講義資料 (11): 多項式環・ガロア体

11.1 多項式環

本節は，教科書 4.1.1 節 (pp.151–156) に対応する．

定義 11.1 $\langle R, +', \cdot', 0, 1\rangle$ を環とする．文字 x を用いた形式的な有限和

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n \quad (a_0, a_1, \ldots, a_n \in R)$$

を R 上の**多項式** (polynomial)，または R を係数とする多項式と呼ぶ．ここで，文字 x を**変数** (variable) または**不定元** (indeterminate) と呼ぶ．特に，$a_n = 1$ であるとき多項式 f の事を**モニック多項式** (monic polynomial) と呼ぶ．また，有限個の i を除いて $a_i = 0$ と約束することにより，$f(x) = \Sigma_i a_i x^i$ とも記す．ここで，a_i を項 $a_i x^i$ の**係数** (coefficient) あるいは i 次の係数と呼ぶ．2 つの多項式 $\Sigma_i a_i x^i$ と $\Sigma_i b_i x^i$ が等しいとは全ての i で $a_i = b_i$ となることである．便宜上，係数が 0 の項は省略し，$1x^i$ は単に x^i で略記する． □

定義 11.2 環 $\langle R, +', \cdot', 0, 1\rangle$ 上の多項式全体からなる集合を $R[x]$ で記す．多項式の和 $(+)$ と積 $(\cdot)$ を以下で定義する．

$$\Sigma_i a_i x^i + \Sigma_i b_i x^i \stackrel{\text{def}}{=\!=} \Sigma_i (a_i +' b_i) x^i, \qquad \Sigma_i a_i x^i \cdot \Sigma_i b_i x^i \stackrel{\text{def}}{=\!=} \Sigma_k (\Sigma_{i+j=k} a_i \cdot' b_j) x^k$$

環 $\langle R, +', \cdot', 0, 1\rangle$ 上の**多項式環** (polynomial ring) とは代数系 $\langle R[x], +, \cdot, 0, 1\rangle$ の事である．以下では慣例に従い $+$ と $+'$ に同じ記号を利用し，$\cdot$ と $\cdot'$ は省略する． □

定理 11.3 環 R 上の多項式環 $R[x]$ は環である． □

証明は割愛する．大変かもしれないが難しくはない．気骨ある若者はチャレンジすべし．

例 11.4 整数環上の多項式環 $\mathbb{Z}[x]$ を考える．

$$\begin{aligned} (1-x) + (1+x+x^2) &= 2 + 0x + x^2 = 2 + x^2 \\ (1-x)(1+x+x^2) &= 1 + 0x + 0x^2 - 1x^3 = 1 - x^3 \end{aligned}$$ □

定義 11.5 多項式 g が多項式 f の約元であるとき，g を f の**因数** (factor) と呼び，$g \mid f$ で記す．また，多項式 g が f, h 双方の因数であるとき g を f と h の**共通因数** (common factor) と呼ぶ． □

定義 11.6 多項式 $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ (ただし $a_n \neq 0$) を考える．このとき，n を多項式 f の**次数** (degree) と呼び，$deg(f)$ で表す． □

NOTE: 上記の定義において $deg(0)$ は未定義になっている．文献によっては，$deg(0) = -1$ または $deg(0) = -\infty$ と定義する場合もある．

定義 11.7 多項式 f が**既約多項式** (irreducible polynomial) であるとは，$deg(f) \geq 1$ で，さらに，$f = gh$ かつ $deg(g), deg(h) \geq 1$ となる多項式 g, h が存在しないことである． □

NOTE: 既約多項式としてモニック多項式のみを考える文化もある．

11.2　可換体上の多項式環

本節も，教科書 4.1.1 節 (pp.151–156) に対応する．
多項式環を考える上で特に重要なのが可換体上の多項式環である．文献によっては，可換体上の多項式環のみを多項式環と呼ぶこともある．注意されたし．
可換体上の多項式環では，整数環 $\mathbb{Z}$ で成立した様々な良い性質が成立する．

定理 11.8 可換体 K 上の多項式環 $K[x]$ は**一意分解整域** (unique factorization domain)，すなわち以下の性質を満たす整域である．

- 任意の $f \in K[x]/K$ は既約分解を持つ．すなわち，ある既約多項式 $f_1, \ldots, f_n$ が存在して $f = f_1 \cdots f_n$ となる．さらに，この既約分解は既約多項式の順序と可逆元の積を除いて一意的である．　□

証明は割愛する．代数学の大抵の専門書に証明が載っているはずなので，興味ある方は参照されたし．

NOTE: 上記の定理は，可換体上の多項式環では整数環で成り立った素因数分解の一意性に相当する概念が成立することを意味する．

定理 11.9 可換体 K 上の多項式環 $K[x]$ において剰余定理が成立する．すなわち，任意の $f, g \in K[x]$ に対し，$g \neq 0$ ならば，以下を満たす多項式 q, r が存在する．

$$f = qg + r \quad (r = 0 \text{ または } deg(r) < deg(g))$$

さらに，上記を満たす多項式 q, r は一意に定まる．

証明 (概略のみ示す) q, r の存在は $deg(f)$ に関する帰納法で示せる．帰納段階の証明は $f = a_0 + a_1 x + \cdots + a_n x^n$ $(a_n \neq 0)$，$g = b_0 + b_1 x + \cdots + b_m x^m$ $(b_m \neq 0)$ とおくと，$f^* = f - a_n b_m^{-1} x^{n-m} g$ を考えることにより帰納法の仮定が適用できる．また，一意性の証明は背理法で証明できる (次数の概念をうまく使うと容易に矛盾が導ける)．　□

定理 11.10 可換体 K 上の多項式環 $K[x]$ はユークリッド整域である．

証明 (概略のみ示す) 定理 11.8 より $K[x]$ は整域になる．さらに，付値 v を $v(f) \stackrel{\text{def}}{=\!=} deg(f)$ で定義すればユークリッド整域になる．　□

例 11.11 以前，ユークリッド整域とは直感的に言うとユークリッドの互除法が適用できる代数である，と説明した．実際，可換体上の多項式環である $\mathbb{R}[x]$ において，以下のようにユークリッドの互除法を用いて最大公約元を求めることができる．
先ず，関係 $\Rightarrow_E$ を $(f, g) \Rightarrow_E (g, r)$ で定義する．ここで，r は定理 11.9 における多項式とする．このとき，$f = x^4 + x^3 + 3x^2 + 2x + 2$，$g = x^3 - 2x^2 - 2x - 3$ とすると，

$$\begin{array}{rcl}
(f, g) & = & ((x+3)g + (11x^2 + 11x + 11), g) \\
& \Rightarrow_E & (g, 11x^2 + 11x + 11) \\
& = & (\frac{1}{11}(x-3)(11x^2 + 11x + 11) + 0, 11x^2 + 11x + 11) \\
& \Rightarrow_E & (11x^2 + 11x + 11, 0) \\
& = & 11x^2 + 11x + 11
\end{array}$$

なお，約元の定義において同伴な元は同一視していたことに注意．それゆえに，f, g の最大公約元としては，$11x^2 + 11x + 11$ でなく，これと同伴でかつモニックになる $x^2 + x + 1$ を取る場合が多い． □

11.3 ガロア体

本節ではガロア体に関する基本的な性質を紹介する．証明は本講義の枠組みをかなり超えてしまうので割愛．

定義 11.12 ある素数 p と自然数 n に対し位数が p^n となる体の事を**ガロア体** (Galois field) と呼び，$GF(p^n)$ で記す． □

命題 11.13 任意の有限体はガロア体である．また，任意の素数 p と自然数 n に対しガロア体 $GF(p^n)$ が同型を除いて一意に存在する． □

命題 11.14 p を素数とし，f を $Z_p[x]$ 上の n 次既約多項式とする．このとき，$Z_p[x]/(f)$ は $GF(p^n)$ を構成する． □

NOTE: 本資料では，記法 $Z_p[x]/(f)$ を紹介していない．ちなみに $Z_p[x]/(f)$ は，多項式環 $Z_p[x]$ のイデアル (f) を法とした剰余環であり，f の既約性により体であることが保証されている．とりあえず，$Z_p[x]/(f)$ は例 11.16 のように $Z_p[x]$ における多項式を f で割ることによって得られる剰余多項式の全体と考えていれば十分．

命題 11.15 ガロア体 $GF(p^n) = \langle F, +, \cdot, 0, 1\rangle$ の乗法群 $F^\times = \langle F \setminus \{0\}, \cdot, 1\rangle$ は巡回群である，すなわち，ある $\alpha \in F \setminus \{0\}$ が存在して，

$$F \setminus \{0\} = \{\alpha^0, \alpha^1, \ldots, \alpha^{p^n-2}\}$$

となる．このとき，α をガロア体 F の**原始元** (primitive element) と呼ぶ．また，任意の $GF(p^n)$ の原始元 α に対し，$Z_p(\alpha)$ は $GF(p^n)$ を構成する． □

NOTE: 本資料では，記法 $Z_p(\alpha)$ を紹介していない．ちなみに $Z_p(\alpha)$ は，体 Z_p に α を付加した拡大体と呼ばれる体である．本資料で $Z_p(\alpha)$ の記法を用いるのは α が $GF(p^n)$ の原始元であるという特殊な場合のみであるため，$Z_p(\alpha) = \{0, \alpha^0, \alpha^1, \ldots, \alpha^{p^n-2}\}$ と考えていれば十分．

例 11.16 $f(x) = x^4 + x + 1$ とし，α を f の根とする ($f(x) = 0$ を満たす複素数)．ここで，f は $Z_2[x]$ における既約多項式となっており，α はガロア体 $GF(2^4)$ の原始元となっている (証明は割愛)．
命題 11.14 より，$Z_2[x]/(f)$ は $GF(2^4)$ を構成する．また，命題 11.15 より，$Z_2(\alpha)$ も $GF(2^4)$ を構成する．さらに，命題 11.13 より，これらのガロア体は同型である．

以下にこれらのガロア体の対応表を記す．なお，$(a_0\ a_1\ a_2\ a_3)$ を多項式 $a_0+a_1x+a_2x^2+a_3x^3$ のベクトル表現と呼ぶことにする．

$Z_2(\alpha)$	$Z_2[x]/(f)$	ベクトル表現	$Z_2(\alpha)$	$Z_2[x]/(f)$	ベクトル表現
0	0	(0 0 0 0)	α^7	$1+x+x^3$	(1 1 0 1)
α^0	1	(1 0 0 0)	α^8	$1+x^2$	(1 0 1 0)
α^1	x	(0 1 0 0)	α^9	$x+x^3$	(0 1 0 1)
α^2	x^2	(0 0 1 0)	α^{10}	$1+x+x^2$	(1 1 1 0)
α^3	x^3	(0 0 0 1)	α^{11}	$x+x^2+x^3$	(0 1 1 1)
α^4	$1+x$	(1 1 0 0)	α^{12}	$1+x+x^2+x^3$	(1 1 1 1)
α^5	$x+x^2$	(0 1 1 0)	α^{13}	$1+x^2+x^3$	(1 0 1 1)
α^6	x^2+x^3	(0 0 1 1)	α^{14}	$1+x^3$	(1 0 0 1)

□

NOTE: 上の例で見るように，ガロア体 $GF(2^n)$ は n ビット符合の全体と対応する．それゆえに，ガロア体の理論は符合理論の基礎をなし，通信のエラー検出・訂正等の基礎理論構築に大活躍する．また，暗号 (共通鍵暗号や楕円暗号等) への応用も盛んに研究されている．

定義 11.17 多項式 $f \in Z_p[x]$ に対し，$f \mid (x^k-1)$ となる最小の自然数 k を f の**周期** (period) と呼ぶ．$Z_p[x]$ 上の n 次既約多項式 f が周期 p^n-1 を持つとき，f を**原始多項式** (primitive polynomial) と呼ぶ． □

命題 11.18 n 次の既約多項式 $f \in Z_p[x]$ に対し以下の性質は全て等価である．

- f は原始多項式である．
- $x^{p^n-1} \equiv 1 \pmod f$ かつ任意の $k < p^n-1$ で $x^k \not\equiv 1 \pmod f$.
- x が $Z_p[x]/(f) = GF(p^n)$ の原始元である．
- $Z_p[x]/(f)$ において，$x^{p^n-1} = 1$ かつ任意の $k < p^n-1$ で $x^k \neq 1$. □

NOTE: 原始多項式は既約多項式であるが，この逆は一般には成立しない．例えば，$x^4+x^3+x^2+x+1$ は $Z_2[x]$ において既約多項式であるが原始多項式ではない．実際，$k=5$ $(\neq 2^4-1)$ に対し $(x^4+x^3+x^2+x+1)^5 = 1$.

演習課題

問 11.1 試験問題を作成せよ．また，作成した問題に対して以下の３項目も作成すること．

- 模範解答
- 予想正答率
- 予想解答時間 (お手上げの人は考慮しなくて良い)

なお，試験問題というものは，解いて貰うための問題であると言うことを忘れないこと．