体論要約 NO.6

今日のテーマ: **既約性の判定**

今回は少しガロア理論の本筋からは外れる。これまで、個々の例の多項式の既約性について証明なしに議論してきたが、だんだん不自由になってきたのでここでまとめておくことにする。

代数についてよく学びたい人のための注: 今回の議論は $\mathbb{Z}$ とその商体 $\mathbb{Q}$ に関してのべるが、一般の UFD R とその商体 $K = Q(R)$ に関しても同様なことが成り立つ。

次の命題は多項式の既約性判定の際に整数係数と有理係数の差をうまく処理してくれる:

命題 6.1. $\mathbb{Z}$ 上の多項式 $f(X) \in \mathbb{Z}[X]$ が $\mathbb{Q}$ 上で可約ならば、$\mathbb{Z}$ 上でも可約である。

証明には「ガウスの補題」を用いる。その説明のためにひとつ言葉を用意しておこう。

定義 6.2. $\mathbb{Z}$ 上の多項式 $f(X) \in \mathbb{Z}[X]$ が**原始的**であるとは f の係数のすべてを割るような整数が ± 1 しかないときにいう。言い換えると、原始的多項式とは係数の gcd が 1 の多項式である。

補題 6.3 (ガウス)**.** 原始多項式 $f, g \in \mathbb{Z}[X]$ の積 fg はまた原始的である。

命題 6.4. 多項式 $h \in \mathbb{Z}[X]$ が多項式 $f, g \in \mathbb{Z}[X]$ の積の時、

(1) h の定数項は f の定数項と g の定数項の積である。
(2) h の最高次の係数は f の最高次の係数と g の最高次の係数との積である。

とくに、モニックな $\mathbb{Z}[X]$ の多項式がもし可約ならばそれはモニックな因数を持つ。

命題 6.5. 体 K 上の 3 次もしくは 2 次の多項式 $f \in K[X]$ について、f が K の中に根を持たなければ f は K 上既約である。

定理 6.6 (アイゼンシュタイン)**.** $\mathbb{Z}$ を係数にもつモニックな

$$f(X) = X^k + a_{k-1}X^{k-1} + a_{k-2}X^{k-2} + \cdots + a_0$$

が、ある素数 p に対して、次の二つの性質をもつとする。

(1) $f(X) \equiv X^k \pmod{p}$
(2) $f(X)$ の定数項は p^2 で割り切れない。

このとき、f は $\mathbb{Q}$ 上既約である。

次のこともよく用いる。

定理 6.7. 任意の $f \in k[X]$ と任意の定数 $c \in k$ に対して、
$f(X)$ が既約 $\Leftrightarrow$ $f(X + c)$ が既約.

定理 6.8. モニックな整係数多項式 $f(X) \in \mathbb{Z}[X]$ が与えられているとする。ある素数 p に対して f が $\mathbb{Z}/p\mathbb{Z}$ 係数の多項式として既約なら、f は $\mathbb{Q}[X]$ の元として既約である。

問題 6.1. $X^2 - 6$ は $\mathbb{Q}$ 上既約であることを示しなさい。(今回はもちろん $\sqrt{6}$ が無理数であることを使ってはならない。)

問題 6.2. $X^3 - X - 1$ は $\mathbb{Q}$ 上既約であることを示しなさい。

[根と解] 体 一変数多項式 $f(X)$ を

$$f(X) = c(X - \alpha_1)(X - \alpha_2)\dots(X - \alpha_d)$$

と因数分解したとき、$\alpha_1, \dots, \alpha_d$ のことを f **の根**と呼ぶ。

- $\alpha_1, \dots, \alpha_d$ 自身は K の元でなくても、K の適当な拡大体 (分かりやすいのは、$K \subset \mathbb{C}$ のときの $\mathbb{C}$ や、K の代数的閉包 (後述) $\bar{K}$) の元でよい。
- 重複はその分も込めて考える。

$f(c) = 0$ を満たす $c \in K$ を $f(X) = 0$ の (K 上の) 解と呼ぶ。

6.1. いくつかの多項式の既約性 (例).

6.1.1. 用いること. 次のことはよく用いる。

命題 6.9. $f(X) \in \mathbb{Z}[X]$ が $\mathbb{Z}$ 上で可約なら、任意の素数 p に対し、$f \mod p$ は $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ 上可約である。

たとえば次のような $\mathbb{Z}[X]$ の元の因数分解を考えよう。

$$X^5 + 2X^4 + 7X^3 + 3X^2 + 2X - 15 = (X^3 + 4X - 5)(X^2 + 2X + 3)$$

(先に言葉の注意をしておく。これは環論的に言えば $\mathbb{Z}[X]$ での因数分解とも言えるし、多項式の言葉で言えば $\mathbb{Z}$ 上の因数分解と言っても良い。) これはそのまま素数 p に依存して定義される剰余環 $\mathbb{Z}/p\mathbb{Z}$ での因数分解とも考えられる。整数 k の $\mathbb{Z}/p\mathbb{Z}$ でのクラスを $[k]_p$ と書くと、

$$[1]_pX^5+[2]_pX^4+[7]_pX^3+[3]_pX^2+[2]_pX-[15]_p = ([1]_pX^3+[4]_pX-[5]_p)([1]_pX^2+[2]_pX+[3]_p)$$

これが命題 6.9 の意味である。(実際には p は素数でなくても整数であれば構わない。しかし p が素数ならば $\mathbb{Z}/p\mathbb{Z}$ が体であるという利点があるので以下では主に p が素数の場合をかんがえよう。$\mathbb{Z}/p\mathbb{Z}$ は体なので $\mathbb{F}_p$ とも書くのであった。)

この分解についてもう少し考えてみる。 $\mathbb{Z}/3\mathbb{Z}$ では

$$[1]_3X^5+[2]_3X^4+[7]_3X^3+[3]_3X^2+[2]_3X-[15]_3 = ([1]_3X^3+[4]_3X-[5]_3)([1]_3X^2+[2]_3X+[3]_3).$$

$\mathbb{Z}/3\mathbb{Z}$ の元は $[0]_3, [1]_3, -[1]_3$ のどれかに等しいから書き換えると:

$$[1]_3X^5 - [1]_3X^4 + [1]_3X^3 - [1]_3X = ([1]_3X^3 + [1]_3X + [1]_3)([1]_3X^2 - [1]_3X)$$

$[1]_3$ のことは 1 と書いてしまえば、$\mathbb{F}_3 = \mathbb{Z}/3\mathbb{Z}$ 上で考えているという注釈 ($/\mathbb{F}_3$ と略記することで以下では表現する) のもとで

$$X^5 - X^4 + X^3 - X = (X^3 + X + 1)(X^2 - X) \qquad (/\mathbb{F}_3)$$

同様に、同じような注釈を書き加えておけば、

$$X^5 + 2X^4 + 2X^3 + 3X^2 + 2X = (X^3 - X)(X^2 + 2X + 3) \qquad (/\mathbb{F}_5)$$
$$X^5 + 2X^4 + 3X^2 + 2X - 1 = (X^3 - 3X + 2)(X^2 + 2X + 3) \qquad (/\mathbb{F}_7)$$
$$X^5 + 2X^4 - 4X^3 + 3X^2 + 2X - 4 = (X^3 + 4X - 5)(X^2 + 2X + 3) \qquad (/\mathbb{F}_{11})$$

を得る。もっとも、

$$X^5 + 2X^4 + 7X^3 + 3X^2 + 2X - 15 = (X^3 + 4X - 5)(X^2 + 2X + 3) \qquad (/\mathbb{F}_p)$$

と書いておけばすべての素数 p についていっぺんに書くことができるわけだが。

命題 6.9 の対偶をとると次の命題を得る。

命題 6.10. ある素数 p について $f \mod p$ が $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ 上既約ならば、$f(X) \in \mathbb{Z}[X]$ は $\mathbb{Z}$ 上で既約である。

6.1.2. 問題.

問題 6.3. $f_1(X) = X^2 - 6$ は $\mathbb{Q}$ 上既約である。

(略解 1) [$\mathbb{Z}$ 上に帰着] ガウスの補題により、 $\mathbb{Z}$ 上既約であることをいえばよい。もし $X^2 - 6$ が $\mathbb{Z}$ 上可約であれば、次数の関係を考えると、一次式の積に分解する他はないことがわかる。最高次の係数を比べることにより、それらの一次式は (符号の調整後) モニックであることがわかるから、

$$X^2 - 6 = (X - a)(X - b) \qquad (\exists a, b \in \mathbb{Z})$$

さらに、一次の項をくらべれば、$b = -a$ であって、

$$a^2 = 6$$

これを満たす整数 a は存在しない (大きさの比較により、$|a| < 10$ で、あとは全数調査。もちろんもっと効率的な方法でもよい。)

(略解 2) ガウスの補題により、 $\mathbb{Z}$ 上既約であることをいえばよい。それには $\mathbb{F}_7 = \mathbb{Z}/7\mathbb{Z}$ で既約であることを言えば十分。$\mathbb{F}_7$ では $a = 0, \pm1, \pm2, \pm3$ に対して、$a^2 = 0, 4, 9 = 2$ であるから、$X^2 - 6$ の根は $\mathbb{F}_7$ の中にはない。

問題 6.4. $f_2(X) = X^3 - X - 1$ は $\mathbb{Q}$ 上既約である。

(略解 1) [$\mathbb{Z}$ 上に帰着]
ガウスの補題により、 $\mathbb{Z}$ 上既約であることをいえばよい。
もし $X^3 - X - 1$ が $\mathbb{Z}$ 上可約であれば、

$$(X^3 - X - 1) = a(X) \cdot b(X)$$

となる $a, b \in \mathbb{Z}[X]$ で、定数でないものが存在する。次数の関係により、a, b のうち一方は 1 次式、もう一方は 2 次式であり、さらに係数の関係により、

$$(X^3 - X - 1) = (X - c)(X^2 + aX + b) \qquad (\exists a, b, c \in \mathbb{Z}).$$

再び係数の関係により、c は 1 の約数、すなわち $\{\pm1\}$ の元でなければならない。$f_2(c) = 0$ でなければならないが、それは不可能。
(略解 2)[$\mathbb{Z}/3\mathbb{Z}$ 上に帰着]
ガウスの補題により、 $\mathbb{Z}$ 上既約であることをいえばよい。そのためには、$\mathbb{F}_3 = \mathbb{Z}/3\mathbb{Z}$ 上既約ならば十分である。$f_2(X)$ は $\mathbb{F}_3$ に根をもたないことがわかるから、f_2 は $\mathbb{F}_3$ 上既約である。(根をもたない 2 次 or 3 次の多項式は既約。)

問題 6.5. $f_3(X) = X^5 - X - 1$ は $\mathbb{Q}$ 上既約である。

(略解)[$\mathbb{Z}/5\mathbb{Z}$ 上に帰着:$X \mapsto X + 1$ に関する不変性を使う]
ガウスの補題により、 $\mathbb{Z}$ 上既約であることをいえばよい。
それには ($f \mod 5$ が) $\mathbb{F}_5$ 上既約であることを示せば十分である。以下 $\mathbb{F}_5$ で議論する。

$$\begin{aligned} f_3(X + 1) &= X^5 + 5X^4 + 10X^3 + 10X^2 + 5X + 1 - (X - 1) - 1 \\ &= X^5 - X - 1 = f_3(X) \qquad (/\mathbb{F}_5) \end{aligned}$$

であるから、

$$f_3(X + 1) = f_3(X) \qquad (/\mathbb{F}_5) \tag{6.1}$$

であることに注意しておく。$f_3(0) = -1 \neq 0$ であることから、(6.1) 式により、

$$f_3(0) = f_3(1) = f_3(2) = f_3(3) = f_3(4) = -1 \neq 0 \qquad (\text{in } \mathbb{F}_5)$$

言い換えると、$\mathbb{F}_5$ 上では f_3 は 1 次の因子をもたない。$f_3(X)$ が仮に 2 次の既約因子 $a(X)$ を持つとする。$a(X)$ はモニックであると仮定してよい。(6.1) 式により、$f_3(X)$ は $a(X+1)$ をも既約因子に持つ。同様にして、

$$a(X), a(X + 1), a(X + 2), a(X + 3), a(X + 4)$$

はすべて f_3 の 2 次の既約因子であることがわかる。素因子分解の一意性と、これらがモニックであることとにより、これら 5 つの多項式のうち少なくとも 2 つは等しい。

$$a(X + i_1) = a(X + i_2) \qquad (\exists i_1, i_2 \in \mathbb{F}_5, i_1 \neq i_2)$$

このことはじつは $a(X+i) \quad (i \in \mathbb{F}_5)$ がすべて等しいことを意味している。(演習問題: $\mathbb{F}_5$ は加法的に $(i_2 - i_1)$ で生成されることを用いる。) とくに

$$a(X + 1) = a(X).$$

このような $\mathbb{F}_5$ 上の 2 次式は存在しない。(練習問題)
(略解 2) [$\mathbb{Z}/3\mathbb{Z}$ 上に帰着:コンピュータを使い全数調査] ガウスの補題により、 $\mathbb{Z}$ 上既約であることをいえばよい。それには ($f_3 \mod 3$ が) $\mathbb{F}_3$ 上既約であることを示せば十分である。以下 $\mathbb{F}_3$ で議論する。$f_3(0) = -1 \neq 0, f_3(1) = -1 \neq 0, f_3(-1) = -1 \neq 0$ であるから、f_3 は $\mathbb{F}_3$ 上 1 次の因数をもたない。

$$f_3(X) = (X^2 + aX + b)(X^3 + cX^2 + dX + e)$$

がなりたつような $a,b,c,d,e \in \mathbb{F}_3$ を機械で総当りに求めると、そのようなものは存在しないことがわかる。(総当りに必要な組み合わせは 3^5 とおり。) よって f_3 は既約である。

後半は次のように処理すると計算をかなり減らせる: $f_3(X)$ を X^2+aX+b で割った余り

$$(b^2+a^4-1)X-2ab^2+a^3b-1$$

の a,b の値として $\mathbb{F}_3$ のどれをとっても 0 にはならない。(a,b の値の選び方は $3^2=9$ とおり。このぐらいならうまく整理しながらやれば人間でも可能。)