東海大学紀要情報通信学部
Vol.14,No.1,2021,pp.17-24

トピックス

大学初年次における数学教材の提案（その 36）
～ 既約多項式 ～

貴田 研司[*1]

A Suggestion on Mathematical Materials for Freshman Education Vol.36
~ Irreducible Polynomial ~

by

Kenshi KIDA[*1]

(received on May. 28, 2021 & accepted on Aug. 3, 2021)

あらまし

本論文においては既約多項式に関する話題として，アイゼンシュタインの基準による既約性の判定方法，そして元の個数が素数である体の上の既約多項式の個数について述べる．

Abstract

In this paper, we give explanation of items for irreducible polynomials. We present specially Eisenstein's Criterion and the number of irreducible polynomials over the finite field of order prime.

キーワード：既約多項式，メービウスの反転公式，有限体，アイゼンシュタインの基準
Keywords: *Irreducible Polynomial, Möbius Inversion Formula, Finite Field, Eisenstein's Criterion*

1. はじめに

$\mathbb{Z}[x]$における多項式の既約性についての判定法として知られるアイゼンシュタインの基準について，R. Singer による証明と係数が一意分解整域のときに拡張された場合について述べる．

一方，$\mathbb{Z}_p[x]$の既約多項式の個数の求め方にも言及するが，その中で

メービウス（Möbius）の反転公式

$$F(n)=\sum_{d|n} f(d)$$

であるならば

$$f(n)=\sum_{d|n} \mu\left(\frac{n}{d}\right) F(d).$$

が重要な役割を演じることにも注目されたい．ただし，$\mu(m)$は，メービウス（Möbius）関数と呼ばれる（整）数論的関数である．

本論文の執筆にあたって，増田真郎「応用のための代数系入門」[1]が大いに役に立った．その他にも多くの好著を参考にさせていただいた[2)3)4)5)6)7)]．

*1 スチューデントアチーブメントセンター
（高輪教養教育センター） 教授
Student Achievement Center
(Liberal Arts Education Center, Takanawa Campus), Professor

2. アイゼンシュタインの基準

定理 2.1（アイゼンシュタインの基準）

n次多項式

$$f(x) = a_0 + a_1x + \cdots + a_nx^n, \qquad (a_i \in \mathbb{Z}\ )$$

に対して，ある素数p が存在して

$$p \nmid a_n, \quad p|a_j \ \ (j = 0,1,\cdots,n-1), \quad p^2 \nmid a_0$$

であるならば，$f(x)$ $\mathbb{Z}[x]$おいて既約である．

（証明）［R. Singer］[6)7)]

環準同型$r_p : \mathbb{Z}[x] \to \mathbb{Z}_p[x]$を

$$\mathbb{Z}[x] \ni \varphi(x) = k_0 + k_1x + \cdots + k_mx^m \mapsto \overline{k_0} + \overline{k_1}x + \cdots + \overline{k_m}x^m = \bar{\varphi}(x) \in \mathbb{Z}_p[x], \quad \overline{k_t} = k_t + (p) \in \mathbb{Z}_p,$$

$$\left(\text{ただし，}\ \overline{k_t} = k_t + (p) \in \mathbb{Z}_p, \quad t = 0,1,\cdots,m\right)$$

によって定義する．

もしも$f(x)$ が$\mathbb{Z}[x]$ において既約ではないと仮定すれば，$\mathbb{Z}[x]$ の多項式

$$g(x) = b_0 + b_1x + \cdots + b_mx^m, \quad h(x) = c_0 + c_1x + \cdots + c_kx^k, \quad n = m + k$$

が存在して，$f(x) = g(x)h(x)$が成り立つ．これにr_p を施すと$p \nmid a_n, \quad p|a_j \ \ (j = 0,1,\cdots,n-1)$ により

$$\bar{f}(x) = \overline{a_n}x^n = \bar{g}(x)\bar{h}(x) \qquad (\overline{a_n} \neq \bar{0} \in \mathbb{Z}_p)$$

となる．すると，$\mathbb{Z}_p[x]$ における素因子分解の一意性により，ある$\mathbb{Z}_p \ni u, v \neq \bar{0}$（すなわち，$\mathbb{Z}_p$の単数）が存在して

$$\bar{f}(x) = \overline{a_n}x^n = ux^m \cdot vx^k$$

となることから

$$\bar{g}(x) = ux^m, \ \bar{h}(x) = \ vx^k$$

であり，$\bar{g}(x)$ の定数項$\overline{b_0} = \bar{0}$，そして$\bar{h}(x)$の定数項$\overline{c_0} = \bar{0}$ となる．これは$p|b_0$かつ$p|c_0$ と同値である．

したがって，$p^2|a_0 = b_0c_0$ となり矛盾が生じることから，$f(x)$ は$\mathbb{Z}[x]$ において既約である．

（証明終）

例 1

$2x^5 + 15x^3 + 9x^2 + 3$ は，アイゼンシュタインの基準において$p = 3$ と取れば，$\mathbb{Z}[x]$ において既約であることがわかる．

例 2

任意の素数p に対して，x^s+pおよびx^s-pは，$\mathbb{Z}[x]$ において既約である．

例 3

$f(x)=x^3-4$ は$\mathbb{Z}[x]$ において既約である．

（証明）

不定元の変換を行った $f(y+1)=(y+1)^3-4=y^3+3y^2+3y-3$ は，アイゼンシュタインの基準において$p=3$ と取れば，$\mathbb{Z}[y]$ において既約であることがわかる．したがって，$f(x)$ は$\mathbb{Z}[x]$ において既約である．

（証明終）

例 4

$f(x)=x^4+1$ は$\mathbb{Z}[x]$ において既約である．

（証明）

不定元の変換を行った $f(y+1)=(y+1)^4+1=y^4+4y^3+6y^2+4y+2$ は，アイゼンシュタインの基準において $p=2$ と取れば，$\mathbb{Z}[y]$ において既約であることがわかる．したがって，$f(x)$ は$\mathbb{Z}[x]$ において既約である．

（証明終）

例 5（円周等分多項式）

$f(x)=x^2+x+1$ は，$\mathbb{Z}[x]$ において既約である．

（証明）

不定元の変換を行った $f(y+1)=(y+1)^2+(y+1)+1=y^2+3y+3$ は，アイゼンシュタインの基準において$p=3$ と取れば，$\mathbb{Z}[y]$ において既約であることがわかる．したがって，$f(x)$ は$\mathbb{Z}[x]$ において既約である．

（証明終）

例 6（円周等分多項式）

任意の素数p に対して

$$f(x)=x^{p-1}+\cdots+x+1\left(=\frac{x^p-1}{x-1}\right)$$

は，$\mathbb{Z}[x]$ において既約である．

（証明）

不定元の変換を行った $f(y+1)$が$\mathbb{Z}[y]$ において既約であることを示せばよい．

$$f(y+1)=\frac{(y+1)^p-1}{(y+1)-1}$$
$$=\frac{y^p+\binom{p}{1}y^{p-1}+\cdots+\binom{p}{k}y^{p-k}+\cdots+\binom{p}{p-2}y^2+\binom{p}{p-1}y}{y}$$
$$=y^{p-1}+\binom{p}{1}y^{p-2}+\cdots+\binom{p}{k}y^{p-k-1}+\cdots+\binom{p}{p-2}y+\binom{p}{p-1}$$

となる．

ところで，$p\nmid k!\,(p-k)!\quad(k=1,2,\cdots,p-1)$ に留意すると

$$p\nmid 1,\quad p\Big|\binom{p}{k}=\frac{p!}{k!\,(p-k)!}\quad(k=1,2,\cdots,p-1),\quad p^2\nmid\binom{p}{p-1}=p$$

であるからアイゼンシュタインの基準が満たされることにより，$f(y+1)$は$\mathbb{Z}[y]$ において既約である．

これにより，$f(x)$が$\mathbb{Z}[x]$ において既約であることが示された．

（証明終）

アイゼンシュタインの基準は，次のように拡張される．

定理 2.2（アイゼンシュタインの基準）

Rを一意分解整域とする．n次多項式

$$f(x)=a_0+a_1x+\cdots+a_nx^n,\qquad(a_i\in R)$$

に対して，ある素元$p\in R$ が存在して

$$p\nmid a_n,\quad p|a_j\ \ (j=0,1,\cdots,n-1),\quad p^2\nmid a_0$$

であるならば，$f(x)$は $R[x]$において既約である．

3. $\mathbb{Z}_p[x]$の既約多項式の個数

pを素数とする．$\mathbb{Z}_p$により$F_p={}^{\mathbb{Z}}\!/_{p\mathbb{Z}}$，すなわち元の個数が素数$p$の有限体を表す．これらは $x^p-x\in\mathbb{Z}_p[x]$の根の全体である．さらに，元の個数が $q=p^f$の有限体F_qは，$x^{p^f}-x\in\mathbb{Z}_p[x]$の根の全体となっている．

さて，$\mathbb{Z}_p[x]$のモニックなm次多項式の個数はp^mである．この章においては，そのうちで既約なものの個数を求める．

定理 3.1

$q(x)$を $\mathbb{Z}_p[x]$のモニックなd次既約多項式とするとき

$$q(x)\big|x^{p^n}-x\ \Leftrightarrow\ d\big|n$$

である．

定理 3.2

$\mathbb{Z}_p[x]$において，$x^{p^n}-x$はn の約数を次数にもつすべてのモニックな既約多項式$p_i(x)$の積である，すなわち

$$(*)\cdots x^{p^n}-x=\prod_{d|n}p_i(x).$$

以下では，$\mathbb{Z}_p[x]$におけるk次のモニックな既約多項式の個数を$N(p,k)$と記すことにする．

定理 3.3（$\mathbb{Z}_p[x]$におけるn次のモニックな既約多項式の個数）

$$N(p,n)=\frac{1}{n}\sum_{d|n}\mu\left(\frac{n}{d}\right)p^d$$

が成り立つ．だだし，μはメービウス（Möbius）の関数，すなわち

$$\mu(m)=\begin{cases}1 & \cdots & m=1\\ (-1)^r & \cdots & m=p_1p_2\cdots p_r\ (p_i\text{ は}m\text{の相異なる素因子})\\ 0 & \cdots & p^2|m\ (p\text{ は}m\text{の素因子})\end{cases}$$

である．

（証明）

定理 3.2 における$(*)$ の両辺の次数を比較すると

$$p^n=\sum_{d|n}d\cdot N(p,d)$$

が得られる．

ここで，$F(n)=p^n,\ f(d)=\ d\cdot N(p,d)$とおいて

メービウス（Möbius）の反転公式

$F(n)=\sum_{d|n}f(d)$ ならば，$f(n)=\sum_{d|n}\mu\left(\frac{n}{d}\right)F(d)$．

を用いると

$$n\cdot N(p,n)=f(n)=\sum_{d|n}\mu\left(\frac{n}{d}\right)F(d)=\sum_{d|n}\mu\left(\frac{n}{d}\right)p^d$$

が成り立つことから

$$N(p,n)=\frac{1}{n}\sum_{d|n}\mu\left(\frac{n}{d}\right)p^d$$

が得られる．

（証明終）

例

$\mathbb{Z}_2[x]$における 5 次以下のモニックな既約多項式を求める．

(i) 1 次

個数は

$$N(2,1)=\frac{1}{1}\sum_{d|1}\mu\left(\frac{1}{d}\right)2^d=\mu(1)2^1=2$$

であり

$$x, x+1$$

の 2 つである．

(ii) 2 次

個数は

$$N(2,2)=\frac{1}{2}\sum_{d|2}\mu\left(\frac{2}{d}\right)p^d=\frac{1}{2}\{\mu(2)2^1+\mu(1)2^2\}=\frac{1}{2}(-2+4)=1$$

である．2 次のモニックな多項式は

$$x^2,\quad x^2+1,\quad x^2+x,\quad x^2+x+1$$

の 4 つしかない．ところが，$(x+1)^2=x^2+1$ だから，既約であるものはx^2+x+1のみである．

$p(x)=x^2+x+1$が既約であることは，$p(0)=1\neq 0,\ p(1)=1\neq 0$ により 1 次因子をもたないことから示すこともできる．

(iii) 3 次

個数は

$$N(2,3)=\frac{1}{3}\sum_{d|3}\mu\left(\frac{3}{d}\right)p^d=\frac{1}{3}\{\mu(3)2^1+\mu(1)2^3\}=\frac{1}{3}(-2+8)=2$$

であり

$$q_1(x)=x^3+x+1,\quad q_2(x)=x^3+x^2+1$$

の 2 つである．

$q_1(x)=x^3+x+1$が既約であることは，$q_1(0)=1\neq 0,\ q_1(1)=1\neq 0$ により 1 次因子をもたないことから示される．

同様にして，$q_2(x)=x^3+x^2+1$が既約であることも示される．

(iv) 4 次

個数は

$$N(2,4)=\frac{1}{4}\sum_{d|4}\mu\left(\frac{4}{d}\right)p^d=\frac{1}{4}\{\mu(4)2^1+\mu(2)2^2+\mu(1)2^4\}=\frac{1}{4}(0-4+16)=3$$

であり

$$x^4+x+1, x^4+x^3+1, x^4+x^3+x^2+x+1$$

の 3 つである.

$r_1(x)=x^4+x+1$が既約であることは，$r_1(0)=1\neq 0,\ r_1(1)=1\neq 0$ により 1 次因子をもたないことと

$$(x^2+x+1)^2=x^4+x^2+1$$

であるから 2 次因子ももたないことにより示される.

同様にして$r_2(x)=x^4+x^3+1,\ r_3(x)=x^4+x^3+x^2+x+1$ が既約であることも示される.

例題

次の $x^{2^n}-x$ の形のモニックな多項式を，定理 3.2 を用いて$\mathbb{Z}_2[x]$において素因子分解せよ.

(1) x^4-x　　(2) x^8-x　　(3) $x^{16}-x$

(解答)

(1) $n=2$ の場合である.

例(i),(ii)により，1 次の既約多項式は$x, x+1$の 2 つ，2 次の既約多項式はx^2+x+1のみである.

したがって，定理 3.2 より

$$x^4-x=x(x+1)(x^2+x+1)$$

と素因子分解される.

(2) $n=3$ の場合である.

例(i),(iii)により,1 次の既約多項式は$x, x+1$ の 2 つ,3 次の既約多項式も$x^3+x+1,\ x^3+x^2+1$ の 2 つである.

したがって，定理 3.2 より

$$x^8-x=x(x+1)(x^3+x+1)(x^3+x^2+1)$$

と素因子分解される.

(3) $n=4$ の場合である.

例(i),(ii),(iv)により，1 次の既約多項式は$x, x+1$ の 2 つ,2 次の既約多項式はx^2+x+1のみ，4 次の既約多項式は

$$x^4+x+1,\ x^4+x^3+1,\ x^4+x^3+x^2+x+1$$

の 3 つである．

したがって，定理 3.2 より

$$x^{16}-x=x(x+1)(x^2+x+1)(x^4+x+1)(x^4+x^3+1)(x^4+x^3+x^2+x+1)$$

と素因子分解される．

（解答終）

参考文献

1) 増田真郎「応用のための代数系入門」サイエンス社，1981
2) 横井英夫，硲野敏博共著「代数演習[新訂版]」サイエンス社，2003
3) 永尾汎「代数学」朝倉書店，1983
4) 岩永恭雄「代数学の基礎」日本評論社，2002
5) 服部昭「現代代数学」朝倉書店，1968
6) Louis Rowen「Algebra―Groups, Rings, and Fields」CRC Press, 1995
7) Joseph J. Rotman 「Advanced Modern Algebra 3rd ed.」AMS, 2017