数理解析研究所講究録
第1764巻 2011年 1-6

実閉体の生い立ち

名古屋大学多元数理科学研究科　塩田昌弘 (MASAHIRO SHIOTA)
GRADUATE SCHOOL OF MATHEMATICS,
NAGOYA UNIVERSITY

1. 序文

実閉体の概念はE.Artinが1927年にHilbertの第17問題を解くために導入したものである。その後1980年代から実閉体上で代数幾何を考えるという、実代数幾何学が盛んに研究されるようになった。

Hilbertの第17問題とは、負の値をどこでもとらない$\mathbf{R}^n$上の多項式関数は有限個の有理関数の2乗の和になるかというものである。問題自身はそう面白いものではない。その証明に注目したい。

Artinによる第17問題の証明は日本語では[2]に書かれていて、読むのに代数の基本的知識をいくつか必要とするだけである。しかし、あまり証明は面白くないのか、役に立たないのか、代数では他で用いられていない。一方実代数幾何学では、その証明を少し代えたものが、代表的な基本的な一つの証明方法になっている。ここではその証明を紹介する。実代数幾何学の一つの研究方法の紹介になる、ともいえる。それは[1]に書かれているが、[1]では実代数幾何学のいろいろな概念が書かれていて、それを理解しないと証明にたどり着けない。簡単な事柄であるが、基礎論の話の進め方になれていない人は時間がかかる。日本人でそれらの概念を知っている人は、ほとんどいないと思う。また日本語で書かれたものはない。よって、その証明方法を日本語で、しかも実代数幾何学の言葉をできるだけ使わずに紹介するのは意味のあることだと思う。それで、この論文を書くことにした。

一言でその証明方法を語れば、ある体でconstructiveに記述された問題で、解けるかどうか分からないとき、問題の形をそのままにして、体のみを変換することである。例としてRを体として、問題$\exists x \in R,\ x^2 = 2$を考える. この問題は$R = \mathbf{R}$では解けて、$R = \mathbf{Q}$では解けない。これでは困るが、体が実閉体ならうまくいく。もしRで解けるかどうか分からない問題のとき、解けるようにRを大きな体$\tilde{R}$に置き換える。次に説明するArtin-Langの定理によればRも$\tilde{R}$も実閉体なら、もし$\tilde{R}$で解ければRで必ず解ける。これが説明したい証明方法である。

問題をconstructiveに記述するとは、考えている集合の元と「足し算」、「掛け算」、「$\exists$」、「$\forall$」、「not」、「かつ」、「又は」をのみ有限回使って問題を記述することである。constructiveに証明するというのも、同じように定義する。

2000 *Mathematics Subject Classification.* 12D15, 12J15, 14P10.
Key words and phrases. Hilbertの第17問題、実代数幾何学、実閉体.

名古屋大学多元数理科学研究科　塩田昌弘

なお私はこの講究録の別の論文で実多項式に関する全く別の問題を、この体を置き換えるという方法で証明する。ただしArtin-Langの定理は使わない。この論文ではArtin-Langの定理を使って、複数の体を行ったり来たりするが、次の論文では、単に一度$\mathbf{R}$を代数的実Puiseuxベキ級数体で置き換えるだけである。またこの論文の終わりに他の応用例を紹介する。

2. 定義と例とその基本的な性質

この証明に必要な最低限の定義とその例と、それから注意として、それらの基本的な性質を述べる。注意は後の証明の中で使う、というか、それを理解すれば証明はほとんど明らかである。例がそこでいっている条件を満たす例になっていることは、それから注意は、代数のほん基本の概念を知っていて、Zornの補題が使えれば証明できる。学部4年生ならできる。しかしZornの補題を長く使っていなければ、思い出すのに時間がかかるかもしれない。半日ほどつぶれるかもしれない。

定義 1．体Rが順序体であるとは、Rに順序（いつも全順序）が定められていて、任意のRの元a,b,cに対して$a>b$なら$a+c>b+c$で、$a>b$かつ$c>0$なら$ac>bc$になることである。すなわち順序とかけ算、足し算が整合していること。

反例．代数的閉体と標数が0でない体はどのように順序を入れても順序体にはならない。

定義 2．体Rが実閉体であるとは、次の同値な条件を満たすことである。
(i) $R[t]/(t^2+1)$が代数的閉体である。（それは$R[i]$になる。）
(ii) Rを係数とする奇数次の一変数多項式はいつも解を持ち、Rの各元aに対してaまたは$-a$はRの有限個の（実は一つの）元の2乗の和の形になる。

例．(i) $\mathbf{R}$は実閉体であるが$\mathbf{Q}$はそうではない。なぜなら$\mathbf{Q}$では方程式$x^3=2$は解けない。
(ii) 最小の実閉体は代数的実数全体の体（全ての一変数$\mathbf{Q}$係数多項式の実根全体）。
(iii) $\mathbf{R}$より大きな実閉体のすべての中で一番小さいのは代数的実Puiseuxベキ級数体である。ここで代数的実Puiseuxベキ級数とは$\sum_{n=p,p+1,..} a_n t^{n/q}$の形のベキ級数。ただし$a_n \in \mathbf{R}$, $p,q \in \mathbf{Z}$, $q>0$かつ0でない2変数多項式$P(t,x)$が存在して$P(t,\sum_{n=p,p+1,...} a_n t^{n/q})$が関数としてではなく、代数的に0となる。

注意 1．ここで体が小さい、大きいといっているが、2つ実閉体があればそれらは比べられる。正確に言うと、どちらかがその他を含む。しかも含み方は一意的である。特に1つの実閉体の同形写像は恒等写像しかない。実閉体は代数的閉体とまったく異なることになる。普通の代数幾何学の議論が実代数幾何学でうまくいかないのは、これが一つの理由である。逆に普通の代数幾何学で成り立たない議論が実代数幾何学でうまくいくことにもなる。

注意 2．実閉体には順序がいつも入って順序体になる。2つの実閉体が体として同形ならばその同形写像は順序を保つ。すなわち順序体としての同形写像になる。よって実閉体には順序は一意的に入る。実閉体は順序体と見なせる。一般に体に順序が入って

順序体になったら、その順序の入れ方は一意的と限らない。例えば、$\mathbf{Q}$ と π で生成する体 $\mathbf{Q}(\pi)$ に順序を入れるとき、π を $\mathbf{Q}$ のどの位置に置くか、3.14... としなくても良い。6.28... でも良い。あるいは $+\infty$ としても良い。すなわち代数的には $\mathbf{Q}(\pi)$ は一変数有理関数体 $\mathbf{Q}(t)$ と同じものである。

注意 3. 標数0の代数的閉体 K に対して K の真部分体 R が存在して、$R[i]=K$ となる。そのとき定義2の (i) より R は実閉体である。(R が代数的閉体のとき $R[t]/(t^2+1)$ は体でない。) よって実閉体は標数0の代数的閉体の実部といえる。ただし R は一意的とはいえない。

注意 4. R を実閉体とする。すると R の元 a に対して、R の元 b が存在して $a=b^2$ または $a=-b^2$ となる。

注意 5. R を標数0の体とし、$X=\{\sum_{i=1}^{k} a_i^2 : a_i \in R,\ k \in \mathbf{Z}\}$ とする。すると R のどの元 $x \neq 0$ も、R にどんな順序であれ、それを入れ、R が順序体にすれば、$x>0$ となる。また $R-X$ の任意の元 x に対して R にある順序が入り、R が順序体になり、$x<0$ となる。これは上で代数的閉体と標数が0でない体はどのように順序を入れても順序体にはならない、といったことと矛盾しない。なぜなら、そんな体では $R-X$ が空集合になる。

注意 6. R を順序体とすれば、R はある実閉体に順序体として埋め込むことができる。そんな実閉体の最小な体を R の実閉包と呼ぶ。

注意 7. すでに何回も2乗の和というのが出てきている。それで Hilbert の第17問題の証明が少し予想できるであろう。有理関数の2乗の和の集合が問題になる。だから、実数体のみを考えずに有理関数体も考えることになる。一変数有理関数体に順序が入り、順序体になり、その実閉包は代数的実 seux ベキ級数体である。この論文では代数的実 Puiseux ベキ級数体を使わないが、次の論文では $\mathbf{R}$ を代数的実 Puiseux ベキ級数体に代えるという方法を使う。そのため、そこは代数的実 Puiseux ベキ級数体を詳しく見る。

定義 3. R を順序体とする。R^n の部分集合 X が準代数的であるとは、有限個の R^n で定義された多項式関数 f_{ij} があり、$X=\cup_i \cap_j \{x \in R^n : f_{ij}(x) *_{ij} 0\}$ となること。ただし $*_{ij}$ は $=$ または $>$ を意味する。

3. 証明の準備—ARTIN-LANG の定理

X を $\mathbf{R}^n \times \mathbf{R}$ の準代数的集合とし、$p: \mathbf{R}^n \times \mathbf{R} \to \mathbf{R}^n$ を射影とする。すると $p(X)$ は $\mathbf{R}^n$ で準代数的集合となることは、広く知られている。実はもう少し詳しく分かっていて、それは Tarski-Seidenberg の定理と呼ばれている。その証明は長くはなく、定理は今の議論に本質的であるが、証明は constructive であるという以外は面白くないので省略する。読みたい人は [1] か [3] をどうぞ。一般に証明が constructive にできるかどうかは大変重要である。なぜなら、ある実閉体上である問題が constructive に証明できたら、その問題はどんな実閉体でもなりたつ。これを Tarski-Seidenberg principle という。しかし、constructive な証明は読んで面白くない。だから省略する。この論文では、明ら

かでないのに証明を省略するのは、この定理のみで、ほかは証明する。証明しないのがあれば、それは証明が容易であるからである。

定理 (**Tarski-Seidenberg**). 有限個の f_{ij} を $(x,y)=(x_1,\dots,x_n,y)$ 変数整数係数多項式関数とする。$*_{ij}$ を $=$ または $>$ を意味するとする。すると有限個の x 変数整数係数多項式関数 g_{ij} と $*'_{ij}\in\{=,>\}$ とが存在して次の条件を満たす。R を任意の実閉体とし、$p:R^n\times R\to R^n$ を射影とする。すると

$$p(\cup_i\cap_j\{(x,y)\in R^n\times R: f_{ij}(x,y)*_{ij}=0\})=\cup_i\cap_j\{x\in R^n: g_{ij}(x)*'_{ij}=0\}$$

が成り立つ。

証明では g_{ij} は f_{ij}, $\frac{\partial f_{ij}}{\partial y}$, $\frac{\partial^2 f_{ij}}{\partial y^2},\dots$ から y を constructive に消去して作る。大事なことは g_{ij} は R によらないことである。ここがこの話の本質的なところである。なお R が実閉体でないと定理は成り立たない。例えば $\{(x,y)\in\mathbf{Q}^2: x-y^2=0\}$ は準代数的であるが、それを x 軸に射影すると 2 乗根が有理数になる有理数全体になり $\mathbf{Q}$ の中で準代数的ではない。この定理を使いやすくしたのが次の定理である。

定理 (**Artin-Lang**). $R_1\subset R_2$ を実閉体とし、$x=(x_1,\dots,x_n)$ を変数とし、$f_{ij}(x)\in R_1[x]$, $*_{ij}\in\{=,>\}$ とする。$X=\cup_i\cap_j\{x\in R_1^n: f_{ij}(x)*_{ij}=0\}$ とおく。f_{ij} を R_2^n に自然に拡張したものを f_{ijR_2} と書き、$X_{R_2}=\cup_i\cap_j\{x\in R_2^n: f_{ijR_2}(x)*_{ij}=0\}$ とおく。すると

$$X_{R_2}\neq\emptyset\Longrightarrow X\neq\emptyset$$

となる。

注意. 上で X_{R_2} と書くのはおかしい。定義からは、X_{R_2} は R_2 と X によって決まるものとはいえなく、R_2 と f_{ij} と $*_{ij}$ によって決まるものである。正確には $X_{R_2,f_{ij},*_{ij}}$ と書くべきである。しかしこの定理を仮定すれば f_{ij} と $*_{ij}$ によらないことが分かる。だから X_{R_2} と書く。実代数幾何学は環論に頼らずに、うまくいく。

証明. n に関する帰納法で証明する。$n=0$ のときは明らか。そこで $n-1$ で成り立つとする。そのとき n で証明したい。$(x',x_n)=(x_1,\dots,x_n)$ と書く。$p_1:R_1^{n-1}\times R_1\to R_1^{n-1}$ と $p_2:R_2^{n-1}\times R_2\to R_2^{n-1}$ を射影とする。

もし f_{ij} の係数が整数なら Tarski-Seidenberg の定理より x' 変数整数係数多項式関数 g_{ij} と $*'_{ij}$ が存在して

$$p_1(X)=\cup_i\cap_j\{x'\in R_1^{n-1}: g_{ij}(x')*'_{ij}=0\},$$

$$p_2(X_{R_2})=\cup_i\cap_j\{x'\in R_2^{n-1}: g_{ij}(x')*'_{ij}=0\}$$

となる。よって、$(p_1(X))_{R_2}=p_2(X_{R_2})$。ゆえに $X_{R_2}\neq\emptyset$ なら $p_2(X_{R_2})=(p_1(X))_{R_2}\neq\emptyset$。ゆえに帰納法の仮定から $p_1(X)\neq\emptyset$。よって $X\neq\emptyset$。

f_{ij} の係数が整数でないときは Tarski-Seidenberg の定理を次のように少しだけ一般化し、それを同様に使えば良い。 □

定理 (**Artin-Lang**)′. R_1 を実閉体とし、$f_{ij}(x,y)$ を $(x_1,\dots,x_n,y)$ 変数 R_1 係数多項式関数とし $*_{ij}\in\{=,>\}$ とする。すると $(x_1,\dots,x_n)$ 変数 R_1 係数多項式関数 $g_{ij}(x)$ と

$*'_{ij} \in \{=, >\}$ が存在して、等式

$$p(\cup_i \cap_j \{(x,y) \in R^n \times R : f_{ij}(x,y) *_{ij} = 0\}) = \cup_i \cap_j \{x \in R^n : g_{ij}(x) *'_{ij} = 0\}$$

がどんな R_1 を含む実閉体 R でいえる。

証明. f_{ij} の係数をすべて順序を決めて並べたのを $a \in R_1^m$ とおき、f_{ij} の中で、a を m 変数 z で置き換えたのを $F_{ij}(x,y,z)$ とおく。すると F_{ij} は (x,y,z) 変数整数係数多項式関数になり、$F_{ij}(x,y,a) = f(x,y)$ となる。F_{ij} と $*_{ij}$ に Tarski-Seidenberg の定理を当てはめると、(x,z) 変数整数係数多項式関数 G_{ij} と $*'_{ij}$ が存在して、どんな実閉体 R に対して

$$q(\cup_i \cap_j \{(x,y,z) \in R^n \times R \times R^m : F_{ij}(x,y,z) *_{ij} = 0\})$$
$$= \cup_i \cap_j \{(x,z) \in R^n \times R^m : G_{ij}(x,z) *'_{ij} = 0\}$$

となる。ただし $q : R^n \times R \times R^m \to R^n \times R^m$ は射影。特に R^m が a を含めば、すなわち a の各成分を R が含めば、この式に $z = a$ を代入し、等式

$$p(\cup_i \cap_j \{(x,y) \in R^n \times R : f_{ij}(x,y) *_{ij} = 0\}) = \cup_i \cap_j \{x \in R^n : G_{ij}(x,a) *'_{ij} = 0\}$$

がいえる。ゆえに $g_{ij}(x) = G_{ij}(x,a)$ とおけば良い。 □

4. HILBERT の第１７問題の証明

定理 (Hilbert の第１７問題). f を $\mathbf{R}^n$ 上の多項式関数で $\mathbf{R}^n$ のあらゆる点で負にならないとする。すると多項式関数 $f_1, \ldots, f_k, g \neq 0$ が存在して、$fg^2 = \sum_{i=1}^k f_i^2$ となる。

証明. ここまで来ると証明は簡単である。f_i, g が存在しないと仮定する。R を $\mathbf{R}^n$ 上の有理関数全体の体とする。$X = \{\sum_{i=1}^l a_i^2 : a_i \in R,\ l \in \mathbf{Z}\}$ と置く。すると f は X に属さない。ゆえに、注意５より R に順序が入り順序体になり $f < 0$ となる。すると注意６より R を部分順序体とする実閉体 $\tilde{R}$ が存在して、$\tilde{R}$ の順序で $f < 0$ となる。$\tilde{R}$ 係数一変数多項式環 $\tilde{R}[t]$ を考える。$t^2 + 1/f \in \tilde{R}[t]$ になる。注意３より、$\tilde{R}[i]$ は代数的閉体なので、$t^2 + 1/f = (t+h)(t-h)$ または $t^2 + 1/f = (t+ih)(t-ih)$ となる $\tilde{R}$ の元 h が存在する。もし $t^2 + 1/f = (t+h)(t-h)$ なら $t^2 + 1/f = t^2 + h^2$。ゆえに $1/f = h^2 > 0$。ゆえに注意５より $f > 0$ となり矛盾。よって $t^2 + 1/f = (t+ih)(t-ih)$ である。ゆえに $fh^2 + 1 = 0$。ここで Artin-Lang の定理を使いたい。$F(x,t) = f(x)t^2 + 1$ と置く。$F(x,t)$ は $\mathbf{R}$ 係数 $n+1$ 変数多項式関数。$\tilde{R}^{n+1}$ 上で F を考える。すなわち $F_{\tilde{R}}(y,z)$ を考える。ただし $y = (y_1, \ldots, y_n), z$ は新しい変数。すると $F_{\tilde{R}}(x, h(x)) = 0$。ここで x も $h(x)$ も $\tilde{R}$ の元で x は変数ではない。ゆえに $F_{\tilde{R}}^{-1}(0) \neq \emptyset$。ゆえに Artin-Lang の定理より $F^{-1}(0) \neq \emptyset$。すなわち実数 $a_1, \ldots, a_n, b$ が存在して、$F(a_1, \ldots, a_n, b) = 0$。ゆえに $f(a_1, \ldots, a_n)b^2 + 1 = 0$。よって $f(a_1, \ldots, a_n) < 0$。矛盾。 □

もちろん上の定理は一般の実閉体で成り立つ。また定理の中の k は n と f の次数によってどのように決まるかとか、$g = 1$ と制限するのは無理であるとか、いろいろ分かっている。しかし私には面白いとは思えないので、述べない。

上の証明と同じようにして次の定理は容易に証明できる。

名古屋大学多元数理科学研究科　塩田昌弘

定理 (零点定理の実閉体の場合). R を実閉体とし、$\mathfrak{p}$ を $R[x]=R[x_1,\ldots,x_n]$ のイデアルとし X を $\mathfrak{p}$ の元の共通零点とする。すると等式

$$\{f\in R[x]:\forall x\in X,\ f(x)=0\}$$
$$=\{f\in R[x]:\exists m\in\mathbf{N}\exists f_1,\ldots,f_l\in R[x],\ f^{2m}+\sum_{i=1}^{l}f_i^2\in\mathfrak{p}\}$$

が成り立つ。

これは代数的閉体のときと大変違う。もし R が代数的閉体のとき

$$\{f\in R[x]:\forall x\in X,\ f(x)=0\}=\{f\in R[x]:\exists m\in\mathbf{N},\ f^m\in\mathfrak{p}\}$$

となり、それは Hilbert の零点定理と呼ばれている。Hilbert の零点定理は大変役に立つが、この実閉体の場合の定理はそれほど役立っていない。少なくとも実代数的集合の研究に役立っていない。その理由はイデアル $\mathfrak{p}$ とイデアル $\{f\in R[x]:\exists m\in\mathbf{N},\ f^m\in\mathfrak{p}\}$ を比べたときと違って、イデアル $\mathfrak{p}$ とイデアル $\{f\in R[x]:\exists m\in\mathbf{N}\exists f_1,\ldots,f_l\in R[x],\ f^{2m}+\sum_{i=1}^{l}f_i^2\in\mathfrak{p}\}$ があまりに違い、代数的な共通点がないからである。例えば $\mathfrak{p}$ を $1+x_1^2$ で生成されたイデアルとすれば、後者は $R[x]$ 全体になる。だからイデアルとその共通零点と、うまく対応がつかないといえる、少なくての普通の代数幾何学から見て。

References

[1] J. Bochnak, M. Coste and M. F. Roy, *Real Algebraic Geometry*, Springer, 1998.

[2] 永田 雅宜、可換体論、裳華房、1967.

[3] A. Seidenberg, *A new decision method for elementary algebra*, Ann. of Math. 60 (1954), 365-374.

E-mail address: shiota@math.nagoya-u.ac.jp