Commutativity theorems for rings in constructive algebra

Ryota Kuroki

University of Tokyo

第 2 回 若手による数理論理学研究集会
August 9, 2024

What is constructive algebra?

Constructive algebra is algebra without nonconstructive principles (excluded middle, Zorn's lemma, ...).

We can extract computational content from a constructive proof. One way of doing this is to use type theories with canonicity (e.g. Martin-Löf type theory (using setoids), cubical type theory, ...).

A simple commutativity theorem

Throughout, all rings are associative with 1.

Theorem 1 (Every Boolean ring is commutative)

$(\forall x \in A.\, x^2 = x) \implies (\forall x, y \in A.\, [x, y] = 0) \quad ([x, y] := xy - yx).$

Proof.

$0 = 2^2 - 2 = 2$. $0 = (x + y)^2 - (x + y) =$
$(x^2 + xy + yx + y^2) - (x + y) = xy + yx = [x, y].$ □

$\mathbb{Z}\langle X, Y\rangle / \langle f^2 - f : f \in \mathbb{Z}\langle X, Y\rangle\rangle$ is commutative by theorem 1. So $[X, Y] =_{\mathbb{Z}\langle X,Y\rangle} \sum_i g_i(f_i^2 - f_i)h_i$ for some $f_i, g_i, h_i \in \mathbb{Z}\langle X, Y\rangle$. Computational content of a proof should give an algorithm to compute f_i, g_i, h_i. From the constructive proof above, we have

$$
\begin{aligned}
&[X, Y] \\
&= (XY + YX) - (2^2 - 2)YX \\
&= ((X + Y)^2 - (X + Y)) - (X^2 - X) - (Y^2 - Y) - (2^2 - 2)YX.
\end{aligned}
$$

More commutativity theorems

Theorem 2 ([Jacobson 1945])

$$(\forall x \in A.\ \exists n \geq 2.\ x^n = x) \implies (\forall x, y \in A.\ [x, y] = 0).$$

Theorem 3 ([Herstein 1957])

$$(\forall x, y \in A.\ \exists n \geq 2.\ [x, y]^n = [x, y]) \implies (\forall x, y \in A.\ [x, y] = 0).$$

We deal with the following theorem:

Theorem 4

$$(\forall x \in A.\ x^3 = x) \implies (\forall x, y \in A.\ [x, y] = 0).$$

See [Buckley and MacHale 2013] for elementary proofs of theorem 4. Rings are not assumed to be unital in the paper, but it does not make much difference ([Brandenburg 2023, Proposition 2.14]).

A subdirect representation theorem (nonconstructive)

Lemma 5 ([Andrunakievič and Rjabuhin 1968], [Klein 1980])

For every ideal $I \subseteq A$, $\mathrm{Nil}\, I = \bigcap_{\mathfrak{p} \supseteq I:\ \text{completely prime}} \mathfrak{p}$.
(For $U \subseteq A$, $\mathrm{Nil}\, U$ is the ideal of A generated by the following constructors ($(-) \in \mathrm{Nil}\, U$ is an inductive family):

$$
\begin{aligned}
\textbf{intro}_x &: & x \in U &\implies x \in \mathrm{Nil}\, U,\\
\textbf{zero} &: & & 0 \in \mathrm{Nil}\, U,\\
\textbf{add}_{x,y} &: & x, y \in \mathrm{Nil}\, U &\implies x + y \in \mathrm{Nil}\, U,\\
\textbf{mult}_{z,x,w} &: & x \in \mathrm{Nil}\, U &\implies zxw \in \mathrm{Nil}\, U,\\
\textbf{red}_x &: & x^2 \in \mathrm{Nil}\, U &\implies x \in \mathrm{Nil}\, U.
\end{aligned}
$$

$\mathrm{Nil}\, U$ is the smallest reduced ideal containing U.)

Every reduced ring A is a subdirect product of domains A_i by lemma 5 (i.e. we have an injective homomorphism $A \to \prod_i A_i$ such that $A \to A_i$ are surjective).

A nonconstructive proof of theorem 4

Assume that $\forall x \in A.\ x^3 = x$.

- If $x^2 = 0$, then $x = x^3 = 0$

So A is reduced. By lemma 5, A is a subdirect product of domains A_i.

- In each A_i, we have $\forall x \in A.\ \overline{x}^3 =_{A_i} \overline{x}$. So $\overline{x} \in \{0, \pm 1\}$. So $\overline{[x, y]} =_{A_i} 0$ for all $x, y \in A$

So $[x, y] =_A 0$

Can we extract $f_i, g_i, h_i \in \mathbb{Z}\langle X, Y \rangle$ such that $[X, Y] =_{\mathbb{Z}\langle X,Y \rangle} \sum_i g_i(f_i^3 - f_i)h_i$ from this proof?

How to constructivize?

1. Generate an entailment relation $\vdash$ by the axioms of a completely prime ideal.
2. Prove $U \vdash a \iff a \in \operatorname{Nil} U$ (this is our main theorem). In classical mathematics, this implies lemma 5 by the completeness theorem for entailment relations (theorem 9).
3. Use $U \vdash a \iff a \in \operatorname{Nil} U$ instead of lemma 5 to prove theorem 4.

Entailment relations

Definition 6

A binary relation $\vdash$ on the set of finite subsets of S is called an entailment relation on S if $\vdash$ satisfies the following conditions:

(id) $a \vdash a$.

(wkn) $(U \subseteq U',\ V \subseteq V',\ U \vdash V) \implies U' \vdash V'$.

(cut) $(U \vdash V, a,\ U, a \vdash V) \implies U \vdash V$.

Entailment relations are closely related to distributive lattices ([Cederquist and Coquand 2000], [Lombardi 2020]).

Completeness theorems (nonconstructive)

Definition 7

$\nu : S \to 2$ is called a model of $\vdash$ if ν satisfies the following condition: $U \vdash V \implies ((\forall u \in U.\ \nu u = 1) \to (\exists v \in V.\ \nu v = 1))$.

Theorem 8 ([Scott 1974, Proposition 1.3])

The following are equivalent:

1. $U \vdash V$.
2. *For all models* ν *of* $\vdash$, $(\forall u \in U.\ \nu u = 1) \to (\exists v \in V.\ \nu v = 1)$.

Theorem 9 ([Scott 1974, Proposition 1.4])

For all (not necessarily finite) subsets $X, Y \subseteq S$, *the following are equivalent:*

1. *There exist finite subsets* $U \subseteq X$, $V \subseteq Y$ *such that* $U \vdash V$. *Let* $X \vdash_e Y$ *denote this statement.*
2. *For all models* ν *of* $\vdash$, $(\forall x \in X.\ \nu x = 1) \to (\exists y \in Y.\ \nu y = 1)$.

Theory of complete prime ideals

We generate an entailment relation on a ring A by the following constructors (axioms):

$$\begin{aligned} &\vdash 0, \\ a, b &\vdash a + b, \\ a &\vdash xay, \\ ab &\vdash a, b, \\ 1 &\vdash . \end{aligned}$$

The models of $\vdash$ correspond to completely prime ideals of A (nonconstructive). So $X \vdash_e a \iff a \in \bigcap_{\mathfrak{p} \supseteq X:\ \text{completely prime}} \mathfrak{p}$ by the completeness theorem.
We prove $U \vdash a \implies a \in \operatorname{Nil} U$ constructively (the converse is trivial).

A useful lemma

Lemma 10 ([Wessel 2018, Lemma 4.34])

Let $\vdash$ be an entailment relation on S generated by constructors (axioms) of the form $U \vdash V$. Let Φ be a predicate on $\mathrm{Pow}_{\mathrm{fin}}(S)$ satisfying the following conditions:

- $U \subseteq U' \implies \Phi(U) \to \Phi(U')$.
- *For all constructors of the form $U \vdash V$, the following holds:* $[\forall U'.\ (\forall v \in V.\ \Phi(U', v)) \implies \Phi(U', U)]$ *($\Phi(U', v)$ means $\Phi(U' \cup \{v\})$).*

Then $U \vdash V$ implies $[\forall U'.\ (\forall v \in V.\ \Phi(U', v)) \implies \Phi(U', U)]$.

Let $\Phi_x(U) := x \in \mathrm{Nil}\, U$. The non-trivial part is the proof of $\forall U'.\ (\Phi_x(U', a),\ \Phi_x(U', b)) \implies \Phi_x(U', ab)$ (corresponding to the axiom $ab \vdash a, b$).
We have to prove $\mathrm{Nil}(U, a) \cap \mathrm{Nil}(U, b) \subseteq \mathrm{Nil}(U, ab)$.

A key lemma

Lemma 11 (key lemma)

Let U be a (not necessarily finite) subset of a ring A and $a, b, x, y \in A$. Then $x \in \mathrm{Nil}(U, a),\ y \in \mathrm{Nil}(U, b) \implies xy \in \mathrm{Nil}(U, ab)$. In particular, $\mathrm{Nil}(U, a) \cap \mathrm{Nil}(U, b) \subseteq \mathrm{Nil}(U, ab)$.

We need the following lemma:

Lemma 12 ([Krempa 1996, Lemma 1.2])

If I is a reduced ideal of A and $\sigma \in S_n$, then $x_1 \cdots x_n \in I \implies x_{\sigma(1)} \cdots x_{\sigma(n)} \in I$.

Proof.

$xzyw \in I \impliedby (xzyw)^3 \in I \impliedby yw(xzyw)x \in I \impliedby (ywxzywx)^2 \in I \impliedby zywxy \in I \impliedby (zywxy)^2 \in I \impliedby wxyz \in I \impliedby (wxyz)^2 \in I \impliedby xyzw \in I$. □

A proof of the key lemma

We prove $\forall x, y.\ (x \in \mathrm{Nil}(U, a),\ y \in \mathrm{Nil}(U, b) \implies xy \in \mathrm{Nil}(U, ab))$. The proof is by induction on the witnesses p, q of $x \in \mathrm{Nil}(U, a)$, $y \in \mathrm{Nil}(U, b)$.

1. If p and q are of the form $\textbf{intro}_x(-)$ and $\textbf{intro}_y(-)$ respectively, then $x \in U \cup \{a\}$ and $y \in U \cup \{b\}$. So $xy \in \mathrm{Nil}(U, ab)$.
2. If p is **zero**, then $xy = 0 \in \mathrm{Nil}(U, ab)$.
3. If p is of the form $\textbf{add}_{x_1,x_2}(-,-)$, then we have $x = x_1 + x_2$ and $x_1 y, x_2 y \in \mathrm{Nil}(U, ab)$ by the inductive hypothesis. So $xy = x_1 y + x_2 y \in \mathrm{Nil}(U, ab)$.
4. If p is of the form $\textbf{mult}_{z,x',w}(-)$, then we have $x = zx'w$ and $x'y \in \mathrm{Nil}(U, ab)$ by the inductive hypothesis. So $xy = zx'wy$ is in $\mathrm{Nil}(U, ab)$ by lemma 12.
5. If p is of the form $\textbf{red}_x(-)$, then we have $x^2 y \in \mathrm{Nil}(U, ab)$ by the inductive hypothesis. So $(xy)^2$ and xy are in $\mathrm{Nil}(U, ab)$ by lemma 12.

the remaining cases can be dealt similarly.

Proofs are programs

$$F : \forall\ x\ y \to ((x \in \mathrm{Nil}(U,a)) \times (y \in \mathrm{Nil}(U,b))) \to xy \in \mathrm{Nil}(U,ab)$$

$$\begin{aligned}
F_{x,y}(\textbf{intro}_x(u), \textbf{intro}_y(v)) &:= \cdots \\
F_{0,y}(\textbf{zero}, q) &:= \textbf{zero} \\
F_{x_1+x_2,y}(\textbf{add}_{x_1,x_2}(u,v), q) &:= \textbf{add}_{x_1 y, x_2 y}(F_{x_1,y}(u,q), F_{x_2,y}(v,q)) \\
F_{zx'w,y}(\textbf{mult}_{z,x',w}(u), q) &:= \textbf{mult}_{z,x'wy,1}(\textbf{red}_{x'wy}(\textbf{mult}_{x'w,yx',wy}(\textbf{red}_{yx'}(\\
&\qquad \textbf{mult}_{y,x'y,x'}(F_{x',y}(u,q)))))) \\
F_{x,y}(\textbf{red}_x(u), q) &:= \textbf{red}_{xy}(\textbf{mult}_{1,xyx,y}(\textbf{red}_{xyx}(\textbf{mult}_{xy,xxy,x}(\\
&\qquad F_{x^2,y}(u,q))))) \\
&\vdots
\end{aligned}$$

Strictly speaking, we have to insert transports because associativity, distributivity, etc., are not judgmental.
We used the induction principle for the inductive family $(-) \in \mathrm{Nil}\,U$.

An alternative proof (essentially the same)

Generate a single-conclusion entailment relation on A by the following constructors:

$$\begin{aligned} &\rhd 0, \\ a, b &\rhd a + b, \\ a &\rhd xay, \\ a^2 &\rhd a. \end{aligned}$$

$U \rhd a \iff a \in \mathrm{Nil}_A U$ holds. By Universal Krull ([Rinaldi, Schuster, and Wessel 2018, Corollary 3]), the key lemma (lemma 11) implies that $\vdash$ is a conservative extension of $\rhd$ (i.e. $U \vdash a \iff U \rhd a$).

A constructive proof of theorem 4

We prove $(\forall x \in A.\ x^3 = x) \implies (\forall x, y \in A.\ [x, y] = 0)$.

Since A is reduced, $\mathrm{Nil}_A\, 0 = 0$.

A proof using $\vdash$.

We have $\vdash x^3 - x$. So $\vdash (x+1), x, (x-1)$. We have $x + 1 \vdash [x, y]$, $x \vdash [x, y]$, and $x - 1 \vdash [x, y]$. So $\vdash [x, y]$. So $[x, y] \in \mathrm{Nil}\, 0 = 0$. □

A proof using the key lemma.

$[x, y] \in \mathrm{Nil}(x + 1) \cap \mathrm{Nil}(x) \cap \mathrm{Nil}(x - 1) \subseteq \mathrm{Nil}\, 0 = 0$. □

Related work

- In the commutative case, $U \vdash a \iff a \in \mathrm{Nil}\, U$ is known as formal Nullstellensatz ([Johnstone 1982, Lemma V-3.2]).
- See [Brandenburg 2023] for an equational proof of some special cases of theorem 2.
- See [Coquand 1997, Section 5.7] for another constructive approach to theorem 4 using topological models.

References I

Andrunakievič, V. A. and Ju. M. Rjabuhin (1968). "Rings without nilpotent elements, and completely prime ideals". In: Dokl. Akad. Nauk SSSR 180, pp. 9–11. ISSN: 0002-3264. URL: https://www.mathnet.ru/php/archive.phtml?wshow=paper&jrnid=dan&paperid=33815&option_lang=eng.

Brandenburg, Martin (2023). Equational proofs of Jacobson's Theorem. arXiv: 2310.05301 [math.RA].

Buckley, Stephen M. and Desmond MacHale (2013). "Variations on a theme: rings satisfying $x^3 = x$ are commutative". In: Amer. Math. Monthly 120.5, pp. 430–440. ISSN: 0002-9890,1930-0972. DOI: 10.4169/amer.math.monthly.120.05.430.

Cederquist, Jan and Thierry Coquand (2000). "Entailment relations and distributive lattices". In: Logic Colloquium '98 (Prague). Vol. 13. Lect. Notes Log. Assoc. Symbol. Logic, Urbana, IL, pp. 127–139. ISBN: 1-56881-113-6. DOI: 10.1017/9781316756140.011.

Coquand, Thierry (1997). "Computational content of classical logic". In: Semantics and logics of computation (Cambridge, 1995). Vol. 14. Publ. Newton Inst. Cambridge Univ. Press, Cambridge, pp. 33–78. ISBN: 0-521-58057-9. DOI: 10.1017/CBO9780511526619.003.

Herstein, I. N. (1957). "A condition for the commutativity of rings". In: Canadian J. Math. 9, pp. 583–586. ISSN: 0008-414X,1496-4279. DOI: 10.4153/CJM-1957-066-0.

Jacobson, Nathan (1945). "Structure theory for algebraic algebras of bounded degree". In: Ann. of Math. (2) 46, pp. 695–707. ISSN: 0003-486X. DOI: 10.2307/1969205.

References II

Johnstone, P. T. (1982). Stone spaces. Vol. 3. Cambridge Studies in Advanced Mathematics. Cambridge University Press, Cambridge, pp. xxi+370. ISBN: 0-521-23893-5.

Klein, Abraham A. (1980). "A simple proof of a theorem on reduced rings". In: Canadian Mathematical Bulletin. Bulletin Canadien de Mathématiques 23.4, pp. 495–496. ISSN: 0008-4395,1496-4287. DOI: 10.4153/CMB-1980-075-7.

Krempa, Jan (1996). "Some examples of reduced rings". In: Algebra Colloq. 3.4, pp. 289–300. ISSN: 1005-3867.

Lombardi, Henri (2020). "Spectral spaces versus distributive lattices: a dictionary". In: Advances in rings, modules and factorizations. Vol. 321. Springer Proc. Math. Stat. Springer, Cham, pp. 223–245. ISBN: 978-3-030-43416-8. DOI: 10.1007/978-3-030-43416-8_13.

Rinaldi, Davide, Peter Schuster, and Daniel Wessel (2018). "Eliminating disjunctions by disjunction elimination". In: Indag. Math. (N.S.) 29.1, pp. 226–259. ISSN: 0019-3577,1872-6100. DOI: 10.1016/j.indag.2017.09.011.

Scott, Dana (1974). "Completeness and axiomatizability in many-valued logic". In: Proceedings of the Tarski Symposium (Proc. Sympos. Pure Math., Vol. XXV, Univ. Calif
Vol. XXV. Proc. Sympos. Pure Math. Published for the Association for Symbolic Logic by the American Mathematical Society, Providence, RI, pp. 411–435.

Wessel, Daniel (2018). "Choice, extension, conservation. From transfinite to finite proof methods in abstract algebra". PhD thesis. University of Trento, University of Verona. URL: http://eprints-phd.biblio.unitn.it/2759/.