Ideals in Computable Rings

Rod Downey

Victoria University

Wellington

New Zealand

References

- Ideals in Computable Rings, Downey, Lempp, Mileti
- Subspaces of computable vector spaces, Downey, Hirschfeldt, Kach,, Lempp, Mileti, and Montalban,

Motivation

- Understand the "effective content" of mathemematics: here algebra
- Understand the "proof theoretical content" of mathematics.

History

- At one time all of mathematics was more or less algorithmic, and it was only in the beginning of the 20th century that it began to become more abstract and non-constructive.
- Modern computational methods highlight the need to understand the algorithmic content of mathematics.
- Often we gain significant algebraic insight.
- For example, combinatorial group theory, word processing in groups etc.

- Dehn etc, Mal'tsev, Ershov, Nerode, Rabin, Frölich, Shepherdson etc

Computability Theory

- "Computable" means $f(n)$ can be computed (in theory) by a machine.
- objects coded as members of $\mathbb{N}$.
- $A \subseteq \mathbb{N}$ is computable means there is an algorithm to decide $n \in A$? uniformly. $\chi_A(n)$ computable.
- A is computably enumerable means $A = \{f(0), f(1), \dots\}$.
- Halting problem $\{\langle x, y\rangle : \varphi_x(y)$ halts $\}$ is famously c.e. but not computable.

Effective content of Field Theory

- Classically : Every countable field has an algebraic closure, and it is unique.
- A *computable field* is $\mathbb{F} = \langle F, \cdot, +, 0, 1, ^{-1} \rangle$.
- here F is a computable set (taken to be $\mathbb{N}$).
- The functions $\cdot, +, ^{-1}$ are all computable. That is given i and j we can compute k with $i +_{\mathbb{F}} j =_{\mathbb{F}}= k$, etc.

- Does a computable field have a computable unique computable algebraic closure?
- No (Frölich and Shepherdson 1956)
- Rabin (1960) Every computable field has a computable algebraic closure.

- (Metakides and Nerode, (1979) The closure is computably unique iff the field has a (separable) splitting algorithm. That is the usual method works in a computable way.

- Fields without splitting algorithms actually implicit in van der Waerden (1930)analysis of Greta Herrmann's analysis of Henzelt-König's work on ideals theory. Though he lacked the language to say it. Concept :"explicit field."

- Take $\mathbb{F} = \mathbb{Q}(\sqrt{p_{f(n)}} : n \in \mathbb{N})$, where p_n is the n-th prime. Then $x^2 - p_n$ splitting decides if $n \in ra(f)$.

- Notice that this means that Rabin's algebraic closure must have be *not* by simply adjoining roots!

- Can use this to calibrate how complicated the operation is. For example, given any computable real closed field, the orderings are in 1-1 correspondence with paths through a infinite binary tree. This is tight, for any such infinite computable binary tree, we can construct a computable real closed field with orderings in effective degree preserving 1-1 correspondence. (Metakides and Nerode 1979)

Reverse Mathematics

- Simpson, Harvey Friedman (ICM Talk)
- Hand in hand with this is understanding the *proof theory*.
- Subsystem of second order arithmetic.
- Individual variable for elements plus the axioms of peano arithmetic for these, with variable for sets of elements X, Y, etc.
- e.g. x+y=y+x, etc

- Σ^0_1 induction. That is, the axiom schema which says that for each Σ^0_1 formula φ, if $\forall n(\varphi(X,n) \rightarrow \varphi(X,n+1))$ then $\forall n(\varphi(X,n))$.

- Here a formula is called Σ^0_1 means that it has a single existential individual quantifier.

Five Basic Systems

- The calibration is based around *comprehension* axioms. These say that if we have a"construction" of a certain complexity, the system can comprehend that the object exists.
- RCA_0 (Recursive comprehension) this says that if X is defined by a recursive formula, X exists. (if φ is Δ^0_1, then $\exists X(n \in X \text{ iff } \varphi(X, n))$.)
- Example (FSS) RCA_0 proves that every (countable) field has an algebraic closure.
- (SS) RCA_0 proves the Hilbert basis theorem

- (Solomon) RCA_0 proves that every free group is orderable.

- It is important to remember that *just because something is "computably true"* does *not* necessarily mean that it is provable in RCA_0.

- For example, it is known that given any infinite computable collection of finite graphs, $G_1, G_2, \ldots$, there are $i < j$ such that G_i is a minor of G_j (the Robertson-Seymour Theorem) but this *cannot* be proven in *any* of the systems I discuss!

- Arithmetic comprehension ACA_0 same thing but φ is arithmetical similarly Π^1_1 comprehension.

- Example RCA_0 proves "Every field has a unique algebraic closure" is equivalent to ACA_0.

- Example RCA_0 proves that the compactness theorem is equivalent to ACA_0.

- Example RCA_0 proves that "every infinite finitely branching tree has an infinite path" is equivalent to ACA_0.

- Example RCA_0 proves Ramsey's Theorem $= \mathrm{ACA}_0$.

- WKL_0 weak König's lemma. Says that every binary infinite tree has a path.
- Provably weaker than ACA_0.
- RCA_0 proves that "every torsion free abelian group is orderable" is equivalent to WKL_0.
- ATR_0 arithmetical transfinite recursion. (says every pair of well orderings are comparible)
- RCA_0 proves Ulm's theorem on invariants for p-groups is equivalent to ATR_0.

- Π^1_1-CA

- (Solomon) RCA_0 proves that "every countable ordered group has order type $\mathbb{Z}^n\mathbb{Q}^m$ for $n \leq \omega$ and $m \in \{0,1\}$" is equivalent to Π^1_1-CA.

- (FSS) RCA_0 proves that every countable abelian group is the dierct sum of a reduced and a divisible group is equivalent to Π^1_1-CA.

- RCA_0 is the usual base system. $RCA_0 < WKL_0 < ACA_0 < ATR_0 < \Pi^1_1 - CA$.

Field Examples

- (Freidman, Simpson, Smith) RCA_0 proves that every countable field has an algebraic closure.
- RCA_0 proves that each such closure is unique is equivalent to ACA_0.
- WKL_0 is equivalent to every real closed field being orderable (over RCA_0).

Rings

- Here "ring"= commutative ring with identity. computable means the atomic acts are computable and the domain is (coded by) $\mathbb{N}$.
- Known Fiedman Simpson Smith
- Every countable ring has a maximal ideal = ACA_0 (over RCA_0) There is a computable ring all of whose maximal ideals are Turing complete.
- RCA_0 proves Every countable ring has a *prime* ideal = WKL_0 For each separating pair of c.e. sets, there is a computable ring coding these separating sets. (More on this below)

- Notice that this need a *different* proof than the usual one, since WKL_0 is provably weaker than ACA_0.

A basic question

- Classical observation: A ring is a field iff it has no nontrivial ideals.
- What about this efficitively. The *point* is that when we move to ideals, things become more complex. If R/I is some computable ring then ideal membership involves coset search "is there some ..." This is apparently Σ_1^0.
- To be computable we would need the ideal I to be a computable subset of R. But for ideal membership $x \in \langle y \rangle$, say, we need to answer whether $\exists z(x = yz)$ meaning $\exists z(x - yz \in I)$.

- What about principal ideals. (as above)
- Must a ring which is not a field have all computable principal ideals? *Any* computable principal ideals? *Any computable ideals*?
- If not, how complicated must they be? How to measure this anyway?

Measuring

- $A \leq_T B$ means that using B as ROM I can compute A.
- Equivalence classes called *degrees*. If there is a c.e. member called a c.e. degree.
- Example Given a c.e. degree $\boldsymbol{a}$, there is a finitely presented group with word problem of degree $\boldsymbol{a}$.
- (Downey, Jockusch, Miller) There is a computable linear ordering with no self embeddings computable $\mathbf{o}'$ the degree of the halting problem.
- Arithmetical Hierarchy $\mathbf{o}''$ etc.

First observations

- Notice that if R is a computable ring, then every finitely generated ideal of R is c. e. and so has degree at most $\mathbf{o}'$.
- In particular, if R is a computable Noetherian ring, then every ideal of R is c. e. and so has degree at most $\mathbf{o}'$.
- If the ring is Artinian then it has an ideal membership algorithm (Stolenberg-Hansen) and the question $x \in \langle y_1, \ldots, y_n \rangle$ is uniformly computable.

- If Noetherian, then whilst each ideal is computable, there are examples with no computable ideal membership algorithm (Siedenberg etc)

Trees and PA degrees

- A *tree* is a subset T of $2^{<\mathbb{N}}$ such that for all $\sigma \in T$, if $\tau \in 2^{<\mathbb{N}}$ and $\tau \subseteq \sigma$, then $\tau \in T$.
- A *branch* of a tree T is a function $f\colon \mathbb{N} \to \{0,1\}$ such that $f \upharpoonright n \in T$ for all $n \in \omega$ (where $f \upharpoonright n$ is the finite sequence of the first n values of f).
- There exists an infinite computable subtree of $2^{<\mathbb{N}}$ with no infinite computable branch.

- (Simpson) Let $\boldsymbol{a}$ and $\boldsymbol{b}$ be Turing degrees. We write $\boldsymbol{a} \gg \boldsymbol{b}$ to mean that every infinite $\boldsymbol{b}$-computable subtree of $2^{<\mathbb{N}}$ has an infinite $\boldsymbol{a}$-computable branch.

- Since there is a computable binary tree with no computable branch, $\mathbf{o} \not\gg \mathbf{o}$.
- (Kreisel Basis Theorem) $\mathbf{o}' \gg \mathbf{o}$; to see this take the leftmost path. It has c.e. degree.
- (Low Basis Theorem-Jockusch and Soare) There exists $\boldsymbol{a} \gg \mathbf{o}$ such that $\boldsymbol{a}' = \mathbf{o}'$. Every computable binary tree has a low path.

Scott-Solovay

- Suppose that $\boldsymbol{a}$ is a degree. The following are equivalent.

  1. $\boldsymbol{a} \gg \mathbf{0}$.
  2. Whenever $A, B \subseteq \mathbb{N}$ are disjoint c. e. sets, there exists an $\boldsymbol{a}$-computable set C such that $A \subseteq C$ and $B \cap C = \emptyset$ (we call C a *separator* for A and B).
  3. $\boldsymbol{a}$ is the degree of a complete extension of Peano Arithmetic (PA degree)

- (Jockusch and Soare) There exists disjoint c. e. sets $A, B \subseteq \mathbb{N}$ such that whenever C is a set with $A \subseteq C$ and $B \cap C = \emptyset$, we have $\deg(C) \gg \mathbf{o}$.

Upper Bound

- Theorem (CLM) Suppose that R is a computable ring which is not a field, and that $\boldsymbol{d} \gg \mathbf{o}$. Then there exists a nontrivial proper ideal I of R such that $\deg(I) \leq \boldsymbol{d}$.
- Proof: Suppose that $a \in R$ is not a unit, and take $b \notin \langle a \rangle_R$. Then consider the tree generated by ideals containing a and not containing b.

The main result

- Our main result here is that there is a computable ring R (in fact, an integral domain), which is not a field, for which the crude upper bound on the complexity of nontrivial proper ideals is achieved.

- (Building computable rings)

- Typical rings such as $\mathbb{Z}$ and $\mathbb{Q}[x]$ come equipped with natural representations as computable rings.

- Suppose more generally that S is an infinite c. e. subset of a computable ring A which is also a subring.

- Take a computable bijective function $h\colon \mathbb{N} \to S$.
- Let R be the computable ring obtained by letting the universe be $\mathbb{N}$, letting $0_R = h^{-1}(0_A)$ and $1_R = h^{-1}(1_A)$, letting $a +_R b = h^{-1}(h(a) +_A h(b))$, and letting $a \cdot_R b = h^{-1}(h(a) \cdot_A h(b))$.
- The R is a computable ring.
- Similarly if I is a computable ideal, the R/I is a computable ring. (In fact you can show that every computable ring is $\mathbb{Z}[x_i : i \in \mathbb{N}]/I$ for suitably chosen computable I.)

The rough idea

- the c. e. sets A and B from and computable functions $\alpha, \beta\colon \mathbb{N} \to \mathbb{N}$ such that $A = \operatorname{ran}(\alpha)$ and $B = \operatorname{ran}(\beta)$.

- Build a computable ring R with distinguished elements x_n for each $n \in \mathbb{N}$, and attempt to satisfy the following requirements:

  1. For all $r \in R$ with $r \neq 0$, we have $r \mid x_{\alpha(n)}$ for all $n \in \mathbb{N}$.
  2. For all $r \in R$ with $r \neq 0$, we have $r \mid (x_{\beta(n)} - 1)$ for all $n \in \mathbb{N}$.

- Then any nontrivial proper ideal must contain $x_{\alpha(n)}$ for each $n \in \mathbb{N}$ and must not contain $x_{\beta(n)}$ for every $n \in \mathbb{N}$ (because otherwise it would contain 1). Thus, from a nontrivial proper ideal we could compute a separator for A and B.

The proof

- Work in the field of fractions F of $\mathbb{Z}[\overline{x}] = \mathbb{Z}[x_1, x_2, \ldots]$.
- We give a c. e. subring S of F by the construction outlined before.
- S is generated by

$$\mathbb{Z}[\overline{x}] \cup \{\frac{x_{\alpha(i)}}{p} : i \in \mathbb{N}, p \in \mathbb{Z}[\overline{x}] - \{0\}\} \cup \{\frac{x_{\beta(j)} - 1}{q} : j \in \mathbb{N}, q \in \mathbb{Z}[\overline{x}] - \{0\}\}$$

- S is c.e. but unfortunately $S = F$

- We need to introduce enough divisibilities in the above strategy to encode what we need into the ideals, while ensuring that we don't introduce too many to collapse S into a field.

- 1. For all $r \in R$ with $r \neq 0$, we have $r \mid x_{\alpha(n)}$ for all but finitely many $n \in \mathbb{N}$.
  2. For all $r \in R$ with $r \neq 0$, we have $r \mid (x_{\beta(n)} - 1)$ for all but finitely many $n \in \mathbb{N}$.
- Finite sets don't affect what is encoded into ideals, and by relaxing the divisibility conditions we can ensure that the ring constructed is not a field.
- $\alpha, \beta \colon \mathbb{N} \to \mathbb{N}$ such that $A = \operatorname{ran}(\alpha)$ and $B = \operatorname{ran}(\beta)$.

- (The real construction) For each $n \in \mathbb{N}$, let $\mathbb{Z}[\overline{x}]_n$ be the subring of $\mathbb{Z}[\overline{x}]$ consisting of those elements f with $i < n$ for all x_i occurring in f. Let

$$A = \{\frac{x_{\alpha(i)}}{p} : i \in \mathbb{N}, p \in \mathbb{Z}[\overline{x}]_{\alpha(i)} - \{0\}\}$$

and let

$$B = \{\frac{x_{\beta(j)} - 1}{q} : j \in \mathbb{N}, q \in \mathbb{Z}[\overline{x}]_{\beta(j)} - \{0\}\}$$

- Notice that A and B are c. e. subsets of F. Let S be the subring of F generated by $\mathbb{Z}[\overline{x}] \cup A \cup B$.

- Since

$$g_1 \cdot \frac{x_{\alpha(i)}}{p_1} + g_2 \cdot \frac{x_{\alpha(i)}}{p_2} = (g_1 p_2 + g_2 p_1) \cdot \frac{x_{\alpha(i)}}{p_1 p_2}$$

and

$$h_1 \cdot \frac{x_{\beta(j)} - 1}{p_1} + h_2 \cdot \frac{x_{\beta(j)} - 1}{p_2} =$$

$$(h_1 p_2 + h_2 p_1) \cdot \frac{x_{\beta(j)} - 1}{p_1 p_2}$$

- Therefore

$$S = \{f + \sum_{i \in I} g_i \cdot \frac{x_{\alpha(i)}}{p_i} + \sum_{j \in J} h_j \cdot \frac{x_{\beta(j)} - 1}{q_j} :$$

$$I, J \subseteq \mathbb{N} \text{ are finite,}$$

$$f, g_i, h_j \in \mathbb{Z}[\overline{x}],$$

$$p_i \in \mathbb{Z}[\overline{x}]_{\alpha(i)} - \{0\},$$

$$q_j \in \mathbb{Z}[\overline{x}]_{\beta(j)} - \{0\}\}$$

- It can be shown that S is not a field.

- Suppose $h \colon R \to S$ be the computable isomorphism.

- Suppose that I is a nontrivial proper ideal of R and fix $a \in I$ with $a \neq 0$. Notice that $h(I)$ is a nontrivial proper ideal of S. Fix $f, g \in \mathbb{Z}[\overline{x}]$ with $\frac{f}{g} = h(a)$.

- Since $h(I)$ is an ideal of S and $g \in S$, it follows that $f \in h(I)$. Fix $\ell \in \mathbb{N}$ such that $f \in \mathbb{Z}[\overline{x}]_\ell$. Let

$$D = \{k \in \mathbb{N} : h^{-1}(x_k) \in I\}$$

and notice that $D \leq_T I$.

- $\alpha(n) \in D$ for all $n \in \mathbb{N}$ with $\alpha(n) \geq \ell$ and that $\beta(n) \notin D$ for all $n \in \mathbb{N}$ with $\beta(n) \geq \ell$.

- Fix $n \in \mathbb{N}$ with $\alpha(n) \geq \ell$. We then have that $\frac{x_{\alpha(n)}}{f} \in S$, hence $x_{\alpha(n)} \in h(I)$ because $h(I)$ is an ideal of S, and so $\alpha(n) \in D$.

- We also have that $\frac{x_{\beta(n)}-1}{f} \in S$, hence $x_{\beta(n)} - 1 \in h(I)$, so $x_{\beta(n)} \notin h(I)$ because $h(I)$ is a proper ideal of S, and so $\beta(n) \notin D$.

A Corollary

- Theorem (DLM) There is a computable integral domain R which is not a field such that $\deg(I) = \mathbf{0}'$ for all nontrivial proper finitely generated ideals I of R.
- (Reversal) Over RCA_0, the following are equivalent to WKL_0.
  1. If a ring R has no nontrivial proper ideals, then it is a field.
  2. If I is a maximal ideal of R, then R/I is a field
- Over RCA_0, ACA_0 is equivalent to every field has a principal ideal.

- Unfortunately this does *not* follow from the PA result since though there will be spaces where each principal ideals is Turing complete by general nonsense about PA degrees, this fact is proven using Arslanov's completeness criterion which is not provable from RCA_0 it needs Σ^0_2 induction.

- It needs more involved arguments via Gröbner basis theory.

The Nilradical

and Jacobson Radical

- Recall $\mathrm{Nil}(R) = \{a \in R : \exists n(a^n = 0)\}$
- If R is a computable ring, then $\mathrm{Nil}(R)$ is Σ^0_1.
- Theorem (DLM) There exists a computable ring R such that $\mathrm{Nil}(R)$ is Σ^0_1-complete.
- The proof uses the ideal construction, to make elements nilpotent when the halting problem tells us to do so.

- If R is a computable ring, then $\mathrm{Jac}(R)$ is Π^0_2.
- Recall

$$\begin{aligned} \mathrm{Jac}(R) &= \{a \in R : ab + 1 \\ &\quad \text{is a unit for all } b \in R\} \\ &= \{a \in R : \forall b \exists c((ab+1)c = 1)\} \end{aligned} \tag{1}$$

- Theorem (DLM) There exists a computable integral domain R such that $\mathrm{Jac}(R)$ is Π^0_2-complete.

Vector Spaces

- Metakides-Nerode, Ershov, Mal'tsev, Dekker $\langle V, +, \cdot, 0, 1_F, \lambda : \lambda \in F \rangle$.
- Each computable vector space is computably isomorphic to a quotient V_∞ / W for a computable $W \leq V_\infty$. V_∞ the standard space of finite support over F.
- (Metakides-Nerode 1980) There are computable vector spaces of infinite dimension where each c.e. independent set is finite.
- Shore completely classified the possible dependence degrees $\boldsymbol{a_1} < \boldsymbol{a_2} \cdots < \boldsymbol{a}_\omega$.

- Friedman Simpson Smith There is a computable vector space where every indendent subset computes the halting problem, and hence RCA_0 proves "Every vector space has a basis is equivalent to ACA_0."

Our Question

- The statement "Every vector space that is not 1-dimensional has a proper subspace."
- If V is not one dimensional then V has two elements a, b with $a \notin \langle b \rangle$. Now play the computable tree game:

- Consider the collection of subspaces that contain a and not b. this can be coded bya tree and hence (i) WKL_0 proves that “Every vector space that is not 1-dimensional has a proper subspace.”

  (ii) There are always subspaces of low degree.

- Reversal? What about finite dimensional subspaces?

Our Results

- Theorem (many) The statement "Every vector space that is not 1-dimensional has a proper subspace," is equivalent to WKL_0 over RCA_0
- Again we use PA degrees.
- Using again, a new argument, there is a the statement "every vector spae that is not a field has a finite dimensional subspace" is equivalent to ACA_0 over RCA_0.