理学部数学科 2000 前期 計算数学 1 [1]

担当：辻下　徹[2]

きょうやること

- 代数的理論の例
- 代数的理論の完全性
- Knuth-Bendix の理論 (1)

目 次

10　普遍代数 (3):代数的理論の論理の完全性

[1]URL:http://fcs.math.sci.hokudai.ac.jp/doc/announce/cs00.html
質問提出アドレス:cs2000@fcs.math.sci.hokudai.ac.jp

[2]Email:tujisita@math.sci.hokudai.ac.jp,
Homepage:http://fcs.math.sci.hokudai.ac.jp/tjst/

10.4　自由代数の例

10.4.1　自由半群

$\{ a \}$ が生成する自由半群は、$\{ a, a^2, a^3, \cdots, a^n, \cdots \}$ となり、自然数の足し算に関する半群と同型である.

$\left\{ a, b \;\middle|\; \text{が} \right\}$ 生成する自由半群は、a, b をアルファベットとする空でない語のなす自由半群 $\{ a, b \}^+$ と同型.

10.4.2　自由モノイド

$\{ a \}$ が生成する自由半群は、$\{ 0, a, a^2, a^3, \cdots, a^n, \cdots \}$ となり、非負整数が足し算に関してなすモノイドと同型である.

$\left\{ a, b \;\middle|\; \text{が} \right\}$ 生成する自由モノイドは、a, b をアルファベットとする語のなすモノイド $\{ a, b \}^*$ と同型.

10.4.3　自由群

$\{ a \}$ が生成する自由群は、整数が足し算に関してなす群と同型である.

$\left\{ a, b \;\middle|\; \text{が} \right\}$ 生成する自由群は単純には記述できない. 単位元以外の要素は、$\left\{ a^n \;\middle|\; n \in \mathbf{Z}, n \neq 0 \right\}$ と $\left\{ b^n \;\middle|\; n \in \mathbf{Z}, n \neq 0 \right\}$ とが交互に現れる文字列で表示される.

練習問題　積、逆の演算を定義し、群となることを確かめよ. また、それが、自由群であることも確かめよ.

10.4.4　自由束

$\{ a \}$ が生成する自由束は、$\{ 0, a, 1 \}$.

$\{ a, b \}$ が生成する自由束は、$\{ 0, a \wedge b, a, b, a \vee b, 1 \}$.

$\{ a, b, c \}$ が生成する自由束は無限集合となり、その元を書き下すことは簡単ではない (1941,P.Whitman)

10.4.5　自由ブール代数

$\{ a \}$ が生成する自由ブール代数は $\{ 0, a, \neg a, 1 \}$ で $\mathbf{pow}\, \{ 1, 2 \}$ と同型.

$\{ a, b \}$ が生成する自由ブール代数は、$\mathbf{pow}\, \{ 1, 2, 3, 4 \}$ と同型.

一般に、有限集合 X の生成する自由ブール代数は、$\mathbf{pow}\, (X \coprod X)$ と同型.

10.5　演習問題

A:定義からすぐ分かる、B:少し工夫が要る,C:やや難しい,D:難しい

問 $[10\text{-}1]_A$　次をしめせ。

(10-1-1)

$$束理論 \vdash x \vee x = x.$$

(10-1-2)

$$ブール代数理論 \vdash \neg\neg x = x.$$

問 $[10\text{-}2]_B$　束論に次の公理を加えたものを分配束という.

$$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z).$$

次を示せ.

$$分配束理論 \vdash x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z).$$

11　Knuth-Bendix の理論

- 有向グラフにおける、合流性
- 項書き換え

代数的理論で $\vdash s = t$ を示す、強力な手段が Knuth-Bendix によって提案された．この方法は項の「標準形」を導入し

$$\vdash s = t \Longleftrightarrow\ s,t \text{ の標準形が同じ}$$

を示すことから成る．標準形によるの方法は、分類問題の解法としては極めて優れたものである。

同値問題についてのミニ知識　ここで、数学的な問題の中で、種々の文脈で生じる同値問題について説明しておこう。数学的対象を何らかの方法で分類することを考える。例えば、平面上の 3 角形を考える。合同変換でうつり合う三角形を合同であると定義し、この関係で分類することは中学校で学習した。

このとき、2 つの三角形 Δ, Δ' が合同かどうかは、それらの三辺の長さを小さい順にならべたもの (a,b,c) と (a',b',c') とが一致するかどうかでわかる。この解法を完全不変量による解決という。(a,b,c) を三角形 Δ の不変量と呼ぶ。

また、別の方法は、それぞれの三角形を、次のものに合同変換で移す：長さが最小の辺を xy 軸にのせ、その辺の端点の角が小さい方を原点に置き、他の頂点は第一象限に置く。これを、その三角形の標準形と呼ぶ。このとき、2 つの三角形が合同かどうかは、それらの標準形が同じかどうかで判定できる。

この方法が使える代数的理論では，$s = t$ が成り立つかどうかは機械的に判定できることになる．しかし、Knuth-Bendix の定理はいつも使えるというわけではない。なぜなら、有名な決定不能問題である**語の問題** (word problem) は，代数的理論の定理判定問題の特殊な場合だからである。

しかし，この方法が使える代数的理論は少なくないし，また，この方法の根底にあるアイディアと概念（項書換え term rewriting，合流性 confluency，単一化 unification）は豊かな普遍性を持っているので，習得していただきたい．

11.1　有向グラフの連結成分

11.1.1　基本的定義の復習

$(A, \to)$ を有向グラフとする。

頂点 a が 頂点 b に**到達する**とは、$a = b$ であるか、または、a から b へ道があることを言う。

a が葉[3] b に到達するとき、b は a の**終点**という．

a, b を結ぶ鎖があるとき $a \sim b$ と書く。これは同値関係で、その同値類が連結成分であった。

[3]出次数 0 の頂点。

有向グラフが**弱合流的 (weakly confluent)** であるとは $a \to b$ が $a \to c$ という辺があるとき、b, c が合流することをいう。ただし、2 頂点が**合流する**とは、同じ頂点に到達することをいう。

無限長の道がないとき， 有向グラフ $(A, \to)$ は**有限条件**を満たすという．

11.1.2　標準形定理

定理 11.1 有向グラフが弱合流的で有限条件を満たすとき，

- どの元 a も唯一つの終点 a^* をもつ．
- a, b が同じ連結成分に入るための条件は、a, b の終点が同じであること．

証明は次の補題による。有向グラフ $(A, \to)$ が**合流的**(confluent) であるとは a が b, c に到達するとき、b, c が合流することをいう。

定理 11.2 *(Diamond Lemma)* 弱合流的で有限条件を満たす有向グラフは合流的である。

11.2　補題 [Diamond Lemma] の証明の概略

11.2.1

有向グラフ $(A, \to)$ が有限条件を満たすとき，$\to^*$ は順序関係となる．

11.2.2　multiset ordering

$P = (X, \leq)$ を順序集合とする．有限多重集合 $P^*(A)$ の順序関係 $\leq$ を、次の 2 項関係 $<^1$ の推移的反射的閉包として定義する。

- $[a] >^1 [a_1, \cdots, a_n N] \stackrel{def}{\Longleftrightarrow} a > a_i \quad \text{for } \forall i = 1, \cdots, N.$
- $\xi >^1 \xi' \Rightarrow \xi + \eta >^1 \xi' + \eta \quad \text{for } \forall \eta \in P^*(A).$

ここで、有限多重集合 $P^*(A)$ の元は形式的有限和 $\sum_{a \in A} n_a a$ （有限個の a を除いて $n_a = 0$.

命題 11.3 $(A, \leq)$ が有限条件を満たすとき，$(P^*(A), \leq)$ も有限条件を満たす．

証明には次の補題を用いる．これはばしば用いられる補題である．

11.2.3　König の補題.

補題 11.4 有限分岐木の頂点数が無限ならば，無限長の道がある．

証明. 子供の中で子孫の数が無限のものを選ぶ，という操作を根から無限に続けられることから明らか.[4]
証終

11.2.4　Diamond lemma の証明.

$c \overset{*}{\to} a \quad c \overset{*}{\to} b$ とする．a を，その下界 $\left\{ d \;\middle|\; a \overset{*}{\to} d \right\}$ の極小元（これは有限条件より存在する）におきなおしてもよい．そこで a,b は既約であるとする．このとき $a = b$ であることを示す．P を次のような multiset $[a_1, \cdots, a_n n$ の集まりに空 multiset $[\,]$ を添加したものとする．

$$a_1 \overset{*}{\to} a, \quad a_n \overset{*}{\to} b \quad \forall i a_i \text{ と } a_{i+1} \text{ は共終 .}$$

仮定より $[c] \in P$ であるから P は $[\,]$ 以外の元を含む．$[\,]$ でない P の元 α に対しては弱合流性により $\alpha > \alpha'$ となる元 α' が存在する．従って，P が有限条件を満たすことにより最後は弱合流性の条件を適用できない状況に到達する．これは，$a \overset{*}{\to} b$ または $b \overset{*}{\to} a$ を意味する．a,b が葉であることにより $a = b$ となる．

[4] この議論は Heine-Borel の定理の証明と似ているが，実はこの補題は「有限集合に離散位相をいれたものの無限直積がコンパクトであること」とほぼ同じ主張である．

第９回の質疑

[**Q10-1**](22960115) 最近の話は計算数学とかけはなれているようですが？

(質問理由：計算機を使ってどのように応用されるのでしょうか。具体的な例を出してもらえるとわかりやすいのですが。)

[**A10-1**] この講義のテーマは「計算数学」の基盤となっている離散数学の基本的な考え方を身に付けてもらうことにあります。

[**Q10-2-1**](22970002) 代数的理論の定義の中で、$\mathcal{E}$ を公理という、とありますが、このことの意味がよくわかりません。

[**Q10-2-2**](22970044)$\mathcal{E}$ を公理というが、公理とは、一番最初のきめごとのことではないのですか？

[**A10-2**] たとえば、群の公理 $(xy)z = x(yz), ex = x, xe = x, x(ix) = e, (ix)x = e$ を集合 $\{ \langle (xy)z, x(yz)\rangle, \langle ex, x\rangle, \langle xe, x\rangle, \langle x(ix), e\rangle, \langle (ix)x, e\rangle \}$ で表現した、というだけのことです。

[**Q10-3-1**](22970049) ゲーデルの不完全性定理というのは、どういったものですか。

[**Q10-3-2**](22980031) 正しいことがらを証明できないものはあるのですか？

[**Q10-3-3**](22990045) 完全性定理というのはどのあたりが「完全」なのですか？

(質問理由：健全性定理とか完全性定理とかと目指すものは近そうですが結果は逆になっていそうに思います。)

[**A10-3**] 「自然数をどのように形式化しても、「正しいが証明できない」命題がかならずある。」

健全性は形式化の正しさを保証するもので、形式化が無意味でないことを保証するもので、証明はやさしい（というよりも、健全性がなりたつような形式化を捜すと言うほうが正しい)。完全性は、形式化したところで考えていればよい、ということを保証するもの。これは形式化の中に現実を完全に写しとることができる、ということを意味するので、形式主義者にとって、形式化が持つべき理想的性質である。

[**Q10-4-1**](22970091) 健全性定理と完全性定理は $\Rightarrow$ と $\Leftarrow$ の違いだけなのですか。

(質問理由：定理を２つつくる必要があるのかと思ったから。)

[**Q10-4-2**](22980011) 健全性定理と完全性定理から

$$\mathcal{T} \vdash t = s \Leftrightarrow \mathcal{T} \models t = s$$

が成り立つとは言えないのですか？

[**Q10-4-3**](22980018) 健全性定理と完全性定理を

$$\mathcal{T} \vdash t = s \Leftrightarrow \mathcal{T} \models t = s$$

とまとめずに、それぞれ個別の定理として扱っているのはなぜか。

[**A10-4**] 定理は「つくる」ものではありません。論理的には、すべての定理を「そして」でつないで一つの定理にしてしまうことができます。「定理」として選び出す基準は、それがメッセージを

持っていることです。完全性定理と健全性定理とでは意味するものが全く違います。そして、他の「形式システム」では、完全性は必ずしもなりたちません。

もちろん両者を合体させた「証明可能であることと真であることとは同じこと」ももちろん重要なメッセージを持っています。しかし、これは系 (Corollary) として位置づけるべきです。

[**Q10-5**](22970051)V が $\mathcal{T}$-代数のとき、V を生成元とする自由 $\mathcal{T}$-代数は V 自身になるのですか。

[**A10-5**] 良い質問です。なりません。自由代数をつくるときは、V の持つ代数的構造は一旦「凍結」されて、単に集合とみなされる。

[**Q10-6**](25970398)$t = s$ における等号 $=$ について

(質問理由：「同じ」という意味ではないと書いてありましたが、2つの項 t, s が代入 σ で同じになるということは、一種の同値関係のようなものなのでしょうか。)

[**A10-6**] 「$\sigma \models t = s$」全体が、項の間の同値関係をさだめています。

[**Q10-7**](22980050)

(11-2-1) p9-4 ページの一番下の註 3 に『$t = s$ における符号 $=$ は、「同じ」という意味はまだない。これからその意味を与えていく』とありますが、「同じ」という意味をもたない等号 $=$ とは、ただの何も意味をもたない記号と思ってよいのですか。

(11-2-2) コンピュータ言語には CASL , C 言語, COBOL, Fortran あどがありますが、それぞれ、どのような違いや特徴があるのですか？

[**A10-7**] 前半：そうです。後半：次回少し説明します。

[**Q10-8**](22980002) 数学における証明には少なくとも Boole 代数を必要とすると思われます。その「証明」には無論「健全性定理」も含まれるのでしょうが、Boole 代数の或る等式が well-defined であるためには、「代数的理論」と云う理論での推論規則が well-defined である為には、「代数的理論」という理論での推論規則が well-defined であるという「健全性定理」を必要とする訳です。すると、堂々巡りの議論 (*) になってしまって、初めに誰かが何かを保証しないと「正しい議論 (**)」は出来ないと思われます。(*,** この議論もブール代数を使う)。あるいは、定理を公理としても良いのでしょうが、それが代数的理論である「代数的理論」の公理として well-defined である為には...（以下略）

(質問理由：確か「ポーランド電卓」ではなく「逆ポーランド電卓」というのが横河ＨＰから出ていた筈です。僕も実物を見てはしませんが。)

[**A10-8**] 重要な様相を（適切に、というわけではないが）指摘していますね。根拠を求める作業は、その作業の根拠を暗黙裏に導入することは避けられないことは普遍的な様相です。ただ、well-defined という意味を拡大解釈しています。well-defined は、見掛け上、多義的な定義が一意に決まっている、ということに特定して使います。ですから、「推論規則が well-defined, 等式が well-defined 等々」という言い方はしません。

なお、この文脈では、Boole 代数より古典論理という言い方をするのがふつうです。数学の証明は背理法を用いますので古典論理を使うことが多い。しかし、古典論理にはそれなりの奇妙なところもあります。2つの命題 P, Q を勝手に持ってくると、$P \Rightarrow Q$ または、$Q \Rightarrow P$ のいずれかが正しいことになってしまいますが、これは、ふつうの感覚では納得できないことです。

なお、古典論理全体が必要でない証明はたくさんあります。特に、背理法を用いなくてよい証明（たとえば構成的な証明）がそうです。

数学と論理の関係はそれほど明確なものではないと思います。

[**Q10-9**](22980007) 問 $[9\text{-}6]_B$
(9-6-1) $x \wedge x \overset{L10}{=} x \wedge (x \vee 0) \overset{L6}{=} x$
(9-6-2) $(B14) \rightarrow 0 \vee \neg 0 = 1 \overset{L4}{\rightarrow} \neg 0 \vee 0 = 1 \overset{L10}{\rightarrow} \neg 0 = 1$
このように証明していって問題ないですか。(9-6-2) の解答の仕方は9．3．3の証明の書き方とは違う気がしますが、十分証明できていると思います。

[**A10-9**] 9.3.3 は特殊な証明図の省略法を説明したものです。君の書き方も証明の中に入っています〔少し簡略化していますが〕

[**Q10-10**](22980008)$b(b(c, u(c)))$ を… と書きましたが… ではないのですか。

[**A10-10**] b のアリティは2ですから、$b(b(c, u(c)))$ は項ではありません。講義でも注意したように誤植です。

[**Q10-11**](22980012) ブール代数はどのようにファジー理論に用いられているのですか。
(質問理由：x と y を $[0, 1]$ 区間内の実数とすると、うまくいくのですが、$\neg$ はマイナスと解釈していいのでしょうか。)

[**A10-11**] マイナスではなく $\neg x = 1 - x$ です。

[**Q10-12**](22980030)$\Omega_B = \{ \top, \bot, \neg, ... \}$ の中の $\top$ の記号等がわかりません。$\Omega_Z = \{ 0, 1, -, +, \times \}$ と $\Omega_{Z'} = \{ 0, 1, -, +, \times, \div \}$ とは違うのか？

[**A10-12**] $\top$ は「恒真命題を表す記号。Ω_Z と $\Omega_{Z'}$ とは集合として違うので違います。（それ以外に「同じ」という言葉は導入していない。）

[**Q10-13**](22980034)9.1.3 で、代入データの定義が出てきましたが、$\Omega X \ni t \mapsto t[\sigma] \in A$ や、その下の拡大された図の意味がよくわかりませんでした。
(質問理由："$\Omega X \ni t \mapsto t[\sigma] \in A$" とは、"$\Omega$　X の元 t があって $t[\sigma]$ は A に含まれる" という意味ですか。… そもそも $t[\sigma]$ とはどのような意味かもわかりません。)

[**A10-13**] $X \ni t \mapsto f(t) \in Y$ という書き方は、X の元を $f(t)$ に写す写像を表します。

[**Q10-14**](22980041)

(11-2-1) 9.2.4 の例の中で、もう３つ位関数記号を増やせば、環や体の公理も表せると思うのですが。
(11-2-2) 9.3.2 推論規則で、横線の意味がいまいちわかりませんでした。

[**A10-14**] 「横線の上が正しければ下も正しい」ことを意味する。

[**Q10-15**](22980047)A, B を Ω 構造とするとき、$A \subset B$ という包含関係は存在するのですか？
(質問理由：もしあるのであれば「$B \models t = s$ ならば $A \models t = s$ ということも成り立つのだろうかと思ったので..)
[**A10-15**] $A \subset B$ という場合もあります。このときは、A の元の積が A からはみ出ないことが重要です。

[**Q10-16**](22980048) 特殊化律がよくわかりませんでした。

[**Q10-17**](22980051)$|A|$ が台集合と呼ばれるのはなぜですか。
[**A10-17**] いろいろな上部構造を乗っける台、ということではないでしょうか。

[**Q10-18**](22007806) 推論規則で、$s = t \Rightarrow t = s$ を $\dfrac{s = t}{t = s}$ という表し方をするのには意味があるのですか。単なる省略でしょうか。
[**A10-18**] 視覚的に見やすくするという意味はありますが、単なる別の書き方に過ぎないと言ってもかまわない

[**Q10-19**](s980033) 質問：　９．２．４の例にある０，１，ｅ　といった関数記号と定数記号の違いがよく分かりませんでした。
(質問理由：（前回の質問にｃとｘの違いは何かという質問がありましたが）０，１，ｅは関数と定数とではどうちがいますか？)
[**A10-19**] 定数は、アリティが０の関数である考えてううださい。

[**Q10-20**](kotone)Ω-構造の定義が良くわかりませんでした。
(質問理由：$\mathcal{A} = (|\mathcal{A}|, \left\{ \omega_{\mathcal{A}} \;\middle|\; \omega \in \Omega \right\})$ がΩ構造であるとは、｜Ａ｜は集合 (台集合と呼ばれる）とありましたが、｜Ａ｜は集合と言う意味がよく分かりませんでした。これは、作用素記号ωがどれだけあるかと言うことを表しているのですか？それとも、|・| は全く別の意味を持つ記号として理解しなければいけないのでしょうか?混乱してきて分からなくなってしまいました。)
[**A10-20**] 次のように書いても分かりませんか。Ω を作用素型とする。$(X, \left\{ \omega_X \;\middle|\; \omega \in \Omega \right\})$ が **Ω-構造である**とは、

- X は集合 (台集合と呼ばれる),

- $\omega_X : \overbrace{X \times \cdots \times X}^{\alpha\omega} \to X$ （$\omega \in \Omega$) は写像.

[**Q10-21**](22980033) 第８回）ポーランド記法はどのようなときにつかわれるのでしょうか？
(質問理由： ポーランド記法は各作用素にアリティを書いたり、読むときは結局、括弧を使ったり木の構造を書いたりと大変な気がします。)
[**A10-21**] それは慣れの問題です。

[**Q10-22**](s970091) Ω項の表示法は他にもあるんですか
[**A10-22**] 原理的には無数にあります。質問にあった逆ポーランド記法などもその例。