otimes s_i \rangle$$

The proof for c-principal follows from this computation as well. □

The converse is usually not true. For example, $\mathbb{Z}/\mathbb{N}$ is not even flat, even though $\mathbb{Z}$ is free over $\mathbb{Z}$. However, as stated in Theorem 2, something close enough to a converse is true for the canonical positive model. This shows that the canonical positive model behaves as well as it can be hoped for.

Theorem 2. *Let R be a subgroup of $\mathbb{R}$ and $S = R_{\geq 0}$. Then S is flat over $\mathbb{N}$. Furthermore, if R is a subring, then*

(i) S is c-Noetherian if and only if S is k-Noetherian, which is if and only if R is Noetherian.
(ii) S is c-principal if and only if R is a PID.
(iii) If R is a real order, then every non-trivial quotient is finite.

Remark 6.1. We claim that Theorem 2 is, in a sense, the best that one could hope from canonical positive models. Let $R \neq \mathbb{Z}$ be a subring of $\mathbb{R}$ and $S = R_{\geq 0}$. We claim that S is never finitely generated or free over $\mathbb{N}$. The finite generation is immediate - any finitely generated $\mathbb{N}$-submodule of $\mathbb{R}_{\geq 0}$ is necessarily discrete, while S is always dense in $\mathbb{R}_{\geq 0}$. For freeness, suppose $S/\mathbb{N}$ is free with basis $\mathcal{B}$. Then $\mathcal{B}$ has at least two elements u, v. As $u \neq v$, we can assume, without loss of generality, that $u > v$. Then $u - v \in S \setminus \{0\}$ would imply that there is a $k \geq 1$, vectors $v_1, \ldots, v_k \in \mathcal{B}$ and natural number $\lambda_1, \ldots, \lambda_k > 0$ such that $u - v = \sum_k \lambda_k v_k$. So $u = \sum_k \lambda_k v_k + v$, contradicting that $\mathcal{B}$ is a basis.

7 Finiteness of a Positive Model of Real Orders

We are now in a position to prove the claimed finiteness result for canonical positive models.

Theorem 17. *Suppose $R \subseteq \mathbb{R}$ is a subring and $S = R_{\geq 0}$. Let $\sim$ be a congruence on S. Given any $x \in S$, define $I_x = \{y \in S : y + x \sim x\}$. Then*

(i) I_x *is a* k*-ideal.*
(ii) If $x \leq y$*, then* $I_x \subseteq I_y$*.*
(iii) If $I_t \neq 0$*, then* $I_x = I_t$ *for each* $x \geq t$*.*
(iv) If $R \neq \mathbb{Z}$*, then* $I_x = I_y$ *for each* $x, y > 0$*.*

Proof. Clearly $0 \in I_x$. Also, if $a, b \in I_x$, then

$$x \sim x + b \sim (x + a) + b$$

would show that $a + b \in I_x$. Similarly $a, b \in S, a, a + b \in I_x$ implies that

$$x + b \sim (x + a) + b \sim x + (a + b) \sim x,$$

proving that I_x is cancellative. Finally, let $a \in I_x, a \neq 0$ and $r \in S$. Let $N \in \mathbb{N}$ be large enough so that $Na > rx$. Then

$$\begin{aligned} x + ra &\sim (x + Na) + ra \\ &= (x + Na - rx) + r(x + a) \\ &\sim (x + Na - rx) + rx \\ &\sim x + Na \sim x \end{aligned}$$

proving that I_x is indeed an ideal. For $x \leq y$, clearly $a \in I_x$ implies that

$$y = (y - x) + x \sim (y - x) + (x + a) \sim y + a$$

proving that $a \in I_y$. So $I_x \subseteq I_y$.

Now suppose that $I_t \neq 0$. Let $y \in I_t \setminus 0$. Let $x \geq t$ and $a \in I_x$. Choose $N \geq 1$ large enough so that $Ny > x$. Then

$$\begin{aligned} t + a &\sim (t + Ny) + a \\ &\sim (t + (a + x)) + (-x + Ny) \\ &\sim (t + x) + (-x + Ny) \\ &= t + Ny \sim t. \end{aligned}$$

This shows that $I_x = I_t$, proving (iii).

Finally, if $R \neq \mathbb{Z}$, then R is dense in $\mathbb{R}$. Let $x > y > 0$. Then there is a $\beta \in S, \beta > 0$ such that $\beta x < y$. Then $\beta I_x \subseteq I_{\beta x} \subseteq I_y \subseteq I_x$. So $I_x = 0$ if and only if $I_y = 0$. Furthermore, (iii) shows that $I_x = I_y$. □

This theorem has many different implications. We now state a few of them. For a semiring A, denote by A_* the set $A \cup \{\omega\}$ and extend the operations $+, \cdot$ on A by setting $\omega + x = x$ and $\omega \cdot x = \omega$. Then A_* is a semiring.

Corollary 17.1. *Suppose that* R, S *is as above and* $R \neq \mathbb{Z}$*. Then the following sets are naturally in bijection.*

(i) $\{$*Nonzero ideals of* $R\} \times \{0, 1\} \sqcup \{0\}$*.*

(ii) $\{$*Nonzero* $k-$ *ideals of* $S\} \times \{0,1\} \sqcup \{0\}$.
(iii) Congruences on S.

The bijection between the first two sets is described in Proposition 12. The map between the second and third sets is given by

$$(I, j) \mapsto \mathcal{C}_j(I) = \langle j + x \sim j : x \in I \rangle, \text{ and } 0 \mapsto \Delta.$$

Also, $S/\mathcal{C}_0(I) \cong R/I$ *and* $S/\mathcal{C}_1(I) \cong (R/I)_*$.

Furthermore, if I *is generated as a* k*-ideal by* $\{x_i : i \in K\}$*, then* $\mathcal{C}_j(I)$ *is generated by* $\langle j \sim j + x_i \rangle$.

Before giving the proof, we would like to point out that

$$\mathcal{C}_0(I) = \{x \sim y : |x - y| \in I\}, \text{ and}$$

$$\mathcal{C}_1(I) = \{x \sim y : |x - y| \in I, x, y > 0\} \cup \{0 \sim 0\}$$

as is immediate from Theorem 17.

Proof. From Theorem 17 and the remark above, it is clear that a congruence is classified by the information of whether $I_0 = 0$ or $I_0 \neq 0$, and what I_1 is. This bijection is just a rephrasing of that fact. The generation part is immediate by considering this data as well.

As for the quotients, note that if $x_1, \ldots, x_k > 0$ are a set of representatives of R/I, then $0, x_1, \ldots, x_k$ represent (perhaps with one repetition) all elements of $S/\mathcal{C}_j(I)$. The degeneracy occurs only if $j = 0$, where we could remove 0 and get $S/\mathcal{C}_0(I) \cong R/I$. In the other case, 0 is not related to any other element, and the rest of the representatives behave like R/I. Hence, we realize that $S/\mathcal{C}_1(I) \cong (R/I)_*$. □

Corollary 17.2. *Suppose* R *is a subring of* $\mathbb{R}$ *and* $S = R_{\geq 0}$*. Then* S *is c-Noetherian if and only if* S *is k-Noetherian, which holds if and only if* R *is Noetherian. Furthermore, if* R *is a PID, then* S *is c-principal. Finally, if* R *is a real order, then any nontrivial quotient of* S *is finite.*

Proof. The claims are immediate for $R = \mathbb{Z}$, so we assume $R \neq \mathbb{Z}$. Observe that, by Corollary 17.1, S is c-Noetherian if and only S is k-Noetherian, which, by Proposition 12 and Theorem 16, is true if and only if R is Noetherian. As this is indeed the case, we are done. Now if R is a PID, then the last line of Corollary 17.1 would imply that S is c-principal. Finally, if R is a real order, then the result on quotients of S in Corollary 17.1 would imply that every nontrivial quotient of R is finite. □

Remark 7.1. What is also immediate from basic algebraic number theory is that if R is a ring of integers (maximal order) to start with, then every congruence on S is generated by at most two elements. Also, for $R = \mathbb{Z}[\pi]$, we find that $S = R_{\geq 0}$ is c-Noetherian, unlike $S' = \mathbb{N}[\pi] \cong N[T]$. This gives us some more evidence that perhaps the canonical positive model is better than a basis-dependent model.

This settles the finiteness part of Theorem 2. However, we point out that this is not the only approach or proof of the theorem. While discussing a complete alternative proof would lead to an unnecessary detour, we state a few lemmas, sketch the proof and make a remark to justify its inclusion. Fix $R \neq \mathbb{Z}$.

Lemma 17.1. *Let A be a semiring, $\sim$ a congruence on A, and suppose that $x \sim x + y$. Then for each $n \geq 1$, we have $x^n \sim x^n + y^n$.*

Proof. We proceed by induction. The base case is assumed. Suppose that the claim is true for $n \geq 1$. Then

$$x^{n+1} \sim x(x^n + y^n) \sim x^{n+1} + y^n(x + y) \sim x(x^n + y^n) + y^{n+1} \sim x^{n+1} + y^{n+1}.$$

The claim is thus established for each $n \geq 1$ by induction. □

Lemma 17.2. *Let $R \subseteq \mathbb{R}$ be any algebraic $\mathbb{Z}$-algebra and $\sim$ be a non-trivial congruence in $S = R_{\geq 0}$. Then there are integers $n > m > 1$ such that $n \sim m$.*

Proof. Let $a \sim a + u$ in S with $a, u > 0$. Then, by Lemma 17.1, for each $n \geq 1$, we have $a^n \sim a^n + u^n$. So for any $q(T) \in T\mathbb{N}[T]$, $q(a) \sim q(a) + q(u)$. Now u satisfies an equation of the form $uf(u) = ug(u)+l$ where $f, g \in \mathbb{N}[X], l \in \mathbb{N}\setminus\{0\}$. So,

$$\begin{aligned} af(a) + ag(a) + l &\sim af(a) + ag(a) + ug(u) + l \\ &= af(a) + ag(a) + uf(u) \\ &\sim af(a) + ag(a). \end{aligned}$$

Now, let m be any integer exceeding $af(a) + ag(a)$ and $n = m + l$. As $\sim$ is a congruence, we have

$$\begin{aligned} m &= (m - af(a) - ag(a)) + af(a) + ag(a) \\ &\sim (m - af(a) + ag(a)) + af(a) + ag(a) + l \\ &= m + l = n. \end{aligned}$$

□

We now sketch the alternate proof of the theorem for real orders.

(i) As $R \neq \mathbb{Z}$ is a real order, we can find for $k = \dim_{\mathbb{Z}} R \geq 2$ elements $\alpha_1, \ldots, \alpha_k \in R, \alpha_i \geq 0$ such that $R = \mathbb{Z}\alpha_1 \oplus \ldots \mathbb{Z}\alpha_k$.

(ii) Now, for every element $x \in S, x > 0$, choose $y \in S, y \neq 0$ such that $my < x$. Write $y = \sum_i \lambda_i \alpha_i$. Assume, without loss of generality, that $\lambda_1 \geq 1$.

(iii) Now using $m \sim n$ repeatedly, we can show that $my \sim m \sum_i \mu_i \alpha_i$ where each $\mu_i \geq 1$.

(iv) Finally, by Euclid's division algorithm and some minor adjustments, one ends up showing that $x \sim \sum_i \theta_i \alpha_i$, where each θ_i is a positive integer smaller than n, proving the finiteness. The proof of c-principal is similar.

REMARK 7.2. It is tempting to try to generalize the above results further. While we are using only certain specific properties of real numbers, we rely on it being totally ordered and Archimedean. However, it follows that a totally ordered Archimedean ring R is isomorphic to a subring of the real numbers. Indeed, consider the map $\phi : R \to \mathbb{R}$ as $x \mapsto \sup\{r/s : r \cdot 1_R \leq s \cdot 1, r \in \mathbb{Z}, s \in \mathbb{N}\}$. This is easily seen to be an injective ring homomorphism. So, in a sense, real subrings are the best cases in which the above techniques work. The same is also valid for cancellative totally ordered Archimedean semirings - these are canonical positive models for some subring of real numbers.

On the other hand, Lemma 17.1 and a weaker version of Lemma 17.2 can be proved without these strong assumptions, giving us an alternative approach and justifying their inclusion.

8 Flatness of a Positive Model of Real Orders

We now prove the following result to complete the proof of Theorem 2.

Theorem 18. *For any subgroup $X \subseteq \mathbb{R}$, $X_{\geq 0}$ is flat over $\mathbb{N}$.*

The only proofs that we are aware of at this point involve some convex methods and analysis. The proof would essentially consist of two parts, namely

(i) Translation of the problem into a problem about semilattices in $\mathbb{R}^n$, and
(ii) Homothetic projection onto a hyperplane and its properties.

Let us do (i) now. For the sake of the theorem, it suffices to prove that every finitely generated $\mathbb{N}$-submodule M of $X_{\geq 0}$ is contained in a finite free submodule of $X_{\geq 0}$. Then $X_{\geq 0}$ is a directed union of free submodules, thus flat.

Lemma 18.1. *To prove the theorem, it suffices to show that for any X finitely generated over $\mathbb{Z}$, S is flat over $\mathbb{N}$.*

Proof. X is a filtered colimit of its finitely generated submodules $\{X_\alpha\}_\alpha$. It is immediate that $X_{\geq 0}$ is the colimit of the filtered collection $\{(X_\alpha)_{\geq 0}\}$. If each $(X_\alpha)_{\geq 0}$ is flat, then so is $X_{\geq 0}$. This proves our claim. □

Henceforth, we assume that X is finitely generated, hence free. Let $\{\alpha_1, \ldots, \alpha_k\}$ be a $\mathbb{Z}$-basis of X such that $\alpha_i > 0$ for each i. Then $X_{\geq 0}$ can be identified with the semilattice $S = \{(n_1, \ldots, n_k) \in \mathbb{Z}^k : \sum_i n_i \alpha_i \geq 0\}$.

Define $\gamma := (\alpha_1, \ldots, \alpha_n) \in \mathbb{R}^n$ and the hyperplane $L := \{\mathbf{v} \in \mathbb{R}^n : \mathbf{v} \cdot \gamma = 0\}$. Then $S = \{\mathbf{v} \in \mathbb{Z}^n : v \cdot \gamma > 0\} \cup \{0\}$. Let $\mathbf{V} = \{\mathbf{v} \in \mathbb{R}^n : v \cdot \gamma > 0\} \cup \{0\}$.

Lemma 18.2. *Suppose $M \subseteq S$ is finitely generated over $\mathbb{N}$. To show that M is contained in a finitely generated free submodule of S, it is sufficient to find vectors $v_1, \ldots, v_n \in \mathbb{Z}^n$ such that*

(i) $X = (v_1 | v_2 | \ldots | v_n) \in GL(n, \mathbb{Z})$,
(ii) $v_i \cdot \gamma > 0$, and

(iii) $\mathbb{R}_{\geq 0}\langle v_1, \ldots, v_n\rangle \supseteq M$.

Proof. The first two conditions would yield that $v_i \in S$ and that $\mathbb{N}\langle v_1, \ldots, v_n\rangle$ is free. This is, in fact, a consequence of the very general Lemma 18.3. Finally, if $m \in M$, then

$$\begin{aligned} & m \in \mathbb{R}_{\geq 0}\langle v_1, \ldots, v_n\rangle \\ \implies & m = \sum_{i=1}^{n} \lambda_i v_i \text{ for some } \lambda_i \in \mathbb{R}_{\geq 0} \\ \implies & (\lambda_1, \ldots, \lambda_n) = \sum_{i=1}^{n} \lambda_i e_i = X^{-1} \sum_{i=1}^{n} \lambda_i v_i = X^{-1} m \in \mathbb{Z}^n. \end{aligned}$$

So $\lambda_i \in \mathbb{Z} \cap \mathbb{R}_{\geq 0} = \mathbb{N}$. Hence, $M \subseteq \mathbb{N}\langle v_1, \ldots, v_n\rangle$, proving our claim. □

Lemma 18.3. *Let S be a cancellative semiring, $R = S \otimes_{\mathbb{N}} \mathbb{Z}$, M an S-module, and $M' = N \otimes_S R$. If M is generated by n elements and $M' \cong R^n$, then M is generated freely by these n generators.*

Proof. Consider the diagram

$$\begin{array}{ccccc} S^n & \hookrightarrow & R^n & & \\ \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f_R} & \searrow^{g} & \\ M & \longrightarrow & M' & \xrightarrow{\sim} & R^n \end{array}$$

As $g : R^n \to R^n$ is surjective and R^n is a free R-module, g is an isomorphism. Hence, f_R is an isomorphism, which immediately implies that f is injective, proving our claim. □

For simplicity, we make the following definition.

Definition 19. A collection of vectors $V = \{v_1, \ldots, v_n\}$ is said to be "nice" if

(i) $(v_1 | \ldots | v_n) \in GL_n(\mathbb{Z})$, and
(ii) $v_i \cdot \gamma > 0$.

For $R = \mathbb{R}_{\geq 0}, \mathbb{N}$, its R-span is denoted by $Sp_R(V)$. Given a "nice" collection $V_0 = \{v_1, \ldots, v_n\}$, an *elementary refinement* is either of the following:

(i) If $1 \leq i \neq j \leq n$ are distinct indices such that $v_i \cdot \gamma > v_j \cdot \gamma$, then a collection $V' = \{v'_1, \ldots, v'_n\}$ of the form $v'_k = v_k$ if $k \neq i$ and $v'_i = v_i - v_j$.
(ii) A permutation $V_0^\sigma = \{v_{\sigma(1)}, \ldots, v_{\sigma(n)}\}$.

We say that another "nice" collection $W = \{w_1, \ldots, w_n\}$ *refines* V if there is a finite sequence of "nice" collections $\{V_n\}_{n=0}^{N}$ such that each V_i is an elementary refinement of V_{i-1}, $V_0 = V$ and $V_N = W$. We would denote this as $V \preceq W$.

It is immediate that $\preceq$ is a partial preorder and that $V \preceq W \preceq V$ if and only if V is a permutation of the indices of W.

Lemma 19.1. *To prove the theorem, it suffices to show that given any "nice" collection W and a vector $m \in S$, there is another "nice" collection V refining W such that $m \in Sp_{\mathbb{R}_{\geq 0}}(V)$.*

Proof. Easy induction. □

REMARK 8.1. It is tempting to think that $V \preceq W$ if and only if $Sp_{\mathbb{N}}(V) \subseteq Sp_{\mathbb{N}}(W)$. Although such an claim is true for $\mathbb{Z}$-spans, or when $n = \dim_{\mathbb{Z}}(X) = 2$, this claim is not true for $n \geq 4$ (thanks to Bryce Kerr). We are yet to find an example for $n = 3$.

The rest of the proof would essentially be an effort to prove the hypothesis of the preceding lemma. That is, given any "nice" collection $W \in \mathbb{Z}^n$ and a vector $m \in S$, we would try to find another "nice" collection V such that $\mathbb{R}_{\geq 0}\langle v_1, \ldots, v_n\rangle \supseteq \{w_1, \ldots, w_n, m\}$. To do this, we move on to part (ii). To study $\mathbb{R}_{\geq 0}$ spans, it suffices to study their homothetic projections onto a fixed hyperplane. So let

$$\begin{aligned} H =& \{x \in \mathbb{R}^n : x \cdot \gamma = 1\}, \\ p :& \mathbf{V} \longrightarrow H \\ & x \longmapsto \frac{x}{x \cdot \gamma} \end{aligned}$$

Also, observe that for $v \in S$, $p(v) = p(w) \iff (v-w)\cdot\gamma = 0 \iff (v-w) = 0$ as $\alpha_1, \ldots, \alpha_n$ are linearly independent over $\mathbb{Z}$. Hence, we may define an inverse map $g : p(S) \to S$. For $v \in V$, define $|v|_\gamma = v \cdot \gamma$. Also, we will say $p(v) >_\gamma p(v')$ for $v, v' \in S$ if $v \cdot \gamma > v' \cdot \gamma$. This is a total order by the above observation.

Given a "nice" collection $W = \{w_1, \ldots, w_n\}$, define $\mathcal{M}(W)$ as the set of all refinements of W. By the previous lemma, it suffices to show that the union

$$\bigcup_{\{v_1,\ldots,v_n\} \in \mathcal{M}(W)} \mathbb{R}_{\geq 0}\langle v_1, \ldots, v_n\rangle = \mathbf{V}.$$

By taking projections, this is equivalent to showing

$$\mathcal{O}(W) = \bigcup_{\{v_1,\ldots,v_n\}} p(\mathbb{R}_{\geq 0}\langle v_1, \ldots, v_n\rangle) = \bigcup_{\{v_1,\ldots,v_n\}} \operatorname{conv}(p(v_1), \ldots, p(v_n)) = H,$$

where conv(.) is the convex hull and the union is taken over $\mathcal{M}(W)$.

To prove that this is indeed the case, we prove multiple lemmas.

Lemma 19.2. *Given any "nice" collection $W = \{w_1, \ldots, w_n\}$ and a collection of indices $J \subseteq \{1, \ldots, n\}$ with $|J| \geq 2$ and any $\delta > 0$, there is a "nice" collection $\{v_1, \ldots, v_n\} \in \mathcal{M}(W)$ such that*

(i) $v_i = w_i$ if $i \notin J$,
(ii) $v_i \cdot \gamma < \delta$ for every $i \in J$, and
(iii) $w_i \in \mathbb{N}\langle v_j | j \in J\rangle$ for each $i \in J$.

Proof. Fix two distinct indices $j_1, j_2 \in J$ and let $x_i = w_{j_i}$. Without loss of generality, let $|x_1|_\gamma < |x_2|_\gamma$ Let $G = \{M \in GL(2,\mathbb{Z}) | M^{-1} \in M(2,\mathbb{N})\}$. Then G is closed under multiplication. We would now produce inductively a sequence of vectors $x^{(n)} = \{x_1^{(n)}, x_2^{(n)}\}$ such that

(i) $x_i^{(0)} = x_i$ for $i = 1, 2$,
(ii) $|x_2^{(n)}|_\gamma > |x_1^{(n)}|_\gamma > 0$ for $n \geq 0$,
(iii) $x^{(n+1)}$ is a refinement of $x^{(n)}$, and
(iv) If $m_n = x_2^{(n)} \cdot \gamma$, then $m_{n+1} < m_n/2$.

The base case is immediate. So we proceed by induction. Assume that we are given $x^{(n)}$. Let $m \geq 1$ be such that $m|x_1^{(n)}|_\gamma < |x_2^{(n)}|_\gamma < (m+1)|x_1^{(n)}|_\gamma$. The injectivity of $x \mapsto x \cdot \gamma$ on $\mathbb{Z}^n$ ensures a strict inequality. Let $x_2^{(n+1)} = x_2^{(n)} - mx_1^{(n)}$. Clearly $0 < |x_2^{(n+1)}|_\gamma < |x_1^{(n)}|_\gamma$. So, let $m' \geq 1$ be such that $m'|x_2^{(n+1)}|_\gamma < |x_1^{(n)}|_\gamma < (m'+1)|x_2^{(n+1)}|_\gamma$ and let $x_1^{(n+1)} = x_1^{(n)} - mx_2^{(n+1)}$. It follows that $0 < |x_1^{(n+1)}|_\gamma < |x_2^{(n+1)}|_\gamma$ and that $x^{(n+1)}$ is a refinement of $x^{(n)}$. Finally, $2m_{n+1} < (1 + mm')|x_2^{(n+1)}|_\gamma + m|x_1^{(n+1)}|_\gamma = |x_2^{(n)}|_\gamma = m_n$, as desired.

By choosing n large enough, we have found a matrix $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ in G and vectors v_1, v_2 such that $0 < |ax_1 + bx_2|_\gamma, |cx_1 + dx_2|_\gamma < \delta$. Let $v_{j_1} = ax_1 + bx_2$, $v_{j_2} = cx_1 + dx_2$. For $j \in J$, $j \neq j_i$, choose k_j such that $k_j|v_{j_1}|_\gamma < |w_j|_\gamma < (k_j+1)|v_{j_1}|_\gamma$ and let $v_j = w_j - k_j v_1$. Also, for $j \notin J$, let $v_j = w_j$. It is immediate that this collection has the desired properties. □

Lemma 19.3. *Given any two indices $1 \leq i < j \leq n$, the complete line through $p(w_i)$ and $p(w_j)$ is in $\mathcal{O}(W)$.*

Proof. By Lemma 19.2, we can construct a sequence $W^{(n)} = \{w_k^{(n)}\}$ of "nice" collections such that $w^{(n+1)} \in \mathcal{M}(w^{(n)})$, $w_k^{(n)} = w_k$ if $k \neq i, j$ and $0 < w_k^{(n)} \cdot \gamma < \frac{1}{n}$. Let $x_n = w_i^{(n)}, y_n = w_j^{(n)}$. From the construction in Lemma 19.2, it is clear that there are integers $a_n, b_n, c_n, d_n \geq 0$ such that $a_n d_n - b_n c_n = 1, x_n = a_n x_{n+1} + b_n y_{n+1}$ and $y_n = c_n x_{n+1} + d_n y_{n+1}$. Thus, the line segments L_n that join $p(x_n)$ and $p(y_n)$ form an ascending chain. Thus, it suffices to show that the usual absolute values $|p(x_n)|, |p(y_n)|$ diverge to infinity. But

$$|p(x_n)| = \frac{|x_n|}{x_n \cdot \gamma} > n|x_n| \geq n$$

as x_n has integer coordinates. So we are done.

□

Note that, in fact, this completes the proof when $n = 2$. We point out a notable similarity of the arguments presented in the previous two lemmas to the theory of continued fractions and convergents.

Lemma 19.4. *Let $n \geq 3$. Given any $V = \{v_1, \ldots, v_n\} \in \mathcal{M}(W)$ and any pair of indices $1 \leq i, j \leq n$, such that $p(w_i) > p(w_j)$ there is a $U = \{u_1, \ldots, u_n\} \in \mathcal{M}(V)$ such that $p(w_i - w_j) \in \operatorname{conv}(p(u_1), \ldots, p(u_n))$.*

Proof. Without loss of generality, assume that $i = 1, j = 2$. As V is a $\mathbb{Z}$-basis of $\mathbb{Z}^n$, there are integers μ_k such that $e = w_1 - w_2 = \sum_k \mu_k v_k$. Let $\gamma_k = v_k \cdot \gamma > 0$. So,

$$\sum_k \mu_k \gamma_k = e \cdot \gamma > 0.$$

Suppose Q is the number of $1 \leq k \leq n$ such that $\mu_k < 0$.

CASE I: $Q = 0$
Just choose $U = V$.

CASE II: $Q = 1$
By possibly permuting the vectors, assume that $\mu_1 = -s < 0$. Let $\delta = \frac{1}{2sn} \min\{e \cdot \gamma, \gamma_1\}$. By Lemma 19.2, we get a $U' = \{u'_1, \ldots, u'_n\} \in \mathcal{M}(V)$ such that $0 < |u'_j|_\gamma < \delta$ for each $j \geq 2$ and $u_1 = v_1$. Furthermore, $v_k \in \mathbb{N}\langle u'_j | j \geq 2\rangle$ for $k \geq 2$. So, $w_1 - w_2 = \sum_j \mu_j u'_j$ where $\mu'_1 = \mu_1$ and $\mu'_j \geq 0$ if $j \geq 2$.

Firstly, observe that

$$\begin{aligned}\delta \sum_{j \geq 2} \frac{\mu'_j}{s} &> \sum_{j \geq 2} \frac{\mu'_j u'_j \cdot \gamma}{s} \\ &= \frac{s\gamma_1 + e \cdot \gamma}{s} \\ &> \gamma_1 \geq 2sn\delta\end{aligned}$$

Hence, $\sum_{j \geq 2} \frac{\mu'_j}{s} \geq 2sn \geq 2n$. Thus, there is a $j \geq 2$ such that $\frac{\mu_j}{s} > 1$. By a possible permutation of indices, assume $\mu_n > s$.

Now we claim that there are integers $\lambda_j, j \geq 2$ such that

(i) $\lambda_j s \leq \mu_j$ if $2 \leq j < n$,
(ii) $(\lambda_n + 1)s \leq \mu_n$,
(iii) If $\eta = \sum_{j \geq 2} \lambda_j u'_j$, then $\gamma_1 > \eta \cdot \gamma$, and
(iv) For each $j \geq 2$, $u'_j \cdot \gamma > \gamma_1 - \eta \cdot \gamma$.

If not, as there are only finitely many cases to be considered, it turns out that the maximal choice for λ_j, that is,

$$\lambda_j = \left\lfloor \frac{\mu'_j}{s} \right\rfloor - \delta_{j,n}$$

should not satisfy the last condition. In particular, we should have

$$\begin{aligned}\gamma_1 &> \sum_{j\geq 2} \lambda_j u'_j \cdot \gamma \\ &> \sum_{j\geq 2} \frac{\mu'_j u'_j}{s} \cdot \gamma - 2u'_j \cdot \gamma \\ &= \frac{e\cdot\gamma}{s} + \gamma_1 - 2\sum_j u'_j \cdot \gamma \\ &> \frac{e\cdot\gamma}{s} + \gamma_1 - 2n\delta.\end{aligned}$$

That is $e \cdot \gamma < 2ns\delta$, a contradiction. So we have a desirable set of integers λ_j. Finally, define

$$u_j = \begin{cases} u'_1 - \eta & j = 1 \\ u'_j + \eta - u'_1 & j \geq 2 \end{cases}$$

It is immediate that $U = \{u_1, \ldots, u_n\} \in \mathcal{M}(U') \subseteq \mathcal{M}(V)$. Furthermore,

$$w_1 - w_2 = \left(\left(\sum_{j\geq 2} (\mu_j - s\lambda_j) \right) - s \right) u_1 + \sum_{j\geq 2} (\mu_j - s\lambda_j) u_j$$

proving our claim.

CASE III: $Q \geq 2$

By a possible permutation of vectors, suppose $\mu_1, \ldots, \mu_t < 0$ and $\mu_{t+1}, \ldots, \mu_n \geq 0$. Observe that the constraint on the sign says that $t < n$. Let $M = \sum_{k>t} \mu_k$ and $\delta = 2nM^{-1} \min(\gamma_{t+1}, \ldots, \gamma_n) > 0$. Then we may use Lemma 19.2 to get a $U' = \{u'_1, \ldots, u'_n\} \in \mathcal{M}(V)$ such that $0 < |u'_j|_\gamma < \delta$ for each $j \leq t$ and $u_j = v_j$ if $j > t$. Also, writing $e = \sum_k \mu'_k u'_k$, we get $\mu'_k < 0$ if $k \leq t$ and $\mu'_k = \mu_k$. We claim the existence of a $Z = \{z_1, \ldots, z_n\} \in \mathcal{M}(U')$ such that if $e = \sum \theta_k z_k$, then $\theta_k = \mu'_k$ if $k \neq t$ and $\theta_t > 0$. Rest would follow from induction and a reduction to Case II.

For $k \geq t+1$, let λ_k be the integers such that $(u'_k - \lambda_k u'_t) \cdot \gamma > 0$ and $\sum_k \mu_k \lambda_k > -\mu'_t$. The existence of such λ_k's is guaranteed by the condition that $e \cdot \gamma > 0$. Now let

$$z_i = \begin{cases} u'_i & i \leq t \\ u'_i - \lambda_i u'_t & i > t. \end{cases}$$

Then

$$\begin{aligned} e &= \sum_k \mu'_k u'_k \\ &= \sum_{k<t} \mu'_k u'_k + \sum_{k>t} \mu'_k (u'_k - \lambda_k u'_t) + \left(\mu'_t + \sum_{k \geq t+1} \mu_k \lambda_k \right) u'_t. \\ &= \sum_{k \neq t} \mu'_k z_k + \theta_t z_t \end{aligned}$$

where $\theta_t = \sum_{k \geq t+1} \mu_k \lambda_k + \mu'_t > 0$. This completes the proof. □

Lemma 19.5. *For any "nice" W, $\mathcal{M}(W)$ is a directed set under refinement.*

Proof. It suffices to show that given any refinement V of W and an elementary refinement W' of W, there is a common refinement of V, W'. If W' is a permutation, then V itself is the common refinement. If W' involves a subtraction, one uses Lemma 19.4 to obtain the desired refinement. □

Lemma 19.6. *For any "nice" $W = \{w_1, \ldots, w_n\}$, $\mathcal{O}(W)$ is H.*

Proof. From Lemma 19.5, $\mathcal{M}(W)$ is a directed collection and hence $\{p(V) : V \in \mathcal{M}(W)\}$ is a directed collection of convex sets. So their union, $\mathcal{O}(W)$ is a convex set as well. Additionally, from Lemmas 19.3 and 19.4, we get that $\mathcal{O}(W)$ contains $n-1$ independent lines (in both directions) starting at any fixed vector v. The only such convex set is indeed the whole of H, proving our claim. □

This completes the proof of the theorem.

Acknowledgments: The author would like to thank Professor James Borger, his PhD supervisor, for his guidance and support. Most of the problems and the work presented here were consequences of several fruitful discussions on semirings and their theory with him. The author would also like to thank the Australian National University and the committee of Deakin PhD Scholarship for supporting his PhD, both academically and financially, as the work was entirely done during the course.

References

[1] J. Borger and J. Jun. *Facets of module theory over semirings.* arXiv:2405.18645 [math.AG], 2025. `https://arxiv.org/abs/2405.18645`.

[2] J. S. Golan. *Semirings and Their Applications.* Springer Netherlands, 1999. ISBN: 9780792357865. `https://books.google.com.au/books?id=DNdTF_4PzpoC`.

[3] J. Abuhlail and R. G. Noegraha. *On k-Noetherian and k-Artinian Semirings*. arXiv:1907.06149 [math.RA], 2019. `https://arxiv.org/abs/1907.06149`.

[4] L. Dale and P. J. Allen. Ideal theory in polynomial semirings. *Publicationes Mathematicae Debrecen*, 23(3–4):183–190, 1976. doi:10.5486/pmd.1976.23.3-4.02.

[5] P. J. Allen. Cohen's theorem for a class of Noetherian semirings. *Publicationes Mathematicae Debrecen*, 17:169–171, 1970. doi:10.5486/pmd.1970.17.1-4.19.

[6] Y. Katsov. On flat semimodules over semirings. *Algebra Universalis*, 51(2–3):287–299, 2004. doi:10.1007/s00012-004-1865-1.

[7] P. J. Allen, J. Neggers, and H. S. Kim. Ideal theory in commutative A-semirings. *Kyungpook Mathematical Journal*, 46(2):261–271, 2006.

[8] J. Borger. Witt vectors, semirings, and total positivity. In *Absolute Arithmetic and $\mathbb{F}_1$-Geometry*, pp. 273–329. European Mathematical Society, Zürich, 2016. ISBN: 978-3-03719-157-6.

[9] L. Dale and P. J. Allen. An extension of the Hilbert basis theorem. *Publicationes Mathematicae Debrecen*, 27(1–2):31–34, 1980. doi:10.5486/pmd.1980.27.1-2.06.

[10] J. Borger and D. Grinberg. Boolean Witt vectors and an integral Edrei–Thoma theorem. *Selecta Mathematica*, 22(2):595–629, 2015. doi:10.1007/s00029-015-0198-6.