Entailment relations for the constructive theory of free modules

Ryota Kuroki

Graduate School of Mathematical Sciences, The University of Tokyo

1 Introduction

Constructive algebra is the study of algebra without using non-constructive principles, such as Zorn's lemma or the law of excluded middle. See [MRR88, LQ15, Yen15, CL24] for recent developments in constructive algebra. It is closely related to computer algebra since constructive proofs have computational content, which can be extracted using proof assistants, such as Agda, Rocq, and Lean.

In classical mathematics, a free module $A^{\oplus S}$ admits an embedding into the direct product A^S, which yields a characterization of the equality of $A^{\oplus S}$. For example, $e_s =_{A^{\oplus S}} e_t$ is equivalent to $(s =_S t) \vee (1 =_A 0)$, where e denotes the standard basis of $A^{\oplus S}$. In constructive mathematics, such an embedding is not available in general, yet the same characterization still holds. (See the constructive proofs collected in [Lum18].) We provide a simple method for obtaining a constructive proof from the classical one. Our approach is based on entailment relations [Lor51, Sco71, Sco74][1], and would essentially be the special case of Barr's theorem [Wra80, Rat16].

2 The equality of elements of a free module

Let A be a ring. The free module $A^{\oplus S}$ generated by a set S can be constructed as follows:

Let A_S be the set generated by the following constructors:

$$\frac{s \in S}{e_s \in A_S}\,, \quad \frac{}{0 \in A_S}\,, \quad \frac{x, y \in A_S}{x + y \in A_S}\,, \quad \frac{a \in A,\ x \in A_S}{ax \in A_S}\,.$$

The free module $A^{\oplus S}$ is the quotient set $A_S/{\sim}$ with the canonical module structure, where $\sim$ is the binary relation on A_S generated by the following constructors:

$$\frac{}{x \sim x}\,, \quad \frac{x \sim y \qquad y \sim z}{x \sim z}\,, \quad \frac{x \sim y}{y \sim x}\,, \quad \frac{x \sim y \qquad z \sim w}{x + z \sim y + w}\,, \quad \frac{x \sim y}{ax \sim ay}\,,$$

$$\frac{}{0 + x \sim x}\,, \quad \frac{}{(x + y) + z \sim x + (y + z)}\,, \quad \frac{}{x + y \sim y + x}\,,$$

$$\frac{}{a0 \sim 0}\,, \quad \frac{}{a(x + y) \sim ax + ay}\,,$$

$$\frac{}{0_A x \sim 0}\,, \quad \frac{}{(a + b)x \sim ax + bx}\,, \quad \frac{}{1_A x \sim x}\,, \quad \frac{}{(ab)x \sim a(bx)}\,.$$

[1] Neuwirth [Lor25] has recently translated [Lor51] into English.

The equality of $A^{\oplus S}$ has a simple characterization. First, define $L : A_S \to \mathsf{List}(A \times S)$ as follows:

$$
\begin{aligned}
L(e_s) &:= [(1, s)], \\
L(0) &:= [], \\
L(x + y) &:= [\pi_0, \dots, \pi_{m-1}, \pi'_0, \dots, \pi'_{n-1}] \quad ([\pi_0, \dots, \pi_{m-1}] = L(x),\ [\pi'_0, \dots, \pi'_{n-1}] = L(y)), \\
L(ax) &:= [(aa_0, s_0), \dots, (aa_{n-1}, s_{n-1})] \quad ([(a_0, s_0), \dots, (a_{n-1}, s_{n-1})] = L(x)).
\end{aligned}
$$

We note that if $L(x) = [(a_0, s_0), \dots, (a_{n-1}, s_{n-1})]$, then $x =_{A^{\oplus S}} \sum_{k=0}^{n-1} a_k e_{s_k}$ holds. Using the function L, we can state the characterization of the equality as follows:

Theorem 2.1. *Let $x, y \in A_S$, $L(x) = [(a_0, s_0), \dots, (a_{m-1}, s_{m-1})]$, and $L(y) = [(b_0, t_0), \dots, (b_{n-1}, t_{n-1})]$. Then $x =_{A^{\oplus S}} y$ if and only if there exist a partition $(A_0, \dots, A_{p-1})$ of $\{0, \dots, m-1\}$ and a partition $(B_0, \dots, B_{p-1})$ of $\{0, \dots, n-1\}$ such that*

- *$\forall j \in \{0, \dots, p-1\}.\ \forall k \in A_j.\ \forall l \in B_j.\ s_k = t_l$, and*
- *$\sum_{k \in A_j} a_k = \sum_{l \in B_j} b_l$ for all j.*

This theorem is constructively provable by induction on the derivation of $x =_{A^{\oplus S}} y$ (i.e., $x \sim y$). See [Lum18] for other constructive proofs. However, in classical mathematics, the most common proof would be the following one, which uses the universal property of the free module:

Classical proof of Theorem 2.1. By the law of excluded middle, we can define $f : S \to A^S$ by

$$
f(s)(t) := \begin{cases} 1 & \text{if } s = t, \\ 0 & \text{if } s \neq t. \end{cases}
$$

This map induces a homomorphism $\tilde{f} : A^{\oplus S} \to A^S$. The assertion follows from the equality $\tilde{f}(\sum_{k=0}^{m-1} a_k e_{s_k}) = \tilde{f}(\sum_{k=0}^{n-1} b_k e_{t_k})$ and the law of excluded middle. □

This paper aims to translate this classical proof into a constructive one by using entailment relations. For simplicity, let us consider the following special case:

Theorem 2.2. *If $e_s =_{A^{\oplus S}} e_t$, then $s =_S t$ or $1 =_A 0$.*

Classical proof. By the law of excluded middle, we can define $f : S \to A^S$ by

$$
f(s)(t) := \begin{cases} 1 & \text{if } s = t, \\ 0 & \text{if } s \neq t. \end{cases}
$$

This map induces a homomorphism $\tilde{f} : A^{\oplus S} \to A^S$. Then we have $f(s)(t) = \tilde{f}(e_s)(t) = \tilde{f}(e_t)(t) = f(t)(t) = 1$.

- If $s = t$, we have $s = t$.
- If $s \neq t$, we have $0 = f(s)(t) = 1$.

By the law of excluded middle, we have $s = t$ or $1 = 0$. □

3 Entailment relations

Let $\mathcal{P}_{\text{fin}} P$ denote the set of finitely indexed subsets of P.

Definition 3.1 ([Lor51, Sco71, Sco74])**.** A binary relation $\vdash \subseteq (\mathcal{P}_{\text{fin}} P) \times (\mathcal{P}_{\text{fin}} P)$ is called an entailment relation on P if $\vdash$ satisfies the following conditions:

$$\frac{}{\varphi \vdash \varphi}\,, \quad \frac{U \vdash V}{U, U' \vdash V, V'}\,, \quad \frac{U, \varphi \vdash V \qquad U' \vdash \varphi, V'}{U, U' \vdash V, V'}\,.$$

The application of entailment relations to constructive algebra dates back to [CC00, CP01]. (The application of distributive lattices dates back to [Joy75].) We generate an entailment relation $\vdash_S$ on $\{\mathrm{Eq}_S(s,t) : s, t \in S\} (\cong S \times S)$ by the following axioms:

$$\vdash \mathrm{Eq}_S(s,s), \quad \mathrm{Eq}_S(s,t), \mathrm{Eq}_S(t,u) \vdash \mathrm{Eq}_S(s,u), \quad \mathrm{Eq}_S(s,t) \vdash \mathrm{Eq}_S(t,s).$$

The following statements can be proved by induction:

Proposition 3.2. *The following hold:*

- $U \vdash_S \varphi_0, \ldots, \varphi_{n-1}$ *if and only if there exists k such that* $U \vdash_S \varphi_k$.
- $U \vdash_S \mathrm{Eq}_S(s,t)$ *if and only if* $s \sim_U t$, *where* $\sim_U$ *is the equivalence relation on S generated by U.*

Corollary 3.3. $\vdash_S \mathrm{Eq}_S(s,t)$ *if and only if* $s = t$.

We define an entailment relation $\vdash_A$ on A similarly. We generate an entailment relation $\vdash_{S,A}$ on $\{\mathrm{Eq}_S(s,t) : s, t \in S\} \coprod \{\mathrm{Eq}_A(a,b) : a, b \in A\}$ by the following axioms:

$$\begin{array}{lll} \vdash \mathrm{Eq}_S(s,s), & \mathrm{Eq}_S(s,t), \mathrm{Eq}_S(t,u) \vdash \mathrm{Eq}_S(s,u), & \mathrm{Eq}_S(s,t) \vdash \mathrm{Eq}_S(t,s), \\ \vdash \mathrm{Eq}_A(a,a), & \mathrm{Eq}_A(a,b), \mathrm{Eq}_A(b,c) \vdash \mathrm{Eq}_A(a,c), & \mathrm{Eq}_A(a,b) \vdash \mathrm{Eq}_A(b,a). \end{array}$$

The following statements can be proved by induction:

Proposition 3.4. *Let* $U_S, V_S \in \mathcal{P}_{\text{fin}}\{\mathrm{Eq}_S(s,t) : s, t \in S\}$ *and* $U_A, V_A \in \mathcal{P}_{\text{fin}}\{\mathrm{Eq}_A(a,b) : a, b \in A\}$. *Then* $U_S, U_A \vdash_{S,A} V_S, V_A$ *if and only if* $U_S \vdash_S V_S$ *or* $U_A \vdash_A V_A$.

Corollary 3.5. $\vdash_{S,A} \mathrm{Eq}_S(s,t), \mathrm{Eq}_A(1,0)$ *if and only if* $s =_S t$ *or* $1 =_A 0$.

4 Conservative extension

We will extend $\vdash_{S,A}$ conservatively so that we can simulate the classical proof of Theorem 2.2.

4.1 Negation and excluded middle

Theorem 4.1 ([Lor51, CC00])**.** *We can conservatively adjoin* $\{\neg\varphi : \varphi \in P\}$ *with the following axioms to an entailment relation*

$$\varphi, \neg\varphi \vdash\,, \qquad \vdash \varphi, \neg\varphi.$$

Proof sketch. Let $\vdash_\neg$ denote the extended entailment relation. By induction, $U_0, \neg U_1 \vdash_\neg V_0, \neg V_1$ implies $U_0, V_1 \vdash V_0, U_1$, where $U_0, U_1, V_0, V_1 \in \mathcal{P}_{\text{fin}} P$ and $\neg U := \{\neg\varphi : \varphi \in U\}$. $\square$

4.2 Operations of distributive lattices

Theorem 4.2 ([Lor51, CC00])**.** *We can conservatively adjoin connectives* $\top, \wedge, \bot, \vee$ *with the following axioms:*

$$\vdash \top, \quad \varphi, \psi \vdash \varphi \wedge \psi, \quad \varphi \wedge \psi \vdash \varphi, \quad \varphi \wedge \psi \vdash \psi,$$
$$\bot \vdash, \quad \varphi \vdash \varphi \vee \psi, \quad \psi \vdash \varphi \vee \psi, \quad \varphi \vee \psi \vdash \varphi, \psi.$$

Informal proof sketch. Let $U \vdash_{\mathsf{DLat}} V$ denote the extended entailment relation and define $[\![U; V]\!]$ as follows:

$$\begin{aligned}
[\![U; V]\!] &:= U \vdash V \quad (U, V\colon\ (\top, \wedge, \bot, \vee)\text{-free}), \\
[\![U, \top; V]\!] &:= [\![U; V]\!], & [\![U; V, \top]\!] &:= \text{true}, \\
[\![U, \varphi \wedge \psi; V]\!] &:= [\![U, \varphi, \psi; V]\!], & [\![U; V, \varphi \wedge \psi]\!] &:= [\![U; V, \varphi]\!] \text{ and } [\![U; V, \psi]\!], \\
[\![U, \bot; V]\!] &:= \text{true}, & [\![U; V, \bot]\!] &:= [\![U; V]\!], \\
[\![U, \varphi \vee \psi; V]\!] &:= [\![U, \varphi; V]\!] \text{ and } [\![U, \psi; V]\!], & [\![U; V, \varphi \vee \psi]\!] &:= [\![U; V, \varphi, \psi]\!],
\end{aligned}$$

Note that the proposition $[\![U; V]\!]$ does not depend (up to equivalence) on the order of computation. By induction, $U \vdash_{\mathsf{DLat}} V$ implies $[\![U; V]\!]$. □

4.3 The functions $f, \tilde{f}$

Proposition 4.3. *We can conservatively adjoin elements of the form* $f(s, t)$ $(s, t \in S)$ *(of type* A*) and function symbols* $+' : A^2 \to A$, $\cdot' : A^2 \to A$ *to* $\vdash_{S,A,\neg}$ *with the following axioms:*

$$\begin{gathered}
\mathrm{Eq}_S(s,t) \vdash \mathrm{Eq}_A(f(s,t), 1), \quad \neg\,\mathrm{Eq}_S(s,t) \vdash \mathrm{Eq}_A(f(s,t), 0), \\
\vdash \mathrm{Eq}_A(\alpha, \alpha), \quad \mathrm{Eq}_A(\alpha, \beta), \mathrm{Eq}_A(\beta, \gamma) \vdash \mathrm{Eq}_A(\alpha, \gamma), \quad \mathrm{Eq}_A(\alpha, \beta) \vdash \mathrm{Eq}_A(\beta, \alpha), \\
\mathrm{Eq}_A(\alpha, \beta), \mathrm{Eq}_A(\gamma, \delta) \vdash \mathrm{Eq}_A(\alpha +' \beta, \gamma +' \delta), \quad \mathrm{Eq}_A(\alpha, \beta), \mathrm{Eq}_A(\gamma, \delta) \vdash \mathrm{Eq}_A(\alpha \cdot' \beta, \gamma \cdot' \delta), \\
\vdash \mathrm{Eq}_A(0 +' \alpha, \alpha), \quad \vdash \mathrm{Eq}_A((\alpha +' \beta) +' \gamma, \alpha +' (\beta +' \gamma)), \quad \vdash \mathrm{Eq}_A(\alpha +' \beta, \beta +' \alpha), \\
\vdash \mathrm{Eq}_A(1 \cdot' \alpha, \alpha), \quad \vdash \mathrm{Eq}_A((\alpha \cdot' \beta) \cdot' \gamma, \alpha \cdot' (\beta \cdot' \gamma)), \quad \vdash \mathrm{Eq}_A(\alpha \cdot' \beta, \beta \cdot' \alpha) \\
(\alpha, \beta, \gamma \textit{ may contain } f, +', \cdot'), \\
\vdash \mathrm{Eq}_A(a +' b, a + b), \quad \vdash \mathrm{Eq}_A(a \cdot' b, ab) \quad (a, b \in A).
\end{gathered}$$

Proof sketch. Let

$$\begin{aligned}
&[\![\varphi(f(s_0, t_0), \ldots, f(s_{n-1}, t_{n-1}))]\!] \\
&:= \bigvee_{i_0, \ldots, i_{n-1} \in \{0,1\}} (\neg^{i_0} \mathrm{Eq}_S(s_0, t_0) \wedge \cdots \wedge \neg^{i_{n-1}} \mathrm{Eq}_S(s_{n-1}, t_{n-1}) \wedge \varphi(1 - i_0, \ldots, 1 - i_{n-1})),
\end{aligned}$$

where $+', \cdot'$ are replaced with $+, \cdot$ on the right hand side. By induction, $U \vdash_{S,A,\neg,f,+',\cdot'} V$ implies $[\![U]\!] \vdash_{S,A,\neg,\mathsf{DLat}} [\![V]\!]$, where $[\![U]\!] := \{[\![\varphi]\!] : \varphi \in U\}$. □

Proposition 4.4. *We can conservatively adjoin elements of the form* $\tilde{f}(x, t)$ $(x \in A_S,\ t \in S)$ *(of type* A*) and function symbols* $+'' : A^2 \to A$, $\cdot'' : A^2 \to A$ *to* $\vdash_{S,A,\neg,f,+',\cdot'}$ *with the following* *axioms:*

$$
\begin{gathered}
\vdash \mathrm{Eq}_A(\tilde{f}(e_s,t), f(s,t)), \quad \vdash \mathrm{Eq}_A(\tilde{f}(0,t), 0_A), \\
\vdash \mathrm{Eq}_A(\tilde{f}(x+y,t), \tilde{f}(x,t) +'' \tilde{f}(x,t)), \quad \vdash \mathrm{Eq}_A(\tilde{f}(ax,t), a \cdot'' \tilde{f}(x,t)), \\
\vdash \mathrm{Eq}_A(0 +'' \alpha, \alpha), \quad \vdash \mathrm{Eq}_A((\alpha +'' \beta) +'' \gamma, \alpha +'' (\beta +'' \gamma)), \quad \vdash \mathrm{Eq}_A(\alpha +'' \beta, \beta +'' \alpha), \\
\vdash \mathrm{Eq}_A(1 \cdot'' \alpha, \alpha), \quad \vdash \mathrm{Eq}_A((\alpha \cdot'' \beta) \cdot'' \gamma, \alpha \cdot'' (\beta \cdot'' \gamma)), \quad \vdash \mathrm{Eq}_A(\alpha \cdot'' \beta, \beta \cdot'' \alpha) \\
(\alpha, \beta, \gamma \textit{ may contain } f, +', \cdot', \tilde{f}, +'', \cdot''), \\
\vdash \mathrm{Eq}_A(a +'' b, a +' b), \quad \vdash \mathrm{Eq}_A(a \cdot'' b, a \cdot' b) \quad (a, b \textit{ may contain } f, +', \cdot').
\end{gathered}
$$

Proof sketch. Define $[\![\tilde{f}(x,t)]\!]$ as follows:

$$
\begin{aligned}
[\![\tilde{f}(e_s,t)]\!] &:= f(s,t), \\
[\![\tilde{f}(0,t)]\!] &:= 0_A, \\
[\![\tilde{f}(x+y,t)]\!] &:= [\![\tilde{f}(x,t)]\!] +' [\![\tilde{f}(y,t)]\!], \\
[\![\tilde{f}(ax,t)]\!] &:= a \cdot' [\![\tilde{f}(x,t)]\!].
\end{aligned}
$$

Let $[\![\varphi]\!]$ be the formula obtained by replacing $\tilde{f}(x,t)$, $+''$, and $\cdot''$ with $[\![\tilde{f}(x,t)]\!]$, $+'$, and $\cdot'$ in φ, respectively. By induction, $U \vdash_{S,A,\neg,f,+',\cdot',\tilde{f},+'',\cdot''} V$ implies $[\![U]\!] \vdash_{S,A,\neg,f,+',\cdot'} [\![V]\!]$, where $[\![U]\!] := \{[\![\varphi]\!] : \varphi \in U\}$. □

Proposition 4.5. *Let $x, y \in A_S$. If $x =_{A^{\oplus S}} y$, then* $\vdash_{S,A,\neg,f,+',\cdot',\tilde{f},+'',\cdot''} \mathrm{Eq}_A(\tilde{f}(x,t), \tilde{f}(y,t))$.

Proof Sketch. Note that $A^{\oplus S} := A_S/{\sim}$, where $\sim$ is defined in Section 2. The assertion follows by induction on the proof of $x \sim y$. □

We can finally present a constructive proof that $e_s =_{A^{\oplus S}} e_t$ implies $s =_S t$ or $1 =_A 0$:

Constructive proof of Theorem 2.2. Suppose $e_s =_{A^{\oplus S}} e_t$. By Proposition 4.5 we have

$$\vdash_{S,A,\neg,f,+',\cdot',\tilde{f},+'',\cdot''} \mathrm{Eq}_A(\tilde{f}(e_s,t), \tilde{f}(e_t,t)).$$

By simulating the classical proof on the entailment relation, we have

$$\vdash_{S,A,\neg,f,+',\cdot',\tilde{f},+'',\cdot''} \mathrm{Eq}_S(s,t), \mathrm{Eq}_A(1,0).$$

By the conservativity, we have $\vdash_{S,A} \mathrm{Eq}_S(s,t), \mathrm{Eq}_A(1,0)$. Hence $s =_S t$ or $1 =_A 0$ holds. □

Acknowledgments

The author would like to thank his supervisor, Ryu Hasegawa, and his secondary supervisor, Takeshi Saito, for their support. The author would also like to thank Haruki Toyota and Yuto Ikeda for their helpful comments.

This research was supported by Forefront Physics and Mathematics Program to Drive Transformation (FoPM), a World-leading Innovative Graduate Study (WINGS) Program, the University of Tokyo.

References

[CC00] Cederquist, J., Coquand, T. (2000). Entailment relations and distributive lattices. In: Buss, S. R., Hájek, P., Pudlák, P., eds. *Logic Colloquium '98. Proceedings of the Annual European Summer Meeting of the Association for Symbolic Logic, Prague, Czech Republic, August 9–15, 1998.* Lecture Notes in Logic, 13. Natick, MA: A K Peters, pp. 127–139.

[CL24] Coquand, T., Lombardi, H. (2024). *Résolutions libres finies: Méthodes constructives.* Paris, France: Calvage et Mounet.

[CP01] Coquand, T., Persson, H. (2001). Valuations and Dedekind's Prague theorem. *J. Pure Appl. Algebra* 155(2–3):121–129.

[Joy75] Joyal, A. (1975). Les Théorèmes de Chevalley-Tarski et Remarques sur l'Algèbre Constructive. *Cah. Top. Géom. Diff. Cat. XVI*, 256–258.

[LQ15] Lombardi, H., Quitté, C. (2015). *Commutative algebra: constructive methods.* (Roblot, T. K., trans.) Algebra and Applications, Vol. 20. Dordrecht, The Netherlands: Springer.

[Lor51] Lorenzen, P. (1951). Algebraische und logistische Untersuchungen über freie Verbände. *Journal of Symbolic Logic.* 16(2):81–106.

[Lor25] Lorenzen, P. (2025). Algebraic and logistic investigations on free lattices. (Neuwirth, S., trans.) *History and Philosophy of Logic.* 46(4):546–570.

[Lum18] Lumsdaine, P. L. (`https://mathoverflow.net/users/2273`), *Constructively, is the unit of the "free abelian group" monad on sets injective?*, URL (version: 2018-11-13): `https://mathoverflow.net/q/302516`

[MRR88] Mines, R., Richman, F., Ruitenburg, W. (1988). *A course in constructive algebra.* Universitext. New York, NY: Springer.

[Rat16] Rathjen, M. (2016). Remarks on Barr's theorem: Proofs in geometric theories. In: Probst, D., Schuster, P., eds. *Concepts of Proof in Mathematics, Philosophy, and Computer Science.* Berlin, Germany: Walter de Gruyter, pp. 347–373.

[Sco71] Scott, D. (1971). On engendering an illusion of understanding. *Journal of Philosophy.* 68(21):787–807.

[Sco74] Scott, D. (1974). Completeness and axiomatizability in many-valued logic. In: Henkin, L., Addison, J., Chang, C. C., Craig, W., Scott, D., Vaught, R., eds. *Proceedings of the Tarski Symposium (Proc. Sympos. Pure Math., Vol. XXV, Univ. California, Berkeley, Calif., 1971)*, Providence, RI: American Mathematical Society, pp. 411–435.

[Wra80] Wraith, G. C. (1980). Intuitionistic algebra: some recent developments in topos theory. In: Lehto, O., ed, *Proceedings of the International Congress of Mathematicians (Helsinki, 1978)*, Helsinki, Finland: Academia Scientiarum Fennica, pp. 331–337.

[Yen15] Yengui, I. (2015). *Constructive commutative algebra.* Lecture Notes in Mathematics. Vol. 2138. Cham, Switzerland: Springer.

Graduate School of Mathematical Sciences
The University of Tokyo
3-8-1 Komaba, Meguro-ku, Tokyo, 153-8914
JAPAN
Email address: `kuroki-ryota128@g.ecc.u-tokyo.ac.jp`

東京大学 大学院数理科学研究科　黒木 亮汰