LETTER

# 埋め込みの原理 (環の場合)

# On Identification of Rings

渡瀬　泰成 [1,*]
Yasushige Watase[1,*]

1 東京都杉並区松ノ木 3-21-6

* yasushige.watase@gmail.com

Proof checked by Mizar Version: 8.1.11 and MML Version: 5.65.1394
Received: December 10, 2022. Revised: May 14, 2023. Accepted: June 13, 2023.

## 要約

We formalized a standard procedure of ring identification appeared as a lemma in §13 of chapter 1 of [2], namely:

**LEMMA.** *If $R$ and $S'$ are rings and if $T_0$ is a given isomorphism of $R$ onto a subring $R'$ of $S'$, then there exists a ring $S$ which contains $R$ as a subring and which is such that $T_0$ can be extended to an isomorphism $T$ of $R$ onto $S'$.*

We discussed the relation between the above lemma and polynomial rings in terms of formalization as well, and concluded that polynomial rings would be regarded as a part of a formal series.

## 1　序論

本稿では環といえば単位元をもつ可換環とする．与えられた 2 つの環 $R$ と $S'$ について, 次の 2 条件 1), 2) をみたすとき $R$ が $S'$ の中に埋め込まれると定義する．

1) $S'$ と同型な環 $S$ が存在.

2) $S$ は $R$ を部分環として含む.

この定義からは次の命題 1 が $S'$ から $S$ への同型写像 $T$ を考え $R$ の $T^{-1}$ による像をとれば示される．

**命題 1.** 「$R$ が $S'$ の中に埋め込まれる」ならば「$S'$ は $R$ と同型な部分環をもつ」

この「$S'$ は $R$ と同型な部分環をもつ」が十分条件となる次の命題も示される.

**命題 2.** 「$S'$ が $R$ と同型な部分環をもつ」ならば「$R$ が $S'$ の中に埋め込まれる」

命題 2 の証明の形式化が本稿の中心的な内容であり所謂「埋め込み原理」といわれ命題 2 を精密にした以下の補題が文献 [2]1 章 §13 の内容であり上述要旨の Lemma である.

**LEMMA.** $R$ が $S'$ が環で $T_0$ が $R$ から $S'$ の部分環 $R'$ への環同型写像ならば, 環 $S$ が存在し $S$ は $R$ を部分環に持ち, $T_0$ を延長して $S$ から $S'$ への同型写像となるように $S$ がとれる.

有理数体の代数拡大を考える場合有理数体が埋め込まれているほうが計算がしやすい. これは拡大体の四則演算で有理数も拡大体の元として扱え計算が実行できるからだ. 単射が存在しているだけでは単射の像として有理数を扱う煩雑さが伴い演算の記述や計算に複雑さが増す. 単射像でなく埋め込まれている状況で計算できる方が実用的である. 上記の Lemma では標準的に与えられた環 $R$ が埋め込まれているように拡大環を構成し、且 $S'$ と同型となる手順を与えている. MML ライブラリには体の拡大においての埋め込みを論じたアーティクル [1] が存在し有理数体 $\mathbb{Q}$ が多項式環 $\mathbb{Q}[X]$ に埋め込まれていることを論じている. 形式的には多項式環では係数環は埋め込まれているのであって部分環ではない. 非形式的には部分環とみなしている. 多項式環についての更なる議論は 3 章に譲る.

## 2　埋め込み原理の形式化

文献 [2]1 章 §1 の Lemma の記号 $R$,$S'$,$S$ を環 $A$,$B$,$C$ と読み替え $A$ から $B$ へ単射があるとき $B$ と同型で $A$ を埋め込みとしてもつ $C$ の構成は以下の Step1,2 のプロセスを踏まえ遂行される. 単射 $A \overset{f}{\rightarrowtail} B$ があたえられ $B \cap C = \emptyset \land B \cong C$ で $A$ が埋め込まれるように $C$ を構成する議論を進める.

Step(I)　$X \cong (B \backslash f(A)) \land X \cap B = \emptyset$ なる集合 $X$ を作る.

Step(II)　$C$ として $X \cup A$ に環の構造を導入し $B$ と同型な環 $C$ で $B \cap C = \emptyset$ と出来る. ($f(A)$ の部分を $A$ で置き換える.)

上記 Step（I）は [3] の 6 章の補題 6.1 に対応し,Step（II）は補題 6.2 に対応するが詳細は次節にて述べる.

### 2.1　埋め込みの原理の形式化

この節では文献 [3] の 6 章の補題, 定理に従って埋め込みの定理の形式化の内容を要約する.

**定理** (補題 6.1. [3] より再掲)**.** 空でない二つの集合 $A, B$ を与えれば, $B \cap C = \emptyset$ であるような空でない集合 $C$ と全単射 $\varphi : A \to C$ の組 $(C, \varphi)$ が少なくとも一つ存在する.

補題 6.1. に対応する形式化は Listing 1 となる.

**Listing 1.** ALGEMBED:2 - Th.2

```
theorem :: ALGEMBED:2
  for a,b be non empty set holds ex c be non empty set st (a /\ c ={})&
  (ex f be Function st f is one-to-one & dom f = b & rng f = c );
```

**定理** (補題 6.2. [3] より再掲)**.** $R$ は環とする. $X$ は空でない集合で, 全単射 $f : R \to X$ が与えられていると仮定せよ. $X$ 上に和と積を

$$a + b = f(f^{-1}(a) + f^{-1}(b)),\ ab = f(f^{-1}(a)f^{-1}(b))$$

で定めると, 集合 $X$ はこの和と積によって環となる.

補題 6.2. における集合 $X$ の和と積の定義を形式化したものがそれぞれ Listing 1 と Listing 2 である.

**Listing 2.** ALGEMBED:def 1 - Def.1

```
definition
let A be Ring, X be non empty set;
let f be Function of A,X;
let a,b be Element of X;
assume that
 f is bijective;
func addemb(f,a,b) -> Element of X equals
:: ALGEMBED:def 1
  f.((the addF of A).(f".a,f".b));
end;
```

**Listing 3.** ALGEMBED:def 3 - Def.3

```
definition
  let A be Ring, X be non empty set;
  let f be Function of A,X;
  let a,b be Element of X;
  assume that
 f is bijective;
  func multemb(f,a,b) -> Element of X equals
:: ALGEMBED:def 3
  f.((the multF of A).(f".a,f".b));
end;
```

補題 6.2 の結論である $X$ が環を為す部分は上記で定義した加法 addemb($f$,a,b) と乗法 multemb($f$,a,b) 及び補題の仮定の写像 $f$ を用いて集合 $X$ を基礎集合にもつ環 emb_Ring($f$) を定義した. この形式化が以下の Listing 4 となる.

**Listing 4.** ALGEMBED:def 5 - Def.5

```
definition
  let A be Ring, X be non empty set;
  let f be Function of A,X;
  assume that
 f is bijective;
  func emb_Ring(f) -> strict non empty doubleLoopStr equals
:: ALGEMBED:def 5
  doubleLoopStr(# X, addemb f, multemb f, f.1.A, f.0.A #);
end;
```

**定理** (定理 6.4 (埋め込みの原理) [3] より再掲)**.** 写像 $f : A \to B$ は環の準同型写像であって，単射と仮定する．このとき，次の条件 1), 2) を満たすような環 $C$ と環の同型写像の組 $(C, g)$ が少なくとも一つ存在する．

*1)* $A$ は環 $C$ の部分環である．

*2)* 写像 $i : A \hookrightarrow C$ によって自然な埋め込み $i(a) = a$ を表すと，等式 $i = gf$ が成り立つ．

以下の定理の内容の理解のため可換図式[1]を示す：

$$\begin{tikzcd} B \arrow[rr, "g"] & & C \\ & A \arrow[ul, "f"] \arrow[ur, "\iota"'] \arrow[u, phantom, "\circlearrowright"] & \end{tikzcd}$$

確かに $C$ が $A$ の拡大系になっていることが 2 番目の条件から $i$ が恒等写像であることから理解される．この定理は文献 [2]Chapter 1.13: Idetification of Rings と同一内容となる．定理 6.4 の形式化は以下の通りである．

**Listing 5.** ALGEMBED:7 - Th.5

```
theorem :: ALGEMBED:7
    for A being Ring, B be A−homomorphic Ring,
    f being Homomorphism of A,B st f is monomorphism & ([#]B \ rng f) <> {}
    holds
    ex C be A−homomorphic Ring,i be (Homomorphism of A,C),
    G be Function of B,C st i is RingMonomorphism &
    G is RingIsomorphism & i = G∗f & i = id A & Image i is Subring of C &
    [#](Image i) = [#]A;
```

**Proof** (定理 6.4)**.** $B = f(A)$ であれば $C = A$ としてよいので $B \neq f(A)$ の場合を示す．
$\varphi : B \setminus f(A) \to X, X \cap A = \emptyset$ となる $(X, \varphi)$ は補題 *6.1* により構成する．
$C = X \cup A$ と定め，$g : B \to C$ を以下の様に定義する．

$$\forall b \in B, \quad g(b) = \begin{cases} a & if\ b \in f(A) \\ \varphi(a) & if\ b \notin f(A). \end{cases}$$

$g$ は全単射であることが確認でき補題 *6.2* を適用し $C$ に環構造が入る．
$\forall a \in A, g(f(a)) = a = \iota(a)$ よって $A$ は $C$ の部分環であることがルーチン的な計算により検証できるので細部は *ALGEMBED:7* の証明本体を参照．

## 3　考察

代数構造の拡大系について「埋め込みの原理」を環を題材に形式化が完了した．「埋め込みの原理」はどの数学的な構造にも本来適用されるべき原理だが構造をパラメータにはとれないので個別に同様の議論をしなければならないことも分かる．環で成り立つことはそのまま体でも成り立つので今回の形式化は汎用性があることも言える．

[1]図式から同型を除き $(C, g)$ が一意に取れれば普遍写像と考えてもよいが，$dom f = A$ となる単射が決まれば $(C, g)$ が決まることは了解されても圏論での解釈は今後の課題である．

### 3.1 多項式の特徴づけについて

多項式環の特徴付けには「埋め込みの原理」と「多項式の不定元の線型結合表示」が入用であるがこれらは未だにライブラリにはない.

**定理** (定理 1.33. [4] より再掲)**.** *環* A *を与えれば, 次の 3 条件* 1) – 3) *を満たす組* $(S, X)$ *が存在する.*

*1). $S$ は環, $A$ は $S$ の部分環である.*

*2). $X \in S$ であって, $X$ は $A$ 上超越的である.*

*3). 環 $S$ の元 $f$ はすべて, 環 $A$ の元の族 $a_{i0\leq i\leq n}$ を選んで,*

$$f = \sum_{i=0}^{n} a_i X^i$$

*という形に表すことができる.*

以上が定理 1.33 であって定理に現れる $S$ が $A$ 上 $X$ を不定元に持つ多項式環と呼び $A[X]$ と表す.

非形式の不定元のべきの線型結合表示で多項式を扱うことが多く現状の形式表現は使いづらい面があるので形式表現の環と同型な係数環が埋め込こまれた環を具体的に形式化できないか考察する. 即ち「埋め込みの原理」を Mizar での 1 変数多項式に適用してみる.

$A$ 係数の 1 変数多項式環の形式化では $A$ 値の無限列の為す環の部分環として構成した. これを $T$ としよう. $\varphi : A \to T(a \mapsto (a, 0, 0, \cdots))$ とすれば $\varphi$ は単射である. また $T$ の不定元は $t = (0, 1, 0, \cdots)$ である. 以上の状況で「埋め込みの原理」を適用すると以下の可換図式を得る.

$$\begin{tikzcd}
T \arrow[rr, "\xi"] & & S \\
& A \arrow[ul, "\varphi"] \arrow[ur, "\iota"'] \arrow[u, phantom, "\circlearrowleft"] &
\end{tikzcd}$$

「埋め込みの原理」により $(S, \xi)$ が構成される ($\xi$ は同型射). $\xi(t) = X$ と置くと $T$ での多項式の準同形像は定理 1.33. 3) と準同型の線型性により $X^j$ の $A-$ 線型結合となって $S(= A[X])$ で非形式での議論が出来るようになる. Mizar で形式化された多項式環 Polynom-Ring $A$ は $S(= A[X])$ と同一視しているのである. $t = (0, 1, 0, \cdots)$ を $T$ の不定元として成り立つことは同型射 $\xi$ で送った先でも成り立っていることを示している. 先に述べた補題 6.1 のなかで現れる集合 $X$ は存在しか示して居らず具体的に構成する術がないので上記の $t = (0, 1, 0, \cdots)$ を不定元として形式化を継続するほかないと判断する. 無論 $S$ や $\xi$ を具体的に構成する方法を追求する途も残る. 当面前者を採用して不定元 $t$ による係数環との線型結合表示を使い易い形に形式化することが優先課題と考える.

### 3.2 形式化での記号の注意点

前節で多項式環と係数環の関係をみた. 係数環 $A$ と $A[X]$ の交わりは定理 1.33 の記号で考えると $A[X] \cap A \neq \emptyset$ であり, Polynom-Ring $A = A[X]$ という意味で使用すると

$A[X] \cap A = \emptyset$ となる．$A[X]$ の記号の使い方を明確に定義していないと正反対の結果を招く．非形式な論文を書く場合, 非形式な表現で利用されている記号を形式化で定義された対象に用いると同一視の介在をわすれてしまうリスクがあることが理解される．

### 3.3 多項式環の係数環の埋め込みの問題

「互いに同型な２つの対象で一方の対象で成り立つ事が他方でもこの同型射 $\Phi$ により翻訳され成り立つ.] という命題を考え $P$ としよう．すると多項式環の係数環の「埋め込み」の議論で見た様に Polynom-Ring $A$ と $A[X]$ は同型である (Polynom-Ring $A = \Phi A[X]$). 他方 Polynom-Ring $A \cap A = \emptyset$ と $A[X] \cap A \neq \emptyset$ とが成り立ち命題 $P$ は成り立っていない様に見え大いに疑問に思う．この議論は係数環とは何か, 記号の定義, 多項環の構成法も含め正確さ欠いているが丹念に調べ形式化していけば議論の不備や多項式環の形式化の改良点が浮き彫りにされこの分野の形式化に寄与出来ると期待している．

## 参考文献


[1] Schwarzweller C. On Monomorphisms and Subfields. Formalized Mathematics. 2019;27(2):133–137.

[2] Zariski O. and Samuel P. Commutative Algebra I, Springer, 1975

[3] 後藤四郎. 2007 年度 明治大学代数学 3 講義用テキスト. `http://www.commalg.jp/~goto/pdf/daisuu3.pdf`

[4] 後藤四郎, 渡辺敬一. 可換環論. 日本評論社, 2011

[5] 島内剛一. 数学の基礎. 日本評論社, 1971


# Mizar article information

## Mizar Mathematical Library (MML)

## Works in Progress

**ALGEMBED** Embeding Principal（Idetification of Rings）
by Y.Watase

```
In the article standard embeding a ring into its over-ring is formalized in Mizar
along with the text book of Zariski & Samuel Commutative Algebra I.
```

**Listing 6.** ALGEMBED - abstract

**environ**
vocabularies NUMBERS, SUBSET_1, RELAT_1, XBOOLE_0, BINOP_1, FUNCT_1, TARSKI, ARYTM_3, ZFMISC_1, ARYTM_1, FUNCT_2, GROUP_1, ALGSTR_0, RLVECT_1, VECTSP_1, LATTICES, SUPINF_2, MESFUNC1, QUOFIELD, MSSUBFAM, FUNCSDOM, RING_2, GROUP_6, FDIFF_1, MOD_4, C0SP1, FIELD_2, STRUCT_0, PEVAL_1;

notations TARSKI, XBOOLE_0, ZFMISC_1, SUBSET_1, RELAT_1, FUNCT_1, RELSET_1, PARTFUN1, FUNCT_2, BINOP_1, STRUCT_0, ALGSTR_0, RLVECT_1, GROUP_1, VECTSP_1, GROUP_6, RINGCAT1, MOD_4, QUOFIELD, RING_1, C0SP1, RING_2;

```
constructors RELSET_1, REALSET1, ORDERS_1, RINGCAT1, MOD_4, C0SP1, RING_1,
  RING_2;

registrations XBOOLE_0, RELAT_1, FUNCT_1, RELSET_1, FUNCT_2, STRUCT_0,
  VECTSP_1, SUBSET_1, RINGCAT1, MOD_4, RING_2;

requirements SUBSET, BOOLE;

equalities STRUCT_0, ALGSTR_0;

expansions VECTSP_1, FUNCT_1;

theorems TARSKI, ZFMISC_1, RLVECT_1, FUNCT_1, FUNCT_2, RELAT_1, CARD_1,
  GROUP_1, XBOOLE_0, XBOOLE_1, WELLORD2, SUBSET_1, XTUPLE_0, VECTSP_1, RING_2,
  BINOP_1, ALGSTR_0, MOD_4, RINGCAT1, GROUP_6, QUOFIELD;

schemes FUNCT_2, BINOP_1;

begin
theorem :: ALGEMBED:1
   for a be non empty set holds
   ex b be object st (for x be set holds not [x,b] in a);

theorem :: ALGEMBED:2
   for a,b be non empty set holds ex c be non empty set st (a /\ c ={})&
   (ex f be Function st f is one-to-one & dom f = b & rng f = c );

theorem :: ALGEMBED:3
  for A be Ring, X be non empty set, f be Function of A,X,
  a,b be Element of X st f is bijective holds
  f.((the addF of A).(f".a,f".b)) is Element of X;

definition
let A be Ring, X be non empty set;
let f be Function of A,X;
let a,b be Element of X;
assume that
 f is bijective;
func addemb(f,a,b) -> Element of X equals
:: ALGEMBED:def 1
  f.((the addF of A).(f".a,f".b));
end;

theorem :: ALGEMBED:4
  for A be Ring, X be non empty set, f be Function of A,X,
  a,b,c be Element of X st f is bijective holds
  addemb(f,a,addemb(f,b,c)) = addemb(f,addemb(f,a,b),c);

definition
  let A be Ring, X be non empty set;
  let f be Function of A,X;
  assume that
 f is bijective;
  func addemb f -> BinOp of X means
:: ALGEMBED:def 2

  for a,b being Element of X holds it.(a,b) = addemb(f,a,b);
end;

theorem :: ALGEMBED:5
  for A be Ring, X be non empty set, f be Function of A,X,
  a,b be Element of X st f is bijective holds
  f.((the multF of A).(f".a,f".b)) is Element of X;

definition
  let A be Ring, X be non empty set;
  let f be Function of A,X;
  let a,b be Element of X;
  assume that
```

```
 f is bijective;
  func multemb(f,a,b) -> Element of X equals
:: ALGEMBED:def 3
  f.((the multF of A).(f".a,f".b));
end;

definition
  let A be Ring, X be non empty set;
  let f be Function of A,X;
  assume that
 f is bijective;
  func multemb f -> BinOp of X means
:: ALGEMBED:def 4
  for a,b being Element of X holds it.(a,b) = multemb(f,a,b);
end;

definition
  let A be Ring, X be non empty set;
  let f be Function of A,X;
  assume that
 f is bijective;
  func emb_Ring(f) -> strict non empty doubleLoopStr equals
:: ALGEMBED:def 5

  doubleLoopStr(# X, addemb f, multemb f, f.1.A, f.0.A #);
end;

theorem :: ALGEMBED:6
  for A be Ring, X be non empty set, f be Function of A,X
  st f is bijective holds emb_Ring(f) is Ring;

::Z-S:ComAlg.Isection 13: Idetification of Rings (Imbeding Theorem)
theorem :: ALGEMBED:7
    for A being Ring, B be A-homomorphic Ring,
    f being Homomorphism of A,B st f is monomorphism & ([#]B \ rng f) <> {}
    holds
    ex C be A-homomorphic Ring,i be (Homomorphism of A,C),
    G be Function of B,C st i is RingMonomorphism &
    G is RingIsomorphism & i = G*f & i = id A & Image i is Subring of C &
    [#](Image i) = [#]A;
```