Bar Inductive Predicates for Constructive Algebra in Rocq

Dominique Larchey-Wendling
Université de Lorraine, CNRS, LORIA
Vandœuvre-lès-Nancy, France
dominique.larchey-wendling@loria.fr

Abstract

In constructive commutative algebra, we revive the Bar inductive characterization of Noetherian rings. We contribute the first constructive (axiom free) implementation of Hilbert's Basis Theorem, in the Rocq proof assistant. We show that the polynomial ring $\mathcal{R}[X]$ is Noetherian when the ring $\mathcal{R}$ is Noetherian, without assuming any additional condition on $\mathcal{R}$, like coherence or else strong discreteness. We also contribute and implement a new result, that Noetherian rings are closed under direct products, again without assuming any supplementary condition on rings. We study induction principles for Noetherian rings, and relate Bar Noetherianity with some other constructive characterizations.

Keywords: Constructive algebra, Noetherian rings, bar inductive predicates, Hilbert basis theorem, Rocq

1 Introduction

Bar inductive predicates, which are linked to but should not be conflated with bar induction, are siblings to Acc(cessibility) predicates, the de facto approach to well-foundedness in the (constructive) Rocq standard library. Bar inductive predicates have been used successfully to give constructive and axiom free[1] accounts of the FAN theorem [3, 7], Ramsey's theorem and Higman's lemma [6], and more generally of well quasi order (WQO) theory through the equivalent notion of inductive almost full (AF) relation [11, 26]. The accessibility predicate and more generally, bar and cover inductive predicates, give a way to quantify over arbitrary sequences, including "lawless" sequences which are (constructively) beyond the reach of the type $\mathbb{N} \to A$ of "lawlike" sequences, that are used in ascending (or descending) chain conditions [3, 12].

[1] in particular, without assuming "Brouwer's thesis" [25].

Conference'17, July 2017, Washington, DC, USA

ACM ISBN 978-x-xxxx-xxxx-x/YY/MM…$15.00
https://doi.org/10.1145/nnnnnnn.nnnnnnn

Using those predicates, one can work constructively, avoiding excluded middle (XM) and dependent choice (DC). Coquand&Persson [5] exploit bar inductive predicates beyond WQO theory and apply them to constructive algebra, giving a bar predicate characterization of Noetherian rings. This allows them to prove Hilbert's Basis theorem (HBT) constructively, moreover *free of any further assumption on the rings* like coherence or else strong discreteness (or both) [4], or variants of these notions [10, 14–16, 20]. The focus of [5] is a certified algorithm for Gröbner bases and the proof of the HBT was only outlined on paper, and not implemented. Despite this initial promising result – a nice and short constructive proof of the HBT, – the bar predicate approach to Noetherianity apparently did not get much traction later on. And, up to now, despite many constructive variants of the HBT, it seems that none of them have actually been implemented in constructive theorem provers, as opposed to classical versions of the theorem, see e.g. [18] but the HBT can also be found in the Mathlib Lean library.[2]

In this work, we propose to follow those footsteps [5] and revive the bar predicate approach to Noetherian rings with a first constructive implementation of the HBT in Rocq, revisiting their pen&paper proof, and also explaining why, in our opinion, that implementation work might have been out of reach at the time [17]. As a second contribution, we adapt the bar inductive proof of Ramsey's theorem [6] and derive a new result: Noetherian rings are closed under direct products, constructively, *without assuming strong discreteness*, as opposed to e.g. [20]. With a Rocq implementation as well.

1.1 Noetherian rings in constructive algebra

We work with commutative rings of which we assume the theory for now. Recall that ideals are subsets of rings closed under linear combinations. An ideal is *finitely generated* if there is a list of its members generating the whole ideal by linear combinations. An ideal is *principal* if it is generated by a singleton. We focus our work on those properties of ideals.

In classical algebra, a *principal ring* has only principal ideals: typical examples include the ring of integers $\mathbb{Z}$ or the ring $\mathcal{F}[X]$ of univariate polynomials over a field $\mathcal{F}$. However $\mathcal{F}[X, Y]$ or $\mathbb{Z}[X]$ are not principal rings. They are nonetheless *Noetherian rings* where every ideal is finitely generated. The original statement of the HBT was:

[2] https://leanprover-community.github.io/mathlib-overview.html

$\mathcal{F}[X_1,\ldots,X_n]$ is a Noetherian ring if $\mathcal{F}$ is a field

and its initial proof, given by David Hilbert [9], was allegedly qualified as "theology" by Paul Gordan[3] because of its non-constructive nature. Later on the HBT was given the form

if $\mathcal{R}$ is a Noetherian ring then so is $\mathcal{R}[X]$

which is more general and is the usually accepted formulation of the HBT in constructive algebra, however with a mandatory update of the definition of "Noetherian ring."

Indeed, to convert the HBT to constructive algebra, one has first to acknowledge that the notions of principal or of Noetherian ring, as defined classically above, are *useless* when interpreted in constructive contexts. In intuitionistic logic (w/o XM), there are too many propositions and hence, too many subsets and ideals. And with such classical definitions, if one can show that the ring $\mathbb{Z}$ (or even just $\mathbb{Z}/2\mathbb{Z}$) is Noetherian (all the more principal), then this entails XM. This observation is often recalled in papers about constructive algebra, and can be made in Bishop's constructive mathematics [14] or in type theory, as we explain in Section 2.2. So one cannot prove that those basic rings are principal or even Noetherian unless one assumes XM. When working in an anticlassical setting, where XM is actually refuted by the assumption of other axioms, one can even show that $\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z}$ are not Noetherian.

Hence, constructively, the classical characterizations of principal and Noetherian rings are usually considered flawed and this has given rise to a large body of work with several competing definitions. The notion of principal ring can be replaced by the notion of Bezout domain: every finitely generated ideal is principal, see e.g. [4]. The constructive notion of Noetherian ring has been given several variations:

- **RS-Noetherian:** any infinite increasing sequence of finitely generated ideals pauses, by Richman [19] and Seidenberg [21];
- **ML-Noetherian:** strict reverse inclusion is (Martin-Löf) well-founded on finitely generated ideals [10];[4]
- **Strongly Noetherian:** finitely generated ideals ordered by strict inclusion are (explicitly) embedded into an well-ordered set [14];
- **Bar Noetherian:** growing finite sequences of finitely generated ideals unavoidably reach a pause, expressed using a bar inductive predicate [5], the one we work with herein;

not claiming exhaustivity for this list.

All these characterizations of Noetherian rings are equivalent to the classical one in a classical context, e.g. assuming XM and DC, but in constructive contexts, they are not equivalent although they may be related modulo some extra hypotheses on rings like coherence or strong discreteness or both. Considering the HBT, [19, 21] show that "if $\mathcal{R}$ is RS-Noetherian and coherent then so is $\mathcal{R}[X]$." In [10], they prove that "if $\mathcal{R}$ is ML-Noetherian, coherent and strongly discrete then so is $\mathcal{R}[X]$."

On the other hand, [5] gives a proof that "if $\mathcal{R}$ is Bar Noetherian then so is $\mathcal{R}[X]$." Moreover, they do not even assume discreteness of the ring. We see that bar inductive predicates allow an orthogonal treatment of Noetherianity and coherence or strong discreteness, at least with respect to the HBT. We confirm this observation with a original proof that (Bar) Noetherian rings are closed under direct products, again w/o assuming strong discreteness, contrary to the Proposition 13 and Theorem 14 of [20] where a similar result is obtained for strongly discrete RS-Noetherian rings. With this work, we hope to revive the interest in bar inductive predicates for constructive algebra and beyond.

1.2 Contents of the paper

In Section 2, we define rings using setoids, types equipped with a pending quotient, so we can confirm by an implementation the most general form of the HBT stated in [5]. Indeed, when we do not assume discreteness for rings,[5] polynomials cannot be given a normal form, so we work with rings up to the equivalence relation given in the setoid. We define ideals, and give two characterizations of finitely generated ideals. We discuss the shortcomings of the classical characterizations of Noetherian rings and of principal rings in constructive type theory. We introduce `bar` inductive predicates and, based on the definition of pausing lists, following [5], we characterize (Bar) Noetherian rings. Using Bezout, we show that $\mathbb{Z}$, the ring of integers, is Noetherian.

In Section 3, we present our original proof that the direct product of two Noetherian rings is a Noetherian ring, that we obtain by reworking and adapting a former proof of a constructive interpretation of Ramsey's theorem [6]. We explain this adaptation and where the two proofs diverge.

In Section 4, we explain how we implement the polynomial ring, discuss alternatives, and give the categorical characterizations of polynomial rings. We formulate and show a critical observation that allows updates on finitely generated ideals of univariate polynomial rings, used in base case of the short (but sophisticated) inductive proof of the HBT.

In Section 5, we detail the first implementation of a constructive proof of the HBT, revisiting the pen&paper outline of [5]. We use the above updates and a tailored lexicographic induction principle. From our experience, we elaborate on why that implementation work might have been unsuccessful (or avoided) at the time.

In Section 6, we derive well-founded induction principles for (Bar) Noetherian rings and compare that notion with the alternate constructive characterizations of RS- and ML-Noetherian rings, when assuming strongly discrete rings.

[3] b.t.w. Paul Gordan was also the later advisor of Emmy Noether.

[4] recall the Definition 3.4 of ML-Noetherian rings in [10] additionally assumes that those rings are coherent with a membership algorithm.

[5] i.e. the ability to distinguish zero from nonzero elements in a ring.

Remarks for reviewers: the results in this submission are backed by an axiom free Rocq artifact readily available. Consult the README file for compile and review instructions. Later on, should the submission be accepted, it would be updated and linked to a publicly available repository, and distributed under the same MPL v2.0 free software license.

1.3 Rocq preliminaries

We briefly recall the basics of Rocq's inductive type theory which distinguishes (logical) propositions in the type `Prop` (denoted $\mathbb{P}$ for short) and computational contents in the type hierarchy `Type`. We assume arithmetic using the type of Peano natural numbers $\mathbb{N}$ and lists in `list` A, polymorphic over a carrier type A. Using a, b for values of type A and l, m for values in `list` A, we write $[]$ for the empty list, $a :: l$ (resp. $l +\!\!+ m$) for the consing of a head element (resp. appending lists) as defined in the `List` module. We write $[a_0; \ldots; a_{n-1}]$ for enumerated lists, and $[a]$ for singletons.[6] Recall the identity $a :: l = [a] +\!\!+ l$ that holds by definition. We write $|l|$ for the length of the list l, and $a \in l$ for the membership predicate, with which we define the carrier of a list $\lfloor l \rfloor : A \to \mathbb{P}$ as $\lfloor l \rfloor := \lambda\, a, a \in l$, and which collects its elements in a subset.

We denote P, Q for *subsets* viewed as predicates in $A \to \mathbb{P}$, and R, T for *binary relations* in $A \to B \to \mathbb{P}$. We use the standard $\subseteq$ notation for either unary or binary predicate inclusion, and write $\equiv$ for extensional equivalence, hence for instance, $\lfloor l \rfloor \subseteq P$ means that all the members of l satisfy property P, and $\lfloor l \rfloor \equiv \lfloor m \rfloor$ means that the two lists have the same members. We use the same notations in the Rocq code, there possibly subscripted by arities like in $\subseteq_2$ or $\equiv_1$.

We manipulate finite sets as predicates $P : A \to \mathbb{P}$ s.t. $P \equiv \lfloor l \rfloor$ holds for some list l, i.e. listable predicates. In the prose, when we define inductive predicates, we use visual rules, as premises above a conclusion, instead of Rocq's `Inductive` statements, hoping they are easier to grasp in this form. Free named parameters (or indices) should then to be understood as universally quantified over.

2 Rings and Ideals in Constructive Algebra

We work in *commutative algebra* and do not consider the non-commutative case herein. We recall the definition of rings and ideals, and discuss the shortcomings of the classical characterizations of principal and Noetherian rings in constructive type theory. We introduce bar inductive predicates and define (Bar) Noetherian rings with them.

To avoid foundational issues related to quotients in Rocq, or else avoid assuming rings to be discrete, we use the `Setoid` framework [22] for generalized rewriting and hence use a congruence in place of the identity relation to represent ring equations. We will discuss this choice in more details in Section 4 when dealing with polynomial rings.

A *ring* is a structure $\mathcal{R} = (\mathcal{R}, +, -, \times, 0, 1, \sim)$ where $\mathcal{R}$ is a type, $(\mathcal{R}, +, -, 0, \sim)$ is a commutative group forming the additive part of the ring ($-$ is the additive inverse operator), while $(\mathcal{R}, \times, 1, \sim)$ is a commutative monoid forming the multiplicative part of the ring. Last, $\times$ distributes over $+$. A *(discrete) field* is a ring where every value is either equivalent to 0 or has a multiplicative inverse.[7] Notice the equivalence relation $\sim$ that is required to be a congruence for $+$, $-$ and $\times$, and moreover, the monoids laws and the distributivity law should be understood up to this equivalence. So for instance the distributivity law becomes $z \times (x + y) \sim z \times x + z \times y$, with the usual precedence of $\times$ over $+$ for these infix notations.

Rocq allows to define such a dependent type `ring` as `Record` structure and overload the notation $\mathcal{R}$ which can be interpreted both as a `ring` structure or as the carrier type for the elements of the ring $\mathcal{R}$ and we make use of the facility in the file `ring.v`. In our implementation, we decorate the ring operators and the equivalence with a suffix "r" as in e.g. $+_r$ to avoid ambiguity with operations on natural numbers. We do not do this in the paper and hope ambiguities can easily be avoided. Rocq however might need to infer which ring do the operators refer to. Often this is solved by the context and unification: if $x : \mathcal{R}$ then Rocq infers that $+$ and 0 refer to the ring $\mathcal{R}$ in the expression $x + 0$. However, the expression $0 + 1 \sim 1$ is ambiguous for Rocq and we sometimes have to hint it to the proper ring through type annotations like e.g. $(0 : \mathcal{R}) + 1 \sim 1$, provided $\mathcal{R}$: `ring` belongs to the context.

Additionally, we exploit the instruments of the `Ring` and `Setoid` modules (which where designed to work together), so that solving ring equations $e_1 \sim e_2$ and rewriting expressions up to $\sim$ becomes effortless. One simply declares ring operators as `Morphisms` and subscribes rings to the `Ring` module to exploit these instruments in the local context.

A *ring homomorphism* is a map between two rings preserving congruences, addition and multiplication operators, and the multiplicative unit 1. As a consequence, they also preserve $-$ and 0. *ring sub-homomorphisms* have a relaxed definition and do not have to preserve the unit 1, but instead they preserve the unit 0 (hence also $-$). Forming a *quotient* ring in the context of setoids is straightforward: for the ring $(\mathcal{R}, +, -, \times, 0, 1, \sim)$, one simply picks up a new congruence $\sim'$ which over approximates $\sim$ (i.e. $\sim \subseteq \sim'$), and then one updates $\sim$ with $\sim'$ in the structure. The identity map $(\mathcal{R}, +, -, \times, 0, 1, \sim) \to (\mathcal{R}, +, -, \times, 0, 1, \sim')$ automatically becomes a surjective ring homomorphism on the quotient.

2.1 Ring ideals

Ring ideals are a fundamental notion of algebra. They are the kernels of ring homomorphisms. An *ideal of a ring* $\mathcal{R}$ is a subset $\mathcal{I} : \mathcal{R} \to \mathbb{P}$ of $\mathcal{R}$ containing 0 (i.e. $\mathcal{I}\ 0$) and closed under $\sim$ (i.e. $\forall\, x\, y : \mathcal{R},\ x \sim y \to \mathcal{I}\ x \to \mathcal{I}\ y$), addition/$+$ (i.e. $\forall\, x\, y : \mathcal{R},\ \mathcal{I}\ x \to \mathcal{I}\ y \to \mathcal{I}\ (x + y)$) and scalar products

[6] Enumerated lists are mostly used in the prose for reader friendliness.

[7] The assumption $\forall x,\ x \sim 0\ \vee \exists i,\ i \times x \sim 1$ entails discreteness.

(i.e. $\forall\, a\, x : \mathcal{R},\ \mathcal{I}\, x \to \mathcal{I}\, (a \times x)$). We skip the obvious Rocq definition here but we denote $\texttt{ideal}\,\mathcal{I}$ for the proposition stating that $\mathcal{I}$ is an ideal of the ring $\mathcal{R}$.[8] That definition and the constructions and results we describe and claim below are implemented in the file `ideal.v`.

We are especially interested in ideals that are generated by some elements, in particular finitely many of them, and how to handle these. Given a subset $P : \mathcal{R} \to \mathbb{P}$ of $\mathcal{R}$, we define $\texttt{idl}\, P : \mathcal{R} \to \mathbb{P}$ inductively using the following rules:

$$\frac{x \sim y \qquad \texttt{idl}\, P\, x}{\texttt{idl}\, P\, y} \qquad \frac{P\, x}{\texttt{idl}\, P\, x} \qquad \frac{}{\texttt{idl}\, P\, 0}$$

$$\frac{\texttt{idl}\, P\, x \qquad \texttt{idl}\, P\, y}{\texttt{idl}\, P\, (x + y)} \qquad \frac{\texttt{idl}\, P\, x}{\texttt{idl}\, P\, (a \times x)}$$

and we (obviously) obtain the smallest ideal containing P, i.e. the *ideal generated by* P. Notice that the definition of $\texttt{idl}\, P\, x$ proceeds by induction on the algebraic structure of x.

Alternatively, for a list $l : \texttt{list}\, \mathcal{R}$, we define $\texttt{lc}\, l : \mathcal{R} \to \mathbb{P}$ ($\texttt{lc}$ stands for linear combination) inductively with the rules:

$$\frac{0 \sim x}{\texttt{lc}\, []\, x} \qquad \frac{a \times x + z \sim y \qquad \texttt{lc}\, l\, z}{\texttt{lc}\, (x :: l)\, y}$$

following the structure of the list l (rather than that of x) and then $\texttt{lc}\, l$ is the smallest ideal containing the members of l. Indeed, we show the (extensional) identity

$$\texttt{idl}\, \lfloor l \rfloor \equiv \texttt{lc}\, l \qquad \text{for any } l : \texttt{list}\, \mathcal{R} \tag{1}$$

i.e. the subsets $\texttt{idl}\, \lfloor l \rfloor$ and $\texttt{lc}\, l$ of $\mathcal{R}$ contain the same members. They are finitely generated ideals, as they are generated by the members of a (finite) list of values. As a side remark, we can generalize the correspondence between $\texttt{idl}$ and $\texttt{lc}$ to a subset $P : \mathcal{R} \to \mathbb{P}$ with the following equivalence

$$\texttt{idl}\, P\, x \leftrightarrow \exists l,\ \lfloor l \rfloor \subseteq P \wedge \texttt{lc}\, l\, x \qquad \text{for any } x : \mathcal{R}$$

but we will not use it herein. We generally favor writing $\texttt{idl}\, \lfloor l \rfloor$ over the equivalent $\texttt{lc}\, l$ because it is more evocative.

Definition 2.1. Let $\mathcal{I} : \mathcal{R} \to \mathbb{P}$ be an ideal of the ring $\mathcal{R}$. $\mathcal{I}$ is a *finitely generated ideal* when there exists $l : \texttt{list}\, \mathcal{R}$ such that $\mathcal{I} \equiv \texttt{idl}\, \lfloor l \rfloor$. It is a *principal ideal* when there exists $g : \mathcal{R}$ such that $\mathcal{I} \equiv \texttt{idl}\, \lfloor [g] \rfloor$.

A ring is *Bezout* if all finitely generated ideals are principal. A ring is *strongly discrete* if finitely generated ideals are (logically) decidable sets, i.e. $\forall\, l\, x,\ \texttt{idl}\, \lfloor l \rfloor\, x \vee \neg \texttt{idl}\, \lfloor l \rfloor\, x$.

Notice that the definition we give for strong discreteness is weaker than the generally understood one, which interprets "decidable" in a computational way (see Section 6).

[8] The first argument $\mathcal{R}$ of $\texttt{ideal}\, \{\mathcal{R} : \texttt{ring}\}\ (\mathcal{I} : \mathcal{R} \to \mathbb{P})$ is implicit.

2.2 Shortcomings of classical definitions

In classical contexts (e.g. under XM and DC), all the ideals of $\mathbb{Z}$ and $\mathcal{F}[X]$ (for a field $\mathcal{F}$) are principal. But, $(\mathbb{Z}/m\mathbb{Z})[X]$ (with m composite), $\mathbb{Z}[X]$ and $\mathcal{F}[X, Y]$ all have non-principal ideals. They are however classically Noetherian in the sense that all their ideals are finitely generated. In this section, we explain why the classical characterizations of principal and Noetherian rings are inappropriate in constructive type theory, see file `noetherian_nc.v`.

Consider any ring $\mathcal{R}$ which is *discrete* (i.e. $\forall x : \mathcal{R},\ x \sim 0 \vee x \nsim 0$), and *non trivial* (i.e. $0 \nsim 1$). Typically, the ring $\mathbb{Z}$ (or even just $\mathbb{Z}/2\mathbb{Z}$) fits these two requirements. Let us fix an arbitrary proposition $P : \mathbb{P}$ and form the ideal $\mathcal{I}_P : \mathcal{R} \to \mathbb{P}$ defined by $\mathcal{I}_P\, x := x \sim 0 \vee P$. If $\mathcal{I}_P$ is finitely generated (a fortiori principal), then one can show $P \vee \neg P$. Indeed, let us assume a list l s.t. $\mathcal{I}_P \equiv \texttt{idl}\, \lfloor l \rfloor$. We discriminate between $\forall x,\ x \in l \to x \sim 0$ and $\exists x,\ x \in l \wedge x \nsim 0$, which is possible because $\mathcal{R}$ is discrete and l is a (finite) list. In the former case, we have $\mathcal{I}_P\, x \leftrightarrow \texttt{idl}\, \lfloor l \rfloor\, x \leftrightarrow x \sim 0$, hence $\neg \mathcal{I}_P\, 1$. As a consequence, $\neg P$ holds. In the later case, there is $x \in l$ s.t. $x \nsim 0$, hence $\mathcal{I}_P\, x$ holds, so $x \sim 0 \vee P$ and this entails P.

So if the ring $\mathcal{R}$ is classically Noetherian (a fortiori principal), then the ideal $\mathcal{I}_P$ is finitely generated and thus $P \vee \neg P$ holds. And this for any proposition $P : \mathbb{P}$. If we can prove that e.g. the ring of integers $\mathbb{Z}$ is Noetherian or principal in the classical understanding, then XM must hold and we are out of constructive logic. This renders these classical understandings inappropriate in constructive algebra.

2.3 Bar Noetherian rings

The above observation led to a wide range of alternative characterizations of Noetherian rings to fit constructive contexts, see e.g. [14]. We do not discuss them in detail here, see Section 6 for some comparisons. We rather directly introduce the bar predicate characterization used in [5].

2.3.1 Bar inductive predicates.

Given a type A and a predicate $P : \texttt{list}\, A \to \mathbb{P}$, we define $\texttt{bar}\, P : \texttt{list}\, A \to \mathbb{P}$ with the two inductive rules/constructors:

$$\frac{P\, l}{\texttt{bar}\, P\, l} \qquad \frac{\forall a,\ \texttt{bar}\, P\, (a :: l)}{\texttt{bar}\, P\, l}$$

$\texttt{bar}$ predicates are linked to bar induction but do not require extra axioms by themselves, unlike Brouwer's bar theorem (see below). We recall the induction principle associated with $\texttt{bar}$ predicates because we are going to use it extensively:

Proposition 2.2 (Induction on $\texttt{bar}$ predicates). *Assume* $P : \texttt{list}\, A \to \mathbb{P}$ *and a property* $K : \texttt{list}\, A \to \mathbb{P}$. *To establish*

$$\forall\, l,\ \texttt{bar}\, P\, l \to K\, l$$

it is sufficient to prove:

1. $\forall l,\ P\, l \to K\, l$;
2. $\forall l,\ \big(\forall a,\ \texttt{bar}\, P\, (a :: l)\big) \to \big(\forall a,\ K\, (a :: l)\big) \to K\, l$.

Rocq generates the principle on its own as a `Fixpoint` structural on the proof of $\mathsf{bar}\ P\ l$. The first induction hypothesis $\forall a,\ \mathsf{bar}\ P\ (a :: l)$ of item 2 is rarely needed, except in the proof in the mutual principle of Proposition 2.3. In the file `bar.v`, we collect basic results about `bar` predicates and highlight some of these below, where $P, Q : \mathtt{list}\ \_ \to \mathbb{P}$.

We give an intuitive understanding of $\mathsf{bar}\ P\ []$ with

$$\mathsf{bar}\ P\ [] \ \to\ \forall \rho : \mathbb{N} \to A,\ \exists n,\ P\ [\rho_{n-1}; \ldots; \rho_0] \tag{2}$$

In plain english, $\mathsf{bar}\ P\ []$ entails that any sequence of shape $n \mapsto [\rho_{n-1}; \ldots; \rho_0]$ unavoidably meets P, regardless of how it is extended by adding elements at its head. In the terminology of bar induction, P *is barred*. The characterization by sequences[9] in $\mathbb{N} \to A$ is called *Brouwer's bar theorem* [3] and can be proved using XM and DC, or alternatively with the weaker intuitionistic principle called *Brouwer's thesis* [25]. Constructively however, universal quantification over sequences is weaker than $\mathsf{bar}\ P\ []$ because the type $\mathbb{N} \to A$ does not account for lawless sequences [3, 12].

We show that `bar` is a *mono(tonic)* operator

$$\forall P\ Q,\ P \subseteq Q \to \mathsf{bar}\ P \subseteq \mathsf{bar}\ Q \tag{3}$$

by a straightforward induction on $\mathsf{bar}\ P\ \_$; more generally, `bar` is a closure operator. We show the following equivalence

$$\forall l\ r,\ \mathsf{bar}\ P\ (l +\!\!+ r) \ \leftrightarrow\ \mathsf{bar}\ (\lambda p, P\ (p +\!\!+ r))\ l. \tag{4}$$

A predicate Q *is monotone* if $\forall a\ l,\ Q\ l \to Q\ (a :: l)$. The `bar` operator preserves monotone predicates:

$$\text{if } P \text{ is monotone then so is } \mathsf{bar}\ P. \tag{5}$$

One observation that was made in [5] and which is used in the proof of the HBT in Section 5.3 is the following: if P is *closed under insertion* then so is $\mathsf{bar}\ P$, or more formally:

$$\begin{array}{l}\big(\forall l\ r,\ P\ (l +\!\!+ r) \to P\ (l +\!\!+ m +\!\!+ r)\big)\\ \to \big(\forall l\ r,\ \mathsf{bar}\ P\ (l +\!\!+ r) \to \mathsf{bar}\ P\ (l +\!\!+ m +\!\!+ r)\big)\end{array} \tag{6}$$

for any $m : \mathtt{list}\ A$, which is a generalization of the preservation of monotone predicates (5) by `bar` above.

In the Section 3, we will reason by mutual induction on two `bar` predicates using the following induction principle:

Proposition 2.3 (Mutual induction on `bar` predicates)**.** *Assume $P : \mathtt{list}\ A \to \mathbb{P}$ and $Q : \mathtt{list}\ B \to \mathbb{P}$ and a (mutual) property $K : \mathtt{list}\ A \to \mathtt{list}\ B \to \mathbb{P}$. To establish*

$$\forall l\ m,\ \mathsf{bar}\ P\ l \to \mathsf{bar}\ Q\ m \to K\ l\ m$$

it is sufficient to show:

1. $\forall l\ m,\ P\ l \to K\ l\ m$;
2. $\forall l\ m,\ Q\ m \to K\ l\ m$;
3. $\forall l\ m,\ \big(\forall a,\ K\ (a :: l)\ m\big) \to \big(\forall b,\ K\ l\ (b :: m)\big) \to K\ l\ m$.

Proof. By nested induction, on $\mathsf{bar}\ P\ l$, then on $\mathsf{bar}\ Q\ m$. □

[9] meaning, as a logical equivalence instead of an implication in Equation (2).

2.3.2 Pausing sequences.

Consider a sequence of finitely generated ideals $\mathcal{I}_n := \mathtt{idl}\ \lfloor[\rho_{n-1}; \ldots; \rho_0]\rfloor$ of a ring $\mathcal{R}$. This sequence is increasing: $\forall n,\ \mathcal{I}_n \subseteq \mathcal{I}_{n+1}$. A *pause* in the sequence is a index n where the associated ideal does not grow, i.e. $\mathcal{I}_{n+1} \subseteq \mathcal{I}_n$, or equivalently $\mathtt{idl}\ \lfloor[\rho_{n-1}; \ldots; \rho_0]\rfloor\ \rho_n$. By Equation (1), at that point, ρ_n is a linear combination of the previous values in the sequence.[10]

Definition 2.4 (Pausing lists)**.** Given a list $m : \mathtt{list}\ \mathcal{R}$, we say that m *pauses* and write $\mathsf{PA}\ m$ if:

$$\mathsf{PA}\ m := \exists l\ x\ r,\ m = l +\!\!+ [x] +\!\!+ r \wedge \mathtt{idl}\ \lfloor r \rfloor\ x.$$

In the file `noetherian.v`, we favor an inductive definition for PA for shorter Rocq proofs, but we nevertheless establish the equivalence with the above given (FOL like) Definition 2.4 of PA. We study the $\mathsf{PA}\ m$ property when m already has a given structure, e.g. $\mathsf{PA}\ (l +\!\!+ [x] +\!\!+ r)$ holds iff

- either $l = l' +\!\!+ [y] +\!\!+ m$ and $\mathtt{idl}\ \lfloor m +\!\!+ [x] +\!\!+ r \rfloor\ y$ hold for some $l', m : \mathtt{list}\ \mathcal{R}$ and $y : \mathcal{R}$, meaning that the pause occurs in l;
- or $\mathtt{idl}\ \lfloor r \rfloor\ x$ (the pause occurs at x);
- or $\mathsf{PA}\ r$ (the pause occurs in r).

We show that PA is closed under arbitrary insertions:

$$\forall l\ m\ r,\ \mathsf{PA}\ (l +\!\!+ r) \to \mathsf{PA}\ (l +\!\!+ m +\!\!+ r)$$

which by (6) entails the same property for $\mathsf{bar}\ \mathsf{PA}$:

$$\forall l\ m\ r,\ \mathsf{bar}\ \mathsf{PA}\ (l +\!\!+ r) \to \mathsf{bar}\ \mathsf{PA}\ (l +\!\!+ m +\!\!+ r) \tag{7}$$

Additionally PA is closed under ring sub-homomorphisms.

Proposition 2.5. *Let $\mathcal{R}$ and $\mathcal{T}$ be two rings and $\varphi : \mathcal{R} \to \mathcal{T}$ be a sub-homomorphism. The entailment $\mathsf{PA}\ l \to \mathsf{PA}\ (\varphi\ l)$ holds for any $l : \mathtt{list}\ \mathcal{R}$, where we simply write $\varphi\ l$ for $\mathtt{map}\ \varphi\ l$.*

2.3.3 Noetherian rings.

Following [5], we characterize the pausing of increasing sequences of finitely generated ideals using a `bar` predicate. The definitions and results below can be reviewed in the file `noetherian.v`.

Definition 2.6 (Noetherian ring)**.** We say that a ring $\mathcal{R}$ *is (Bar) Noetherian* and write $\mathtt{noetherian}\ \mathcal{R}$ if:

$$\mathtt{noetherian}\ \mathcal{R} := \mathsf{bar}\ (@\mathsf{PA}\ \mathcal{R})\ []$$

where $@\mathsf{PA}\ \mathcal{R}$ is a Rocq notation to specify the otherwise implicit argument $\mathcal{R}$ of PA.

Notice that [5] employs the term "Good" instead "pauses" but we favor terminology from constructive algebra rather than importing one we find a bit specific to WQO theory.

Since $\mathsf{bar}\ \mathsf{PA}\ []$ entails that PA is barred (2), in a Noetherian ring, any sequence $n \mapsto \mathtt{idl}\ \lfloor[\rho_{n-1}; \ldots; \rho_0]\rfloor$ pauses.[11] Finite rings are Noetherian, and Noetherian rings are closed under surjective homomorphisms and quotients. In particular,

(Bar) Noetherian rings are closed under isomorphism.

[10] Richman [19] and Seidenberg [21] characterize RS-Noetherian rings this way: any increasing sequence of finitely generated ideals contains a pause.
[11] but this is not exactly the same as RS-Noetherian, see Section 6.

To show that $\mathbb{Z}$ is Noetherian, we implement the following:

Theorem 2.7. *Consider a Bezout ring $\mathcal{R}$ where divisibility is (logically) decidable and strict divisibility is a well-founded relation. Then $\mathcal{R}$ is (Bar) Noetherian.*

Proof. In a Bezout ring every finitely generated ideal is generated by a singleton. We write $x \mid y := \exists k,\, k \times x \sim y$ for divisibility and $x \mid_s y := x \mid y \wedge y \nmid x$ for strict divisibility which are both logically decidable binary relations. We show

$$\forall\, g\, l,\ \mathtt{idl}\ \lfloor l \rfloor \equiv \mathtt{idl}\ \lfloor [g] \rfloor \longrightarrow \mathtt{bar}\ \mathtt{PA}\ l \tag{8}$$

by induction on g using the well-founded strict divisibility relation $\mid_s$. The induction hypothesis is:

$$IH : \forall e,\ e \mid_s g \longrightarrow \forall l,\ \mathtt{idl}\ \lfloor l \rfloor \equiv \lfloor [e] \rfloor \longrightarrow \mathtt{bar}\ \mathtt{PA}\ l$$

and assuming l s.t. $\mathtt{idl}\ \lfloor l \rfloor \equiv \lfloor [g] \rfloor$, we need to prove $\mathtt{bar}\ \mathtt{PA}\ l$. We apply the second constructor of bar and hence pick any x and the goal becomes $\mathtt{bar}\ \mathtt{PA}\ (x :: l)$. By Bezout, we get e s.t. $\mathtt{idl}\ \lfloor x :: l \rfloor \equiv \lfloor [e] \rfloor$. From $\mathtt{idl}\ \lfloor x :: l \rfloor\ g$ we deduce $e \mid g$. We discriminate between $g \mid e$ or $g \nmid e$:

- in the former case, we have $\mathtt{idl}\ \lfloor x :: l \rfloor \equiv \mathtt{idl}\ \lfloor [e] \rfloor \equiv \mathtt{idl}\ \lfloor [g] \rfloor \equiv \mathtt{idl}\ \lfloor l \rfloor$ and then $\mathtt{idl}\ \lfloor l \rfloor\ x$, so $x :: l$ pauses;
- in the later case, we have $e \mid_s g$ and we apply IH and immediately get the goal $\mathtt{bar}\ \mathtt{PA}\ (x :: l)$.

Having proved Statement (8), we then instantiate it on $g := 0$ and $l := []$, and derive that $\mathtt{bar}\ \mathtt{PA}\ []$ holds. □

Corollary 2.8. *The ring $\mathbb{Z}$ of integers is (Bar) Noetherian.*

3 The Direct Product is a Noetherian Ring

As we consider it an original theoretical contribution of our work, we give a quite detailed account for the below result:

Theorem 3.1. *If $\mathcal{R}$ and $\mathcal{T}$ are Noetherian rings then so is their direct product $\mathcal{R} \times \mathcal{T}$.*

3.1 The origins of the proof

In [20], a weaker result is established for RS-Noetherian rings; they further assume that $\mathcal{R}$ (or $\mathcal{T}$) is a strongly discrete ring. Their proof reminded us of that of Dickson's lemma, which itself classically follows from Ramsey's theorem. This translates constructively using a different statement of Ramsey's theorem: the direct product of two WQOs is a WQO, where WQOs are interpreted as AF relations [26].

We rather started from [6] because it is based on an equivalent bar characterization of AF relations for its statement of Ramsey's theorem. We simplified that proof in the hope of being able to adapt it to the context of algebra.[12] It turned out that we could indeed convert this simplified proof and establish our intended result *w/o assuming strong discreteness*. The file `product_noetherian.v` mechanizes this new result and we now give an overview of the arguments. Of course we first need to give an explicit construction of the direct product ring $\mathcal{R} \times \mathcal{T}$ (in `product.v`) and show that this construction is correct in the sense of category theory, as the terminal object in the category of product diagrams (see `category.v`). We do not elaborate on these standard considerations here.

[12] The auxiliary file `ramsey.v` records that reworked proof.

3.2 The detailed account

Turning to the statement of Theorem 3.1, we want to show

$$\mathtt{bar}\ (@\mathtt{PA}\ \mathcal{R})\ [] \longrightarrow \mathtt{bar}\ (@\mathtt{PA}\ \mathcal{T})\ [] \longrightarrow \mathtt{bar}\ \big(@\mathtt{PA}\ (\mathcal{R} \times \mathcal{T})\big)\ [] \tag{9}$$

but unfolded as such, induction is not possible. So following the scheme of [6], we first generalize the statement to

$$\forall\, lx\, ly,\ \mathtt{bar}\ \mathtt{PA}\ lx \longrightarrow \mathtt{bar}\ \mathtt{PA}\ ly \longrightarrow \mathtt{bar}\ (\theta\ lx\ ly)\ [] \tag{10}$$

where $\theta : \mathtt{list}\,\mathcal{R} \to \mathtt{list}\,\mathcal{T} \to \mathtt{list}\,(\mathcal{R} \times \mathcal{T}) \to \mathbb{P}$ must be wisely chosen. However [6] has a overly complex way of describing θ and a critical aspect of our work was to give it a much nicer form. Skipping the details, we ended up with the following simple definition for our adaptation:

$$\theta\ lx\ ly\ l := \mathtt{PA}\ (l +\!\!+ \varphi\ lx +\!\!+ \psi\ ly)$$

where $\varphi(x : \mathcal{R}) := (x, 0)$ and $\psi(y : \mathcal{T}) := (0, y)$, both output values belonging to the ring $\mathcal{R} \times \mathcal{T}$. Clearly, φ and ψ are ring sub-homomorphisms. Additionally, we write $\pi_1 : \mathcal{R} \times \mathcal{T} \to \mathcal{R}$ and $\pi_2 : \mathcal{R} \times \mathcal{T} \to \mathcal{T}$ for the canonical projections $\pi_1(x, y) := x$ and $\pi_2(x, y) := y$ which are ring homomorphisms.

The predicate $\theta\ lx\ ly$ being based on PA, it is monotone and so is $\mathtt{bar}\ (\theta\ lx\ ly)$. When lx and ly are empty lists then $\theta\ []\ []\ l$ is identical to $\mathtt{PA}\ l$. Hence statement (10) instantiates to statement (9) with that empty assignment for lx and ly, exactly the unfolding of Theorem 3.1.

To prove statement (10), we proceed by mutual induction using Proposition 2.3. It is enough to show:

1. $\mathtt{bar}\ (\theta\ lx\ ly)\ []$ assuming $\mathtt{PA}\ lx$;
2. $\mathtt{bar}\ (\theta\ lx\ ly)\ []$ assuming $\mathtt{PA}\ ly$;
3. $\mathtt{bar}\ (\theta\ lx\ ly)\ []$ assuming $\forall x,\ \mathtt{bar}\ \big(\theta\ (x :: lx)\ ly\big)\ []$ and $\forall y,\ \mathtt{bar}\ \big(\theta\ lx\ (y :: ly)\big)\ []$.

For item 1, if lx pauses then so does $[] +\!\!+ \varphi\ lx +\!\!+ \psi\ ly$ because φ is a sub-homomorphism. Hence $\theta\ lx\ ly\ []$ holds and we get $\mathtt{bar}\ (\theta\ lx\ ly)\ []$ using the first constructor for bar. A similar argument applies when ly pauses (item 2).

The difficult case is item 3 for which we need to show $\mathtt{bar}\ (\theta\ lx\ ly)\ []$ under two induction hypotheses. We first apply the second constructor for bar. We fix an arbitrary $z : \mathcal{R} \times \mathcal{T}$ and we now need to establish the goal $\mathtt{bar}\ (\theta\ lx\ ly)\ [z]$. We instantiate our two induction hypotheses on $\pi_1\ z / \pi_2\ z$ as

$$IH_1 : \mathtt{bar}\ \big(\theta\ (\pi_1\ z :: lx)\ ly\big)\ [] \quad IH_2 : \mathtt{bar}\ \big(\theta\ lx\ (\pi_2\ z :: ly)\big)\ []$$

and, to achieve the goal $\mathtt{bar}\ (\theta\, lx\, ly)\ [z]$, we prove the generalized statement

$$\forall m,\ \mathtt{bar}\ \big(\theta\, lx\, (\pi_2\, z :: ly)\big)\ m \longrightarrow \mathtt{bar}\ \big(\theta\, (\pi_1\, z :: lx)\, ly\big)\ m \longrightarrow \mathtt{bar}\ (\theta\, lx\, ly)\ (m +\!\!+ [z]) \quad (11)$$

that, for $m := []$, in combination with our two instances IH_1 and IH_2, delivers us the required conclusion $\mathtt{bar}\ (\theta\, lx\, ly)\ [z]$ for completing the proof of item 3.

So far, we followed a script similar to our adaptation of the proof of Ramsey's theorem [6], except of course for our definition of θ which is novel. However, the arguments we now use to establish (11) largely diverge from that script.

Proof of statement (11). In a first phase, we observe that

$$\mathtt{idl}\ \lfloor ly \rfloor\ (\pi_2\, z) \longrightarrow \theta\ (\pi_1\, z :: lx)\, ly\, m \longrightarrow \theta\, lx\, ly\ (m +\!\!+ [z]) \quad (12)$$

holds. Indeed, the second hypothesis states that there is a pause in $m +\!\!+ [\varphi(\pi_1\, z)] +\!\!+ \varphi\, lx +\!\!+ \psi\, ly$ and we analyze this situation. If the pause occurs in either m or $\varphi\, lx$ or $\psi\, ly$, then there is a corresponding pause in $m +\!\!+ [z] +\!\!+ \varphi\, lx +\!\!+ \psi\, ly$ because $\varphi(\pi_1\, z) \sim (1, 0) \times z$. If the pause occurs at $\varphi(\pi_1\, z)$ (the delicate case), then we have $\mathtt{idl}\ \lfloor \varphi\, lx +\!\!+ \psi\, ly \rfloor\ \varphi(\pi_1\, z)$. But since we assume $\mathtt{idl}\ \lfloor ly \rfloor\ (\pi_2\, z)$, we get $\mathtt{idl}\ \lfloor \psi\, ly \rfloor\ \psi(\pi_2\, z)$ by Proposition 2.5. We deduce $\mathtt{idl}\ \lfloor \varphi\, lx +\!\!+ \psi\, ly \rfloor\ \psi(\pi_2\, z)$ by inclusion of lists. From the equation $z \sim \varphi(\pi_1\, z) + \psi(\pi_2\, z)$ we finally get $\mathtt{idl}\ \lfloor \varphi\, lx +\!\!+ \psi\, ly \rfloor\ z$ and thus $m +\!\!+ [z] +\!\!+ \varphi\, lx +\!\!+ \psi\, ly$ pauses. This concludes the proof of statement (12).

Because bar is monotonic (3), we derive

$$\mathtt{idl}\ \lfloor ly \rfloor\ (\pi_2\, z) \longrightarrow \mathtt{bar}\ \big(\theta\, (\pi_1\, z :: lx)\, ly\big)\ m \longrightarrow \mathtt{bar}\ (\theta\, lx\, ly)\ (m +\!\!+ [z]) \quad (13)$$

from Observation (12), also using Equivalence (4).

In a second phase, we can deal with the proof of (11). We proceed by induction on $\mathtt{bar}\ \big(\theta\, lx\, (\pi_2\, z :: ly)\big)\ m$:

- in the base case, we have the hypotheses

  $$H_1 : \theta\, lx\, (\pi_2\, z :: ly)\ m$$
  $$H_2 : \mathtt{bar}\ \big(\theta\, (\pi_1\, z :: lx)\, ly\big)\ m$$

  and we target the goal $\mathtt{bar}\ (\theta\, lx\, ly)\ (m +\!\!+ [z])$. We analyze the pause H_1 in $m +\!\!+ \varphi\, lx +\!\!+ [\psi(\pi_2\, z)] +\!\!+ \psi\, ly$. If the pause occurs in either m or $\varphi\, lx$ or $\psi\, ly$ then there is a corresponding pause in $m +\!\!+ [z] +\!\!+ \varphi\, lx +\!\!+ \psi\, ly$, which entails $\theta\, lx\, ly\ (m +\!\!+ [z])$ hence our goal using the first constructor of bar.
  While we omit some details about how to transfer the above pause, we instead put the focus on the delicate case where the pause is at $\psi(\pi_2\, z)$, and in that case we have $\mathtt{idl}\ \lfloor \psi\, ly \rfloor\ \psi(\pi_2\, z)$. Since $\pi_2 \circ \psi$ is the identity map, we deduce $\mathtt{idl}\ \lfloor ly \rfloor\ (\pi_2\, z)$ by Proposition 2.5 (using π_2 as a sub-homomorphism). The situation now corresponds to Statement (13) that we established in the first phase, first phase which de facto implements a nested recursive call on $\mathtt{bar}\ \big(\theta\, (\pi_1\, z :: lx)\, ly\big)\ m$;

- in the recursive case, we have an hypothesis

  $$H_2 : \mathtt{bar}\ \big(\theta\, (\pi_1\, z :: lx)\, ly\big)\ m$$

  and an additional induction hypothesis

  $$IH : \forall z',\ \mathtt{bar}\ \big(\theta\, (\pi_1\, z :: lx)\, ly\big)\ (z' :: m) \longrightarrow \mathtt{bar}\ (\theta\, lx\, ly)\ (z' :: m +\!\!+ [z])$$

  and we have to establish the goal $\mathtt{bar}\ (\theta\, lx\, ly)\ (m +\!\!+ [z])$. We apply the second constructor of bar and hence we pick an arbitrary $z' : \mathcal{R} \times \mathcal{T}$ and prove

  $$\mathtt{bar}\ (\theta\, lx\, ly)\ (z' :: m +\!\!+ [z]).$$

  We apply the induction hypothesis IH and the goal becomes $\mathtt{bar}\ \big(\theta\, (\pi_1\, z :: lx)\, ly\big)\ (z' :: m)$ which follows from hypothesis H_2 because $\mathtt{bar}\ (\theta\ \_\ \_)$ is monotone.

This concludes our account of the proof of Theorem 3.1. □

3.3 Discussion

The above proof might look a bit intricate, especially for those unfamiliar with inductive reasoning in general, or those troubled with the inductive formulation of bar predicates in particular. One might feel that it does not give a lot of intuition about what is going on. We argue that generalized inductive reasoning is hard to communicate on paper, especially for readers unused to its mechanics: many different statements, hypotheses or goals, need to be tracked down.

This feeling given by the pen&paper outline, reflecting the happy conclusion of a proof search process, is however quite different from the experience of actually unfolding the proof search process with the help of the Rocq proof assistant. In particular, a lot of statements are inferred by the assistant itself, which also largely supports the mechanics of applying induction principles. What remains difficult is to devise which induction principle is best suited and which generalization is required before performing induction. In the dynamics of a proof, having an intuition about the "meaning" of a specific bar statement is not as critical as being able to pickup the "right" induction principle. This observation could be viewed in the light of Von Neumann's quote:

> Young man, in mathematics you don't understand things. You just get used to them.

The proof script in the file product_noetherian.v was designed to be human readable. Despite giving more details than the above pen&paper account, it has a comparable size and most sub proofs are shorter than 5 loc, with the exceptions of those of Statement (12) which is 12 loc (first phase), and of Statement (11) which is 30 loc (second phase).

4 Construction of the Polynomial Ring

We now turn to the construction of the polynomial ring which we discuss within this section. This construction is of course critical in the implementation of the HBT because it deals with polynomials. Notice that the choice we made for

our implementation of rings as setoids was also influenced by the requirements of the construction of polynomial rings.

4.1 What is a polynomial?

The notion of polynomial can be understood in contexts much larger than ring algebra. In general, they can be viewed as expressions built from values of the carrier algebra $\mathcal{A}$, combined with (the syntactic counterparts of) algebraic operators (given by a signature) and some unknowns in U. E.g. for rings, an example could look like $(1 + X \times Y) \times (Y + Z)$. One then defines the least congruence satisfying the algebraic laws (e.g. with an inductive predicate) and the quotient forms the algebra of polynomials, denoted $\mathcal{A}[U]$. At this level of abstraction there is no canonical representative of a given expression: think of the Lindenbaum algebra for intuitionistic logic for instance. Even for rings where canonical forms may exist, notions like degrees, head coefficients, or monomials require *computing* canonical forms.

When introduced to students in algebra, polynomials in the unknown X over a ring $\mathcal{R}$ (often it is even a field) are rather defined as formal expressions $x_0X^0 + x_1X^1 + \cdots + x_nX^n$, where x_n is must be nonzero.[13] This gives a canonical (and unique) form to the polynomial. But unless assuming a discrete ring, it is not possible to ensure the existence of a canonical form: computing the canonical representative of the sum $P + Q$ where $P = \cdots + aX^n$ and $Q = \cdots + bX^n$ requires being able to discriminate $a + b$ from 0.

4.2 Polynomial representations

This representation of polynomials as an ordered sequence of monomials $x_0 + x_1X + \cdots + x_nX^n$ is assumed for the proof of the HBT in [5], and generally, even classical proofs of the HBT work with sum of (multivariate) monomials.

In our implementation file `poly.v`, instead of trying to normalize arbitrary polynomial expressions into ordered sequences, we view *polynomial representations* over a ring $\mathcal{R}$ and (a single variable X) as lists $[x_0; \ldots; x_n]$ in $\mathcal{R}[X] := \texttt{list}\,\mathcal{R}$, however *not requiring* that x_n is nonzero. That is why we call them representations, and those are not unique. E.g. $[x_0; x_1]$ and $[x_0; x_1; 0; 0]$ are two representations of the same polynomial, but they are "identified" under a suitable congruence $\sim$. Using setoids is critical here because we do not need to find the shortest representation, hence the discreteness of $\mathcal{R}$ need not be assumed.[14] Compared to the C-CoRN library [13], we proceed similarly except that they hardwire the list structure in the `cpoly` type: i.e. they view the polynomial $x_0X^0 + x_1X^1 + x_2X^2$ in its Horner form $x_0 + X(x_1 + X(x_2 + X.0))$. We favor lists in order to exploit the generic tools of the `List` module, rather than having to create a copy of that library specialized on `cpoly`.

[13] Formally, the expression is just a list $[x_0; \ldots; x_n]$ of coefficients.
[14] later allowing us to confirm the generality of the HBT as claimed in [5].

The construction of the polynomials in $\mathcal{R}[X]$ as lists otherwise follows the same guideline as in the C-CoRN library: *if a coefficient is missing, then pick* 0 *instead.* For instance, the equivalence $[x_0; x_1] \sim [x_0']$ holds for polynomial representations when $x_0 \sim x_0'$ and $x_1 \sim 0$ hold in $\mathcal{R}$. We will not detail here how we implemented the algebraic structure over $\mathcal{R}[X] := (\texttt{list}\,\mathcal{R}, \ldots)$. With the right tools, we view it as an "easy" exercise; but see the discussion in Section 5.4.

How do we know that our implementation of polynomial representations is really the intended polynomial ring $\mathcal{R}[X]$, and not an arbitrary ring? This is where category theory helps: below we show that polynomial representations, together with its ring structure, form an initial object in the category of pointed extensions of the ring $\mathcal{R}$.

4.3 The categorical characterization

We describe the categorical characterization of the polynomial ring $\mathcal{R}[X]$, and more generally of the multivariate polynomial ring $\mathcal{R}[U]$ where U is an arbitrary type of unknowns, not just a singleton $\{X\}$. It might be less well known than the characterization of the direct product $\mathcal{R} \times \mathcal{T}$ that we encountered in Section 3.1. The corresponding file in the code is still `category.v`.

Definition 4.1 (Multivariate polynomial ring $\mathcal{R}[U]$)**.** Let $\mathcal{R}$ be a ring and U be a type. A *multivariate extension of* $\mathcal{R}$ *with unknowns in* U is a tuple $(\mathcal{E}, \varphi, e)$ where $\mathcal{E}$ is a ring, $\varphi : \mathcal{R} \to \mathcal{E}$ is a ring homomorphism, and $e : U \to \mathcal{E}$ is simply a map. A *homomorphism of multivariate extensions* $(\mathcal{E}, \varphi, e)$ and $(\mathcal{F}, \psi, f)$ is a ring homomorphism $\gamma : \mathcal{E} \to \mathcal{F}$ s.t. $\gamma \circ \varphi \equiv \psi$ and $\gamma \circ e \equiv f$. Multivariate extensions of $\mathcal{R}$ with unknowns in U form a category of which initial objects are called *multivariate polynomial rings over* $\mathcal{R}$ *with unknowns in* U, and are denoted by $\mathcal{R}[U]$.

As initial objects in a category, all multivariate polynomial rings over $\mathcal{R}$ with unknowns in U are isomorphic, which somehow justifies denoting them all with $\mathcal{R}[U]$. Any bijective correspondence between the types U and V gives rises to an isomorphism between the rings $\mathcal{R}[U]$ and $\mathcal{R}[V]$.

Definition 4.2 (Univariate polynomial ring $\mathcal{R}[X]$)**.** Given a name X for the unknown, a *univariate polynomial ring* is a multivariate polynomial ring for $U := \{X\}$, a singleton type, and is denoted $\mathcal{R}[X]$. Hence, they are the initial objects of the category of univariate (or pointed) extensions of $\mathcal{R}$.

Because there is a bijection between the singleton $\{X\}$ and the singleton $\{Y\}$ (and in fact any other singleton), the polynomial rings $\mathcal{R}[X]$ and $\mathcal{R}[Y]$ are isomorphic as well.

Theorem 4.3. *Given a ring* $\mathcal{R}$*, one can compute a ring denoted* $\texttt{poly\_ring}\,\mathcal{R} := (\texttt{list}\,\mathcal{R}, \ldots)$ *based on the carrier type* $\texttt{list}\,\mathcal{R}$*. Moreover the pointed extension*

$$(\texttt{poly\_ring}\,\mathcal{R}, \varphi, [0; 1]) \quad \textit{where } \varphi := \lambda\, x, [x]$$

is a (univariate) polynomial ring over $\mathcal{R}$*, i.e.* $\mathcal{R}[X]$*.*

Proof. We build the ring $\texttt{poly\_ring}\ \mathcal{R} : \texttt{ring}$ based on the polynomial representation as described in Section 4.2. Recall that the `ring` record type is based on setoids which allows for several representations of the same polynomial. The named unknown X is associated to the list $[0; 1]$ representing the polynomial $0.X^0 + 1.X^1$. The map φ associates any value $x : \mathcal{R}$ to the polynomial $x.X^0$ represented by the list $[x]$. □

In the sequel, we may denote $\mathcal{R}[X]$ for the particular implementation $\texttt{poly\_ring}\ \mathcal{R}$ of a univariate polynomial ring, which is standard practice. However, the statements and proofs of upcoming Theorems 4.4 and 5.2, and of Lemma 5.5 actually work only with this implementation of $\mathcal{R}[X]$, and not at the more abstract level of Definition 4.2.

4.4 Critical observation for the HBT

We describe the critical observation that serves in the base case of the short but (somewhat) sophisticated `bar` inductive proof of the HBT [5]. For a simpler formulation, we abusively write "polynomial" instead of "polynomial representation" in its informal statement below:

Theorem 4.4. *Given a polynomial $p : \mathcal{R}[X]$ and a list $m : \texttt{list}\,\mathcal{R}[X]$ of shorter polynomials s.t. the head coefficient of p is a linear combination of the head coefficients in m, there is a polynomial $q : \mathcal{R}[X]$, strictly shorter than p and s.t. $p - q$ is a linear combination of m.*

Before we state it formally, we need some tools. Recall that $|l| : \mathbb{N}$ is the *length* and it applies in particular to polynomial representations (i.e. lists). We capture the *head coefficient* of a polynomial representation with the inductive predicate $\texttt{is\_last}\ \{A\} : A \to \texttt{list}\,A \to \mathbb{P}$ defined by the single rule:

$$\frac{}{\texttt{is\_last}\ a\ (l +\!\!+ [a])}$$

Notice that the length and the head coefficient are notions attached to polynomial representations, *not to polynomials*.[15] Moreover, these notions are simple to define for the representation of polynomials as ordered lists of monomials, and much less so with polynomials as algebraic expressions (see Section 4.1).

We recall the $\texttt{Forall}_1\ \{A\}\ (P : A \to \mathbb{P}) : \texttt{list}\,A \to \mathbb{P}$ and $\texttt{Forall}_2\ \{A\,B\}\ (R : A \to B \to \mathbb{P}) : \texttt{list}\,A \to \texttt{list}\,B \to \mathbb{P}$ predicates that characterize finite universal quantification over one or two lists, as defined inductively in the `List` module of the standard library, with two rules each:

$$\frac{}{\texttt{Forall}_1\ P\ []} \qquad \frac{P\ a \qquad \texttt{Forall}_1\ P\ l}{\texttt{Forall}_1\ P\ (a :: l)}$$

$$\frac{}{\texttt{Forall}_2\ R\ []\ []} \qquad \frac{R\ a\ b \qquad \texttt{Forall}_2\ R\ l\ m}{\texttt{Forall}_2\ R\ (a :: l)\ (b :: m)}$$

[15] Polynomials have representations with different lengths and heads. The "degree" as used in [5] only exists for polynomials over a discrete ring.

With those definitions, the statement of Theorem 4.4 can be formalized as: for any $p : \texttt{poly\_ring}\ \mathcal{R}$ and any $m : \texttt{list}\,(\texttt{poly\_ring}\ \mathcal{R})$, if the two following conditions hold:

1. $\texttt{Forall}_1\ (\lambda\, q, |q| \le |p|)\ m$;
2. $\exists\, x\, h, \texttt{is\_last}\ x\ p \wedge \texttt{Forall}_2\ \texttt{is\_last}\ h\ m \wedge \texttt{lc}\ h\ x$;

then $\exists q : \texttt{poly\_ring}\ \mathcal{R}, |q| < |p| \wedge \texttt{lc}\ m\ (p - q)$.

Proof of Theorem 4.4. First multiply each polynomial in m by some suitable X^k so that all the lengths in m match that of p. We get a new list m' with the same head coefficients as m, and all the polynomials in m' have length $|p|$.

We replay the linear combination of the head coefficients of m/m' on the polynomials in m' themselves and obtain a polynomial p' which has the same length and same head as p, and is moreover a linear combination of m', hence of m.

Then we define $q := p - p'$ while removing its 0 head coefficient to ensure $|q| < |p|$. Moreover $p - q \sim p'$ holds. The mechanized statement is named `update_lead_coef` and its proof can be reviewed in `poly.v`. □

5 Hilbert's Basis Theorem

We now switch to Hilbert's basis theorem which we state as:

Theorem 5.1. *Let $\mathcal{R}$ be a Noetherian ring and $X_1, \ldots, X_n$ be $n : \mathbb{N}$ different unknowns. Then the ring $\mathcal{R}[X_1, \ldots, X_n]$ of multivariate polynomials is Noetherian.*

Notice that the original statement of Hilbert assumes that $\mathcal{R}$ is a field (which is thus automatically Noetherian), but of course with the classical understanding of Noetherian ring that is not suitable in constructive setting, see Section 2.2.

We state it for (Bar) Noetherian rings instead and it becomes a direct consequence of the restricted statement:

Theorem 5.2. *For any ring $\mathcal{R}$ the following entailment holds:*

$$\texttt{noetherian}\ \mathcal{R} \to \texttt{noetherian}\ (\texttt{poly\_ring}\ \mathcal{R}).$$

Proof of Theorem 5.1. The ring $\mathcal{R}[X_1][X_2]\ldots[X_n]$ is a multivariate polynomial ring for $\mathcal{R}$ with unknowns $\{X_1, \ldots, X_n\}$ because it satisfies the categorical characterization of Definition 4.1. Moreover $\mathcal{R}'[X_i]$ and $\texttt{poly\_ring}\ \mathcal{R}'$ are isomorphic for any $\mathcal{R}' := \mathcal{R}[X_1][X_2]\ldots[X_{i-1}]$. Hence an induction on n combined with Theorem 5.2 gives a direct proof. The reader can consult the file `hbt.v` for details. □

Concerning the proof of Theorem 5.2, we follow the outline given in [5] while reformulating some arguments. In particular, we abstract the notion of update in a finitely generated ideal, and we replace "open induction" by a lexicographic induction principle, deviating a bit from the minimal bad sequences argument that open induction emulates.

5.1 Updating finitely generated ideals

In `ideal.v`, we characterize the update operation on list of elements of a ring $\mathcal{R}$ as an inductive binary relation `update` :

$\texttt{list}\,\mathcal{R} \to \texttt{list}\,\mathcal{R} \to \mathbb{P}$ defined by two rules:

$$\frac{\texttt{lc}\ l\ (y - x)}{\texttt{update}\ (x :: l)\ (y :: l)} \qquad \frac{\texttt{update}\ l\ m}{\texttt{update}\ (x :: l)\ (x :: m)}$$

The update relation is symmetric and preserves the generated ideal, i.e. $\forall\, l\, m$, $\texttt{update}\, l\, m \to \texttt{idl}\, \lfloor l \rfloor \equiv \texttt{idl}\, \lfloor m \rfloor$. As a consequence, updating also preserves pauses and $\texttt{bar}\,\texttt{PA}$; see noetherian.v for proofs.

Proposition 5.3. *For any $l, m : \texttt{list}\,\mathcal{R}$, the two following entailments hold:*

1. $\texttt{update}\, l\, m \to \texttt{PA}\, l \to \texttt{PA}\, m$;
2. $\texttt{update}\, l\, m \to \texttt{bar}\,\texttt{PA}\, l \to \texttt{bar}\,\texttt{PA}\, m$.

In Theorem 4.4, we find a polynomial q s.t. $\texttt{lc}\ m\ (p - q)$ which entails that $\texttt{update}\ (q :: m)\ (p :: m)$ (first rule), and as a consequence $\texttt{bar}\,\texttt{PA}\ (q :: m) \to \texttt{bar}\,\texttt{PA}\ (p :: m)$ holds as well. We will use this in the proof of the upcoming Lemma 5.5.

5.2 A tailored lexicographic induction principle

Let $A : \texttt{Type}$ and $T : A \to A \to \mathbb{P}$ be a binary relation. We form a binary relation $<_T : \texttt{list}\, A \to \texttt{list}\, A \to \mathbb{P}$ defined inductively with two rules, where we write $<_T$ infix:

$$\frac{T\ a\ b}{a :: m <_T b :: m} \qquad \frac{l <_T m}{l <_T b :: m}$$

Using a repeated application of the second rule, we show:

$$l <_T m \to l <_T k +\!\!+ m \qquad \text{for any } k, l, m : \texttt{list}\, A$$

The relation $<_T$ is a kind of lexicographic product and is thus well-founded as soon as T is. The proof of well-foundedness would proceed by nested induction but here, we can alternatively remark that $<_T$ is included into the *shortlex* lexicographic relation,[16] which is itself well-founded.

We do not actually need this level of generality, and instead implement a tailored induction principle:

Theorem 5.4. *Assume T is well-founded. Let $k : \texttt{list}\, A$ be a list and $P : \texttt{list}\, A \to \mathbb{P}$ by a property of lists. To show $\forall a,\ P\ (a :: k)$ it is sufficient to establish:*

1. $\forall l,\ l <_T k \to P\, l$;
2. $\forall a,\ (\forall l,\ l <_T a :: k \to P\, l) \to P\ (a :: k)$.

Proof. We prove $P\ (a :: k)$ by well-founded induction on a using T for the well-founded relation, hence we assume

$$IH : \forall b,\ T\ b\ a \to P\ (b :: k).$$

We apply item 2 and the goal becomes $\forall l, l <_T a :: k \to P\, l$. Let us pick l s.t. $l <_T a :: k$ and let us show that $P\, l$ holds. Inverting $l <_T a :: k$, we distinguish two cases: either $l = b :: k$ with $T\ b\ a$ for some b (left rule), thus $P\ (b :: k)$ holds by IH, and we get $P\, l$ as required; or else $l <_T k$ holds (right rule) and we get $P\, l$ using item 1. □

[16] l is *shortlex smaller* that m if $|l| < |m|$, or if $|l| = |m|$ and l is R-lexicographically smaller than m.

According to that tailored induction principle, when the goal $P\ (a :: k)$ presents itself, we just need to check: in the *base case* that $P\, l$ holds for any $l <_T k$, and in the *recursive case*, we can further assume that $P\, l$ holds for any $l <_T a :: k$.

5.3 The main inductive proof

Let $\mathcal{R}$ be a ring and let $\mathcal{R}[X] := \texttt{poly\_ring}\ \mathcal{R}$ be its ring of univariate polynomials, implemented using lists (see Theorem 4.3). We define the relation $T : \mathcal{R}[X] \to \mathcal{R}[X] \to \mathbb{P}$ by $T\ p\ q := |p| < |q|$, i.e. p is strictly shorter than q. As the strict natural order on $\mathbb{N}$ is well-founded then so is T and we use this instance for $<_T : \texttt{list}\,\mathcal{R}[X] \to \texttt{list}\,\mathcal{R}[X] \to \mathbb{P}$ and activate the tailored lexicographic principle of Theorem 5.4.

Lemma 5.5 (HBT, recursive)**.** *Let $h : \texttt{list}\,\mathcal{R}$ be a list (of head coefficients). The following statement holds:*

$$\texttt{bar}\,\texttt{PA}\, h \to \forall k,\ \texttt{Forall}_2\ \texttt{is\_last}\, h\, k \to (\forall m,\ m <_T k \to \texttt{bar}\,\texttt{PA}\, m) \to \texttt{bar}\,\texttt{PA}\, k.$$

Proof. Notice the implicit type $k : \texttt{list}\,(\texttt{poly\_ring}\ \mathcal{R})$ in the statement, so Rocq knows that the members of k belong to a (polynomial) ring, and are more than lists of values in $\mathcal{R}$. We proceed by induction on $\texttt{bar}\,\texttt{PA}\, h$. In the *base case* we have $H_1 : \texttt{PA}\, h$. Let us pick k s.t.

$$H_2 : \texttt{Forall}_2\ \texttt{is\_last}\, h\, k \qquad H_3 : \forall m,\ m <_T k \to \texttt{bar}\,\texttt{PA}\, m$$

and we aim at the goal $\texttt{bar}\,\texttt{PA}\, k$. By H_1, there is a pause in h so $h = u +\!\!+ [x] +\!\!+ v$ with $\texttt{idl}\, \lfloor v \rfloor\ x$ or equivalently $\texttt{lc}\, v\, x$. As $\texttt{Forall}_2\ \texttt{is\_last}\, h\, k$ holds, we split k accordingly into $k = l +\!\!+ [p] +\!\!+ m$ where $\texttt{Forall}_2\ \texttt{is\_last}\, u\, l$, $\texttt{is\_last}\, x\, p$ and $\texttt{Forall}_2\ \texttt{is\_last}\, v\, m$.

We discard l and replace the goal $\texttt{bar}\,\texttt{PA}\ (l +\!\!+ [p] +\!\!+ m)$ by $\texttt{bar}\,\texttt{PA}\ (p :: m)$ because $\texttt{bar}\,\texttt{PA}$ is monotone. We now discriminate between two possibilities: either all the polynomials in m are shorter than p or one of those is strictly longer:

- if all are shorter, i.e. $\texttt{Forall}_1\ (\lambda\, q, |q| \le |p|)\ m$, then we use Theorem 4.4. Let $q : \mathcal{R}[X]$ such that $|q| < |p|$ and $\texttt{lc}\ m\ (p - q)$. We deduce $\texttt{update}\ (q :: m)\ (p :: m)$ and using Proposition 5.3 item 2, we can replace the goal $\texttt{bar}\,\texttt{PA}\ (p :: m)$ with $\texttt{bar}\,\texttt{PA}\ (q :: m)$. But $q :: m <_T l +\!\!+ p :: m = k$ holds and we conclude using H_3;
- if there is $q \in m$ s.t. $|p| < |q|$, then we write $m = m' +\!\!+ [q] +\!\!+ r$. Instead of $\texttt{bar}\,\texttt{PA}\ ([p] +\!\!+ (m' +\!\!+ [q]) +\!\!+ r)$, we can just show $\texttt{bar}\,\texttt{PA}\ (p :: r)$ because $\texttt{bar}\,\texttt{PA}$ is closed under insertions. But $p :: r <_T (l +\!\!+ [p] +\!\!+ m') +\!\!+ q :: r = k$ holds hence the goal follows from H_3.

In the *recursive case*, we assume[17]

$$IH_h : \forall\, x\, k,\ \texttt{Forall}_2\ \texttt{is\_last}\ (x :: h)\ k \to (\forall m,\ m <_T k \to \texttt{bar}\,\texttt{PA}\, m) \to \texttt{bar}\,\texttt{PA}\, k$$

[17] The induction principle of Proposition 2.2 generates another hypothesis that we do not need and discard right away.

and pick k s.t.

$$H_2 : \texttt{Forall}_2\,\texttt{is\_last}\,h\,k \quad H_3 : \forall m,\ m <_T k \to \texttt{bar}\,\texttt{PA}\,m$$

and let us prove $\texttt{bar}\,\texttt{PA}\,k$. We apply the second constructor of bar so let us pick $a : \mathcal{R}[X]$ and let us show $\texttt{bar}\,\texttt{PA}\,(a :: k)$ instead. We now use the tailored lexicographic induction encoded in Theorem 5.4.

For the base case, we need to prove $\texttt{bar}\,\texttt{PA}\,m$ for any $m <_T k$ which is precisely the statement of H_3.

For the recursive case, the goal $\texttt{bar}\,\texttt{PA}\,(a :: k)$ remains unchanged but we can further assume

$$IH : \forall l,\ l <_T a :: k \to \texttt{bar}\,\texttt{PA}\,l.$$

We choose whether $a = []$ is the empty list, or $a = q +\!\!+ [x]$ has a head coefficient:

- if $a = []$ then $a \sim 0$ as a polynomial, and $\texttt{idl}\,\lfloor k \rfloor\,a$ holds in $\mathcal{R}[X]$. Hence $a :: k$ pauses and $\texttt{bar}\,\texttt{PA}\,(a :: k)$ holds using the first constructor of bar;
- if $a = q +\!\!+ [x]$ then we apply IH_h to the goal $\texttt{bar}\,\texttt{PA}\,(a :: k)$, which generates two sub-goals:
  - $\texttt{Forall}_2\,\texttt{is\_last}\,(x :: h)\,(a :: k)$ which holds because of H_2 and $a = q +\!\!+ [x]$;
  - $\forall m,\ m <_T a :: k \to \texttt{bar}\,\texttt{PA}\,m$ which is exactly IH.

This concludes the proof. □

Proof of Theorem 5.2. Recall the definition $\texttt{noetherian}\,\mathcal{R} := \texttt{bar}\,(@\texttt{PA}\,\mathcal{R})\,[]$. We instantiate Lemma 5.5 with $h := []$ and $k := []$. Two sub goals remain: first $\texttt{Forall}_2\,\texttt{is\_last}\,[]\,[]$ which is trivial, and second $\forall m,\ m <_T [] \to \texttt{bar}\,\texttt{PA}\,m$ which holds because $m <_T []$ is impossible. □

5.4 Discussion

The mechanized proofs in the code are not that long. The critical observation in Theorem 4.4 is decomposed in two successive proofs each about 20 loc to be found in the poly.v file. In hbt.v, the tailored lexicographic induction of Theorem 5.4 involves 10 loc (incl. the definition of $<_T$). The HBT main Lemma 5.5 is 25 loc (excl. comments), with 2 loc extra to get Theorem 5.2, and the HBT Theorem 5.1 requires no more than a total of 25 extra loc.

One may wonder why an implementation of such a landmark result as the constructive HBT had been pending for so long, considering that the pen&paper outline [5] is 25 years old, and that this work already contained Agda code for Dickson's lemma to be used in the certification of Buchberger's algorithm. Moreover, several other constructive proofs precede (and succeed) the one we put the focus on, albeit with other characterizations of Noetherian rings.

We try to answer that question based on guesses informed by our own experience. First of all, most pen&paper constructive accounts of the HBT are not as short and synthetic as that of [5]. We attribute this feature to the characterization of Noetherian rings using bar inductive predicates.

In some followup work in Coq, Persson [17] mentions some difficulties with the bar predicate that he seemingly needs to convert into an Acc(essibility) predicate (a singleton with one constructor only) before he can implement the proof of the HBT, and which he leaves as an "open problem" in his conclusions. We did not encounter that difficulty. He also imported the implementation of polynomials in Théry's work [23, 24] on Buchberger's algorithm, where (multivariate) polynomials are ordered lists of monomials in $\mathcal{F}[X_1, \ldots, X_n]$ that need to be normalized, hence assuming the ring $\mathcal{F}$ to be discrete field. This makes sense for Buchberger's algorithm but basing on this view of polynomials, one cannot follow the outline of [5] because it really needs the construction of $\mathcal{R}[X]$ for a ring $\mathcal{R}$ (and not for a field), to be able to iterate Theorem 5.2.

But why did Persson (apparently) not try to implement abstract rings and polynomial rings by himself? Because as discussed in Section 4.2, we did not find it to be an overwhelming task. Notice the work on the C-CoRN library [13] came somewhat later so he could not have relied on it, but we did not have to either.[18]

We speculate that the difficulty may have come from the lack of versatile instruments in proof assistants at the time. Indeed, the construction of the polynomial ring in poly.v weights around 500 loc but that code makes heavy use of both the ring tactic [8] and setoid rewriting [22]. Both sets of tools were absent for Agda, and w.r.t. Coq, they were either lacking or too embryonic at the time, and started to mature only several years later.

These are however essential tools in our implementation, avoiding us to painfully solve ring equations by hand. Also notice that $\mathcal{R}[X]$ forms a ring (as required by the ring tactic) only once the structure has been proved to satisfy the ring axioms. So there is a part of the code, in fact most of poly.v, which deals with polynomial representations not as elements of a ring, but exclusively as lists of coefficients. Setoid rewriting is key in this temporary situation.

6 Well-foundedness for Noetherian rings

We define the notion of *witnessed strict inclusion*:

$$P \subset_{\mathrm{w}} Q := P \subseteq Q \wedge \exists x,\ Q\,x \wedge \neg P\,x$$

and, as usual, we write $\supset_{\mathrm{w}}$ for the converse relation $\subset_{\mathrm{w}}^{-1}$. In noetherian_wf.v, we present several well-founded induction principles that hold for $\supset_{\mathrm{w}}$ on Noetherian rings.

Theorem 6.1. *If the ring $\mathcal{R}$ is (Bar) Noetherian then the relation $\supset_{\mathrm{w}}$ is well-founded on the ideals of $\mathcal{R}$. As a consequence the following relations are well-founded as well:*

1. *$\supset_{\mathrm{w}}$ on the finitely generated ideals of $\mathcal{R}$;*
2. *$\lambda\,P\,Q : \mathcal{R} \to \mathbb{P}, \texttt{idl}\,P \supset_{\mathrm{w}} \texttt{idl}\,Q$;*

[18] B.t.w. the focus of C-CoRN are constructive real numbers in Coq and, even thought it contains a significant algebraic hierarchy, that library does not deal with Noetherian algebra.

3. $\lambda\, l\, m : \texttt{list}\,\mathcal{R}, \texttt{idl}\,\lfloor l\rfloor \supset_{\mathrm{w}} \texttt{idl}\,\lfloor m\rfloor$.

Proof. Let use define the binary relation T over $\mathcal{R} \to \mathbb{P}$ as $T := \lambda\, P\, Q : \mathcal{R} \to \mathbb{P}, Q \subset_{\mathrm{w}} P \wedge \texttt{ideal}\, Q$. We first show

$$\forall l,\ \texttt{bar}\,\texttt{PA}\, l \to \neg\texttt{PA}\, l \to \forall P,\ \lfloor l\rfloor \subseteq P \to \texttt{Acc}\, T\, P \quad (14)$$

by induction on $\texttt{bar}\,\texttt{PA}\, l$. In the base case where $\texttt{PA}\, l$ holds, it cancels out with the next hypothesis $\neg\texttt{PA}\, l$. In the recursive base, we further assume the induction hypothesis

$$IH : \forall x,\ \neg\texttt{PA}\,(x :: l) \to \forall P,\ \lfloor x :: l\rfloor \subseteq P \to \texttt{Acc}\, T\, P$$

and picking up some P, the additional hypotheses

$$H_1 : \neg\texttt{PA}\, l \qquad H_2 : \lfloor l\rfloor \subseteq P$$

and the goal is to prove $\texttt{Acc}\, T\, P$. We apply the constructor for Acc and pick up Q such that $H_3 : T\, Q\, P$ and the goal becomes $\texttt{Acc}\, T\, Q$. We unfold H_3 as

$$H_4 : P \subseteq Q \quad H_5 : Q\, x \quad H_6 : \neg P\, x \quad H_7 : \texttt{ideal}\, P$$

for some $x : \mathcal{R}$. We apply IH using that x on the goal $\texttt{Acc}\, T\, Q$, and this generates two sub-goals:

- $\neg\texttt{PA}\,(x :: l)$ which follows from H_1, H_2, H_6 and H_7;
- and $\lfloor x :: l\rfloor \subseteq Q$ which follows from H_2, H_4 and H_5.

Having completed the proof of the statement (14), we instantiate it with $l := []$ and derive $\texttt{bar}\,\texttt{PA}\,[] \to \forall P,\ \texttt{Acc}\, T\, P$ because the empty list $[]$ contains no pause and $\lfloor []\rfloor \subseteq P$ always holds. Said otherwise, we have proved:[19]

$$\texttt{noetherian}\,\mathcal{R} \to \texttt{well\_founded}\,(\lambda\, P\, Q, P \supset_{\mathrm{w}} Q \wedge \texttt{ideal}\, Q).$$

It follows that $\supset_{\mathrm{w}}$ is well-founded on the ideals of $\mathcal{R}$: we simply transfer well-foundedness using a surjective morphism. The same tool works to derive items 1, 2 and 3. □

Using the above well-foundedness results, we study the links between (Bar) Noetherian rings and alternate constructive characterizations, see noetherian_alt.v. We write $\subset$ infix for *strict inclusion*, i.e. $P \subset Q := P \subseteq Q \wedge Q \nsubseteq P$ and $\supset$ for the converse relation $\subset^{-1}$. Notice that $\subset$ is constructively weaker than witnessed strict inclusion $\subset_{\mathrm{w}}$, but they coincide on the finitely generated ideals of strongly discrete rings.

Definition 6.2 (Noetherian, constructive variants)**.** A ring is *RS-Noetherian* if any infinite increasing sequence of finitely generated ideals pauses. A ring is *ML-Noetherian* if the relation $\supset$ is well-founded on its finitely generated ideals.

Notice that the original definition of ML-Noetherian in [10, Def. 3.4] further assumes a coherent ring, with a "membership algorithm." There are other terminologies for this concept like "has detachable ideals" [14, p. 514] or "strongly discrete" [20, Def. 5] (or [4, p. 278]), all of them giving a computational interpretation (informative in Rocq terminology) of our (non-informative) Definition 2.1 of strongly discrete rings. We do not need the assumptions of coherence and computability for the results below.

Theorem 6.3. *Let $\mathcal{R}$ be a strongly discrete ring. Then $\mathcal{R}$ is (Bar) Noetherian iff it is ML-Noetherian.*

Proof. The *only if* part follows from Theorem 6.1 (item 1) since strict inclusion and witnessed strict inclusion are equivalent for the finitely generated ideals of a strongly discrete ring. For the *if* part, we show that the predicate PA is (logically) decidable on strongly discrete rings, hence bar PA is equivalent to an Acc(essibility) predicate and, we conclude with a relational morphism. □

Theorem 6.4. *Any strongly discrete ML-Noetherian ring is RS-Noetherian.*

Proof. Assume a strongly discrete ML-Noetherian ring $\mathcal{R}$, and a sequence $\rho : \mathbb{N} \to \mathcal{R} \to \mathbb{P}$ s.t. $\rho_n \subseteq \rho_{n+1}$ (increasing) and ρ_n is a finitely generated ideal, for any $n : \mathbb{N}$. The binary relation $T : \mathbb{N} \to \mathbb{N} \to \mathbb{P}$ defined by $T\, n\, m := \rho_m \subset_{\mathrm{w}} \rho_n$ is well-founded because $\mathcal{R}$ is ML-Noetherian. We show

$$\forall n \exists m,\ n \leq m \wedge \rho_{m+1} \subseteq \rho_m$$

by well-founded induction on n using T. We get the pause using the instance where $n := 0$. □

However, even in the strongly discrete case, the universal quantification over sequences used in the ascending chain condition for RS-Noetherian rings is weaker than the inductive predicates bar and Acc used in the definitions of Bar and ML-Noetherian rings, hence getting the converse implication involves assuming extra axioms [12]. Possibly one could here adapt to constructive algebra the counter example given by Blass [1] for WQO theory (see also [2]).

7 Conclusion and Perspectives

We emphasize Bar inductive predicates as a constructive foundation for Noetherian rings worthy of renewed interest. Without any other assumption on rings like e.g. coherence or (strong) discreteness, we implement a pen&paper proof of Hilbert's basis theorem. Additionally we show that Noetherian rings are closed under direct products, with an implementation as well. We derive well-foundedness principles for Bar Noetherian rings and compare with other constructive approaches like RS- and ML-Noetherianity. All the claimed results are sustained by an axiom free Rocq artifact.

There are many questions open for some follow up work. The strong similarity between the proofs of Ramsey's theorem, i.e. the closure of WQOs under direct products, and the closure of Noetherianity under direct products, make us wonder whether one result may be derived from the other? Or whether they both derive from a more abstract statement? In the same vein, one may wonder what could be the counterpart of the HBT in WQO theory (if any)? The Bar

[19] Rocq's StdLib defines $\texttt{well\_founded}\,(T : A \to A \to \mathbb{P}) := \forall a,\ \texttt{Acc}\, T\, a$.

inductive predicate proofs of Higman's lemma that we are aware of seem to differ largely from that of the HBT.

Since the results we implement work for non-discrete rings, what about constructive real numbers, the primary example of a non-discrete field: classically, the zero test function is not continuous. Can we find a field of constructive real numbers that would be Bezout? Bar Noetherian?

Finally, the termination of Buchberger's algorithm that computes Gröbner bases is usually grounded in Dickson's lemma [24]. Can we alternatively justify its termination using the HBT? There are other algorithms [16] for the same task. May be the HBT could be of some help there as well?

References

[1] A. Blass. 1986. Well-Ordering and Induction in Intuitionistic Logic and Topoi. In *Mathematical Logic and Theoretical Computer Science*. Taylor&Francis Group, Boca Raton, 29–48.

[2] G. Buriola, P. Schuster, and I. Blechschmidt. 2023. A Constructive Picture of Noetherian Conditions and Well Quasi-orders. In *Unity of Logic and Computation (CiE 2023)*. Springer, Cham, 50–62. https://doi.org/10.1007/978-3-031-36978-0_5

[3] T. Coquand. 2004. About Brouwer's Fan Theorem. *Revue internationale de philosophie* 58, 230 (4) (2004), 483–489. http://www.jstor.org/stable/23955601

[4] T. Coquand, A. Mörtberg, and V. Siles. 2012. Coherent and Strongly Discrete Rings in Type Theory. In *Certified Programs and Proofs (CPP'12)*. Springer Berlin Heidelberg, 273–288. https://doi.org/10.1007/978-3-642-35308-6_21

[5] T. Coquand and H. Persson. 1999. Gröbner Bases in Type Theory. In *Types for Proofs and Programs (TYPES'98)*. Springer Berlin Heidelberg, 33–46. https://doi.org/10.1007/3-540-48167-2_3

[6] D. Fridlender. 1998. Higman's lemma in type theory. In *Types for Proofs and Programs (TYPES'96)*. Springer Berlin Heidelberg, 112–133. https://doi.org/10.1007/BFb0097789

[7] D. Fridlender. 1999. An Interpretation of the Fan Theorem in Type Theory. In *Types for Proofs and Programs (TYPES'98)*. Springer Berlin Heidelberg, 93–105. https://doi.org/10.1007/3-540-48167-2_7

[8] B. Grégoire and A. Mahboubi. 2005. Proving Equalities in a Commutative Ring Done Right in Coq. In *Theorem Proving in Higher Order Logics (TPHOLs 2005)*. Springer Berlin Heidelberg, 98–113. https://doi.org/10.1007/11541868_7

[9] D. Hilbert. 1890. Ueber die Theorie der algebraischen Formen. *Math. Ann.* 36 (1890), 473–534. https://doi.org/10.1007/BF01208503

[10] C. Jacobsson and C. Löfwall. 1991. Standard bases for general coefficient rings and a new constructive proof of Hilbert's basis theorem. *Journal of Symbolic Computation* 12, 3 (1991), 337–371. https://doi.org/10.1016/S0747-7171(08)80154-X

[11] D. Larchey-Wendling. 2024. The Coq-Kruskal project. https://github.com/DmxLarchey/Coq-Kruskal

[12] D. Larchey-Wendling. 2025. Constructive Substitutes for Kőnig's Lemma. In *Types for Proofs and Programs (TYPES 2024) (LIPIcs, Vol. 336)*. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2:1–2:23. https://doi.org/10.4230/LIPIcs.TYPES.2024.2

[13] E. Makarov et al. 2006. Constructive Coq Repository at Nijmegen. https://github.com/rocq-community/corn.

[14] H. Perdry. 2004. Strongly Noetherian rings and constructive ideal theory. *Journal of Symbolic Computation* 37, 4 (2004), 511–535. https://doi.org/10.1016/j.jsc.2003.02.001

[15] H. Perdry. 2008. Lazy bases: a minimalist constructive theory of Noetherian rings. *Mathematical Logic Quarterly* 54, 1 (2008), 70–82. https://doi.org/10.1002/malq.200710042

[16] H. Perdry and P. Schuster. 2014. Constructing Gröbner bases for Noetherian rings. *Mathematical Structures in Computer Science* 24, 2 (2014), e240206. https://doi.org/10.1017/S0960129513000509

[17] H. Persson. 2001. *An Integrated Development of Buchberger's Algorithm in Coq*. Technical Report RR-4271. INRIA. https://inria.hal.science/inria-00072316

[18] B. Puyobro, B. Ballenghien, and B. Wolff. 2025. A Proof of Hilbert Basis Theorem and an Extension to Formal Power Series. *Archive of Formal Proofs* (2025). https://isa-afp.org/entries/Hilbert_Basis.html, Formal proof development.

[19] F. Richman. 1974. Constructive Aspects of Noetherian Rings. *Proc. Am. Math. Soc.* 44 (1974), 436–441. https://doi.org/10.2307/2040452

[20] P. Schuster and I. Yengui. 2025. An iterative constructive Hilbert basis theorem. *Journal of Algebra* 676 (2025), 56–68. https://doi.org/10.1016/j.jalgebra.2025.03.027

[21] A. Seidenberg. 1974. What is Noetherian? *Rend. Sem. Mat. Fis. Milano* 44 (1974), 55–61. https://doi.org/10.1007/BF02925651

[22] M. Sozeau. 2009. A New Look at Generalized Rewriting in Type Theory. *Journal of Formalized Reasoning* 2, 1 (2009), 41–62. https://doi.org/10.6092/issn.1972-5787/1574

[23] L. Théry. 1998. A Certified Version of Buchberger's Algorithm. In *Conference on Automated Deduction (CADE-15)*. Springer-Verlag, Berlin, Heidelberg, 349–364. https://dl.acm.org/doi/10.5555/648234.753471

[24] L. Théry. 2001. A Machine-Checked Implementation of Buchberger's Algorithm. *Journal of Automated Reasoning* 26 (2001), 107–137. https://doi.org/10.1023/A:1026518331905

[25] W. Veldman. 2006. Brouwer's Real Thesis on Bars. *Philosophia Scientiæ* (2006), 21–42. https://doi.org/10.4000/philosophiascientiae.404

[26] D. Vytiniotis, T. Coquand, and D. Wahlstedt. 2012. Stop When You Are Almost-Full. In *Interactive Theorem Proving*. Springer Berlin Heidelberg, 250–265. https://doi.org/10.1007/978-3-642-32347-8_17