Decidability of the theory of modules over Bézout domains with infinite residue fields

Carlo Toffalori (Camerino)

Padova, September 26, 2017
XXVI Incontro AILA

Joint work with Lorna Gregory, Sonia L'Innocente and Gena Puninski

Decidability of the theory of modules over a given ring R?

- A topic out of fashion? How effective a decision algorithm is (when it exists)? See computational complexity, $P = NP$, ...
- It requires strong assumptions on R, for instance countability (otherwise the decision problem makes no sense, or the theory of R-modules is undecidable).

In detail, assuming R a commutative domain with unity, R should be *effectively given*, meaning that its elements can be listed, possibly with repetitions, as $a_0 = 0$, $a_1 = 1$, $a_2, \ldots, a_n, \ldots$ ($n \in \mathbb{N}$) so that suitable algorithms effectively perform the following, when m, n range over non negative integers:

1. Deciding whether $a_m = a_n$ or not.
2. Calculating $a_m + a_n$ and $a_m \cdot a_n$ (or rather indices of these elements in the list).
3. Establishing whether a_m divides a_n.

Then other familiar procedures can be effectively carried out, such as determining units, calculating additive and (when possible) multiplicative inverses, computing in the right frameworks gcd and lcm.

On the other hand, for a given domain R, decidability still provides, beyond any countability restriction, a nice reference point towards

- the analysis of pp-formulae over R,
- the description of the Ziegler spectrum of R (both the points and the topology),
- through them, the classification of R-modules when convincing algebraic concepts of *wildness* and *tameness* are lacking.

General notation:

- L_R = first order language of (right) R-modules,
- T_R = first order theory of R-modules in L_R.

For $a \in R$,

- $a \mid x$ denotes the *divisibility formula* of L_R, defining in a module M the submodule Ma;
- $xa = 0$ is the *annihilator formula* defining in M the kernel of the multiplication by a.

The Ziegler spectrum Zg_R

- points = (isomorphism types of) indecomposable pure injective R-modules,
- basic open sets = $(\varphi(x)/\psi(x)) :=$ $\{N \in Zg(R) : \varphi(N) \supset \psi(N) \cap \varphi(N)\}$ where $\varphi(x)$, $\psi(x)$ range over pp-formulae.

We focus on **Bézout domains**, more generally on **Prüfer domains**.

A commutative domain R with identity is *Bézout* if every 2-generated ($\Rightarrow$ finitely generated) ideal is principal.

A Bézout domain is *coherent*: the intersection of 2 principal ideals is also principal.

Then one can determine, for every $a, b \in R$,

- a greatest common divisor $\gcd(a, b)$,
- a least common multiple $\operatorname{lcm}(a, b)$,

both defined up to invertible factors, and satisfying the Bézout identities: for some suitable $u, v, g, h \in R$, $au + bv = \gcd(a, b)$, $\gcd(a, b) = ga$, $\gcd(a, b) = hb$.

Bézout domains include

- principal ideal domains *PID*,
- the ring of algebraic integers (not a *PID*, but a directed union of Dedekind domains),
- the ring of entire (complex or real) functions in 1 variable,
- $\mathbb{Z} + X\mathbb{Q}[X]$, and more generally the rings coming from the so-called $D + M$-construction, namely $D + XQ[X]$ where D is a *PID* that is not a field and Q is its field of fractions (get in this way a Bézout domain, which is neither Noetherian nor a *UFD*),
- (commutative) valuation domains.

Prüfer domains are a larger setting. A domain is *Prüfer* if all its localizations at maximal ideals, and consequently at non zero prime ideals, are commutative valuation domains.

Some decidability results over Bézout domains

The $D + M$-construction

A(n effectively given) principal ideal domain D is called *strongly effectively given* if the following hold:

- there is an algorithm that lists all the prime elements of D;
- there is an algorithm that lists all the irreducible polynomials of $Q[X]$;
- there is an algorithm calculating, for every prime p the size of the field D/pD.

For instance $\mathbb{Z}$ is strongly effectively given (Kronecker).

Theorem

(Puninski-T., 2014) Let D be a strongly effectively given principal ideal domain and let $R = D + XQ[X]$ be the corresponding Bézout domain. Then T_R is decidable.

In particular the theory of modules over $\mathbb{Z} + X\mathbb{Q}[X]$ is decidable.

The key step in the proof: a full description of Zg_R (the Cantor-Bendixson rank is 4), independently of the assumption that D is strongly effectively given.

Algebraic integers

Theorem

(L'Innocente-Puninski-T., 2017) The theory of modules over the ring $\mathbb{A}$ of algebraic integers is decidable.

The proof applies to effectively given Bézout domains R such that

- every non zero prime ideal $\mathfrak{p}$ is maximal,
- the residue field $R/\mathfrak{p}$ is infinite,
- the maximal ideal of the localization $R_{\mathfrak{p}}$ is finitely generated.

No extensive analysis of $\mathrm{Zg}_{\mathbb{A}}$ is used. Instead, the *(prime) radical relation*, $a \in \mathrm{rad}(b)$, plays a crucial role.

Entire complex valued functions

Also worth mentioning (despite the uncountable setting), because a description of the Ziegler spectrum of the ring of entire complex valued functions is provided (L'Innocente, Point, Puninski, T., 2017).

Note that also in this case residue fields with respect to maximal ideals are infinite.

Valuation domains

Theorem

(Gregory, 2015, extending Puninski-Puninskaya-T., 2007) The theory T_V of modules over a(n effectively given) valuation domain V is decidable if and only if there is an algorithm which decides the prime radical relation in V, namely, for every $a, b \in V$, answers whether $a \in \mathrm{rad}(b)$ (equivalently whether the prime ideals of V containing b also include a).

Our aim: enlarge this analysis over Bézout (or even Prüfer) domains.

The main result

Theorem

(Gregory-L'Innocente-Puninski-T., 2017) Let R be a(n effectively given) Bézout domain with an infinite residue field for every maximal ideal. Then T_R is decidable if and only if there is an algorithm that answers a double prime radical relation, that is, decides, given $a, b, c, d \in R$, whether, for all prime ideals $\mathfrak{p}, \mathfrak{q}$ of R with $\mathfrak{p} + \mathfrak{q} \neq R$, $b \in \mathfrak{p}$ implies $a \in \mathfrak{p}$ or $d \in \mathfrak{q}$ implies $c \in \mathfrak{q}$.

Generalization to Prüfer domains are also obtained.

The hypothesis on infinite residue fields applies to a large class of noteworthy algebraic examples.
Using it, by the Baur-Monk theorem, in order to prove decidability it suffices to check effectively the inclusions of basic open sets of the Ziegler topology of the form

$$(\star) \qquad (\varphi/\psi) \subseteq \cup_{i=1}^{n}(\varphi_i/\psi_i).$$

where φ, ψ, φ_i, ψ_i $(i = 1, \ldots, n)$ range over pp-formulae in one free variable.

Step 1. Reduce the open sets in $(\star)$ to simple forms $(x = x/xd = 0)$, $(xb = 0/x = 0)$, $(x = x/c \mid x)$, $(xb = 0/c \mid x)$.

Tools

- Over Bézout domains, gcd.
- In the Prüfer setting, a result by Tuganbaev: If R is a Prüfer domain, then for all $a, b \in R$ there exist $\alpha, r, s \in R$ such that $a\alpha = br$ and $b(\alpha - 1) = as$.
- Also, over a Prüfer domain R, any indecomposable pure injective R-module N is *pp-uniserial*, i. e. its lattice of pp-definable submodules is a chain.

Crucial: all the required reductions can be performed effectively when R is effectively given.

Step 2. Localize at prime ideals $\mathfrak{p}$ of a Prüfer domain R and use Gregory's results over valuation domains.

A crucial order relation: For $a, b \in R\backslash\{0\}$, $a \leq_{\mathfrak{p}} b$ if and only if $bR_{\mathfrak{p}} \subseteq aR_{\mathfrak{p}}$.

Can express that in equivalent ways using Tuganbaev or (over a Bézout domain) gcd.

- (Over any Prüfer domain) Let $a, b \in R$, $\alpha, r, s \in R$, $b\alpha = as$ and $a(\alpha - 1) = br$. Then $a \leq_{\mathfrak{p}} b$ if and only if either $\alpha \notin \mathfrak{p}$ or $r \notin \mathfrak{p}$.
- (Over a Bézout domain R) Let $a, b \in R\backslash\{0\}$. Then $a \leq_{\mathfrak{p}} b$ if and only if $a/\gcd(a, b) \notin \mathfrak{p}$.

Now translate $(\star)$ – as reduced after Step 1 – in the local setting into order relations between elements a, b, c, d etc.

The *double prime radical relation* DPR: for every Bézout domain R (actually for every commutative ring R) and $a, b, c, d \in R$,

$$(a, b, c, d) \in \mathrm{DPR}(R)$$

if and only if

for all prime ideals $\mathfrak{p}, \mathfrak{q}$, if $\mathfrak{p} + \mathfrak{q} \neq R$ then $a \in \mathfrak{p}$ or $b \notin \mathfrak{p}$ or $c \in \mathfrak{q}$ or $d \notin \mathfrak{q}$.

Some equivalent characterizations.

- Let R be any commutative domain. For $a, b, c, d \in R$, $(a, b, c, d) \notin \mathrm{DPR}(R)$ if and only if there is some maximal ideal $\mathfrak{m}$ of R such that $a \notin \mathrm{rad}(bR_{\mathfrak{m}})$ and $c \notin \mathrm{rad}(dR_{\mathfrak{m}})$.
- Let R be a Prüfer domain. For $a, b, c, d \in R$, $(a, b, c, d) \notin \mathrm{DPR}(R)$ if and only if $(\mathrm{rad}(b) : a) + (\mathrm{rad}(d) : c)$ is a proper ideal of R.
- Let R be a Prüfer domain. For $a, b, c, d \in R$, $(a, b, c, d) \in \mathrm{DPR}(R)$ it and only if $(xb = 0 \,/\, d \mid x) \subseteq (xa = 0 \,/\, x = 0) \cup (x = x \,/\, c \mid x)$.

Let R be an effectively given Bézout domain with all its residue fields infinite.

Look at *Boolean combinations of conditions on a pair of prime ideals*, that is, Boolean combinations Δ of conditions of the form $a \in P$, $b \notin P$, $c \in Q$ and $d \notin Q$ where $a, b, c, d \in R$ and P, Q are variables for prime ideals.

Lemma

Let R be a(n effectively given) Bézout domain, and Δ be a Boolean combination of conditions as before. If $\mathrm{DPR}(R) \subseteq R^4$ is recursive, then there is an algorithm which answers whether for all prime ideals $\mathfrak{p}, \mathfrak{q}$, $\mathfrak{p} + \mathfrak{q} \neq R$ implies that $(\mathfrak{p}, \mathfrak{q})$ satisfie Δ

A key role of gcd.

The case of algebraic integers is now a consequence.

Corollary

Let R be an effectively given Bézout domain of Krull dimension 1 *all of whose residue fields are infinite. The theory of R-modules is decidable.*

From Bézout to Prüfer

We introduce a larger family of "prime radical" relations over a Prüfer domain R: for every positive integer n let DPR_n be the $(2n+2)$-ary relation DPR_n such that, for $a, c, b_i, d_i \in R$ $(1 \leq i \leq n)$,

$$(a, c, b_1, \ldots, b_n, d_1, \ldots, d_n) \in \mathrm{DPR}_n(R)$$

if and only if for all prime ideals $\mathfrak{p}$ and $\mathfrak{q}$ of R with $\mathfrak{p} + \mathfrak{q} \neq R$, either $a \in \mathfrak{p}$ or $c \in \mathfrak{q}$ or some b_i is out of $\mathfrak{p}$ or some d_i is out of $\mathfrak{q}$. Hence DPR is just DPR_1.

Theorem

Let R be an effectively given Prüfer domain with an infinite residue field for every maximal ideal. If there are algorithms deciding in R the membership to DPR_n for every positive integer n, then the theory T_R of all R-modules is decidable.

References

- L. Gregory, Decidability for theories of modules over valuation domains, *J. Symbolic Logic* 80 (2015), 684–711.
- L. Gregory, S. L'Innocente, G. Puninski, C. T., Decidability of the theory of modules over Bézout domains with infinite residue field, arXiv:1706.08940 [math.LO].
- S. L'Innocente, F. Point, G. Puninski, C. T., The Ziegler spectrum of the ring of entire complex valued functions, arXiv:1703.01752 [math.LO].
- S. L'Innocente, C. T., G. Puninski, On the decidability of the theory of modules over the ring of algebraic integers, Ann. Pure Appl. Logic 168 (2017), 1507-1516.

- G. Puninski, V. Puninskaya, C. T., Decidability of the theory of modules over commutative valuation domains, *Ann. Pure Appl. Logic* 145 (2007), 258–275.
- G. Puninski – C. T., Some model theory of modules over Bézout domains. The width, *J. Pure Applied Algebra* 219 (2015), 807–829.
- G. Puninski – C. T., Decidability of modules over a Bézout domain $D + XQ[X]$ with D a principal ideal domain and Q its field of fractions, *J. Symbolic Logic* 79 (2014), 296–305.
- A. Tuganbaev, Distributive rings, uniserial rings of fractions and endo-Bezout modules, *J. Math. Sciences* 114 (2003), 1185–1203.