ガロア理論 12 講　ノート

NS

2023 年 11 月 18 日

序章：ガロア理論とは何か

方程式論のが歴史を概観する。具体的な 1-4 次の解の公式が記述される。5 次は見つからず、ラグランジュ、ルフィニ、アーベルが頑張った経緯など。

お気持ちというよりは事実の列挙なので、ガチ初心者にとっては意味不明な記述が多い。

いくつか注目したい記述はある：

> ガロアはラグランジュによって見出された「根の置換」による方程式論のアイデア、すなわち方程式に隠された「対称性」から、解法の可能性を解析するという新しい、そして極めて現代的な視点を打ち出した。つまり、「何かについての対称性」という見方から脱却して、対称性そのものの構造の中に重要な鍵が隠されていることを見出したのである。これが現代数学における群という考え方に繋がっている。

あとの知識から振り返ると、「根の置換」だけに注目するのではなく、**有理数並びにそれを拡大した体上での自己同型（自分自身への同型写像）全体を考えよう**という発想が慧眼だ、という話な気がする。

1　複素数と方程式

1.1　概要

代数の入門（体、複素数、多項式の定義および性質など）から始めている。すでに知っている人は飛ばし読みできるが、ちょこちょこハッとする記述はある。ハイライトは拡大と最小多項式の定義・性質の理解。振り返ってみると、以降の章で使い倒している。

標準的物理学徒は学ばない数学（大学数学の学部生程度の知識）も必要最小限準備されている。（好感度＋＋）

■部分体・拡大体・中間体　体 K が体 L の部分体とは、L の演算が体 K の和と積で L 内に閉じることをいう。

これ自体は部分群、部分環などほかの代数構造と同じ使い方だが、体の場合だけ、自身を含む大きい体のことを**拡大体**と特別に呼称する。（なんでだ？）

具体例: $\mathbb{C}/\mathbb{R}, \mathbb{R}/\mathbb{Q}, \mathbb{Q}(\sqrt{2})/\mathbb{Q}$

■多項式　高校までの多項式の定義は何だったか全く思い出せないが、ここで改めて定義しよう。特に重要なのは係数に何が許されるかを指定すること。

Definition 1. K 係数の多項式とは、K とシンボル x が生成する環のこと。記号では $K[x]$ と書く。

多項式 $f \in K[x]$ には代入という操作が定義される。a を f に代入するとは、x を $a \in K$ に書き換え、x の和・積をすべて K 上の和・積に移す操作のことである。このようにして置き換えた値を $f(a)$ と書く。

「K 上の」という定義が重要な理由は、基本的には解がどの集合に属すかを議論するためではあるが、**どこまで体を拡大すれば解があるのか**という問いを立てられるのが本質的である。

整数係数の多項式（環上の多項式だが）1 変数の場合は代数学の基本定理によって、複素数体まで拡大すれば必ず解があることがわかるのだが、最小限どこまで拡大しなければならないか（このような拡大体を「最小分解体」と呼ぶ）の議論が本質的になってくる。

1.2　注目ポイント

■冪根の添加による拡大が体になることの証明　高校で習った「分母の有理化」の真髄がここにある。つまり、添加した元の逆元は拡大体の元でかけるよという話。

$$(a+b\sqrt{c})^{-1} = \frac{a-b\sqrt{c}}{a^2-b^2c} \tag{1}$$

Proof. $a, b \in \mathbb{Q}$ とすれば、「逆元」の分母である $a^2 - b^2c$ が 0 でないことを示さなければならない。

分母が 0 となる条件を書き直していくと、

$$a^2 - b^2c = 0 \tag{2}$$

$$\frac{a^2}{b^2} = c \tag{3}$$

$$\left(\frac{a}{b}\right)^2 = c \tag{4}$$

ところで、c へ平方数でない正の整数であるべきだ。でないと $\sqrt{c}$ は有理数になるので、拡大体 $\mathbb{Q}(\sqrt{\ })$ は $\mathbb{Q}$ 自体になる。

この条件は分母が 0 とならないための条件と一致している。証明終了。　□

なぜ有理化すべきなのか、高校の先生に聞いた記憶があるが、明確な答えはなかった。まあ、中学生に向かって有理数の拡大が体となることが重要！　だなんて説明すべくもないとは思うが。

複素数が体になることも証明できるが、その時は分母が $a^2 + b^2$ なので証明は自明だった。

ここら辺で、何等かの共通点を感じる人も多いはず。実際、あとでてくる「共役」という概念が共通している。最小多項式の概念を使わないと述べられないので後回しにする。

2　体の代数拡大

2.1　概要

多項式論の基本から丁寧に展開する章。内容的には高校数学で刷り込まれているものが多いが、ちょこちょこ新しい用語や概念が登場するのが見どころ。また、著者の癖なのか代数幾何の話が始まってもおかしくない

ような論理展開も見える。

体の代数拡大、最小多項式、などの基本概念をそろえていく章。

- 定義：既約・可約
- 定理：解をもつ＝因数がある（代数幾何で使う考え方）
- 定理：アイゼンシュタインの可約判定法
- 定義：代数的な元
- 定義：最小多項式（性質から定義）
-

2.2 注目ポイント

■代数的な元 K 上の代数方程式 $f(x)=0$ の解が K に解を持つとは限らないことは散々知っている。たとえば整数環 $\mathbb{Z}$ 上の多項式は当然そうだし、

$$f(x)=-1+2x\in\mathbb{Z}[x]\to f(x)=0\leftrightarrow x=\frac{1}{2}\notin\mathbb{Z} \tag{5}$$

べき乗根が満たす方程式とかもそう：

$$f(x)=-2+x^2\in\mathbb{Q}[x]\to f(x)=0\leftrightarrow x=\sqrt{2}\notin\mathbb{Q}. \tag{6}$$

K 上の代数方程式 $f(x)=0$ の解 α が K からはみだして拡大体 E/K の元になっているとする。K 上の代数方程式の解になってる元だよ、という意味を込めて $\alpha\in E/K$ は K 上代数的であると称する。

■最小多項式 代数方程式 $f(x)=0$ の解 α が元の体の元である $(\alpha\in K)$ 場合、その多項式 f は $(x-a)\in K[x]$ という因数をもっていた。（因数定理の主張）言い換えれば、f の解は f の形をかなり制約する。ちなみに、この事実は解という数 $\alpha\in K$ と多項式 $(x-\alpha)\in K[x]$ がなんらか対応していることを意味している。（これを突き詰めるところから代数幾何が始まる）

では、その解が元の体からはみでている場合も含めると (つまり α は K 上代数的な元だと)、f の形にはどのような制約が入るだろうか？たとえば $f(x)=-1+x^2$ の場合は $f(x)=(x-\sqrt{2})g(x)$ のような形で因数分解できない。（実数の範囲ではできるが、これは $K[x]$ 上の多項式ではない！）じゃあ何の手掛かりもないか、というとそういうわけではないよというのが「最小多項式」である。