The complexity of radicals in rings and modules

Huishan Wu

Chinese Annual Conference on Mathematical Logic 2021
Nankai University

July 9-11, 2021

Outline

- Introduction
- Ideals in rings
- Radicals in rings
- Radicals in modules

Introduction

A brief history

- Van der Waerden (1930): study splitting algorithm of “explicitly given” fields.
- Church (1936), Kleene(1936), Turing(1937): provide formal definition of algorithm (i.e., finite procedure).
- Fröhlich and Shepherdson (1956): provide formal definition of explicit fields,
  - construct an explicit field with no splitting algorithm.
- Rabin (1960): study subgroups of computable groups, algebraic closures of computable fields,
  - every computable field has a computable algebraic closure.

Computability

- Computable functions (or sets): Turing computable, intuitive computable.
- Partial computable functions: $\varphi_0, \varphi_1, \cdots, \varphi_e, \cdots$.
- Computably enumerable sets ($=\Sigma^0_1$ sets): $W_0, W_1, \cdots, W_e, \cdots$.
  - $\emptyset' = \{e : \varphi_e(e)\downarrow\}$ (i.e., the Halting set) is Σ^0_1-complete.
  - Fin$= \{e : |W_e| < \infty\}$ is Σ^0_2-complete.
  - Inf$= \{e : |W_e| = \infty\}$ is Π^0_2-complete.
- Computably enumerable trees: $T_0, T_1, \cdots, T_e, \cdots$
- WF$= \{ e : T_e$ is well-founded computable tree $\}$ is Π^1_1-complete.

Turing reducibility

(1) $\leq_T$: Turing reducibility on subsets of $\mathbb{N}$.

(2) $\equiv_T$: Turing equivalence relation.

(3) Turing degrees (or degrees): equivalence classes of $\equiv_T$.

- $\mathbf{0}$: the degree of computable sets;
- $\mathbf{0}'$: the degree of Halting problem.

(4) c.e. degrees.

(5) PA degrees.

- A set is PA if it can compute an infinite path of any infinite computable binary tree.

RCA_0 : the base system that captures effective proofs.

- $\mathsf{RCA}_0 \vdash$ "every field has an algebraic closure".

WKL_0 : RCA_0+ "for any X, there is a set Y that is of PA degree relative to X".

ACA_0 : RCA_0+ "for any X, the Halting set X' relative to X exists".

Ideals in rings

Computable ring

A computable ring is a computable set $R \subseteq \mathbb{N}$ together with computable binary operations $+_R$ and $\cdot_R$ on R and elements 0_R, 1_R in R such that $(R, +_R, \cdot_R, 0_R, 1_R)$ satisfies axioms of a ring.

Examples:

- $\mathbb{Z}[x_1, x_2, \cdots, x_n]$,$\mathbb{Q}[x_1, x_2, \cdots]$.

The ideal membership problem

Given a computable ring R, how about the complexity of its:

- maximal ideals, prime ideals, finitely generated ideals, or even general ideals$\cdots$?

Friedman, Simpson, Smith (1983): Countable algebra and set existence axioms, *Ann. Pure Appl. Logic*.

Theorem(FSS, 1983)

Over RCA_0, the following are equivalent.

(1) WKL_0.

(2) Any commutative ring contains a prime ideal.

Theorem(FSS, 1983)

Over RCA_0, the following are equivalent.

(1) ACA_0.

(2) Any commutative ring contains a maximal ideal.

Downey, Lempp, Mileti (2007): Ideals in computable rings, *J. Algebra*.

Theorem(DLM, 2007)

Over RCA_0, the following are equivalent.

(1) WKL_0.

(2) Any commutative ring that is not a field has a nontrivial ideal.

Theorem (DLM, 2007)

The following are equivalent over RCA_0.

(1) ACA_0.

(2) Any commutative ring that is not a field has a nontrivial finitely generated ideal.

- A commutative ring containing no infinite ascending chain of ideals is called Noetherian.
- A commutative ring containing no infinite descending chain of ideals is called Artinian.

Theorem(Conidis, 2010)

There is a computable ring R containing an infinite uniformly computable increasing sequence $I_0 \subset I_1 \subset \cdots$ of ideals such that

(1) every ideal $I \subseteq R$ that is not PA is computable, and it is equal to I_n for some $n \in \mathbb{N}$ or $I_\infty = \bigcup_{i \in \mathbb{N}} I_n$;

(2) every infinite decreasing sequence $J_0 \subset J_1 \subset \cdots$ of ideals in R contains some J_n that is of PA degree.

Theorem

- Conidis (2010): over RCA_0, "every Artinian ring is Noetherian" proves WKL_0.
- Conidis (2013): WKL_0 proves "every Artinian ring is Noetherian".

Radicals of rings

Nilracials of rings

Let R be a commutative ring.

- The nilradical of R: $Nil(R) = \{x \in R : \exists n[x^n = 0_R]\}$.
- Classically, $Nil(R)$ =the intersection of all prime ideals of R, also known as the prime radical of R

Theorem

- Downey, Lempp, Mileti (2007): There is a computable commutative ring R such that $Nil(R) = \{x \in R : \exists n[x^n = 0_R]\}$ is Σ^0_1-complete.
- Conidis (2009): There is a computable **noncommutative** ring R such that the prime radical of it is Π^1_1-complete.

Jacobson radicals of commutative rings

Let R be a commutative ring.

- The Jacobson radical of R: $Jac(R) = \{x \in R : \forall y \in R \exists z \in R[z(1_R - yx) = 1_R]\}$.
- Classically, $Jac(R)$= the intersection of all maximal ideals of R.

Theorem(Downey, Lempp, Mileti, 2007)

There exists a computable ring R such that $Jac(R) = \{x \in R : \forall y \in R \exists z \in R[z(1_R - yx) = 1_R]\}$ is Π^0_2-complete.

A natural question:

- What is the complexity of Jacobson radicals of *noncommutative* rings?

Jacobson radicals of noncommutative rings

For a ring R not necessarily commutative, we propose the following notions.

- The first order left Jacobson radical of R:
  $Jac_l^0(R) = \{x \in R : \forall y \in R \exists z \in R[z(1_R - yx) = 1_R]\}$.
- The first order right Jacobson radical of R:
  $Jac_r^0(R) = \{x \in R : \forall y \in R \exists z \in R[(1_R - xy)z = 1_R]\}$.
- The second order left Jacobson radical of R:
  $Jac_l^1(R) = \bigcap\{\mathfrak{M} : \mathfrak{M} \text{ is a maximal left ideal of } R\}$.
- The second order right Jacobson radical of R:
  $Jac_r^1(R) = \bigcap\{\mathfrak{M} : \mathfrak{M} \text{ is a maximal right ideal of } R\}$.

First order Jacobson radicals

Proposition(Wu, 2021)

Over RCA_0, the following nine sets are equal for a ring R.

$$A_1 := \{x \in R : \forall y_1, y_2 \in R \exists z \in R[z(1_R - y_1 x y_2) = (1_R - y_1 x y_2)z = 1_R]\}.$$
$$A_2 := \{x \in R : \forall y_1, y_2 \in R \exists z \in R[z(1_R - y_1 x y_2) = 1_R]\}$$
$$A_3 := \{x \in R : \forall y_1, y_2 \in R \exists z \in R[(1_R - y_1 x y_2)z = 1_R]\}$$
$$A_4 := \{x \in R : \forall y \in R \exists z \in R[z(1_R - yx) = (1_R - yx)z = 1_R]\}$$
$$A_5 := \{x \in R : \forall y \in R \exists z \in R[z(1_R - yx) = 1_R]\} = Jac_l^0(R)$$
$$A_6 := \{x \in R : \forall y \in R \exists z \in R[(1_R - yx)z = 1_R]\}$$
$$A_7 := \{x \in R : \forall y \in R \exists z \in R[z(1_R - xy) = (1_R - xy)z = 1_R]\}$$
$$A_8 := \{x \in R : \forall y \in R \exists z \in R[z(1_R - xy) = 1_R]\}$$
$$A_9 := \{x \in R : \forall y \in R \exists z \in R[(1_R - xy)z = 1_R]\} = Jac_r^0(R)$$

Corollary

Over RCA_0, $Jac_l^0(R) = Jac_r^0(R)$.

In the following, $Jac^0(R) = Jac_l^0(R) = Jac_r^0(R)$ means the first order radical of R.

Theorem(Sato, 2016)

The following are equivalent over RCA_0.

(1) ACA_0.

(2) For any ring R, $Jac^0(R) = Jac_l^1(R)$.

(3) For any ring R, $Jac^0(R) = Jac_r^1(R)$.

Corollary

For any ring R, ACA_0 can prove $Jac_l^1(R) = Jac_r^1(R)$.

Second order Jacobson radicals

Motivating question

Can RCA_0 prove $Jac_l^1(R) = Jac_r^1(R)$ for a noncommutative ring R?

- For general rings, the question is unknown currently!

Definition(RCA_0)

- A ring R is local if the set $U(R)$ of invertible elements exists and $R - U(R)$ is closed under addition.
- A ring R is left local if the set $U_l(R)$ of left invertible elements exists and $R - U_l(R)$ is closed under addition.
- A ring R is right local if the set $U_r(R)$ of right invertible elements exists and $R - U_r(R)$ is closed under addition.

Lemma

Over RCA_0, the following are equivalent for a ring R.

(1) R is left local.

(2) $Jac^1_l(R)$ exists and $Jac^1_l(R) = R - U_l(R)$.

Similar for right local rings.

Theorem(Wu, 2021)

Over RCA_0, for a left local ring R, $Jac^1_l(R) = Jac^1_r(R)$.

Corollary

The following are equivalent over RCA_0.

(1) R is a left local ring.

(2) R is a right local ring.

(3) R is a local ring.

Proposition(ACA_0)

For a ring R, the first order Jacobson radical $Jac^0(R)$ is equal to each of the following sets.

- $B_1 :=$ the intersection of all maximal left ideals of $R = Jac_l^1(R)$.
- $B_2 :=$ the intersection of the annihilators of all simple left R-modules.
- $B_3 :=$ the largest superfluous left ideal of R.
- $B_4 :=$ the sum of all superfluous left ideals of R.
- $B_5 :=$ the intersection of all maximal right ideals of $R = Jac_r^1(R)$.
- $B_6 :=$ the intersection of the annihilators of all simple right R-modules.
- $B_7 :=$ the largest superfluous right ideal of R.
- $B_8 :=$ the sum of all superfluous right ideals of R.

Radicals of modules

Definition

Let R be a commutative ring with identity 1_R, a module M over R is an abelian group together with a scalar operation $\cdot$ from $R \times M$ to M such that for all $m, m_1, m_2 \in M$ and $r, r_1, r_2 \in R$, the following axioms hold:

- $(r_1 + r_2) \cdot m = r_1 \cdot m + r_2 \cdot m$;
- $(r_1 r_2) \cdot m = r_1 \cdot (r_2 \cdot m)$;
- $1_R \cdot m = m$;
- $r \cdot (m_1 + m_2) = r \cdot m_1 + r \cdot m_2$.

We often write $r \cdot m$ as rm for convenience.

Examples:

- Modules over the integer ring $\mathbb{Z}$ are abelian groups.
- Modules over fields are vector spaces.

In this section, let R be a commutative ring.

Definition

For an R-module M, the radical of M $rad(M)$ is the intersection of all maximal submodules of M.

- Classically, $rad(M) = \bigcap\{\mathfrak{M}M : \mathfrak{M} \text{ is a maximal ideal of } R\}$.

Question: What is the complexity of radicals of modules over commutative rings?

- For $\mathbb{Z}$-modules M, $rad(M) = \bigcap_{i \in \mathbb{N}} p_i M$ is Π^0_2, where p_i is the i-th prime number, and $p_i M = \{p_i x : x \in M\}$.

Theorem(Wu, 2020)

The following are equivalent over RCA_0.

(1) ACA_0.

(2) For any $\mathbb{Z}$-module M, $rad(M)$ exists.

Theorem(Wu, 2021)

There is a computable $\mathbb{Z}$-module M such that $rad(M)$ is Π^0_2-complete.

Theorem(Conidis, 2021)

There is a computable module M over a computable ring R such that $rad(M)$ is Π^1_1-complete.

Corollary

The following are equivalent over RCA_0.

(1) $\Pi^1_1 - CA_0$.

(2) For any module M over a commutative ring R, $rad(M)$ exists.

Thank you!