Reverse Mathematics and Commutative Ring Theory

Takeshi Yamazaki
Mathematical Institute, Tohoku University

Computability Theory and Foundations of Mathematics
Tokyo Institute of Technology, February 18 - 20, 2013

Outline of this talk:

1. What is Reverse Ring Theory?

2. Basics on R-modules

Background of reverse mathematics: Second order arithmetic (Z_2) is a two-sorted system.

Number variables $m, n, \ldots$ are intended to range over $\omega = \{0, 1, 2 \ldots\}$.

Set variables $X, Y, ...$ are intended to range over subsets of ω.

We have $+$, $\cdot$, $=$ on ω, plus the membership relation

$$\in = \ \{(n, X) : n \in X\} \subseteq \omega \times \mathcal{P}(\omega).$$

Within subsystems of second order arithmetic, we can formalize rigorous mathematics (analysis, algebra, geometry, . . .).

Themes of Reverse Mathematics:

Let τ be a mathematical theorem. Let S_τ be the weakest natural subsystem of second order arithmetic in which τ is provable.

I. Very often, the principal axiom of S_τ is logically equivalent to τ (over $\mathsf{RCA_0}$).

II. Furthermore, only few subsystems of second order arithmetic arise in this way.

Such subsystems are

($\mathsf{RCA_0}$), $\mathsf{WKL_0}$, $\mathsf{ACA_0}$, $\mathsf{ATR_0}$, Π^1_1-CA_0

We say these are big 5 systems!

Reverse Ring Theory is a part of R.M. given by restricting the subject to the theorems of Commutative Ring Theory.

Definition 1 (RCA_0) *A (code for a)* **commutative ring** *(with identity) is a subset R of $\mathbb{N}$, together with computable binary operations $+$ and $\cdot$ on R, and elements $0, 1 \in R$, such that $(R, 0, 1, +, \cdot)$ is a ring (with identity $1 \in R$).*

We often write $(R, 0, 1, +, \cdot)$ by R for short.

By a ring, we mean a commutative ring (with identity) throughout the rest of this talk.

Theorem 1 (Friedman-Simpson-Smith) ACA_0 *is equivalent to the statement that every countable ring has a maximal ideal over* RCA_0.

Theorem 2 (FSS) WKL_0 *is equivalent to the statement that every countable ring has a prime ideal over* RCA_0.

The following definitions are made in RCA_0. Let R be a ring. An abelian group M is said to be an R-module if R acts linearly on it, that is, A triple $(M, R, \cdot)$ is an R-module if a function $\cdot : R \times M \to M$ satisfies the usual axioms of scalar. We often write $\cdot(a, x)$ by ax and $(M, R, \cdot)$ by M for short.

Theorem 3 *The following assertions are pairwise equivalent over* RCA_0.

(1) ACA_0

(2) *Any R-submodules M_1 and M_2 of an R-module M has the sum $M_1 + M_2$ in M.*

(3) *Any sequense $\langle M_i : i \in \mathbb{N} \rangle$ of submodules of an R-module M has the sum $\sum_{i \in \mathbb{N}} M_i$ in M.*

For R-module M, the annihilator of M is the set of all elements r in R such that for each m in M, $rm = 0$.

Theorem 4 *The assertion that any R-module has the annihilator, is equivalent to* ACA_0 *over* RCA_0*.*

Theorem 5 *The following assertions are pairwise equivalent over* RCA_0*.*

(1) ACA_0

(2) *Any ideals I and J of a countable ring has the ideal quotient exists.*

(3) *Any ideal I of a countable ring has the annihilator.*

A R-module M is a *semi-simple* if M is a direct sum of irreducible modules.

Theorem 6 *The following assertions are pairwise equivalent over* RCA_0.

(1) ACA_0

(2) *Any submodule of a semi-simple* R*-modele is a direct summand.*

A R-module is said to be *projective* if any epimorphism of R-modules, say $g : A \to B$, and any R-homomorphism $f : M \to B$, there exists an R-homomorphism $f' : M \to A$ such that $f = g \circ f'$.

Any free module is projective.

Theorem 7 (RCA_0) *A R-module M is projective if and only if it is a direct summand of a free module.*

A R-module is said to be *injective* if any monomorphism of R-modules, say $g : A \longrightarrow B$, and any R-homomorphism $f : A \longrightarrow M$, there exists an R-homomorphism $f' : B \longrightarrow M$ such that $f = f' \circ g$.

Theorem 8 *The following assertions are pairwise equivalent over* RCA_0.

(1) ACA_0

(2) *Baer's test: if an R-module M is injective, then for any ideal I of R and any R-homomorphism $f : I \longrightarrow M$ can be extended to $f' : R \longrightarrow M$.*

Then an R-module T is a *tensor product of M and N* if there exists a R-bilinear function $F : M \times N \to T$ such that for any R-module P and R-bilinear function $G : M \times N \to P$, there exists a unique R-linear function $H : T \to P$ satisfying $G = H \circ F$. We write the tensor product of M and N by $M \otimes_R N$.

Theorem 9 *The following assertions are pairwise equivalent over* RCA_0.

(1) ACA_0

(2) *For any two R-modules M and N, $M \otimes_R N$ exists.*

(3) *For any R-module M, $M \otimes_R M$ exists.*

Proof of (3) $\Rightarrow$ (1) Let $f : \mathbb{N} \to \mathbb{N}$ be a one-to-one function. Then for each $n \in \mathbb{N}$, define an abelian group X_{n+1} by $X_0 = \mathbb{Z}/2\mathbb{Z}$ and

$$X_{n+1} = \begin{cases} \mathbb{Z}/(2m+1)\mathbb{Z} & \text{if } f(m) = n \\ \mathbb{Z} & \text{if } n \notin \mathrm{Im}(f) \end{cases}$$

Let $M = \oplus X_n$. Now we denote a generator for X_n by x_n. Then, for each $x_0 \otimes x_{n+1} \in M \otimes_{\mathbb{Z}} M$,

$$x_0 \otimes x_{n+1} = 0 \text{ iff } n \text{ is in the image of } f.$$

$\square$

Basic properties on tensor product can be shown within RCA_0 if its tensor product exists.

References

[1] H. M. Friedman, S. G. Simpson, R. L. Smith, Countable algebra and set existence axioms, Ann. Pure Appl. Logic 25 (1983), 141–181.

[2] H. M. Friedman, S. G. Simpson, R. L. Smith, Addendum to: " Countable algebra and set existence axioms, " Ann. Pure Appl. Logic 28 (1985), 319–320.

[3] Stephen G. Simpson, *Subsystems of Second Order Arithmetic*, Springer-Verlag, 1999.

[4] Dodney G. Downey, Steffen Lempp and Joseph R. Mileti, Ideals In Computable Rings, J. Algebra 314 (2007), 872–887.