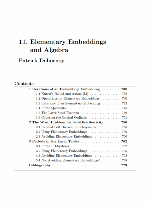
等式$x(yz) = (xy)(xz)$を満たす代数系

でぃぐにゃん

2024年3月31日

参考文献

[Deh10]

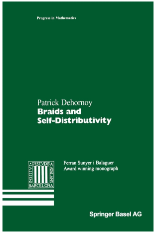


11. Elementary Embeddings and Algebra

Patrick Dehornoy

Contents

[Deh12]



[Deh10] Patrick Dehornoy. “Elementary embeddings and algebra”. In: *Handbook of Set Theory* (2010), pp. 737–774.

[Deh12] Patrick Dehornoy. *Braids and Self-Distributivity*. Progress in Mathematics. Birkhäuser Basel, 2012.

[Kan08] Akihiro Kanamori. *The higher infinite: large cardinals in set theory from their beginnings*. Springer Science & Business Media, 2008.

[KDT08] C. Kassel, O. Dodane, and V. Turaev. *Braid Groups*. Graduate Texts in Mathematics. Springer New York, 2008.

目次

目次

LDシステム

定義

集合 S とその上の二項演算 $*$ について $(S, *)$ が **LD システム**をなすとは，等式

$$x * (y * z) = (x * y) * (x * z)$$

を満たすことを言う．

この等式を今後 **LD 等式**と呼ぶ．
LD は Left Distributivity の頭文字である．

LD システムは組み紐群でも集合論でも自然に出てくる！

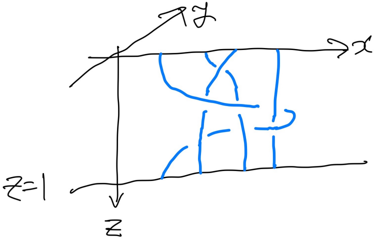
幾何的組み紐

単位区間 $[0,1]$ を I と書く．

定義

n 本の糸の幾何的組み紐とは $b \subseteq \mathbb{R}^2 \times I$ であって，b は次のような n 本の「糸」の互いの素な和集合である：

- 各糸は I と同相で各平面 $z = c$ $(c \in I)$ と一回ずつ交わる．
- $b \cap (\mathbb{R}^2 \times \{0\}) = \{(j,0,0) : 1 \leqslant j \leqslant n\}$.
- $b \cap (\mathbb{R}^2 \times \{1\}) = \{(k,0,0) : 1 \leqslant k \leqslant n\}$.



定義

幾何的組み紐 b, b' が**アイソトピー**とは，ある連続写像
$F\colon b \times I \to \mathbb{R}^2 \to I$ があって，各 $s \in I$ について
$F_s\colon b \to \mathbb{R}^2 \times I; x \mapsto F(x, s)$ は像が幾何的組み紐であり，
$F_0 = \mathrm{id}_b, F_1(b) = b'$ となることをいう．

アイソトピー関係による幾何的組み紐の同値類を**組み紐**という．

積

定義

幾何的組み紐 b, c に対して新しい幾何的組み紐 bc を

$$(x, y, z) \in bc \Leftrightarrow \begin{cases} (x, y, 2z) \in b & (\text{if } 0 \leqslant z \leqslant 1/2) \\ (x, y, 2z - 1) \in c & (\text{if } 1/2 \leqslant z \leqslant 1) \end{cases}$$

で定める．これを b と c との積という．

この演算はアイソトピー関係を保つ．つまり組み紐の間の演算を誘導する．

組み紐群

糸 n 個の組み紐すべてがなす集合を B_n と書き，そこに演算として積を考えた構造を n **次組み紐群**という．

定理

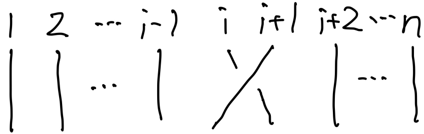
B_n は群であり，表示

$$\begin{aligned}\langle \sigma_1, \ldots, \sigma_{n-1} | \sigma_i\sigma_j &= \sigma_j\sigma_i \text{ for } |i-j| \geqslant 2 \text{ and} \\ \sigma_i\sigma_j\sigma_i &= \sigma_j\sigma_i\sigma_j \text{ for } |i-j| = 1\rangle\end{aligned}$$

を持つ．

組み紐群の生成系

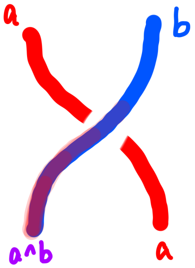
$n-1$ 個の組み紐 $\sigma_1, \ldots, \sigma_{n-1}$ を次で定める：

$\sigma_i =$ 

ただし $1 \leqslant i \leqslant n-1$．
このときこれらが関係式を満たすことはかんたんにチェックできる．だから普遍性により準同型が得られ，それが全単射である (が，かんたんではない)．

組み紐群の色塗り

組み紐に色を塗ることを考える．しかし，各糸に単に色を塗るだけだと面白くない．そこで色の集合 S に二項演算を与えておいて，糸が交差したら色を変化させるようにしよう！



組み紐群の色塗り

$(S, \wedge, \vee)$ を二つの二項演算 $\wedge, \vee$ が入った集合とする (S は色の集合)．n 次組み紐群 B_n を色の n 個組の集合 S^n に(右) 作用させて

$$
\begin{aligned}
\vec{a} \bullet e_{B_n} &= \vec{a} \\
\vec{a} \bullet \sigma_i w &= (a_1, \ldots, a_i \wedge a_{i+1}, a_i, a_{i+2}, \ldots, a_n) \bullet w \\
\vec{a} \bullet \sigma_i^{-1} w &= (a_1, \ldots, a_i, a_i \vee a_{i+1}, a_i, a_{i+2}, \ldots, a_n) \bullet w
\end{aligned}
$$

(for $\vec{a} = (a_1, \ldots, a_n) \in S^n, w \in B_n$) と定めたい！
が，これは well-defined か？

実は次が (かんたんな計算で) わかる：

命題

前ページの定義が well-defined なことは次と同値：$(S, \wedge)$ と $(S, \vee)$ がともに LD システムであり，

$$x \wedge (x \vee y) = y, x \vee (x \wedge y) = y$$

を満たす．

目次

語の問題

LD システムの言語の二つの項 $s(v_1, \ldots, v_n)$ と $t(v_1, \ldots, v_n)$ が与えられたとき，等式 $s(v_1, \ldots, v_n) = t(v_1, \ldots, v_n)$ が LD システムの公理から導出されるか？ これを LD システムの**語の問題**という．

- たとえば，交換法則や結合法則は出ない．それは具体的な有限な LD システム (たとえば濃度 2 のもの) を考えればわかる．
- たとえば，$x(y(zw)) = (xy)((xz)(xw))$ は公理から導出される．

語の問題

定理 (Laver–Dehornoy)

LD システムの語の問題は決定可能．つまり，LD システムの項 2 つを入力としてその 2 つが等しいことが LD システムの公理から導出されるとき，$\textsc{Yes}$ を返し，そうでないとき $\textsc{No}$ を返す関数は計算可能である．

この定理は当初 Laver によって I3 という巨大基数を仮定して証明された．のちに Dehornoy がその仮定を外した．

語の問題

語の問題の決定性のために次の定理を使う．これが当初巨大基数を使っていた部分．これの証明はまた次節．

定理

一個の生成子で生成される自由 LD システムにおいて，左割り算はサイクルを持たない．

ここで LD システム S において，左割り算のサイクル $a \in S$ とは，$a = ((\ldots(ab_1)b_2)\ldots)b_n$ となる有限個の元 $b_1, \ldots, b_n \in S$ があるもののことをいう．

LD 展開と LD 等価

項といったら，変数 $x_1, x_2, \ldots,$ と二講演算 $*$ を使って書ける well-formed な文字列のことを指す (変数は可算無限個ある)．項 t' が t の **LD 展開である**とは，t のある部分項で $t_1 * (t_2 * t_3)$ の形のものを $(t_1 * t_2) * (t_2 * t_3)$ に置き換える操作を有限回行って得られるときだとする．

項 t' と t が **LD 等価である**とは，その二つが LD 等式を使った書き換えで移り合えるときをいう．すなわち，LD 展開とその反対の操作「縮約」を有限回行って移るときをいう．これを $t \equiv_{\mathrm{LD}} t'$ と書く．

left と $\sqsubset$

項の間の left という部分関数を $\mathrm{left}(v)$ は未定義 (v は変数), $\mathrm{left}(t_1 * t_2) = t_1$ と定める．自然数 k に対して left の k 回合成を left^k と書く．

$t_1 \sqsubset t_2$ とはある項 t_1', t_2' があって，$t_1 \equiv_{\mathrm{LD}} t_1'$ かつ $t_2 \equiv_{\mathrm{LD}} t_2'$ かつ，ある $k \geqslant 1$ について $t_1' = \mathrm{left}^k(t_2')$ なこと．

必要な補題

補題

1. 変数が v のみのどんな項 t についても十分大きいすべての n で $v^{[n+1]} \equiv_{\mathrm{LD}} v * v^{[n]}$.
2. 二つの LD 等価な項は共通の LD 展開を持つ.

ここで，$v^{[1]} = v$, $v^{[n+1]} = v * v^{[n]}$.

なお，②は見た目以上に非自明.

比較可能性

命題

t_1, t_2 を (共通の) 一変数のみからなる項としたとき，次の 3 条件のうち少なくとも 1 つが成立：すなわち，$t_1 \sqsubset t_2$, $t_1 \equiv_{\mathrm{LD}} t_2$ または $t_2 \sqsubset t_1$.

証明．十分大きい n について $t_1 * v^{[n]} \equiv_{\mathrm{LD}} v^{[n+1]} \equiv_{\mathrm{LD}} t_2 * v^{[n]}$ なのでそういう n を一個固定．さっきの補題の②より，$t_1 * v^{[n]}$ と $t_2 * v^{[n]}$ は共通の LD 展開を持つ．それを t とする．するとある自然数 n_1, n_2 があって，$\mathrm{left}^{n_i}(t)$ は $\mathrm{left}(t_i * v^{[n]})$ の LD 展開である ($i = 1, 2$)．つまり，$\mathrm{left}^{n_i}(t)$ は t_i の LD 展開．$n_1 = n_2$ なら $t_1 \equiv_{\mathrm{LD}} t_2$ だし，$n_1 > n_2$ なら $t_1 \sqsubset t_2$ だし $n_1 < n_2$ なら $t_2 \sqsubset t_1$ となる． □

決定可能性

定理 (Laver–Dehornoy)

LD システムの語の問題は決定可能．

証明．一変数のときのアルゴリズムのみ記述する．t_1, t_2 が入力されたとする．組 (t_1', t_2') であって t_1' は t_1 と LD 等価，t_2' は t_2 と LD 等価なものをすべて (無限個あるかもしれないが，) 計算可能に枚挙できる．
先ほどの比較可能性の命題より，$t_1' = t_2'$ となる組が見つかるか，あるいは t_1' が t_2' の反復左部分項であるものか見つかるか，さもなくば t_2' が t_1' の反復左部分項であるものか見つかる．$t_1' = t_2'$ ならば，t_1 と t_2 は等価だ ($\textsc{Yes}$) と出力する．

決定可能性

定理 (Laver–Dehornoy)

LD システムの語の問題は決定可能．

証明続き．t_1' が t_2' の反復左部分項であるものか見つかったか，さもなくば t_2' が t_1' の反復左部分項であるものか見つかったときは，t_1 と t_2 は等価でない $(\mathrm{No1})$ と出力する．本当にこのときに等価でないことは「一個の生成子で生成される自由 LD システムにおいて，左割り算はサイクルを持たない」ことから従う． $\square$

目次

左割り算がサイクルを持たない LD システム

この節では次を示そう．

定理

一個の生成子で生成される自由 LD システムにおいて，左割り算はサイクルを持たない．

ここで LD システム S において，左割り算のサイクル $a \in S$ とは，$a = ((\ldots(ab_1)b_2)\ldots)b_n$ となる有限個の元 $b_1, \ldots, b_n \in S$ があるもののことをいう．
自由 LD システムの普遍性より，左割り算がサイクルを持たない LD システムを一個見つければ良い．

無限組み紐群とその演算 $\wedge$

n 次組み紐群 B_n たちは自然に順系をなすが，その順極限を B_∞ と書く．これは，最初の有限個いくつかが絡まっているが，それ以外は全部真下に垂れた糸たちからなる組み紐たちがなす群．
$x, y \in B_\infty$ に対して

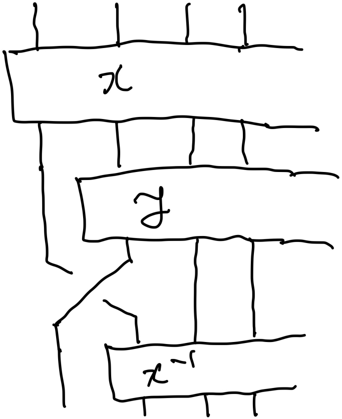
$$x \wedge y := x \operatorname{sh}(y)\sigma_1 \operatorname{sh}(x^{-1})$$

とおく．ここで $\operatorname{sh}\colon B_\infty \to B_\infty$ は σ_i を σ_{i+1} に送る自己準同型である．
なんと，$(B_\infty, \wedge)$ が左割り算がサイクルを持たない LD システムをなす！

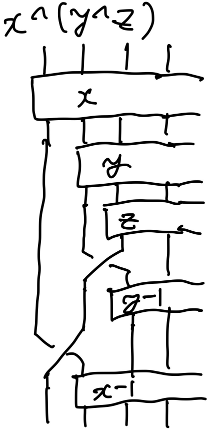
無限組み紐群とその演算 $\wedge$

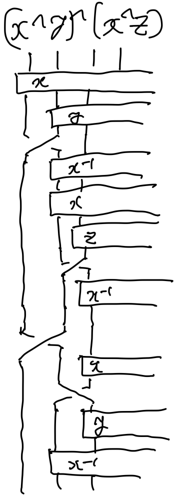
時間の都合上，$(B_\infty, \wedge)$ の左割り算がサイクルを持たないことの証明は省略する．ただ，これが LD システムであることだけは確かめておく．

$x \wedge y = x\,\mathrm{sh}(y)\sigma_1\,\mathrm{sh}(x^{-1})$ は図に描くと右の通り：



$x \wedge (y \wedge z)$ と $(x \wedge y) \wedge (x \wedge z)$





□

目次

初等埋め込み

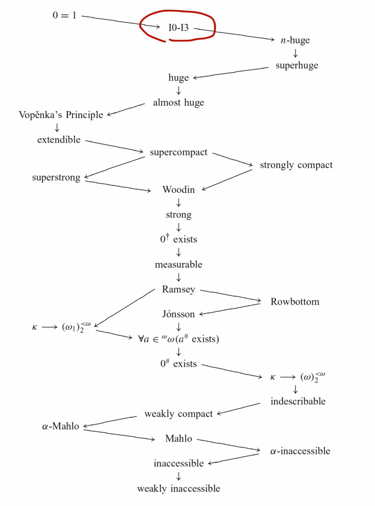
M を集合とする．$f\colon M \to M$ が初等埋め込みであるとは，

$$(M, \in) \models \varphi(x_1, \ldots, x_n) \iff (M, \in) \models \varphi(f(x_1), \ldots, f(x_n))$$

が任意の論理式と $x_1, \ldots, x_n \in M$ について成り立つことをいう．
ここで言語は $\{\in\}$ である．
V 階層とは次のように定義されていた:
$V_0 = \varnothing, V_{\alpha+1} = \mathcal{P}(V_\alpha), V_\gamma = \bigcup_{\alpha<\gamma} V_\alpha$ (γ は極限順序数)

公理 I3 は次の主張である：ある極限基数 λ について，恒等写像以外の初等埋め込み $f\colon V_\lambda \to V_\lambda$ が存在する．
公理 I3 のもとで，次の集合に恒等写像以外の元が属する：

$$\mathcal{E}_\lambda := \{ f : f \text{ は } V_\lambda \text{ から } V_\lambda \text{ への初等埋め込み} \}$$



公理 I3

$\mathcal{E}_\lambda$ に次のような二項演算 $*$ を入れる：$f, g \in \mathcal{E}_\lambda$ について，
$f * g \in \mathcal{E}_\lambda$ とは

$$(f * g)(x) = f(g \restriction V_\alpha)(x).$$

で定まる初等埋め込み．ただし α は x に依存して決めてよい十分大きな順序数．
$(\mathcal{E}_\lambda, *)$ は LD システムをなす．

Laver の定理

$f \in \mathcal{E}_\lambda$ が恒等写像でないとき，f が $*$ によって生成する部分 LD システムは左割り算がサイクルを持たない．

臨界点の数え上げ

$f \in \mathcal{E}_\lambda$ が恒等写像でないとする．このとき順序数の集合

$$A_f := \{\mathrm{crit}(g) : g \text{ は } f \text{ が } * \text{ と合成によって生成する部分 LD システムの元}\}$$

は順序型 ω の無限集合であることがわかる．ここに
$\mathrm{crit}(g) = \min\{\alpha \text{ 順序数} : g(\alpha) \neq \alpha\}$.
$\mathrm{count}_f : \omega \to \omega$ を $\mathrm{count}_f(n)$ が $f^n(\mathrm{crit}(f))$ 未満の A_f の元の個数を表す関数とする．

臨界点の数え上げ

Ackermann 関数は $A_0(n) = n + 1$, $A_{p+1}(0) = A_p(1)$, $A_{p+1}(n+1) = A_p(A_{p+1}(n))$ で定義されていた．

事実 $\mathrm{count}_f(n)$ は十分大きいすべての n で Ackermann 関数 $A_n(n)$ より大きい．

事実 $\mathrm{count}_f(0) = 0, \mathrm{count}_f(1) = 1, \mathrm{count}_f(2) = 2, \mathrm{count}_f(3) = 4$ だが，$\mathrm{count}_f(4) > A_9(A_8(A_8(254)))$.

目次

有限な LD システムはたくさんあるが，代表的なものが次の補題から得られる Laver 表と呼ばれる LD システム (の族)．

補題

各自然数 N について $\{1, 2, \ldots, N\}$ 上の二項演算 $*$ が一意的に存在し， $a * 1 = a + 1$ for $a \in [1, N)$ かつ $N * 1 = 1$ かつ

$$a * (b * 1) = (a * b) * (a * 1).$$

この演算を $*_N$ と呼ぶと，$(\{1, \ldots, N\}, *_N)$ が LD システムとなるのは N が 2 のべき乗のとき，またそのときに限る．

第 n-Laver 表とは，$N = 2^n$ に対する $(\{1, \ldots, N\}, *_N)$ のことを指す．

Laver 表の具体例

Table: 第 0Laver 表

$a \diagdown b$	1
1	1

Table: 第 1Laver 表

$a \diagdown b$	1	2
1	2	2
2	1	2

Table: 第 2Laver 表

$a \diagdown b$	1	2	3	4
1	2	4	2	4
2	3	4	3	4
3	4	4	4	4
4	1	2	3	4

I3 と Laver 表の関連

$f\colon V_\lambda \to V_\lambda$ を恒等写像でない初等埋め込みとする．このとき f が生成する部分 LD システムを「$\mathrm{crit}_n(f)$ 同値性」という自然な同値関係で割って得られる LD システムを考えると，これは第 n-Laver 表と同型．
このことから次が出る：

定理 (Laver)

ZFC+I3 を仮定する．このとき任意の自然数 a に対して，n を増大させるに従って第 n-Laver 表の中での a の周期も無限大に増大する．

この定理が ZFC で出るかどうかは未解決⋯．

目次

まとめ

- LD システムは組み紐群でも集合論でも自然に出てくる代数系
- LD システムの語の問題は左割り算がサイクルを持たない LD システムの存在に帰着される
- それの存在は，当初は巨大基数公理によって証明されていたが，Dehornoy が ZFC での証明を与えた
- 有限の LD システムの代表例として Laver 表があり，これの周期性については巨大基数を仮定した証明はあるが ZFC での証明はまだ知られていない！

Dehornoy の興味深いコメント

巨大基数公理が必要なくなったことで組み紐群への応用なども集合論の応用と呼ぶことはできなくなったのではないか，という疑念について Dehornoy はそれに同意しないと主張した上で次のようにコメントしている： [Deh10] より邦訳

> “集合論がなければ，少なくとも同じくらい早く，組み紐の順序が発見されなかった可能性がある．これを集合論の応用の定義として受け入れることはできないか？
> ここでの集合論の役割を，標準的な数学の枠組みで証明されずに残っている公式の証拠を与える物理学の役割と比較したくなる．”

触れられなかったこと

- 組み紐群に良い順序が入ることについては，紹介できなかった．緑の本 [Deh12] の第 3 章を読んでください！