Maximal ideals in countable rings, constructively

Ingo Blechschmidt[1] and Peter Schuster[2]

[1] Universität Augsburg, Universitätsstr. 14, 86159 Augsburg, Germany
ingo.blechschmidt@math.uni-augsburg.de
[2] Università di Verona, Strada le Grazie 15, 37134 Verona, Italy
petermichael.schuster@univr.it

Abstract. The existence of a maximal ideal in a general nontrivial commutative ring is tied together with the axiom of choice. Using the relative interpretation of negation (that is, as "implies $0 = 1$") we show, in constructive set theory with minimal logic, how for countable rings one can do without any kind of choice and without the usual decidability assumption that the ring is strongly discrete (membership in finitely generated ideals is decidable). By a functional recursive definition we obtain a maximal ideal in the sense that the quotient ring is a residue field (every noninvertible element is zero), and with strong discreteness even a geometric field (every element is either invertible or else zero). Krull's lemma for the related notion of prime ideal follows by passing to rings of fractions. All this equally applies to rings indexed by any well-founded set, and can be carried over to Heyting arithmetic with minimal logic. We further show how a metatheorem of Joyal and Tierney can be used to expand our treatment to arbitrary rings. Along the way we do a case study for proofs in algebra with minimal logic. An Agda formalization is available at an accompanying repository.[3]

Let A be a commutative ring with unit. The standard way of constructing a maximal ideal of A is to apply Zorn's lemma to the set of proper ideals of A; but this method is less an actual construction and more an appeal to the transfinite.

If A is countable with enumeration $x_0, x_1, \ldots$, we can hope to provide a more explicit construction by successively adding generators to the zero ideal, skipping those which would render it improper:

$$\mathfrak{m}_0 = \{0\} \qquad\qquad \mathfrak{m}_{n+1} = \begin{cases} \mathfrak{m}_n + (x_n), & \text{if } 1 \notin \mathfrak{m}_n + (x_n), \\ \mathfrak{m}_n, & \text{else.} \end{cases}$$

A maximal ideal is then obtained in the limit as the union of the intermediate stages $\mathfrak{m}_n$. For instance, Krull in his 1929 Annals contribution [30, Hilfssatz] and books on constructive algebra [34, Lemma VI.3.2], [31, comment after Theorem VII.5.2] proceed in this fashion. A similar construction concocts Henkin models for the purpose of proving Gödel's completeness theorem for countable languages, successively adding formulas which do not render the current set inconsistent [51, Satz I.56], [15, Lemma 1.5.7], [49, Lemma III.5.4], [25, Lemma 2.1].

[3] https://github.com/iblech/constructive-maximal-ideals/

This procedure avoids any form of choice by virtue of being a functional recursive definition, but still requires some form of omniscience in order to carry out the case distinction. In the present text we study a variant of this construction which avoids any non-constructive principles and decidability assumptions, similar to a construction which has been studied by Krivine [29, p. 410] and later Herbelin and Ilik [21, p. 11] in the context of Gödel's completeness theorem. In this generality, the resulting maximal ideal has an elusive quality to it, but useful properties can still be extracted; and not only do we recover the original construction under certain decidability assumptions, we can also exploit a relativity phenomenon of mathematical logic in order to drop, with some caveats, the assumption that A is countable.

Conventions. Throughout this note, we fix a ring A, and work in a constructive metatheory. In the spirit of Lombardi and Quitté [31], we employ *minimal logic* [26], where by "not φ" we mean "$\varphi \Rightarrow 1 =_A 0$", and do *not* assume any form of the axiom of choice. Consequently, by "$x \notin M$" we mean $x \in M \Rightarrow 1 =_A 0$, and a subset $M \subseteq A$ is *detachable* if and only if for all $x \in A$, either $x \in M$ or $x \notin M$. For general background on constructive mathematics, we refer to [8,7,10].

For an arbitrary subset $M \subseteq A$, not necessarily detachable, the ideal (M) generated by M is given by $\left\{ \sum_{i=1}^n a_i v_i \,\middle|\, n \geq 0, a_1, \ldots, a_n \in A, v_1, \ldots, v_n \in M \right\}$. Notice that, for every element $v \in (M)$, either $v = 0$ or M is inhabited, depending on whether $n = 0$ or $n > 0$ in $\sum_{i=1}^n a_i v_i$. This can also be seen from the alternative inductive generation of (M) by the following rules:

$$\frac{v = 0}{v \in (M)} \qquad \frac{v \in M}{v \in (M)} \qquad \frac{v \in (M) \quad w \in (M)}{v + w \in (M)} \qquad \frac{a \in A \quad v \in (M)}{av \in (M)}$$

Here we adhere to the paradigm of generalized inductive definitions [1,2,40].

1 A construction

We assume that the ring A is countable, with $x_0, x_1, \ldots$ an enumeration of the elements of A. We do *not* assume that A is discrete (that is, that $x = y$ or $x \neq y$ for all elements of A) or that it is strongly discrete (that is, that finitely generated ideals of A are detachable).

We study the following recursive construction of ideals $\mathfrak{m}_0, \mathfrak{m}_1, \ldots$ of A:

$$\mathfrak{m}_0 := \{0\} \qquad\qquad \mathfrak{m}_{n+1} := \mathfrak{m}_n + (\{x_n \mid 1 \notin \mathfrak{m}_n + (x_n)\}).$$

Finally, we set $\mathfrak{m} := \bigcup_n \mathfrak{m}_n$. The construction of $\mathfrak{m}_{n+1}$ from $\mathfrak{m}_n$ is uniquely specified, requiring no choices of any form.

The set $M_n := \{x_n \mid 1 \notin \mathfrak{m}_n + (x_n)\}$ occurring in this construction contains the element x_n if and only if $1 \notin \mathfrak{m}_n + (x_n)$; it is obtained from the singleton set $\{x_n\}$ by bounded separation. This set M_n is inhabited precisely if $1 \notin \mathfrak{m}_n + (x_n)$, in which case $\mathfrak{m}_{n+1} = \mathfrak{m}_n + (x_n)$. However, in the generality we work in, we cannot assume that M_n is empty or inhabited.

We can avoid the case distinction only by the flexibility of nondetachable subsets, rendering it somewhat curious that—despite the conveyed flavor of a conjuring trick—the construction can still be used to obtain concrete positive results.

The ideal (M_n) is given by $(M_n) = \{ax_n \mid (a = 0) \vee (1 \notin \mathfrak{m}_n + (x_n))\}$.

Proposition 1.1. *The subset* $\mathfrak{m}$ *is an ideal.*

Proof. Directed unions of ideals are ideals.

Proposition 1.2. *The ideal* $\mathfrak{m}$ *is* proper *in the sense that* $1 \notin \mathfrak{m}$.

Proof. Assume $1 \in \mathfrak{m}$. Then $1 \in \mathfrak{m}_n$ for some number $n \geq 0$. We verify $1 = 0$ by induction over n. If $n = 0$, then $1 \in \mathfrak{m}_0 = \{0\}$. Hence $1 = 0$.

If $n > 0$, then $1 = y + ax_{n-1}$ for some elements $a, y \in A$ such that $y \in \mathfrak{m}_{n-1}$ and such that $a = 0$ or $1 \notin \mathfrak{m}_{n-1} + (x_{n-1})$. In the first case, we have $1 = y \in \mathfrak{m}_{n-1}$, hence $1 = 0$ by the induction hypothesis. In the second case we have $1 = 0$ by modus ponens applied to the implication $1 \notin \mathfrak{m}_{n-1} + (x_{n-1})$ and the fact $1 \in \mathfrak{m}_{n-1} + (x_{n-1})$ (which follows directly from the equation $1 = y + ax_{n-1}$).

Lemma 1.3. *For every number* $n \in \mathbb{N}$*, the following are equivalent:*
(1) $x_n \in \mathfrak{m}_{n+1}$. *(2)* $x_n \in \mathfrak{m}$. *(3)* $1 \notin \mathfrak{m} + (x_n)$. *(4)* $1 \notin \mathfrak{m}_n + (x_n)$.

Proof. It is clear that $(3) \Rightarrow (4) \Rightarrow (1) \Rightarrow (2)$. It remains to show that $(2) \Rightarrow (3)$.

Assume $x_n \in \mathfrak{m}$. In order to verify $1 \notin \mathfrak{m} + (x_n)$, assume $1 \in \mathfrak{m} + (x_n)$. Since $\mathfrak{m} + (x_n) \subseteq \mathfrak{m}$, we have $1 \in \mathfrak{m}$. Hence $1 = 0$ by Proposition 1.2.

Proposition 1.4. *The ideal* $\mathfrak{m}$ *is* maximal *in the sense that it is proper and that for all elements* $x \in A$*, if* $1 \notin \mathfrak{m} + (x)$*, then* $x \in \mathfrak{m}$.

Proof. Immediate by Lemma 1.3.

This first-order maximality condition is equivalent to the following higher-order version: For every ideal $\mathfrak{n}$ such that $1 \notin \mathfrak{n}$, if $\mathfrak{m} \subseteq \mathfrak{n}$, then $\mathfrak{m} = \mathfrak{n}$.

Corollary 1.5. *The ideal* $\mathfrak{m}$ *is* prime *in the sense that it is proper and that for all elements* $x, y \in A$*, if* $xy \in \mathfrak{m}$ *and* $x \notin \mathfrak{m}$*, then* $y \in \mathfrak{m}$.

Proof. By maximality of $\mathfrak{m}$, it suffices to verify that $1 \notin \mathfrak{m} + (y)$. If $1 \in \mathfrak{m} + (y)$, then $x = x \cdot 1 \in (x) \cdot \mathfrak{m} + (xy) \subseteq \mathfrak{m}$ by $xy \in \mathfrak{m}$, hence $x \in \mathfrak{m}$, thus $1 = 0$ by $x \notin \mathfrak{m}$.

The foregoing proof in fact shows that every maximal ideal in the sense of Proposition 1.4 is a prime ideal in the sense of Corollary 1.5.

Corollary 1.6. *The ideal* $\mathfrak{m}$ *is* radical *in the sense that for every natural number* k*, if* $x^k \in \mathfrak{m}$*, then* $x \in \mathfrak{m}$.

Proof. Let $x^k \in \mathfrak{m}$. Then $1 \notin \mathfrak{m} + (x)$, for if $1 \in \mathfrak{m} + (x)$, then also $1 = 1^k \in (\mathfrak{m} + (x))^k \subseteq \mathfrak{m} + (x^k) \subseteq \mathfrak{m}$. Hence $x \in \mathfrak{m}$ by Proposition 1.4.

Remark 1.7. The ideal $\mathfrak{m}$ is double negation stable in the sense that for every ring element x, if $\neg\neg(x \in \mathfrak{m})$, then $x \in \mathfrak{m}$. This is because by Lemma 1.3 membership of $\mathfrak{m}$ is a negative condition and $\neg\neg\neg\varphi \Rightarrow \neg\varphi$ is a tautology of minimal logic.

The quotient ring $A/\mathfrak{m}$ is a *residue field* in that its unit is not zero and every element which is not invertible is zero—as with the real or complex numbers in intuitionistic mathematics.[4] Each of the latter is in fact a *Heyting field*: a residue field which also is a *local ring* in the sense that if a finite sum is invertible then one of the summands is.

Example 1.8. If we enumerate $\mathbb{Z}$ by $0, 1, -1, 2, -2, \ldots$, the ideal $\mathfrak{m}$ coincides with (2). If the enumeration starts with a prime p, the ideal $\mathfrak{m}$ coincides with (p).

Example 1.9. If A is a local ring with group of units $A^\times$, then $\mathfrak{m} = A \setminus A^\times$.

Example 1.10. We can modify the construction by using an arbitrary ideal $\mathfrak{a}$ as $\mathfrak{m}_0$ instead of the zero ideal. All results in this section remain valid, provided "not φ" is redefined as "$\varphi \Rightarrow 1 \in \mathfrak{a}$"; the resulting ideal $\mathfrak{m}$ is then a maximal ideal above $\mathfrak{a}$; it is proper in the sense that $1 \in \mathfrak{m} \Rightarrow 1 \in \mathfrak{a}$. It can also be obtained by applying the original version of the construction in the quotient ring $A/\mathfrak{a}$ (which is again countable) and taking the inverse image of the resulting ideal along the canonical projection $A \to A/\mathfrak{a}$.

Example 1.11. Assume that A is a field. Let $f \in A[X]$ be a nonconstant monic polynomial. Since f is monic, it is not invertible; thus Example 1.10 shows that there is a maximal ideal $\mathfrak{m}$ above (f). Hence $A[X]/\mathfrak{m}$ is a field in which f has a zero, namely the equivalence class of X. Iterating this *Kronecker construction*, we obtain a splitting field of f. No assumption regarding decidability of reducibility has to be made, but in return the resulting fields are only residue fields.

If we can decide whether a finitely generated ideal contains the unit or not, we can improve on Proposition 1.4. For instance this is the case for strongly discrete rings such as the ring $\mathbb{Z}$, more generally for the ring of integers of every number field, and for polynomial rings over discrete fields [34, Theorem VIII.1.5].

Proposition 1.12. *Assume that for every finitely generated ideal $\mathfrak{a} \subseteq A$ we have $1 \notin \mathfrak{a}$ or $\neg(1 \notin \mathfrak{a})$. Then:*

1. *Each ideal $\mathfrak{m}_n$ is finitely generated.*
2. *The ideal $\mathfrak{m}$ is detachable.*

[4] Residue fields have many of the basic properties of the fields from classical mathematics. For instance, minimal generating families of vector spaces over residue fields are linearly independent, finitely generated vector spaces do (up to $\neg\neg$) have a finite basis, monic polynomials possess splitting fields and Noether normalization is available (the proofs in [34] can be suitably adapted). The constructively rarer *geometric fields*—those kinds of fields for which every element is either invertible or zero—are required to ensure, for instance, that kernels of matrices are finite dimensional and that bilinear forms are diagonalizable.

If even $1 \in \mathfrak{a}$ *or* $1 \notin \mathfrak{a}$ *for every finitely generated ideal* $\mathfrak{a} \subseteq A$*, then:*

3. *The ideal* $\mathfrak{m}$ *is maximal in the strong sense that for every element* $x \in A$*,* $x \in \mathfrak{m}$ *or* $1 \in \mathfrak{m} + (x)$*, which is to say that the quotient ring* $A/\mathfrak{m}$ *is a* geometric field *(every element is zero or invertible).*[5]

Proof. We verify claim (1) by induction over n. The case $n = 0$ is clear. Let $n > 0$. By the induction hypothesis, the ideal $\mathfrak{m}_{n-1}$ is finitely generated, hence so is $\mathfrak{m}_{n-1} + (x_{n-1})$. By assumption, $1 \notin \mathfrak{m}_{n-1} + (x_{n-1})$ or $\neg(1 \notin \mathfrak{m}_{n-1} + (x_{n-1}))$. In the first case $\mathfrak{m}_n = \mathfrak{m}_{n-1} + (x_{n-1})$. In the second case $\mathfrak{m}_n = \mathfrak{m}_{n-1}$. In both cases the ideal $\mathfrak{m}_n$ is finitely generated.

To verify claim (2), let an element $x_n \in A$ be given. By assumption, $1 \notin \mathfrak{m}_n + (x_n)$ or $\neg(1 \notin \mathfrak{m}_n + (x_n))$. Hence $x_n \in \mathfrak{m}$ or $x_n \notin \mathfrak{m}$ by Lemma 1.3.

For claim (3), let an element $x_n \in A$ be given. If $1 \in \mathfrak{m}_n + (x_n)$, then also $1 \in \mathfrak{m} + (x_n)$. If $1 \notin \mathfrak{m}_n + (x_n)$, then $x_n \in \mathfrak{m}$ by Lemma 1.3.

It is remarkable that under the assumption of Proposition 1.12, the ideal $\mathfrak{m}$ is detachable even though in general it fails to be finitely generated. Usually in constructive mathematics, ideals which are not finitely generated are seldom detachable. For instance the ideal $\{x \in \mathbb{Z} \mid x = 0 \vee \varphi\} \subseteq \mathbb{Z}$ is detachable if and only if $\varphi \vee \neg\varphi$.

Remark 1.13. There is an equivalent description of the maximal ideal $\mathfrak{m}$ which uses sets G_n of generators as proxies for the intermediate ideals $\mathfrak{m}_n$:

$$G_0 := \emptyset \qquad\qquad G_{n+1} := G_n \cup \{x_n \mid 1 \notin (G_n \cup \{x_n\})\}$$

An induction establishes the relation $(G_n) = \mathfrak{m}_n$; setting $G := \bigcup_{n\in\mathbb{N}} G_n$, the analogue of Lemma 1.3 states that for every number $n \in \mathbb{N}$, the following are equivalent: (1) $x_n \in G_{n+1}$. (2) $x_n \in G$. (3) $1 \notin (G) + (x_n)$. (4) $1 \notin (G_n) + (x_n)$.

In particular, not only do we have that $(G) = \mathfrak{m}$, but G itself is already an ideal. This description of $\mathfrak{m}$ is in a sense more "economical" as the intermediate stages G_n are smaller (not yet being ideals), enabling arithmetization in Section 3.

Remark 1.14. All results in this section carry over mutatis mutandis if A is only assumed to be subcountable, that is, if we are only given a *partially defined* surjection $\mathbb{N} \rightharpoonup A$. In this case, we are given an enumeration $x_0, x_1, \ldots$ where some x_i might not be defined; we then define $\mathfrak{m}_{n+1} := \mathfrak{m}_n + (\{x_n \mid x_n \text{ is defined} \wedge 1 \notin \mathfrak{m}_n + (x_n)\})$. The generalization to the subcountable case is particularly useful in the Russian tradition of constructive mathematics as exhibited by the effective topos [24,36,38,6], where many rings of interest are subcountable, including uncountable ones such as the real numbers [24, Prop. 7.2].

[5] This notion of a maximal ideal, together with the corresponding one of a complete theory in propositional logic, has been generalized to the concept of a complete coalition [44,46] for an abstract inconsistency predicate.

2 On the intersection of all prime ideals

Classically, Krull's lemma states that the intersection of all prime ideals is the *nilradical*, the ideal $\sqrt{(0)}$ of all nilpotent elements. In our setup, we have the following substitute concerning complements:

$$\sqrt{(0)}^c = \bigcup_{\substack{\mathfrak{p} \subseteq A \\ \mathfrak{p} \text{ prime} \\ \mathfrak{p} \text{ } \neg\neg\text{-stable}}} \mathfrak{p}^c = \bigcup_{\substack{\mathfrak{p} \subseteq A \\ \mathfrak{p} \text{ prime} \\ \mathfrak{p} \text{ radical}}} \mathfrak{p}^c.$$

Lemma 2.1. *Let $x \in A$. Then there is an ideal $\mathfrak{p} \subseteq A$ which is*

1. *"x-prime" in the sense that $1 \in \mathfrak{p} \Rightarrow x \in \sqrt{(0)}$ and $ab \in \mathfrak{p} \wedge \big(b \in \mathfrak{p} \Rightarrow x \in \sqrt{(0)}\big) \Longrightarrow a \in \mathfrak{p}$, that is, prime if the negations occurring in the definition of "prime ideal" are understood as "$\varphi \Rightarrow x \in \sqrt{(0)}$",*
2. *"x-stable" in the sense that $\big((a \in \mathfrak{p} \Rightarrow x \in \sqrt{(0)}) \Rightarrow x \in \sqrt{(0)}\big) \Rightarrow a \in \mathfrak{p}$,*
3. *radical,*
4. *and such that $x \in \mathfrak{p}$ if and only if x is nilpotent.*

Proof. The localization $A[x^{-1}]$ is again countable, hence the construction of Section 1 can be carried out to obtain a maximal (and hence prime) ideal $\mathfrak{m} \subseteq A[x^{-1}]$. Every negation occurring in the terms "maximal ideal" and "prime ideal" refers to $1 = 0$ in $A[x^{-1}]$, which is equivalent to x being nilpotent.

The preimage of $\mathfrak{m}$ under the localization homomorphism $A \to A[x^{-1}]$ is the desired x-prime ideal.

Corollary 2.2 (Krull [30]). *Let $x \in A$ be an element which is not nilpotent. Then there is a (radical and $\neg\neg$-stable) prime ideal $\mathfrak{p} \subseteq A$ such that $x \notin \mathfrak{p}$.*

Proof. Because x is not nilpotent, the notion of an x-prime ideal and an ordinary prime ideal coincide. Hence the claim follows from Lemma 2.1.

An important part of constructive algebra is to devise tools to import proofs from classical commutative algebra into the constructive setting. The following two statements are established test cases exploring the power of such tools [43,37,39,4,41,12,13].

Proposition 2.3. *Let $f \in A[X]$ be a polynomial.*

1. *If f is nilpotent in $A[X]$, then all coefficients of f are nilpotent in A.*
2. *If f is invertible in $A[X]$, then all nonconstant coefficients of f are nilpotent.*

These facts have abstract classical proofs employing Krull's lemma as follows.

Proof of 1. Simple induction if A is reduced; the general case reduces to this one: For every prime ideal $\mathfrak{p}$, the coefficients of f vanish over the reduced ring $A/\mathfrak{p}$. Hence they are contained in the intersection of all prime ideals and thereby nilpotent.

Proof of 2. Simple induction if A is an integral domain; the general case reduces to this one: For every prime ideal $\mathfrak{p}$, the nonconstant coefficients of f vanish over the integral domain $A/\mathfrak{p}$. Hence they are contained in all prime ideals and are thereby nilpotent.

Both statements admit direct computational constructive proofs which do not refer to prime ideals; the challenge is not to find such proofs, but rather to imitate the two classical proofs above constructively, staying as close as possible to the original. It is remarkable that the construction of Section 1 meets this challenge at all, outlined as follows, despite its fundamental reliance on nondetachable subsets.

We continue assuming that A is countable: Section 4 indicates how this assumption can be dropped in quite general situations, while for the purposes of specific challenges such as Proposition 2.3 we could also simply pass to the countable subring generated by the polynomial coefficients or employ the method of indeterminate coefficients.

Proof (of Proposition 2.3). The first claim follows from a simple induction if A is a reduced ring.

In the general case, write $f = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_0$. Let $\mathfrak{p}$ be a radical a_n-prime ideal as in Lemma 2.1. Since $A/\mathfrak{p}$ is reduced, the nilpotent coefficient a_n vanishes over $A/\mathfrak{p}$. Thus $a_n \in \mathfrak{p}$, hence a_n is nilpotent. Since the polynomial $f - a_nX^n$ is again nilpotent, we can continue by induction.

The second claim follows by a simple inductive argument if A is an integral domain with double negation stable equality.

In the general case, write $f = a_nX^n + \cdots + a_0$ and assume $n \geq 1$. To reduce to the integral situation, let $\mathfrak{p}$ be an a_n-prime ideal as in Lemma 2.1. With negation "$\neg\varphi$" understood as "$\varphi \Rightarrow a_n \in \sqrt{(0)}$", the quotient ring $A/\mathfrak{p}$ is an integral domain with double negation stable equality. Hence $a_n = 0$ in $A/\mathfrak{p}$, so $a_n \in \mathfrak{p}$ whereby a_n is nilpotent. The polynomial $f - a_nX^n$ is again invertible in $A[X]$ (since the group of units is closed under adding nilpotent elements) so that we can continue by induction.

Just as Corollary 2.2 is a constructive substitute for the recognition of the intersection of all prime ideals as the nilradical, the following proposition is one for the recognition of the intersection of all maximal ideals as the Jacobson radical. As is customary in constructive algebra [31, Section IX.1], by *Jacobson radical* we mean the ideal $\{x \in A \mid \forall y \in A.\ 1 - xy \in A^\times\}$. An element x is said to be *apart from the Jacobson radical* if and only if there exists an element $y \in A$ such that $1 - xy$ is not invertible.

Proposition 2.4. *Let $x \in A$. If x is apart from the Jacobson radical, then there is a maximal ideal $\mathfrak{m}$ such that $x \notin \mathfrak{m}$.*

Proof. The standard proof as in [31, Lemma IX.1.1] applies: There is an element y such that $1-xy$ is not invertible. By Example 1.10, there is an ideal $\mathfrak{m}$ above $\mathfrak{a} := (1 - xy)$ which is maximal not only as an ideal of $A/\mathfrak{a}$ (where "$\neg\varphi$" means "$\varphi \Rightarrow 1 \in \mathfrak{a}$") but also as an ideal of A (where "$\neg\varphi$" means "$\varphi \Rightarrow 1 = 0$"). If $x \in \mathfrak{m}$, then $1 = (1 - xy) + xy \in \mathfrak{m}$; hence $x \notin \mathfrak{m}$.

The two test cases presented in Proposition 2.3 only concern prime ideals. In contrast, the following example crucially rests on the maximality of the ideal $\mathfrak{m}$.

Proposition 2.5. *Let $M \in A^{n\times m}$ be a matrix with more rows than columns. Assume that the induced linear map $A^m \to A^n$ is surjective. Then $1 = 0$.*

Proof. By passing to the quotient $A/\mathfrak{m}$, we may assume that A is a residue field. In this case the claim is standard linear algebra:

If any of the matrix entries is invertible, the matrix could be transformed by elementary row and column operations to a matrix of the form $\left(\begin{smallmatrix} 1 & 0 \\ 0 & M' \end{smallmatrix}\right)$, where the induced linear map of the submatrix M' is again surjective. Thus $1 = 0$ by induction.

Hence by the residue field property all matrix entries are zero. Hence $1 = 0$. In fact, since $n > m$, we have $n > 0$; and the vector $(1, 0, \ldots, 0) \in A^n$ by hypothesis belongs to the range of $M = 0$.

Remark 2.6. A more significant case study is Suslin's lemma, the fundamental and originally non-constructive ingredient in his second solution of Serre's problem [50]. The classical proof, concisely recalled in Yengui's constructive account [55], proceeds by working modulo maximal ideals. The construction of Section 1 offers a constructive substitute. However, since greatest common divisor computations are required in the quotient rings, it is not enough that the quotients are residue fields; they need to be geometric fields. Hence our approach has to be combined with the technique variously known as *Friedman's trick*, *nontrivial exit continuation* or *baby version of Barr's theorem* in order to yield a constructive proof [18,35,5,9].

3 In Heyting arithmetic

The construction presented in Section 1 crucially rests on the flexibility of nondetachable subsets: In absence of additional assumptions as in Proposition 1.12, we cannot give the ideals $\mathfrak{m}_n$ by decidable predicates $A \to \{0, 1\}$—without additional hypotheses on A, membership of the ideals $\mathfrak{m}_n$ is not decidable. As such, the construction is naturally formalized in intuitionistic set theories such as CZF or IZF, which natively support such flexible subsets.

In this section, we explain how with some more care, the construction can also be carried out in much weaker foundations such as Heyting arithmetic HA. While formulation in classical Peano arithmetic PA is routine, the development in HA crucially rests on a specific feature of the construction, namely that the condition for membership is a negative condition.

To set the stage, we specify what we mean by a *ring* in the context of arithmetic. One option would be to decree that an arithmetized ring should be a single natural number coding a finite set of ring elements and the graphs of the corresponding ring operations; however, this perspective is too narrow, as we also want to work with infinite rings.

Instead, an arithmetized ring should be given by a "formulaic setoid with ring structure", that is: by a formula $A(n)$ with free variable n, singling out which natural numbers constitute representatives of the ring elements; by a formula $E(n, m)$ describing which representatives are deemed equivalent; by a formula $Z(n)$ singling out representatives of the zero element; by a formula $P(n, m, s)$ singling

out representatives s of sums; and so on with the remaining data constituting a ring; such that axioms such as

$\forall n.\, Z(n) \Rightarrow A(n)$	"every zero representative belongs to the ring"
$\exists n.\, Z(n)$	"there is a zero representative"
$\forall n, m.\, Z(n) \wedge Z(m) \Longrightarrow E(n, m)$	"every two zero representatives are equivalent"
$\forall z, n.\, Z(z) \wedge A(n) \Longrightarrow P(z, n, n)$	"zero is neutral with respect to addition"

hold. This conception of arithmetized rings deviates from the usual definition in reverse mathematics [49, Definition III.5.1] to support quotients even when Heyting arithmetic cannot verify the existence of canonical representatives of equivalence classes.

Although first-order arithmetic cannot quantify over ideals of arithmetized rings, specific ideals can be given by formulas $I(n)$ such that axioms such that

$\forall n.\, I(n) \Rightarrow A(n)$	"$I \subseteq A$"
$\exists n.\, Z(n) \wedge I(n)$	"$0 \in I$"

hold. It is in this sense that we are striving to adapt the construction of Section 1 to describe a maximal ideal.

In this context, we can arithmetically imitate any set-theoretic description of a single ideal as a subset cut out by an explicit first-order formula. However, for recursively defined families of ideals, we require a suitable recursion theorem: If we are given (individual formulas $M_n(x)$ indexed by numerals representing) ideals $\mathfrak{m}_0, \mathfrak{m}_1, \mathfrak{m}_2, \ldots$, we cannot generally form $\bigcup_{n\in\mathbb{N}} \mathfrak{m}_n$, as the naive formula "$\bigvee_{n\in\mathbb{N}} M_n(x)$" representing their union would have infinite length. We can take the union only if the family is *uniformly represented* by a single formula $M(n, x)$ (expressing that x represents an element of $\mathfrak{m}_n$).

This restriction is a blocking issue for arithmetizing the construction of the chain $\mathfrak{m}_0 \subseteq \mathfrak{m}_1 \subseteq \cdots$ of Section 1. Because $\mathfrak{m}_n$ occurs in the definition of $\mathfrak{m}_{n+1}$ in negative position, naive arithmetization results in formulas of unbounded logical complexity, suggesting that a uniform definition might not be possible.

This issue has a counterpart in type-theoretic foundations of mathematics, where the family $(\mathfrak{m}_n)_{n\in\mathbb{N}}$ cannot be given as an inductive family (failing the positivity check), and is also noted, though not resolved, in related work on a constructive version of Gödel's completeness theorem [21, p. 11]. The issue does not arise in the context of PA, where the law of excluded middle allows us to bound the logical complexity: We can blithely define the joint indicator function $g(n, i)$ for the sets G_n (such that $G_n = \{x_i \,|\, i \in \mathbb{N}, g(n, i) = 1\}$) of Remark 1.13 by the recursion

$$g(0, i) = 0$$
$$g(n+1, i) = \begin{cases} 1, & \text{if } g(n, i) = 1 \vee (i = n \wedge 1 \notin (g(n, 0)x_0, \ldots, g(n, n-1)x_{n-1}, x_n)) \\ 0, & \text{else.} \end{cases}$$

This recursion can be carried out within PA since the recursive step only references the finitely many values $g(n, 0), \ldots, g(n, i)$. Heyting arithmetic, however, does

not support this case distinction. The formalization of the construction in HA is only unlocked by the following direct characterization.

Lemma 3.1. *(In the situation of Remark 1.13.) For every finite binary sequence $v = [v_0, \dots, v_{n-1}]$, set $\mathfrak{a}_v := (v_0 x_0, \dots, v_{n-1} x_{n-1}, x_n)$. Then:*

1. *For every such sequence $v = [v_0, \dots, v_{n-1}]$, if $\bigwedge_{i=0}^{n-1}(v_i = 1 \Leftrightarrow 1 \notin \mathfrak{a}_{[v_0,\dots,v_{i-1}]})$, then $\mathfrak{a}_v = (G_n) + (x_n)$. In particular, in this case $x_n \in G$ if and only if $1 \notin \mathfrak{a}_v$.*
2. *For every natural number $n \in \mathbb{N}$,*

$$x_n \in G \quad \iff \quad \neg\exists v \in \{0,1\}^n.\ 1 \in \mathfrak{a}_v \wedge \bigwedge_{i=0}^{n-1}(v_i = 1 \Leftrightarrow 1 \notin \mathfrak{a}_{[v_0,\dots,v_{i-1}]}).$$

Proof. The first part is by induction, employing the equivalences of Remark 1.13. The second rests on the tautology $\neg\alpha \iff \neg(\alpha \wedge (\varphi \vee \neg\varphi))$:

$$\begin{aligned} x_n \in G &\iff \neg\big(1 \in (G_n) + (x_n)\big) \iff \neg\Big(1 \in (G_n) + (x_n) \ \wedge \bigwedge_{i=0}^{n-1}(x_i \in G \vee x_i \notin G)\Big) \\ &\iff \neg\exists v \in \{0,1\}^n.\ \Big(1 \in (G_n) + (x_n) \ \wedge \bigwedge_{i=0}^{n-1}(v_i = 1 \Leftrightarrow x_i \in G)\Big) \\ &\iff \neg\exists v \in \{0,1\}^n.\ \Big(1 \in \mathfrak{a}_v \ \wedge \bigwedge_{i=0}^{n-1}(v_i = 1 \Leftrightarrow 1 \notin \mathfrak{a}_{[v_0,\dots,v_{i-1}]})\Big) \end{aligned}$$

Condition (2) is manifestly formalizable in arithmetic, uniformly in n.

4 For general rings

The construction in Section 1 of a maximal ideal applies to countable rings. In absence of the axiom of choice, some restriction on the rings is required, as it is well-known that the statement that any nontrivial ring has a maximal ideal implies (over Zermelo–Fraenkel set theory ZF) the axiom of choice [47,22,3,16,23].

However, this limitation only pertains to the abstract existence of maximal ideals, not to concrete consequences of their existence. Mathematical logic teaches us by way of diverse examples to not conflate these two concerns. For instance, although ZF does not prove the axiom of choice, it does prove every theorem of ZFC pertaining only to natural numbers (by interpreting the given ZFC-proof in the constructible universe L and exploiting that the natural numbers are absolute between V and L [19,42]); similarly, although intuitionistic Zermelo–Fraenkel set theory, IZF, does not prove the law of excluded middle, it does prove every Π^0_2-theorem of ZF (by the double negation translation combined with Friedman's trick of the nontrivial exit continuation [17]).

A similar phenomenon concerns countability. Set theory teaches us that whether a given set is countable depends not only on the set itself, but is more aptly regarded as a property of the ambient universe [20]: Given any set M, there is a (non-Boolean) extension of the universe in which M becomes countable. Remarkably, the passage to such an extension preserves and reflects first-order

logic. Hence we have the metatheorem, due to Joyal and Tierney, that *countability assumptions from intuitionistic proofs of first-order statements can always be mechanically eliminated.*[6] Crucially, the first-order restriction is only on the form of the statements, not on the form of the proofs. These may freely employ higher-order constructs.

"First-order" statements are statements which only refer to elements, not to subsets; for instance, the statements of Proposition 2.3 are first-order and hence also hold without the countability assumption. In contrast, the statement "there is a maximal ideal" is a higher-order statement; hence we cannot eliminate countability assumptions from proofs of this statement.

The metatheorem expands the applicability of the construction of Section 1 and underscores the value of its intuitionistic analysis—the metatheorem cannot be applied to eliminate countability assumptions from classical proofs. Taken together, they strengthen the view of maximal ideals as convenient fictions [45, Section 1]. Maximal ideals can carry out their work by any of the following possibilities: (1) For countable (or well-founded) rings, no help is required. Section 1 presents an explicit construction of a maximal ideal. (2) For arbitrary rings, the existence of a maximal ideal follows from the axiom of choice. (3) Intuitionistic first-order consequences of the existence of a maximal ideal are true even if no actual maximal ideal can be constructed.

Remark 4.1. The dynamic approach as presented in the textbook by Lombardi and Quitté [31, Section XV.6] is another technique for constructively reinterpreting, without countability assumptions, classical proofs involving maximal ideals. We sketch here how the dynamic approach is intimately connected with the technique of this section, even though it is cast in entirely different language.

Suppose that a given classical proof appeals to the maximality condition "$x \in \mathfrak{m}$ or $1 \in \mathfrak{m} + (x)$" ("x is zero modulo $\mathfrak{m}$ or invertible modulo $\mathfrak{m}$") only for a finite number $x_0, \ldots, x_{n-1}$ of ring elements fixed beforehand. In this case we can, even if no enumeration of all elements of A exists or is available, apply the construction in Section 1 to this finite enumeration and use the resulting ideal $\mathfrak{m}_n$ as a partial substitute for an intangible maximal ideal.

[6] For every set M, there is a certain locale X (the *classifying locale of enumerations of* M) which is overt, positive and such that its constant sheaf $\underline{M}$ is countable in the sense of the internal language of the topos of sheaves over X. A given intuitionistic proof can then be interpreted in this topos [11,32,48]; since the constant sheaf functor preserves first-order logic (by overtness), the sheaf $\underline{M}$ inherits any first-order assumptions about M required by the proof; and since it also reflects first-order logic (by overtness and positivity), the proof's conclusion descends to M.

When we apply the construction of Section 1 internally in this topos, the result will be a certain sheaf of ideals; it is in that sense that every ring constructively possesses a maximal ideal. This sheaf will not be constant, hence not originate from an actual ideal of the given ring; but first-order consequences of the existence of this sheaf of ideals pass down to the ring. Details are provided by Joyal and Tierney [28, pp. 36f.], and introductions to pointfree topology and topos theory can be found in [9,27,53,52]. A predicative account on the basis of [33,54,14] is also possible. The phenomenon that size is relative also emerges in the Löwenheim–Skolem theorem.

The tools from pointfree topology driving Joyal and Tierney's metatheorem widen the applicability of this partial substitute to cases where the inspected ring elements are not fixed beforehand, by dynamically growing the partial enumeration as the proof runs its course. If required, a continuation-passing style transform as in Remark 2.6 can upgrade the maximal ideal from one only satisfying the weaker condition "$1 \notin \mathfrak{m} + (x)$ implies $x \in \mathfrak{m}$" to one satisfying the stronger condition "$x \in \mathfrak{m}$ or $1 \in \mathfrak{m} + (x)$".

Unfolding the construction of $\mathfrak{m}$ and the proof of Joyal and Tierney's metatheorem, we arrive at the dynamical method.

Acknowledgments The present study was carried out within the project "Reducing complexity in algebra, logic, combinatorics – REDCOM" belonging to the program "Ricerca Scientifica di Eccellenza 2018" of the Fondazione Cariverona and GNSAGA of the INdAM.[7] Important steps towards this paper were made during the Dagstuhl Seminar 21472 "Geometric Logic, Constructivisation, and Automated Theorem Proving" in November 2021. This paper would not have come to existence without the authors' numerous discussions with Daniel Wessel, and greatly benefited from astute comments of Karim Becher, Nicolas Daans, Kathrin Gimmi, Matthias Hutzler, Lukas Stoll and the three anonymous reviewers.

References

1. Aczel, P., Rathjen, M.: Notes on constructive set theory. Tech. rep., Institut Mittag–Leffler (2000), report No. 40
2. Aczel, P., Rathjen, M.: Constructive set theory (2010), book draft
3. Banaschewski, B.: A new proof that 'Krull implies Zorn'. Math. Log. Quart. **40**(4), 478–480 (1994)
4. Banaschewski, B., Vermeulen, J.: Polynomials and radical ideals. J. Pure Appl. Algebra **113**(3), 219–227 (1996)
5. Barr, M.: Toposes without points. J. Pure Appl. Algebra **5**(3), 265–280 (1974)
6. Bauer, A.: Realizability as the connection between computable and constructive mathematics (2005), http://math.andrej.com/asset/data/c2c.pdf
7. Bauer, A.: Intuitionistic mathematics and realizability in the physical world. In: Zenil, H. (ed.) A Computable Universe. World Scientific Pub Co (2012)
8. Bauer, A.: Five stages of accepting constructive mathematics. Bull. Amer. Math. Soc. **54**, 481–498 (2017)
9. Blechschmidt, I.: Generalized spaces for constructive algebra. In: Mainzer, K., Schuster, P., Schwichtenberg, H. (eds.) Proof and Computation II, pp. 99–187. World Scientific (2021)
10. Bridges, D., Palmgren, E.: Constructive mathematics. In: Zalta, E. (ed.) The Stanford Encyclopedia of Philosophy. Metaphysics Research Lab, Stanford University, summer 2018 edn. (2018)
11. Caramello, O.: Topos-theoretic background (2014)
12. Coquand, T., Lombardi, H.: A logical approach to abstract algebra. Math. Structures Comput. Sci **16**(5), 885–900 (2006)

[7] The opinions expressed in this paper are solely those of the authors.

13. Coste, M., Lombardi, H., Roy, M.F.: Dynamical method in algebra: effective nullstellensätze. Ann. Pure Appl. Logic **111**(3), 203–256 (2001)
14. Crosilla, L.: Exploring predicativity. In: Mainzer, K., Schuster, P., Schwichtenberg, H. (eds.) Proof and Computation, pp. 83–108. World Scientific (2018)
15. van Dalen, D.: Logic and Structure. Universitext, Springer (2004)
16. Erné, M.: A primrose path from Krull to Zorn. Comment. Math. Univ. Carolin. **36**(1), 123–126 (1995)
17. Friedman, H.: The consistency of classical set theory relative to a set theory with intuitionistic logic. J. Symbolic Logic **38**, 315–319 (1973)
18. Friedman, H.: Classical and intuitionistically provably recursive functions. In: Müller, G., Scott, D. (eds.) Higher Set Theory, Lecture Notes in Math., vol. 669, pp. 21–27. Springer (1978)
19. Gödel, K.: The consistency of the axiom of choice and of the generalized continuum-hypothesis. Proc. Natl. Acad. Sci. USA **24**(12), 556–557 (1938)
20. Hamkins, J.: The set-theoretic multiverse. Rev. Symb. Log. **5**, 416–449 (2012)
21. Herbelin, H., Ilik, D.: An analysis of the constructive content of Henkin's proof of Gödel's completeness theorem (draft) (2016)
22. Hodges, W.: Krull implies Zorn. J. Lond. Math. Soc. **19**(2), 285–287 (1979)
23. Howard, P., Rubin, J.: Consequences of the Axiom of Choice. Math. Surveys Monogr., American Mathematical Society (1998)
24. Hyland, M.: The effective topos. In: Troelstra, A.S., van Dalen, D. (eds.) The L. E. J. Brouwer Centenary Symposium. pp. 165–216. North-Holland (1982)
25. Ishihara, H., Khoussainov, B., Nerode, A.: Decidable kripke models of intuitionistic theories. Ann. Pure Appl. Logic **93**, 115–123
26. Johansson, I.: Der Minimalkalkül, ein reduzierter intuitionistischer Formalismus. Compos. Math. **4**, 119–136 (1937)
27. Johnstone, P.T.: The point of pointless topology. Bull. Amer. Math. Soc. **8**(1), 41–53 (1983)
28. Joyal, A., Tierney, M.: An extension of the Galois theory of Grothendieck, Mem. Amer. Math. Soc., vol. 309. AMS (1984)
29. Krivine, J.L.: Une preuve formelle et intuitionniste du théorème de complétude de la logique classique. Bull. Symbolic Logic **2**, 405—-421 (1996)
30. Krull, W.: Idealtheorie in Ringen ohne Endlichkeitsbedingung. Math. Ann. **101**, 729–744 (1929)
31. Lombardi, H., Quitté, C.: Commutative Algebra: Constructive Methods. Springer (2015)
32. Maietti, M.: Modular correspondence between dependent type theories and categories including pretopoi and topoi. Math. Structures Comput. Sci. **15**(6), 1089–1149 (2005)
33. Maietti, M.: Joyal's arithmetic universes as list-arithmetic pretoposes. Theory Appl. Categ. **23**(3), 39–83 (2010)
34. Mines, R., Richman, F., Ruitenburg, W.: A Course in Constructive Algebra. Universitext, Springer (1988)
35. Murthy, C.: Classical proofs as programs: How, what and why. In: Myers, J., O'Donnell, M. (eds.) Constructivity in Computer Science. pp. 71–88. Springer (1992)
36. van Oosten, J.: Realizability: An Introduction to its Categorical Side, Stud. Logic Found. Math., vol. 152. Elsevier (2008)
37. Persson, H.: An application of the constructive spectrum of a ring. In: Type Theory and the Integrated Logic of Programs. Chalmers University and University of Göteburg (1999)

38. Phoa, W.: An introduction to fibrations, topos theory, the effective topos and modest sets. Tech. rep., University of Edinburgh (1992)
39. Powell, T., Schuster, P., Wiesnet, F.: A universal algorithm for krull's theorem. Information and Computation (2021)
40. Rathjen, M.: Generalized inductive definitions in constructive set theory. Oxford Logic Guides **48** (2005)
41. Richman, F.: Nontrivial uses of trivial rings. Proc. Amer. Math. Soc. **103**, 1012–1014 (1988)
42. Schoenfield, J.: The problem of predicativity. In: Bar-Hillel, Y., Poznanski, E., Rabin, M., Robinson, A. (eds.) Essays on the Foundations of Mathematics, pp. 132–139. Magnes (1961)
43. Schuster, P.: Induction in algebra: a first case study. 2012 27th Annual ACM/IEEE Symposium on Logic in Computer Science pp. 581–585 (2012)
44. Schuster, P., Wessel, D.: The Computational Significance of Hausdorff's Maximal Chain Principle. In: Anselmo, M., Vedova, G., Manea, F., Pauly, A. (eds.) Beyond the Horizon of Computability: 16th Conference on Computability in Europe, CiE 2020. Lecture Notes in Comput. Sci. (2020)
45. Schuster, P., Wessel, D.: Syntax for Semantics: Krull's Maximal Ideal Theorem. In: Heinzmann, G., Wolters, G. (eds.) Paul Lorenzen: Mathematician and Logician, Log. Epistemol. Unity Sci., vol. 51, pp. 77–102. Springer (2021)
46. Schuster, P., Wessel, D.: The Jacobson radical for an inconsistency predicate. Computability (2022), forthcoming
47. Scott, D.: Prime ideal theorems for rings, lattices and Boolean algebras. Bull. Amer. Math. Soc. **60**, 390 (1954)
48. Shulman, M.: Categorical logic from a categorical point of view (draft for AARMS Summer School 2016) (2016), https://mikeshulman.github.io/catlog/catlog.pdf
49. Simpson, S.: Subsystems of Second Order Arithmetic. Perspectives in Mathematical Logic, Springer (1999)
50. Suslin, A.: On the structure of the special linear group over polynomial rings. Izv. Akad. Nauk SSSR Ser. Mat. **41**, 235–252 (1977)
51. Tarski, A.: Fundamentale Begriffe der Methodologie der deduktiven Wissenschaften. I. Monatsh. Math. Phys. **37**, 361–404 (1930)
52. Vickers, S.: Locales and toposes as spaces. In: Aiello, M., Pratt-Hartmann, I., van Benthem, J. (eds.) Handbook of Spatial Logics, pp. 429–496. Springer (2007)
53. Vickers, S.: Continuity and geometric logic. J. Appl. Log. **12**(1), 14–27 (2014)
54. Vickers, S.: Sketches for arithmetic universes. J. Log. Anal. **11**(FT4), 1–56 (2016)
55. Yengui, I.: Making the use of maximal ideals constructive. Theoret. Comput. Sci. **392**, 174–178 (2008)

A Generalization to the well-founded case

In this section, we relax the assumption that the ring A is countable to the assumption that A is the image of a well-founded set I. There are several definitions of well-foundedness in the literature; we require transfinite recursion and induction over I, and that both I and every subset of the form $\downarrow(n) := \{k \in I \mid k < n\}$ which is inhabited is directed. The latter condition is for instance satisfied if $(<)$ is a linear order.

Writing $A = \{x_n \mid n \in I\}$, we recursively construct ideals $(\mathfrak{m}_n)_{n\in I}$ by

$$\mathfrak{m}_n := \mathfrak{m}_{<n} + (\{x_n \mid 1 \notin \mathfrak{m}_{<n} + (x_n)\}),$$

where $\mathfrak{m}_{<n} := \sum_{k<n} \mathfrak{m}_k$. We set $\mathfrak{m} := \bigcup_{n\in I} \mathfrak{m}_n$. As before, no choices of any kind are required.

Proposition A.1. *1. The subset $\mathfrak{m}$ is an ideal.*
2. The ideal $\mathfrak{m}$ is proper.
3. For an element $x_n \in A$, the following are equivalent: (a) $x_n \in \mathfrak{m}_n$; (b) $x_n \in \mathfrak{m}$; (c) $1 \notin \mathfrak{m} + (x_n)$; (d) $1 \notin \mathfrak{m}_{<n} + (x_n)$.
4. The ideal $\mathfrak{m}$ is maximal (and hence prime).
5. Assume that for ideals of the form $\mathfrak{a} = (f(k))_{k<n}$, where f is a map $\downarrow(n) \to A$, we have $1 \notin \mathfrak{a}$ or $\neg(1 \notin \mathfrak{a})$. Then the ideal $\mathfrak{m}$ is detachable. If furthermore $1 \in \mathfrak{a}$ or $1 \notin \mathfrak{a}$ for such ideals, then $\mathfrak{m}$ is maximal in the strong sense.

Proof. The proofs of the countable case carry over word for word.