Logical Methods in Computer Science
Vol. 9(3:20)2013, pp. 1–19
www.lmcs-online.org

Submitted Mar. 16, 2013
Published Sep. 17, 2013

INDUCTION IN ALGEBRA: A FIRST CASE STUDY *

PETER SCHUSTER

Pure Mathematics, University of Leeds, Leeds LS2 9JT, England
e-mail address: pschust@maths.leeds.ac.uk

Abstract. Many a concrete theorem of abstract algebra admits a short and elegant proof by contradiction but with Zorn's Lemma (ZL). A few of these theorems have recently turned out to follow in a direct and elementary way from the Principle of Open Induction distinguished by Raoult. The ideal objects characteristic of any invocation of ZL are eliminated, and it is made possible to pass from classical to intuitionistic logic. If the theorem has finite input data, then a finite partial order carries the required instance of induction, which thus is constructively provable. A typical example is the well-known theorem "every nonconstant coefficient of an invertible polynomial is nilpotent".

1. Introduction

Many a concrete theorem of abstract algebra admits a short and elegant proof by contradiction but with Zorn's Lemma (ZL). A few of these theorems have recently turned out to follow in a direct and elementary way from the Principle of Open Induction (OI) distinguished by Raoult [42]. A proof of the latter kind may be extracted from a proof of the former sort. If the theorem has finite input data, then a finite partial order carries the required instance of induction, which thus is provable by mathematical induction—or, if the size of the data is fixed, by fully first-order methods.

But what is Open Induction? In a nutshell, OI is transfinite induction for subsets of a directed-complete partial order that are open with respect to the Scott topology. While OI was established [42] as a consequence of ZL, by complementation these two principles are actually equivalent [21] with classical logic but in a natural way. Hence OI is the fragment of transfinite induction of which the corresponding minimum principle just is ZL.

Our approach is intended as a contribution to a partial realisation in algebra [13] of the revised Hilbert Programme à la Kreisel and Feferman (see [17] for a recent account including references), and was motivated by related work in infinite combinatorics [8, 11, 14, 42] as well as by the methods of dynamical algebra [16, 39, 51] and formal topology [30, 44, 46]. In Hilbert's terminology, the "ideal objects" characteristic of any invocation of ZL are eliminated by passing to OI, and it is made possible to work with "finite methods" only, e.g. to pass from classical to intuitionistic logic.

2012 ACM CCS: [**Theory of computation**]: Logic—Proof theory / Constructive mathematics.
Key words and phrases: constructive algebra; Hilbert's Programme; intuitionistic logic; open induction; Zorn's Lemma.

* This is a revised and extended journal version of the author's LICS 2012 conference paper [48].

LOGICAL METHODS IN COMPUTER SCIENCE
DOI:10.2168/LMCS-9(3:20)2013

A typical example, studied before [41, 43] and taken up in this paper, is the well-known theorem "every nonconstant coefficient of an invertible polynomial is nilpotent". More formally, this can be put as

$$fg = 1 \to \exists e \, (u^e = 0) \tag{1.1}$$

where f and g are polynomials with coefficients in an arbitrary commutative ring

$$f = \sum_{i=0}^{n} a_i T^i \,, \quad g = \sum_{i=0}^{m} b_j T^j$$

and $u = a_{i_0}$ where $1 \leq i_0 \leq n$. The customary short and elegant proof of (1.1) works by reduction to the case of polynomials over an integral domain

$$fg = 1 \to u = 0$$

or, equivalently, by reduction modulo any prime ideal P of the given ring:

$$fg = 1 \to \forall P \, (u \in P) \, . \tag{1.2}$$

This special case is readily settled by looking at the degrees, or more explicitly by a polynomial trick due to Gauß [15, 29]. In order to reduce (1.1) to (1.2), it is natural to invoke

$$\forall P \, (u \in P) \to \exists e \, (u^e = 0) \, . \tag{1.3}$$

But the latter, a variant of Krull's Lemma, is normally deduced from ZL by a proof by contradiction, which is anything but an argument using only finite methods. In addition, a universal quantification over prime ideals P occurs, which are ideal objects (see e.g. [17]).

These foundational issues aside, there is a practical problem. By decomposing (1.1) into (1.2) and (1.3) one virtually loses the computational information the hypothesis of (1.1) is made of; in particular [41, 43] the proof falls short of being an algorithm for computing an exponent e under which the nilpotent u vanishes. However, we can still extract a proof that is based on induction over a finite partial order; and the proof tree one can grow alongside the induction encodes an algorithm which computes the desired exponent.

That our method does work may seem less surprising if one takes into account that the theorem has already seen constructive proofs before [41, 43], and that an entirely down-to-earth proof is possible anyway [4, Chapter 1, Exercise 2]. Needless to say, each of those proofs embodies an algorithm; one of them [41] has even been partially implemented in Agda, a proof assistant based on Martin–Löf type theory.

Just as the proof in [41], our constructive proof is gained from a given classical one, the one by reduction to the case of integral domains we have mentioned above. As compared with [41], we keep somewhat closer to the classical proof. The price we have to pay is that we have to suppose certain decidability hypotheses, which need to—and can—be eliminated afterwards by a variant of the Gödel–Gentzen and Dragalin–Friedman translations. In [41] a simpler instance of this elimination method is built directly into the proof.

To be slightly more specific, we we first turn the indirect proof of (1.3) with ZL into a direct deduction from OI; and then transform the latter into a constructive proof of (1.1) by induction over a finite poset. This is possible because the hypothesis of (1.1)—unlike the one of (1.3)—consists of computationally relevant information about a finite amount of elementary data: of nothing but the finitely many equations

$$a_0 b_0 = 1, \, a_0 b_1 + a_1 b_0 = 0 \, , \ldots , \, a_n b_m = 0 \, .$$

Heuristics aside, all this makes redundant the reduction, and the prime ideals disappear.

1.1. **Preliminaries.**

1.1.1. *Foundations.* The overall framework of this note is *constructive* algebra à la Kronecker and Bishop [31, 35]. Due to the corresponding choice of intuitionistic logic, one or the other assumption needs to be made explicit that would be automatic in *classical* algebra, by which we mean algebra as carried out within **ZFC** set theory and thus, in particular, with classical logic. For example, we say that an assertion A is *decidable* whenever $A \vee \neg A$ holds; and that a subset S of a set T is *detachable* if $t \in S$ is decidable for each $t \in T$.

As moreover the principle of countable choice will not occur, let alone the one of dependent choice, our constructive reasoning can be carried out within (a suitable elementary fragment of) the Constructive Zermelo–Fraenkel Set Theory **CZF** which Aczel [1, 2, 3] has interpreted within Martin-Löf's [34] Intuitionistic Theory of Types. Unlike Friedman's [19] impredicative Intuitionistic Zermelo–Fraenkel Set Theory **IZF**, this **CZF** does not contain the axiom of power set. Hence in **CZF** an unrestricted quantification over subsets—such as the one crucial for this paper, over all prime ideals of an arbitrary ring—in general is a quantification over the members of a class.

1.1.2. *Rings.* Throughout this paper, R will denote a commutative ring (with unit). We briefly recall some related concepts [4]. An *ideal* of R is a subset I that contains 0, is closed under addition, and satisfies

$$s \in I \to rs \in I$$

for all $r, s \in R$. We write (S) for the ideal *generated* by a subset S of R: that is, (S) consists of the linear combinations $r_1 s_1 + \ldots + r_n s_n$ of elements $s_1, \ldots, s_n$ of S with coefficients $r_1, \ldots, r_n$ from R.

A *radical ideal* of R is an ideal I such that

$$r^2 \in I \to r \in I$$

for all $r \in R$. The *radical*

$$\sqrt{I} = \{r \in R : \exists e \in \mathbb{N}\,(r^e \in I)\}$$

of an ideal I is a radical ideal with $I \subseteq \sqrt{I}$. An ideal I is a radical ideal if and only if $I = \sqrt{I}$. The radical $\sqrt{0}$ of the zero ideal $0 = \{0\}$ is the *nilradical*, and its elements are the *nilpotents*.

An ideal P is a *prime ideal* if $1 \notin P$ and

$$ab \in P \to a \in P \vee b \in P \tag{1.4}$$

for all $a, b \in R$. Clearly, every prime ideal is a radical ideal. A ring R is an *integral domain*—for short, a *domain*—if $1 \neq 0$ in R and

$$ab = 0 \to a = 0 \vee b = 0 \tag{1.5}$$

for all $a, b \in R$. A quotient ring R/P is a domain if and only if P is a prime ideal.

1.1.3. *Induction.* Let $(X, \leq)$ be a partial order. We do not specify from the outset whether X is a set in the sense of **CZF**, which in the case of our definite interest will anyway be the case, but during heuristics will depend on the choice of a more generous set theory such as **IZF**. Unless specified otherwise every quantification over the variables x, x', y, and z is understood as over the elements of the partial order X under consideration.

Let U be a predicate on X. We say that U is *progressive* if

$$\forall x \, (\forall y > x \, U(y) \to U(x)), \tag{1.6}$$

where $y > x$ is understood as the conjunction of $y \geq x$ and $y \neq x$. About the antecedent of (1.6), note that $y > x$ is used rather than $y < x$, as is common in other contexts; our choice allows us to avoid reversing the naturally given order (i.e., inclusion) later on. Also, in the relevant instantiations below, the predicate U will define—and be identified with—a subset of the set X; and $\leq$ will be a decidable relation (that is, for all $x, y \in X$, the assertion $x \leq y$ is decidable).

By *induction for U and X* we mean the following:

If U is progressive, then $\forall x \, U(x)$.

Classically, induction holds for *every* U precisely when X is *well-founded* in the sense that every inhabited predicate on X has a maximal element—or, in classically equivalent terms, that there is no strictly increasing sequence in X.

We will use induction in cases in which X has a least element $\perp$, in which $U(\perp)$ is equivalent to $\forall x \, U(x)$ whenever U is *monotone:* that is, if $x \leq y$, then $U(x)$ implies $U(y)$. Note finally that if U is progressive, then U is satisfied by every maximal element of X, and thus by the greatest element $\top$ of X whenever this exists.

2. Noetherian Rings

As a warm-up we first revisit the perhaps historically first—albeit implicit—occurrence of induction in algebra: Krull's proof [27, pp. 8–9] of the Lasker–Noether decomposition theorem for Noetherian rings. According to one of the constructively meaningful variants of this concept [23], a ring is *Noetherian* if induction holds for the partial order consisting of the finitely generated ideals, which by the way is a set in **CZF**. We now prove, using this instance of induction, the following corollary of the *Lasker–Noether Theorem*:

LN: *The radical $\sqrt{I}$ of every finitely generated ideal I of a commutative Noetherian ring is the intersection of finitely many finitely generated prime ideals.*

Constructive proofs given before [39] with related notions of "Noetherian" have motivated our choice of this example; see also [40].

Before proving LN we recall a well-known fact (see e.g. the proof of [4, Proposition 1.8]), which however will be crucial for a large part of this paper.

Lemma 2.1. *Let R be a commutative ring. If I is an ideal of R, and $a, b \in R$, then*

$$\sqrt{I + Ra} \cap \sqrt{I + Rb} = \sqrt{I + Rab}.$$

Proof. Since $\supseteq$ is clear, we only verify $\subseteq$. Let $x \in \sqrt{I + Ra}$ and $x \in \sqrt{I + Rb}$, which is to say that $x^k = u + sa$ and $x^\ell = v + tb$ where $k, \ell \in \mathbb{N}$, $u, v \in I$, and $s, t \in R$. Then

$$x^k x^\ell = \underbrace{uv + utb + sav}_{\in I} + st \, ab$$

and thus $x^{k+\ell} \in I + Rab$ as required. ∎

In addition to this, and the aforementioned instance of induction, we need to employ a distinction-by-cases that is known as *Strong Primality Test (SPT)* [39]. This says that for every finitely generated ideal I of R one of the following three conditions is fulfilled:

(i) $I = R$, which is to say that $1 \in I$;
(ii) for all $a, b \in R$, if $ab \in I$, then either $a \in I$ or $b \in I$;
(iii) there are $a, b \in R$ for which $ab \in I$ but neither $a \in I$ nor $b \in I$.

In other words, the SPT tells us whether I is a prime ideal; and moreover if the answer is in the negative, then the SPT provides us with witnesses for this fact. Clearly SPT is classically valid, but it also holds constructively whenever R is a fully Lasker–Noether ring [39].

To prove LN by induction, consider "$\sqrt{I}$ is the intersection of finitely many prime ideals" as a predicate U of the finitely generated ideals I of R. To show that U is progressive, let I be a finitely generated ideal of R. If $I = R$, then clearly $U(I)$; if I is a prime ideal, then in particular $\sqrt{I} = I$, and thus $U(I)$. If however $a, b \in R$ are as in case (iii) of SPT, then $I \subsetneqq I + Ra$ and $I \subsetneqq I + Rb$ but $I = I + Rab$; whence $U(I + Ra)$ and $U(I + Rb)$ hold by induction, and $U(I)$ follows with Lemma 2.1 at hand.

This proof of LN can be carried over in a relatively easy way to the full Lasker–Noether theorem, and as such can be viewed as an "unwinding" not only of Krull's proof, but also of the better-explicated proofs given in [4, 37]. We refrain from doing this transfer to the full theorem, for no further insight into the method would be gained.

3. Some Induction Principles

When does induction hold more in general, regardless of the specific partial order under consideration? A fairly general induction principle has been coined by Raoult [42] as follows. A partial order X is *chain-complete* if every chain Y in X has a least upper bound $\bigvee Y \in X$. A predicate U on X is *open* in the lower topology if, for every chain Y in X,

$$U(\bigvee Y) \to \exists x \in Y \, U(x).$$

(Think of the elements x of Y as of "neighbourhoods" of the "limit" $\bigvee Y$ of Y.) Now Raoult's *Open Induction (OI)* is induction for chain-complete X and open U. It is easy to see [42] that OI follows classically from *Zorn's Lemma (ZL)*, and thus holds in **ZFC**; moreover OI and ZL are classically equivalent [21], by complementation.

Open Induction implies *Well-Founded Induction (WI)* which is induction for well-founded X and arbitrary U.[1] In fact, if X is well-founded, then every chain in X has a greatest element; whence X is chain-complete, and every U is open. Unlike OI, WI is provable in **ZF**, but most partial orders that are classically well-founded lack this property from a constructive perspective. For the notion of a Noetherian ring one can, as we have recalled above, circumvent this problem by simply defining a commutative ring to be Noetherian if one can perform induction on the finitely generated ideals [23].

We say that a partial order X is *finite* if X has finitely many elements (that is, $X = \{x_1, \ldots, x_n\}$ for some $n \geq 0$, which includes the case $n = 0$ of $X = \emptyset$), and if, in addition,

[1] This principle is also known as *Noetherian Induction* and, in the case of a well-ordered X, as *Transfinite Induction*; see e.g. [10, p. 21].

$\leq$ is a decidable relation. In this case, X is a *discrete* set, which is to say that equality $=$ is decidable;[2] whence so is $<$ too.

Classically, every finite X is well-founded; whence WI implies *Finite Induction (FI)*: that is, induction for finite X and for arbitrary U. Unlike WI, this FI is even constructively provable, as in **CZF**, by means of mathematical induction. To see this note first that if X is finite, then one can exhibit a maximal element x of X, for which $U(x)$ anyway. In fact, if X has only finitely many elements, then $\neg\forall x\exists y\,(x < y)$, which is to say that $\exists x\neg\exists y\,(x < y)$ if, in addition, $\leq$ is decidable.

4. A Proof Pattern

In all cases considered later in this paper, X consists in certain ideals of a commutative ring, with the partial order given by inclusion, for which $\wedge$ simply is $\cap$. Following the terminology which is standard for this special case, we also say for a general partial order X that $x \in X$ is *reducible* if there are $y, z \in X$ such that $x < y$, $x < z$, and $x = y \wedge z$. Here $x = y \wedge z$ is to be understood as that x is the greatest lower bound of y and z: that is,

$$\forall x'\,(x' \leq x \longleftrightarrow x' \leq y \wedge x' \leq z).$$

In the following, let again U be a predicate on a partial order X. We say that U is *good* if, for every $x \in X$, either $U(x)$ or x is reducible. Also, we say that U is *meet-closed* whenever if $x = y \wedge z$ in X, then $U(x)$ follows from $U(y) \wedge U(z)$.

Lemma 4.1. *Let U be a predicate on a partial order X. If U is meet-closed and good, then U is progressive.*

All this allows us to state a proof pattern that has been prompted by [20]:

Theorem 4.2. *Assume that induction holds for U and X. If U is meet-closed and good, then $\forall x\, U(x)$.*

We will next look into applications of this proof pattern.

5. Krull's Lemma with Open Induction

Let R again be a commutative ring. For heuristic purposes we first look at the contrapositive of a variant of *Krull's Lemma*:

KL: *If $r \in P$ for all prime ideals P of R, then $r \in \sqrt{0}$.*

As is well known (see, for example, the proof of [4, Proposition 1.8]), with ZL at hand one can give a proof by contradiction of KL: if $r^e \neq 0$ for all $e \in \mathbb{N}$, which is to say that $0 \notin S$ for the multiplicative set $S = \{r^e : e \in \mathbb{N}\}$, then by ZL there is a prime ideal P of R with $P \cap S = \emptyset$ and, in particular, $r \notin P$. If R is Noetherian in the sense of [23], then KL is an instance of LN, which we have already reproved by induction, without any talk of ZL.

For an arbitrary ring R, KL can be deduced from OI in a direct way, by Theorem 4.2 and as follows. As OI requires a chain-complete X, this time we have to let X consist of all the radical ideals of R. This X actually is a frame with $\perp = \sqrt{0}$ and $\top = R$, and a

[2] For any such X, in particular, there is no need to distinguish between "X is finite" and "X is finitely enumerable", as is customary in constructive mathematics: these two variants of the notion of a finite set coincide in the case of a discrete set [35, p. 11].

set in **IZF**. Accordingly, we need a strong primality test for arbitrary (radical) ideals, but remember that we are still doing heuristics.

Now, let $r \in P$ for all prime ideals P of R. To prove $r \in \sqrt{0}$ we define the predicate U on X by $U(F) \equiv r \in F$ whenever $F \in X$, for which clearly $U(\top)$. Further, U is meet-closed and monotone. In particular, to show that $U(F)$ holds for all $F \in X$ is tantamount to showing that $U(\bot)$, i.e. $r \in \sqrt{0}$, which is exactly what we are after.

To see that U is good, let $F \in X$: that is, $F = \sqrt{I}$ for some ideal I of R. If $F = R$, then trivially $U(F)$; if F is a prime ideal, then $U(F)$ by hypothesis; if however there are $a, b \in R$ such that $ab \in F$ but neither $a \in F$ nor $b \in F$, then $F \subsetneqq \sqrt{I + Ra}$ and $F \subsetneqq \sqrt{I + Rb}$ but $\sqrt{I + Rab} = F$; whence F is reducible by Lemma 2.1. In all, Theorem 4.2 applies.

6. Nilpotent Coefficients with Finite Induction

We now can proceed to our principal example. Once more let R be a commutative ring, which we now suppose to be a set in **CZF**. Recall that $r \in R$ is said to be a *unit* or *invertible* if there is $s \in R$ such that $rs = 1$. As usual let $R[T]$ stand for the ring of polynomials with indeterminate T and coefficients from R. Pick an arbitrary $f \in R[T]$ and write it as $f = \sum_{i=0}^{n} a_i T^i$. We consider the following statement about *nilpotent coefficients*:

NC: *If f is a unit of $R[T]$, then $a_i \in \sqrt{0}$ for $i > 0$.*

This is well-known, and can be put as

$$\exists g \in R[T]\ (fg = 1) \to \forall i \in \{1, \ldots, n\} \exists e \in \mathbb{N}\ (a_i^e = 0)$$

or equivalently as

$$\forall g \in R[T]\, \forall i \in \{1, \ldots, n\}\, (fg = 1 \to \exists e \in \mathbb{N}\ (a_i^e = 0)\,)\ .$$

Pick $g \in R[T]$ and $i_0 \in \{1, \ldots, n\}$, and set $u = a_{i_0}$. Hence the essence of NC is

$$fg = 1 \to \exists e \in \mathbb{N}\ (u^e = 0)\ .$$

Write f, g as

$$f = \sum_{i=0}^{n} a_i T^i\,, \quad g = \sum_{i=0}^{m} b_j T^j\ .$$

Since then

$$fg = \sum_{k=0}^{n+m} c_k T^k\,, \quad c_k = \sum_{i+j=k} a_i b_j\,,$$

the hypothesis $fg = 1$ can be expressed as

$$c_0 = 1 \wedge c_1 = 0 \wedge \ldots \wedge c_{n+m} = 0 \tag{6.1}$$

or even more explicitly as

$$a_0 b_0 = 1 \wedge a_0 b_1 + a_1 b_0 = 0 \wedge \ldots \wedge a_n b_m = 0\,. \tag{6.2}$$

In particular $fg = 1$ is a finite conjunction of atomic formulas of the language of rings.

By swapping f and g one could also take u from the $b_1, \ldots, b_m$ rather than from the $a_1, \ldots, a_n$. We do not follow this option, but note for later use that under the hypothesis $fg = 1$ we have

$$\forall i > 0\ (a_i \in F) \leftrightarrow \forall j > 0\ (b_j \in F) \tag{6.3}$$

for every ideal F of R; in the particular case $F = 0$ this means

$$\forall i > 0\ (a_i = 0) \leftrightarrow \forall j > 0\ (b_j = 0)\ . \tag{6.4}$$

As for (6.3), let $i \in \{1, \ldots, n\}$. If $b_j \in F$ for all $j \in \{1, \ldots, \min\{i, m\}\}$, then

$$F \ni c_i = \underbrace{a_0 b_i + \ldots + a_{i-1} b_1}_{\in F} + a_i b_0$$

by (6.1) and thus $a_i b_0 \in F$, from which we get $a_i \in F$ because $a_0 b_0 = 1$ by (6.2). A similar argument deals with the converse implication in (6.3).

As Richman has observed [43], the statement NC above

> ... admits an elegant proof upon observing that each a_i with $i \geq 1$ must be in every prime ideal of R, and that the intersection of the prime ideals of R consists of the nilpotent elements of R. This proof gives no clue as to how to calculate n such that $a_i^n = 0$, while such a calculation can be extracted from the proof that we present.

Richman's fairly short proof [43] is in fact a clever "nontrivial use of trivial rings", and of course is fully constructive. The elementary character of NC anyway suggests an equally elementary proof, by mathematical induction, as indicated in [4, Chapter 1, Exercise 2]. Just as for the approach [41] via point-free topology, the point of our subsequent considerations is that we "unwind" the classical proof that Richman has rightly deemed "elegant", and thus get a constructive one from which the required exponent can equally be extracted.

6.1. **A Classical Proof with Krull's Lemma.** We next review the "elegant" proof of NC which works by reduction to the case of a domain. Since in a domain every nilpotent is zero, NC for domains reads as

$\mathrm{NC}_{\mathrm{int}}$: *Let R be a domain. If f is a unit of $R[T]$, then $a_i = 0$ for $i > 0$.*

With the notation from before, the essence of $\mathrm{NC}_{\mathrm{int}}$ is

$$fg = 1 \to u = 0\,.$$

A quick proof goes as follows. Let R be a domain. Then the degree of non-zero polynomials (remember that we are in a classical setting) satisfies

$$\deg(fg) = \deg(f) + \deg(g)\ . \tag{6.5}$$

Now if $fg = 1$, then $\deg(fg) = 0$ in view of (6.1) and of $1 \neq 0$ (recall that R is a domain); whence $\deg(f) = 0$ and thus in particular $u = 0$ as required. Note that the special case

$$\deg(fg) = 0 \to \deg(f) = 0 \tag{6.6}$$

of (6.5) is sufficient for proving $\mathrm{NC}_{\mathrm{int}}$.

Alternatively one can prove $\mathrm{NC}_{\mathrm{int}}$ by means of a trick that has been ascribed to Gauß [15, 29], and which is nothing but an explicit version of (6.6). To this end let again R be a domain, and suppose that $fg = 1$. Now assume towards a contradiction that $a_i \neq 0$ for some $i > 0$; whence by (6.4) also $b_j \neq 0$ for some $j > 0$. Pick i, j both maximal with these properties, for which

$$0 = c_{i+j} = \underbrace{\sum_{q>j} a_p b_q}_{=0} + a_i b_j + \underbrace{\sum_{p>i} a_p b_q}_{=0} \tag{6.7}$$

and thus $a_i b_j = 0$; whence either $a_i = 0$ or $b_j = 0$, a contradiction.

Following a time-honoured tradition, the case of NC for an arbitrary ring R is handled by working modulo a generic prime ideal P of R, for which the quotient ring R/P is indeed a domain. Hence if P is a prime ideal, then we can apply $\mathrm{NC}_{\mathrm{int}}$ with R/P in place of R. This yields that for all prime ideals P of R we have $u = 0$ in R/P, which is to say that $u \in P$. In all, u is nilpotent by KL, which we have deduced from OI before.

6.2. **Discussion and Outline.** In the classical proof above one first aims at the implication

$$fg = 1 \to \forall P\,(u \in P)\ ,$$

and then combines it with the appropriate instance of KL:

$$\forall P\,(u \in P) \to \exists e\,(u^e = 0)\ .$$

The corresponding invocation of ZL or OI aside, there is another foundational problem with this classical proof: it rests upon a universal quantification over all the prime ideals of R, which are ideal objects in Hilbert's sense. This is reflected by the practical problem that the computational information of $fg = 1$ is virtually lost when passing to $\forall P\,(u \in P)$.

However, in the given situation one can do better. Before following our own route, we briefly sketch the dual of the translation [41] of the "elegant" proof into point-free terms.[3] The key move is to rewrite the classical proof by reduction to R/P where P is any prime ideal, by replacing every occurrence of $x \in P$ by one of $D\,(x) = 0$. Here one considers the bounded distributive lattice [25]—see also, for instance, [6, 24]—that is generated by the symbolic expressions $D\,(x)$ indexed by the $x \in R$ and subject to the relations

$$\begin{array}{ll} D(1) = 1\,, & D(xy) = D(x) \wedge D(y)\,, \\ D(0) = 0\,, & D(x+y) \leq D(x) \vee D(y)\,, \end{array}$$

which are dual to the characteristic properties of a prime ideal P:

$$\begin{array}{ll} 1 \notin P\,, & xy \in P \leftrightarrow x \in P \vee b \in P\,, \\ 0 \in P\,, & x \in P \wedge y \in P \to x + y \in P\,. \end{array}$$

Having shown by rewriting that $D\,(u) = 0$, the key observation is that one can realise this lattice by definining $D\,(x_1) \vee \ldots \vee D\,(x_n)$ as the radical of the ideal generated by $x_1, \ldots, x_n$. In particular the least element 0 of the lattice is turned into the nilradical $\sqrt{0}$, and $D\,(u) = 0$ is interpreted as $u \in \sqrt{0}$. The resulting proof [41] is fully constructive, and works without any of the decidability assumptions we will have to make—and to eliminate eventually by a combination of the Gödel–Gentzen and Dragalin–Friedman proof translations. In [41] only the essence of this elimination method occurs, already within the proof and at a lower level.

In our own constructive proof of NC we still follow the lines along which we have deduced KL from OI, but since the hypothesis of NC is computationally more informative than the one of KL, we can get by with much less: with FI in place of OI. For short, we pass from the top to the bottom side of the following square:

$$\begin{array}{ccc} \mathrm{OI} & \to & \mathrm{KL} \\ \downarrow & & \downarrow \\ \mathrm{FI} & \to & \mathrm{NC} \end{array}$$

Yet we have to make a move that in the first place may seem nonconstructive: as we had to assume (a variant of) SPT before, we now employ another type of a classically valid distinction-by-cases, which has occurred in constructive and computable algebra [31, 35, 49].

[3] This has kindly been pointed out to us by one of the anonymous referees.

However, as we have hinted at above and will sketch below (Section 6.4.7), this use of fragments of the Law of Excluded Middle can be eliminated by proof theory.

6.3. **Constructive Proofs by Induction.**

6.3.1. *With the Proof Pattern.* To deduce NC from FI, let X be the partial order that consists of the radical ideals of the ideals generated by some of the nonconstant coefficients of f and g. In other words, an element F of X is of the form $F = \sqrt{I}$ where $I = (D)$ is the ideal generated by a detachable subset D of the set E of the nonconstant coefficients of f and g: that is,

$$E = \{a_1, \dots, a_n, b_1, \dots, b_m\}.$$

This X, ordered by inclusion, possesses $\bot = \sqrt{0}$ and $\top = \sqrt{(E)}$, corresponding to $D = \emptyset$ and $D = E$. We assume that $r \in F$ is decidable for all $r \in E$ and $F \in X$; whence in particular the partial order X is finite in the sense coined before (recall that $\sqrt{I} \subseteq \sqrt{J}$ if and only if $I \subseteq \sqrt{J}$). Now define the predicate U on X by

$$U(F) \equiv u \in F\,.$$

Both X and U are sets in **CZF**. Again $U(\top)$, and U is meet-closed and monotone. Once more our goal is to show $U(\bot)$, and to apply the proof pattern from Theorem 4.2 we prove that U is good. Let $F \in X$. By our decidability assumption we can distinguish the following two cases.

Case 1. If $a_i \in F$ for all $i > 0$, then $u \in F$ and thus $U(F)$.

Case 2. If $a_i \notin F$ for some $i > 0$, then by (6.3) also $b_j \notin F$ for some $j > 0$. In this case—following Gauß's trick again—we pick i, j that are maximal of this kind, for which (where in each sum $p + q = i + j$)

$$F \ni c_{i+j} = \underbrace{\sum_{q>j} a_p b_q}_{\in F} + a_i b_j + \underbrace{\sum_{p>i} a_p b_q}_{\in F} \tag{6.8}$$

and thus $a_i b_j \in F$. Pretty much as in the deduction of KL from OI, one can now see that F is reducible. In detail, let $F = \sqrt{I}$ where $I = (D)$ for a detachable subset D of E, and set

$$G = \sqrt{I + Ra_i}\,, \quad H = \sqrt{I + Rb_j}\,, \tag{6.9}$$

for which $G, H \in X$, and $F \subsetneqq G$ and $F \subsetneqq H$ according to the particular choice of i and j. Moreover, $F = \sqrt{F}$ since F is a radical ideal; and $\sqrt{F} = G \cap H$ by Lemma 2.1 and because $a_i b_j \in F$. Hence $F = G \cap H$ is the required decomposition of F.

6.3.2. *An Alternative Proof.* We now give an alternative deduction of NC from FI in which the exponents are moved from X to U. This allows for a conceptually simpler X, and for a better understanding of the corresponding tree and algorithm (see below). However we can no longer follow the proof pattern encapsulated in Theorem 4.2, because Lemma 2.1 fails once the radicals are removed. The modified predicate can still be proved to be progressive, and induction is possible.

Here let X be the partial order that consists of *all* the ideals generated by some of the nonconstant coefficients of f and g: that is, an element of X is of the form $I = (D)$ where

D is a detachable subset of E as before. Again, X has finitely many elements, and we may assume that $\subseteq$ is a decidable relation on X, which is to say that

$$\forall r \in E \forall F \in X \ (r \in F \vee r \notin F) \ . \tag{6.10}$$

In all, X ordered by inclusion is a finite partial order. Now we define the predicate U on X in a slightly different way by

$$U(I) \equiv \exists e \in \mathbb{N} \, (u^e \in I) \, .$$

Once more both X and U are sets in **CZF**, and U is monotone. To prove $U\,(0)$ by induction, or equivalently that $U\,(I)$ for all $I \in X$, let $I \in X$. As before yet with I in place of F, we distinguish two cases.

Case 1. If $a_i \in I$ for all $i > 0$, then $u \in I$, and $e = 1$ witnesses $U\,(I)$.

Case 2. If $a_i \notin I$ for some $i > 0$, then by (6.3) also $b_j \notin I$ for some $j > 0$. Pick i, j that are maximal of this kind. As before, still with I in place of F, one can show that $a_i b_j \in I$. Set

$$K = I + Ra_i \, , \quad L = I + Rb_j \tag{6.11}$$

Now $K, L \in X$, and $I \subsetneqq K$ and $I \subsetneqq L$. By induction, $U\,(K)$ and $U\,(L)$: that is, there are $k, \ell \in \mathbb{N}$ such that $u^k \in K$ and $u^\ell \in L$. Hence $u^k u^\ell \in I + Ra_i b_j$ (see the proof of Lemma 2.1), and thus $u^{k+\ell} \in I$ because $a_i b_j \in I$; so $e = k + \ell$ witnesses $U\,(I)$.

6.4. **Tree and Algorithm.**

6.4.1. *Growing a Tree.* It is well-known how a tree can be grown along a proof by induction. We next instantiate this method for the preceding proof, the notations and hypotheses of which we adopt. In parallel to creating the nodes, we label them by elements of X. To start the construction, we label the root by 0. If a node N labelled by $I \in X$ has just been constructed, then we proceed according to the distinction-by-cases made during the proof, as follows:

Case 1. Declare N to be a leaf.

Case 2. Endow N with two children labelled by K and L as in (6.11).

We thus get a full binary tree: every node either is a leaf or else is a parent with exactly two children. Moreover the labelling is strictly increasing: if a parent is labelled by I, and any one of its children by J, then $I \subsetneqq J$. In particular, the tree is finite.

By construction, the label I of a node N satisfies U whenever either N is a leaf or else N is a parent both children of which have labels satisfying U. In fact, in Case 1 we have $U(I)$ anyway; in Case 2 if $U(K)$ and $U(L)$, then $U(I)$ as shown in the proof. Climbing down from the leaves to the root—that is, doing induction on the height of a node, i.e. its distance from the nearest leaf—one can thus show $U\,(I)$ for every I that occurs as the label of a node. In particular, the label 0 of the root satisfies U: that is, $U\,(I)$ for all $I \in X$.

6.4.2. *About Size.* To get an idea of the size of the tree we review its construction in terms of the generators of the labels. First, the label 0 of the root is generated by the empty set $\emptyset$. Secondly, the label of a child is obtained by adding a single element to the generators of the label I of the parent: an element a_i of $\{a_1, \dots, a_n\} \setminus I$ for the one child and an element b_j of $\{b_1, \dots, b_m\} \setminus I$ for the other child, where both i and j are maximal among the remaining indices. Thirdly, a node is a leaf whenever either all the $a_1, \dots, a_n$ or equivalently all the $b_1, \dots, b_m$ belong to the generators of the label.

This said, what are the extremal lengths of the paths from the root to the leaves? The height of the tree, i.e. the length of the longest path, is at most $n + m - 1$. In fact, the longest paths have to be taken whenever for the choice of new generators one keeps switching between the $a_1, \dots, a_n$ and the $b_1, \dots, b_m$. This is the case, for example, if one adds first a_n, secondly b_m, thirdly a_{n-1}, next b_{m-1}, and so on. From the root this requires adding all the $a_2, \dots, a_n$ and all the $b_2, \dots, b_m$, and thus possibly $n-1+m-1$ nodes, before one arrives at a leaf by eventually adding either a_1 or b_1.

However there are shorter paths, which have length $\leq \min\{n, m\}$: the path along which only the $a_1, \dots, a_n$ (respectively, only the $b_1, \dots, b_m$) are successively added to the generators has length $\leq n$ (respectively, length $\leq m$). Even shorter paths are possible whenever the $a_1, \dots, a_n$ and $b_1, \dots, b_m$ fulfil additional conditions; some of these coefficients may indeed be equal or otherwise related in an appropriate way. In general however the tree is uniform in the given data. We henceforth assume the generic situation in which the $a_0, \dots, a_n$ and $b_0, \dots, b_m$ do not satisfy any further algebraic dependence relation apart from (6.2), and accordingly can be seen as indeterminate coefficients [31, p. 82] only subject to (6.2).

6.4.3. *Removing Redundancy.* The tree is repetitive inasmuch as some subtrees occur several times. To remove this redundancy, one can identify all subtrees of the same form, and rearrange the arrows accordingly. One thus transforms the tree into a simple acyclic digraph with the source and the sinks coming from the root and the leaves, respectively:

$$\begin{array}{ccccccc}
0 & \to & (b_m) & \to \dots \to & (b_2, \dots, b_m) & \to & (b_1, \dots, b_m) \\
\downarrow & & \downarrow & & \downarrow & & \\
(a_n) & \to & (a_n, b_m) & \to \dots \to & (a_n, b_2, \dots, b_m) & \to & (a_n, b_1, \dots, b_m) \\
\downarrow & & \downarrow & & \downarrow & & \\
\vdots & & \vdots & & \vdots & & \vdots \\
\downarrow & & \downarrow & & \downarrow & & \\
(a_2, \dots, a_n) & \to & (a_2, \dots, a_n, b_m) & \to \dots \to & (a_2, \dots, a_n, b_2, \dots, b_m) & \to & (a_2, \dots, a_n, b_1, \dots, b_m) \\
\downarrow & & \downarrow & & \downarrow & & \\
(a_1, \dots, a_n) & & (a_1, \dots, a_n, b_m) & \dots & (a_1, \dots, a_n, b_2, \dots, b_m) & &
\end{array}$$

While the only source is in the top left corner, the $n + m$ sinks form the rightmost column and the bottom row. There are $nm + n + m$ vertices; and if we removed the sinks, then we would get a square grid graph with n rows and m columns.

6.4.4. *Computing Witnesses.* In the foregoing we have proved constructively, with FI, that $u^e = 0$ for some $e \in \mathbb{N}$. Hence the tree grown alongside the induction encodes an algorithm to compute a witness for this existential statement: that is, an exponent e under which $u^e = 0$. This algorithm terminates since, as we have observed before, the tree is finite.

Proof, tree, and algorithm are furthermore independent of the choice of u among the $a_1, \dots, a_n$; and thus only depend on n and m. In fact the e produced by the algorithm works for each of the u from the $a_1, \dots, a_n$, though—as in the example below—a smaller exponent may suffice for some. One could also have shortened proof, tree, and algorithm by stopping already when the given u belongs to the ideal I under consideration; for the sake of uniformity we have disregarded this option.

We now look back to see where the exponents come from and how they grow during the course of the algorithm.[4] For any node N labelled by $I \in X$, we say that e *witnesses* $U(I)$ whenever $u^e \in I$. If N is a leaf (Case 1), then 1 witnesses $U(I)$. If N is a parent (Case 2) labelled by I, with children labelled by K and L, and k and ℓ witness $U(K)$ and $U(L)$, respectively, then $k + \ell$ witnesses $U(I)$, as we see from the proof. Hence $U(0)$ is witnessed by the number of leaves, which in turn is bounded by 2^{n+m-1} (recall that the height of the tree is at most $n + m - 1$).

To get a sharper bound, one may switch to the digraph, this time labelled by the exponents and with reversed arrows:

$$\begin{array}{ccccccccccc}
 & & & & & & & & \cdots & \leftarrow & 1 \\
 & & & & & & & & & & \vdots \\
 & & & & & & & & \ddots & \leftarrow & 1 \\
 & & & & & & & & \uparrow & & \\
 & & & & & & \ddots & \leftarrow & 4 & \leftarrow & 1 \\
 & & & & & & \uparrow & & \uparrow & & \\
 & & & & \ddots & \leftarrow & 6 & \leftarrow & 3 & \leftarrow & 1 \\
 & & & & \uparrow & & \uparrow & & \uparrow & & \\
\vdots & & \ddots & \leftarrow & 4 & \leftarrow & 3 & \leftarrow & 2 & \leftarrow & 1 \\
\uparrow & & \uparrow & & \uparrow & & \uparrow & & \uparrow & & \\
1 & \cdots & 1 & & 1 & & 1 & & 1 & &
\end{array}$$

This in fact is a finite fragment of Pascal's triangle; whence standard theory can be used to calculate the number in the top left corner: that is, the e under which $u^e = 0$.

Note in this context that the construction of the tree and thus the design of the algorithm are not affected by the relations expressing the hypothesis $fg = 1$. This information is only used for proving that the algorithm meets its specification: that is, $u^e = 0$ whenever e is the exponent present at the root. More specifically, (6.1) and (6.2) are invoked for proving (6.3) and (6.8), and thus for proving that in Case 2 above the certificate for e witnessing $U(I)$ is bestowed from the children to the parent.

6.4.5. *A Concrete Example.* Let $n = 2$ and $m = 1$, and set

$$G = (b_1)\,,\ F = (a_2)\,,\ L = (a_2, b_1)\,,\ K = (a_1, a_2)\,.$$

The digraphs labelled by finitely generated ideals and exponents are as follows:

$$\begin{array}{ccccc}
0 & \to & F & \to & K \\
\downarrow & & \downarrow & & \\
G & & L & &
\end{array}
\qquad\qquad
\begin{array}{ccccc}
3 & \leftarrow & 2 & \leftarrow & 1 \\
\uparrow & & \uparrow & & \\
1 & & 1 & &
\end{array}$$

[4]The author is indebted to Ulrich Berger for prompting these investigations.

In particular, $e = 3$ is the output exponent under which $u^e = 0$ for any choice of u.

Now, for the sake of simplicity, assume that $a_0 = 1$ and $b_0 = 1$. Apart from $a_0 b_0 = 1$, which in this case is trivial, (6.2) then contains the following information:

$$a_1 + b_1 = 0\,, \quad a_1 b_1 + a_2 = 0\,, \quad a_2 b_1 = 0\,.$$

With these equations at hand, the certificates for $u^e \in I$ where $u \in \{a_1, a_2\}$ and $I \in \{K, L, F, G, 0\}$ are achieved as follows:

$$\begin{array}{ll}
\text{Case } u = a_1. & \text{Case } u = a_2. \\
a_1 \in K & a_2 \in K \\
a_1 = -b_1 \in L & a_2 \in L \\
a_1^2 = -a_1 b_1 = a_2 \in F & a_2 \in F \\
a_1 = -b_1 \in G & a_2 = -a_1 b_1 \in G \\
a_1^3 = a_1^2 a_1 = -a_2 b_1 = 0 & a_2^2 = -a_2 a_1 b_1 = 0
\end{array}$$

Note that $e = 2$ suffices for $u = a_2$, whereas $e = 3$ is required for $u = a_1$.

Finally, let $R = \mathbb{Z}/(8)$, and set $a_1 = 2$, $a_2 = 4$, $b_1 = 6$. In this case,

$$f = 4T^2 + 2T + 1\,, \quad g = 6T + 1\ ,$$

for which indeed, as we are doing integer arithmetic modulo 8,

$$fg = 24T^3 + 16T^2 + 8T + 1 = 1\,.$$

Here $e = 2$ suffices for $u = a_2 = 4$, whereas $e = 3$ is required for $u = a_1 = 2$.

6.4.6. *A Representation.* For any implementation on a computer, a more concrete representation of the elements of X may be required: that is, of the ideals generated by a detachable subset of E. Especially in view of the independence assumption made above, a natural choice is to represent any element I of X by a pair (λ, μ) of increasing binary lists $\lambda = (\lambda_1 \dots \lambda_n)$ and $\mu = (\mu_1 \dots \mu_m)$ of length n and m. Here $\lambda_i = 1$ and $\mu_j = 1$ indicate that a_i and b_j, respectively, belong to the generators of I. The inclusion order on X is then represented by the pointwise order of binary sequences.

With this representation at hand the tree can be described as follows. The root is labelled by $(0^n, 0^m)$. A generic node is labelled by $(0^k 1^\ell, 0^p 1^q)$ where $k+\ell = n$ and $p+q = m$; and has two children with labels $(0^{k-1} 1^{\ell+1}, 0^p 1^q)$ and $(0^k 1^\ell, 0^{p-1} 1^{q+1})$, unless either $k = n$ or $\ell = m$, in which case this node is a leaf. If we write $\overline{0}$ and $\overline{1}$ for finite lists $0 \dots 0$ and $1 \dots 1$, respectively, of variable but appropriate lengths, then the corresponding digraph is as follows:

$$\begin{array}{ccccccccc}
(\overline{0},\overline{0}) & \to & (\overline{0},\overline{0}1) & \to & \dots & \to & (\overline{0},0\overline{1}) & \to & (\overline{0},\overline{1}) \\
\downarrow & & \downarrow & & & & \downarrow & & \\
(\overline{0}1,\overline{0}) & \to & (\overline{0}1,\overline{0}1) & \to & \dots & \to & (\overline{0}1,0\overline{1}) & \to & (\overline{0}1,\overline{1}) \\
\downarrow & & \downarrow & & & & \downarrow & & \\
\vdots & & \vdots & & & & \vdots & & \vdots \\
\downarrow & & \downarrow & & & & \downarrow & & \\
(0\overline{1},\overline{0}) & \to & (0\overline{1},\overline{0}1) & \to & \dots & \to & (0\overline{1},0\overline{1}) & \to & (0\overline{1},\overline{1}) \\
\downarrow & & \downarrow & & & & \downarrow & & \\
(\overline{1},\overline{0}) & & (\overline{1},\overline{0}1) & & \dots & & (\overline{1},0\overline{1}) & &
\end{array}$$

6.4.7. *Elimination of Decidability.* We roughly sketch, as promised before, how we can eliminate the classically valid decidability assumptions, such as (6.10), used in the constructive proofs. Those assumptions form a finite set Δ of instances of the Law of Excluded Middle. Let Γ consist of the finitely many equations listed in (6.2); and let $\vdash_i$ and $\vdash_c$ stand for deducibility with intuitionistic and classical logic, respectively. If we neglect technical details, then with our constructive proof above—of NC with FI—we have established $\Gamma, \Delta \vdash_i C$ where

$$C \equiv \exists e\,(u^e = 0)\,.$$

Since, clearly, $\vdash_c \Delta$, we thus have $\Gamma \vdash_c C$. Now, since both C and the elements of Γ are of a sufficiently simple logical form, e.g. geometric formulas, by proof–theoretic techniques such as syntactic versions of Barr's Theorem—see e.g. [22, 36, 38]—we arrive at $\Gamma \vdash_i C$. The logical form of the formulas in Δ is irrelevant for this argument; and a similar method [50] applies if C is seen as an infinite disjunction rather than as an existential formula.

One possible road from $\Gamma \vdash_c C$ to $\Gamma \vdash_i C$ is via the generalisation (see e.g. [22, 38]) of the Gödel–Gentzen negative translation for which, in the spirit of the Dragalin–Friedman A–translation, the falsum $\bot$ is replaced by an arbitrary formula A. This A typically is the conclusion of the deduction under consideration.[5] In particular, one sets $\bot^A \equiv A$, and an atomic formula $B \not\equiv \bot$ is assigned to

$$B^A \equiv (B \to A) \to A\,;$$

the existential quantifier moreover is translated as follows:

$$(\exists x\, B)^A \equiv \forall x\,\left(B^A \to A\right) \to A\,.$$

Hence if $B \not\equiv \bot$ is atomic, then

$$\vdash_i \left(B^A \to A\right) \leftrightarrow (B \to A)$$

and thus

$$\vdash_i (\exists x\, B)^A \leftrightarrow (\exists x B \to A) \to A \tag{6.12}$$

provided that the variable x does not occur freely within the formula A.

With this translation, and for Γ and C as above, one can prove that $\Gamma \vdash_c C$ implies $\Gamma^A \vdash_i C^A$. In view of the simple form of the elements of Γ, we further have $\Gamma \vdash_i \Gamma^A$. Hence $\Gamma \vdash_c C$ implies $\Gamma \vdash_i C^A$, which in the specific case $A \equiv C$ yields $\Gamma \vdash_i C$. In fact, we have $\vdash_i C^C \leftrightarrow (C \to C) \to C$ by (6.12), and thus $\vdash_i C^C \leftrightarrow C$.

7. Conclusion

Our choices of the partial orders X and the predicates U were crucial to make induction work. In particular, the objects X from the constructive proofs are finite partial orders, as required for FI, and, by the way, are sets in the sense of **CZF**. Moreover, we thus have eventually kept close to the data of the given problem: that is, the coefficients a_i and b_j of the polynomials f and g. We could have done so much earlier, and perhaps more efficiently: by the method of indeterminate coefficients [31, p. 82]. This would have meant to pass from the arbitrary given R to the ring

$$R_0 = \mathbb{Z}[a_0, \ldots, a_n, b_0, \ldots, b_m]/(a_0 b_0 - 1, a_0 b_1 + a_1 b_0, \ldots, a_n b_m\,)\,.$$

[5] Thierry Coquand has kindly pointed us toward this method. As we have learned from Christoph-Simon Senjak, the proof translation at use is related—via the Curry-Howard isomorphism—to the continuation-passing style in programming.

with generators $a_0, \dots, a_n, b_0, \dots, b_m$ and relations (6.2). This R_0 indeed encodes all the data and information we would have needed for phrasing and proving NC. For its simple structure, moreover, R_0 is Noetherian [23]; and SPT holds constructively for R_0 since this is a fully Lasker–Noether ring [39]. Hence LN for R_0 is constructively provable [39], and KL for R_0 follows without any talk of OI, let alone of ZL.

The universal quantification required for KL, over all possible prime ideals of R, could then be replaced by the more manageable one over the finitely many finitely generated prime ideals of R_0 as produced by LN. Modulo each of the latter prime ideals we could have followed Gauß's argument for the case of a domain, yet replacing—as we have done anyway—the proof by contradiction by an appropriate distinction-by-cases. In all, we would have got a perfectly constructive proof of NC. This avenue, however, might not have forced us to seek an invocation of FI, and thus to keep close to the given data. In particular, we would not have made explicit a tree and an algorithm as simple as they have resulted from the constructive proofs with FI.

With hindsight, the proof pattern coined with Theorem 4.2, including the crucial notion of reducibility, stands already behind many a post-war textbook proof of the Lasker–Noether theorem [4, 37], and more implicitly behind Krull's proof [27]. It is not yet clear however whether any constructive "unwinding" of this type of classical proof can be brought under that pattern. We have anyway seen how the pattern can be applied to NC, a lemma in polynomial algebra, and yet another application of the pattern has proved possible in the area of inversion problems for Banach algebras [20]. A further case study will be undertaken about Gauß's lemma "the product of two primitive polynomials is primitive", which leads over its generalisation, ascribed to Joyal, to the so-called Dedekind Prague Theorem [5, 15, 29, 12].

We have conceived the constructive proofs of NC along the lines of the classical proof with Gauß's trick that we have recalled earlier. In particular, (6.3) and (6.8) are nothing but (6.4) and (6.7), respectively, with "$= 0$" replaced by "$\in F$". Now if "$= 0$" is considered within a domain, as in the classical proof, then it actually corresponds to "$\in P$" where P is a prime ideal of an arbitrary ring. Hence the move from "$= 0$" to "$\in F$" is in accordance with a paradigm that goes back to the so-called D5 philosophy of dynamic evaluation in computer algebra [18]: to handle the prime ideals P by way of their incomplete specifications F [16, 28, 29], which are (radicals of) finitely generated ideals but not necessarily prime.

In all, we have carried out a case study for a further potentially systematic way to gain finite methods from ideal objects in algebra. As discussed above (Section 6.2), our main competitor [41] has studied the same case but with a different method taken from point-free topology. We thus have started yet another attempt to make constructive sense of the notion of prime ideals, which "... play a central role in the theory of commutative rings" [26, p. 1]. In constructive algebra the notion of prime ideals has seen a revival [9] after it was considered problematic in general: "If an ideal P in a commutative ring is not detachable, it is is not clear just what it should mean for P to be prime" [35, p. 77].

Our work may further give evidence for the practicability of the recent proposals of a controlled use of ideal objects in constructive mathematics [45, 47] on the basis of a two-level foundations with forget-restore option [33, 32]. Last but not least, we have put some mathematical flesh on Bell's conjecture that ZL is "constructively neutral" [7].

Acknowledgements

Useful hints came from many participants of the 2011 Oberwolfach Workshop on Proof Theory and Constructive Mathematics, such as Ulrich Berger, Thierry Coquand, Erik Palmgren, and Per Martin-Löf. The author is further grateful to many others—especially to Martin Hofmann, Henri Lombardi, Davide Rinaldi, Pedro Francisco Valencia Vizcaíno, and Olov Wilander—for stimulating discussions; to Jean-Claude Raoult, Bernhard Reus, and Fred Richman for commenting on draft versions; to the anonymous referees for their constructive critique; and last but not least to Matthew Hendlass, who first asked for a proof pattern.

This paper was first written during a fellowship at the Isaac Newton Institute for Mathematical Sciences, programme "Semantics and Syntax: A Legacy of Alan Turing". It was revised later during a visit to the University of Stockholm funded by the European Science Foundation Research Networking Programme "New frontiers of infinity: mathematical, philosophical, and computational prospects"; and during a visit to Swansea University with a Computer Science Small Grant of the London Mathematical Society.

This line of research was started when the author had a Feodor Lynen Research Fellowship for Experienced Researchers granted by the Alexander von Humboldt Foundation from sources of the German Bundesministerium für Bildung und Forschung; and when he was a visiting professor supported by a grant from the Italian Istituto Nazionale di Alta Matematica—Gruppo Nazionale per le Strutture Algebriche, Geometriche e le loro Applicazioni. The author is particularly grateful to Andrea Cantini, Giovanni Sambin, and various colleagues at Padua and Florence for their most welcoming hospitality.

References

[1] Peter Aczel. The type theoretic interpretation of constructive set theory. In *Logic Colloquium '77 (Proc. Conf., Wrocław, 1977)*, volume 96 of *Stud. Logic Foundations Math.*, pages 55–66. North-Holland, Amsterdam, 1978.

[2] Peter Aczel. The type theoretic interpretation of constructive set theory: choice principles. In *The L. E. J. Brouwer Centenary Symposium (Noordwijkerhout, 1981)*, volume 110 of *Stud. Logic Found. Math.*, pages 1–40. North-Holland, Amsterdam, 1982.

[3] Peter Aczel. The type theoretic interpretation of constructive set theory: inductive definitions. In *Logic, methodology and philosophy of science, VII (Salzburg, 1983)*, volume 114 of *Stud. Logic Found. Math.*, pages 17–49. North-Holland, Amsterdam, 1986.

[4] Michael F. Atiyah and Ian G. Macdonald. *Introduction to Commutative Algebra*. Addison-Wesley Publishing Co., 1969.

[5] B. Banaschewski and J. J. C. Vermeulen. Polynomials and radical ideals. *J. Pure Appl. Algebra*, 113(3):219–227, 1996.

[6] Bernhard Banaschewski. Radical ideals and coherent frames. *Comment. Math. Univ. Carolin.*, 37(2):349–370, 1996.

[7] John L. Bell. Zorn's lemma and complete Boolean algebras in intuitionistic type theories. *J. Symbolic Logic*, 62(4):1265–1279, 1997.

[8] Ulrich Berger. A computational interpretation of open induction. In F. Titsworth, editor, *Proceedings of the Ninetenth Annual IEEE Symposium on Logic in Computer Science*, pages 326–334. IEEE Computer Society, 2004.

[9] Douglas S. Bridges. Prime and maximal ideals in constructive ring theory. *Commun. Algebra*, 29:2787–2803, 2001.

[10] Paul M. Cohn. *Universal Algebra*. Harper & Row Publishers, New York, 1965.

[11] Thierry Coquand. Constructive topology and combinatorics. In *Constructivity in computer science (San Antonio, TX, 1991)*, volume 613 of *Lecture Notes in Comput. Sci.*, pages 159–164. Springer, Berlin, 1992.

[12] Thierry Coquand. Space of valuations. *Ann. Pure Appl. Logic*, 157:97–109, 2009.

[13] Thierry Coquand and Henri Lombardi. A logical approach to abstract algebra. *Math. Struct. in Comput. Science*, 16:885–900, 2006.

[14] Thierry Coquand and Henrik Persson. Gröbner bases in type theory. In *Types for proofs and programs (Irsee, 1998)*, volume 1657 of *Lecture Notes in Comput. Sci.*, pages 33–46. Springer, Berlin, 1999.

[15] Thierry Coquand and Henrik Persson. Valuations and Dedekind's Prague theorem. *J. Pure Appl. Algebra*, 155(2–3):121–129, 2001.

[16] Michel Coste, Henri Lombardi, and Marie-Françoise Roy. Dynamical method in algebra: Effective Nullstellensätze. *Ann. Pure Appl. Logic*, 111(3):203–256, 2001.

[17] Laura Crosilla and Peter Schuster. Finite Methods in Mathematical Practice. In G. Link and M. Detlefsen, editors, *Formalism and Beyond*, Mathematical Logic. Ontos, Heusenstamm, 201x.

[18] Jean Della Dora, Claire Dicrescenzo, and Dominique Duval. About a new method for computing in algebraic number fields. In *European Conference on Computer Algebra (2)*, pages 289–290, 1985.

[19] Harvey Friedman. Set theoretic foundations for constructive analysis. *Ann. of Math. (2)*, 105(1):1–28, 1977.

[20] Matthew Hendtlass and Peter Schuster. A direct proof of Wiener's theorem. In S. B. Cooper, A. Dawar, and B. Löwe, editors, *How the World Computes. Turing Centenary Conference and Eighth Conference on Computability in Europe*, volume 7318 of *Lect. Notes Comput. Sci.*, pages 294–303, Berlin and Heidelberg, 2012. Springer. Proceedings, CiE 2012, Cambridge, UK, June 2012.

[21] Simon Huber and Peter Schuster. Maximalprinzipien und Induktionsbeweise. Technical report, University of Leeds, 2013. In preparation.

[22] Hajime Ishihara. A note on the Gödel-Gentzen translation. *MLQ Math. Log. Q.*, 46(1):135–137, 2000.

[23] Carl Jacobsson and Clas Löfwall. Standard bases for general coefficient rings and a new constructive proof of Hilbert's basis theorem. *J. Symb. Comput.*, 12(3):337–372, 1991.

[24] Peter T. Johnstone. *Stone Spaces.* Number 3 in Cambridge Studies in Advanced Mathematics. Cambridge etc.: Cambridge University Press, 1982.

[25] André Joyal. Les théoremes de Chevalley-Tarski et remarques sur l'algèbre constructive. *Cah. Topol. Géom. Différ. Catég.*, 16:256–258, 1976.

[26] Irving Kaplansky. *Commutative Rings.* The University of Chicago Press, Chicago and London, 1974. Revised edition.

[27] Wolfgang Krull. *Idealtheorie.* Ergebnisse der Mathematik und ihrer Grenzgebiete, vol. 4, no. 3. Springer, Berlin, 1935.

[28] Henri Lombardi. Dimension de Krull, Nullstellensätze et évaluation dynamique. *Math. Zeitschrift*, 242:23–46, 2002.

[29] Henri Lombardi. Hidden constructions in abstract algebra. I. Integral dependance. *J. Pure Appl. Algebra*, 167:259–267, 2002.

[30] Henri Lombardi. Algèbre dynamique, espaces topologiques sans points et programme de Hilbert. *Ann. Pure Appl. Logic*, 137:256–290, 2006.

[31] Henri Lombardi and Claude Quitté. *Algèbre commutative. Méthodes constructives. Modules projectifs de type fini.* Calvage & Mounet, Paris, 2012.

[32] Maria Emilia Maietti. A minimalist two-level foundation for constructive mathematics. *Ann. Pure Appl. Logic*, 160(3):319–354, 2009.

[33] Maria Emilia Maietti and Giovanni Sambin. Toward a minimalist foundation for constructive mathematics. In L. Crosilla and P. Schuster, editors, *From Sets and Types to Topology and Analysis*, volume 48 of *Oxford Logic Guides*, pages 91–114. Oxford: Oxford University Press, 2005.

[34] Per Martin-Löf. *Intuitionistic type theory*, volume 1 of *Studies in Proof Theory. Lecture Notes*. Bibliopolis, Naples, 1984. Notes by Giovanni Sambin.

[35] Ray Mines, Fred Richman, and Wim Ruitenburg. *A Course in Constructive Algebra*. Springer, New York, 1988. Universitext.

[36] Sara Negri. Contraction-free sequent calculi for geometric theories with an application to Barr's theorem. *Arch. Math. Logic*, 42(4):389–401, 2003.

[37] Douglas G. Northcott. *Ideal Theory.* Cambridge University Press, 1953.

[38] Erik Palmgren. An intuitionistic axiomatisation of real closed fields. *MLQ Math. Log. Q.*, 48(2):297–299, 2002.

[39] Hervé Perdry. Strongly Noetherian rings and constructive ideal theory. *J. Symb. Comput.*, 37(4):511–535, 2004.

[40] Hervé Perdry and Peter Schuster. Noetherian orders. *Math. Structures Comput. Sci.*, 21:111–124, 2011.
[41] Henrik Persson. An application of the constructive spectrum of a ring. In *Type Theory and the Integrated Logic of Programs*. Chalmers University and University of Göteborg, 1999. PhD thesis.
[42] Jean-Claude Raoult. Proving open properties by induction. *Inform. Process. Lett.*, 29(1):19–23, 1988.
[43] Fred Richman. Nontrivial uses of trivial rings. *Proc. Amer. Math. Soc.*, 103(4):1012–1014, 1988.
[44] Giovanni Sambin. Intuitionistic formal spaces—a first communication. In *Mathematical Logic and its Applications, Proc. Adv. Internat. Summer School Conf., Druzhba, Bulgaria, 1986*, pages 187–204. Plenum, 1987.
[45] Giovanni Sambin. Steps towards a dynamic constructivism. In P. Gärdenfors et al., editor, *In the Scope of Logic, Methodology and Philosophy of Science*, volume 315 of *Synthese Library*, pages 263–286, Dordrecht, 2002. Kluwer. 11th International Congress of Logic, Methodology and Philosophy of Science. Krakow, Poland, August 1999.
[46] Giovanni Sambin. Some points in formal topology. *Theoret. Comput. Sci.*, 305(1-3):347–408, 2003.
[47] Giovanni Sambin. Real and ideal in constructive mathematics. In *Epistemology versus ontology*, volume 27 of *Log. Epistemol. Unity Sci.*, pages 69–85. Springer, Dordrecht, 2012.
[48] Peter Schuster. Induction in algebra: a first case study. In *2012 27th Annual ACM/IEEE Symposium on Logic in Computer Science*, pages 581–585. IEEE Computer Society Publications, 2012. Proceedings, LICS 2012, Dubrovnik, Croatia, June 2012.
[49] Viggo Stoltenberg-Hansen and John V. Tucker. Computable rings and fields. In *Handbook of computability theory*, volume 140 of *Stud. Logic Found. Math.*, pages 363–447. North-Holland, Amsterdam, 1999.
[50] Pedro Francisco Valencia Vizcaíno. *Some Uses of Cut Elimination*. Phd thesis, University of Leeds, 2013.
[51] Ihsen Yengui. Making the use of maximal ideals constructive. *Theoret. Comput. Sci.*, 392:174–178, 2008.