Chapter 3 : Algebra (前半) 発表レジュメ

當眞 ジェイソン翔

2018 年 6 月 18 日

1 準備

まずは基本的な話題の復習を行う。

定義 1.1. (演算)
X が集合であるとき、写像 $\phi : X \times X \to X$ のことを集合 X 上の演算という。誤解の恐れがないときには、$\phi(a, b)$ の代わりに ab と書く。

定義 1.2. (群)
G を空でない集合とする。G 上の演算が定義されていて、次の性質を満たすとき、G を群 (group) という。

1. 単位元とよばれる元 $e \in G$ があり、すべての $a \in G$ に対し $ae = ea = a$ となる。
2. すべての $a \in G$ に対し $b \in G$ が存在し、$ab = ba = e$ となる。元 b は a の逆元と呼ばれ、a^{-1} と書く。
3. (結合法則) すべての $a, b, c \in G$ に対し、$(ab)c = a(bc)$ が成り立つ。

定義 1.3. (群の位数)
G を群とする。G の元の個数を G の位数といい、$|G|$ と表す。位数が有限な群のことを有限群といい、有限群でない群を無限群という。

定義 1.4. (可換群)
G を群とする、このとき、$^\forall a, b \in G$ に対して $ab = ba$ が成り立つとき、G を可換群 (commutative group) という。可換群は Abel 群、加法群、あるいは加群とも呼ばれる。

定義 1.5. (元の位数)
G を群、$a \in G$ とする。もし、$a^n = e$ となる正の整数が存在すれば、その中で最小のものを a の位数とする。もしそのような n が存在しなければ、a の位数は ∞ である、または a は無限位数であるという。

定義 1.6. (部分群)
G を群とする。G の空でない部分集合 H が次の性質を満たすとき、H を G の部分群 (subgroup) といい、$H \leq G$ と書く。

- すべての $a, b \in H$ に対して $ab \in H$ かつ $a^{-1} \in H$ が成り立つ。

定義 1.7. (巡回群)
一つの元で生成される群を巡回群 (cyclic group) という。群の部分群で巡回群であるものを巡回部分群という。$a \in G$ に対して a のべきの作る群を $\langle a \rangle$ と書く。

定理 1.8.
G を有限群とする。$g \in G$ の位数は $|G|$ の約数である。

(証明)

$H = \langle g \rangle$ とし、g の位数を d とする。$n \in \mathbb{Z}$ なら $n = qd + r(0 \leq r < d)$ となる整数 q, r が存在する。すると $g^n = g^r$ なので $H = \{1, g, \cdots, g^{d-1}\}$ である。$0 \leq i < j \leq d-1$ なら $0 < j - i \leq d-1$ なので、$g^{j-i} = e$ なら g の位数が d であることに矛盾する。よって $g^{j-i} \neq e$ である。 $g^i = g^j$ なら $g^{j-i} = e$ なので $g^i \neq g^j$。よって $|H| = d$、すなわち $|H|$ は g の位数である。ラグランジュの定理より $|H|$ は $|G|$ の約数であり、よって g の位数は $|G|$ の約数である。■

定義 1.9. (環)

集合 R において加法 "+" : $R \times R \to R$ と乗法 "·" : $R \times R \to R$ が定まっており、加法 $+$ に関して R は可換群で、更に次の条件が満たされるとき R は **環** (ring) であるという。

1. (乗法の結合法則) すべての $a, b, c \in R$ に対し、$(a \cdot b) \cdot c = a \cdot (b \cdot c)$ が成り立つ。
2. (分配法則) すべての $a, b, c \in R$ に対し、$(a + b) \cdot c = a \cdot c + b \cdot c,\ a \cdot (b + c) = a \cdot b + a \cdot c$ が成り立つ。

定義 1.10. (単位的な環)

環 R に関して乗法の単位元 1 が存在するとき、R は**単位的** (unitary) であるという。

2 体

定義 2.1. (体)

単位的な環 R において、0 以外のすべての元が逆元を持つとき R を**斜体** (skew field) という。(乗法に関して) 可換な斜体を**体** (field) という。

例 2.2. (体の例)

次の体は数学の諸分野によく登場するものの例である。

1. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$(それぞれ有理数体、実数体、複素数体)
2. $\mathbb{Z}/p\mathbb{Z}$ (素数 p を法とする剰余体)。$\mathbb{Z}/p\mathbb{Z}$ は $\mathbb{F}_p$ や $\mathrm{GF}(p)$ とも書く。

定義 2.3. (ベクトル空間)

$\mathbb{F}$ を体とするとき、$\mathbb{F}$ **上のベクトル空間**とは、$+$ を演算とする可換群 M と写像 $\mathbb{F} \times M \ni (a, x) \mapsto a \cdot x \in M$ で、次の性質を満たすものである。以下、x, x_1, x_2 は M の任意の元を、a, b は $\mathbb{F}$ の任意の元を表す。

1. $a \cdot (b \cdot x) = (ab) \cdot x$
2. $(a + b) \cdot x = a \cdot x + b \cdot x$
3. $a \cdot (x_1 + x_2) = a \cdot x_1 + a \cdot x_2$
4. $1 \cdot x = x$

定義 2.4. (拡大体)

$\mathbb{K}$ を体とする。$\mathbb{F} \subseteq \mathbb{K}$ が体となるとき、$\mathbb{F}$ を $\mathbb{K}$ の**部分体** (subfield)、$\mathbb{K}$ を $\mathbb{F}$ の**拡大体** (extension field) という。

注意 2.5.

$\mathbb{K}$ が $\mathbb{F}$ の拡大体であるとき、定義 2.3 における写像の定義を $\mathbb{K}$ 上の乗法とすることで、$\mathbb{K}$ が $\mathbb{F}$ 上のベクトル空間であるということがわかる。

定義 2.6. (拡大次数)

$\mathbb{K}$ を $\mathbb{F}$ の拡大体であるとする。$\mathbb{K}$ の $\mathbb{F}$ 上のベクトル空間としての次元が有限であるとき、**有限次拡大**(finite extension) という。このベクトル空間の次元を**拡大次数**といい、$[\mathbb{K} : \mathbb{F}]$ で表す。

例 2.7.

$\mathbb{C}$ は $\mathbb{R}$ の拡大体であり、有限次拡大である。$\mathbb{C} = \{x + iy | x, y \in \mathbb{R}\}$ と表されるので、$[\mathbb{C} : \mathbb{R}] = 2$ である。

定義 2.8. (付加してできる部分体)

$\mathbb{K}$ を $\mathbb{F}$ の拡大体とする。$\mathbb{M} \subseteq \mathbb{K}$ に対し、$\mathbb{F}$ と $\mathbb{M}$ を含む最小の部分体を $\mathbb{F}(\mathbb{M})$ と書き、$\mathbb{F}$ に $\mathbb{M}$ を付加してできる部分体という。$\mathbb{M} = \{\alpha_1, \cdots, \alpha_n\}$ のときは $\mathbb{F}(\alpha_1, \cdots, \alpha_n)$ と書く。特に $\mathbb{M}$ がただ一つの要素 α からなるとき、$\mathbb{F}(\alpha)$ と書いて**単純拡大**という。

定義 2.9. (R 上の多項式)

R を環、$X = (X_1, \cdots, X_m)$ を m 個の文字とする。R 上の m 変数の多項式とは、$\mathbb{N}^m$ から R への写像で、有限個の $(i_1, \cdots, i_m) \in \mathbb{N}^m$ を除いて値が 0 であるものと、変数 $X = (X_1, \cdots, X_m)$ の組のことである。

写像の $(i_1, \cdots, i_m) \in \mathbb{N}^m$ での値が $a_{i_1, \cdots, i_m}$ なら、この多項式を

$$f(X_1, \cdots, X_m) = \sum_{i_1, \cdots, i_m \geq 0} a_{i_1, \cdots, i_m} X_1^{i_1} \cdots X_m^{i_m}$$

などと書く。

定義 2.10. (多項式環)

体 $\mathbb{F}$ および変数の集合 $X = \{X_1, \cdots, X_m\}$ 上の**多項式環**とは、$X_1, \cdots, X_m$ を変数とする m 変数多項式全体からなる環であり、$\mathbb{F}[X]$ と表す。$\mathbb{F}[X]$ の元に対する加算と乗算は、通常の多項式に対しての加算と乗算と同様の方法で行う。

$f, g \in \mathbb{F}[X]$ に対し、g が f を**割り切る**とは、多項式 $h \in \mathbb{F}[X]$ が存在し $f = gh$ と表されることである。

$f \in \mathbb{F}[X]$ に対して $g, h \in \mathbb{F}[X]$ を用いて $f = gh$ と表すことを考える。このとき g または h が必ず定数になるとき、f は**既約多項式**という。既約多項式は整数の世界での素数のようなものである。

以下、この節では多項式の次数は 1 であるとする。

定義 2.11. (次数、モニック多項式)

X を変数とする 1 変数多項式の次数とは、0 でない係数を持つ X のべきのうち、一番べきが大きいものである。多項式が**モニック**であるとは、多項式の次数を d として、X^d の項の係数が 1 になっているもののことを指す。

注意 2.12.

多項式環は一意分解整域である。

定義 2.13. (代数的)

$\mathbb{F}$ を体 $\mathbb{K}$ の部分体とする。$\alpha \in \mathbb{K}$ が、ある $\mathbb{F}[X]$ に属する多項式の根であるとき、α は $\mathbb{F}$ 上**代数的**であるという。α が $\mathbb{F}$ 上代数的であるとき、α を根とする最低次のモニック多項式を α の $\mathbb{F}$ に関する**最小多項式**という。

定義 2.14. (共役)

α の最小多項式の α 以外の根は、α と $\mathbb{F}$ 上**共役**であるという。すべての共役な根をかけ合わせたものを**ノルム**という。α' と α が共役であるとき、$\mathbb{F}(\alpha)$ と $\mathbb{F}(\alpha')$ は α を α' に置き換える同型写像によって同型になる。もし $\mathbb{F}(\alpha) = \mathbb{F}(\alpha')$ となる場合、α を α' に置き換える写像は $\mathbb{F}$ の**自己同型**を与えるという。

例 2.15.

$\mathbb{Q}$ は $\mathbb{R}$ の部分体である。$\sqrt{2}$ は多項式 $x^2 - 2 \in \mathbb{Q}[x]$ の根であるため $\mathbb{Q}$ 上代数的である。また $-\sqrt{2}$ も $\sqrt{2}$ の最小多項式の根であるため、$-\sqrt{2}$ は $\sqrt{2}$ と $\mathbb{Q}$ 上共役である。ここで、写像 $a + b\sqrt{2} \mapsto a - b\sqrt{2}$ $(a, b \in \mathbb{Q})$ は $\mathbb{Q}(\sqrt{2})$ の自己同型写像になっている。

定義 2.16. (微分、偏微分)

1 変数多項式の微分および多変数多項式の偏微分を、多項式の aX^d の項を $(a + \cdots + a)X^{d-1}$ (a が d 個) に置き換えて作られる新しい多項式と定義する。

定義 2.17. (分解体)

$f \in \mathbb{F}[X]$ と $\mathbb{F}$ の拡大体 $\mathbb{K}$ について、f が $\alpha_1, \cdots, \alpha_n \in \mathbb{K}$ によって $f(X) = a(X-\alpha_1)\cdots(X-\alpha_n)$ と 1 次因子の積にかけるとき、f は $\mathbb{K}$ で分解するという。$\mathbb{F}(\alpha_1, \cdots, \alpha_n)$ を f の分解体 (splitting field) という。

注意 **2.18.**

分解体は同型写像による変換を除いて一意である。

例 **2.19.**

$\mathbb{Q}(\sqrt{2})$ は $f(x) = x^2 - 2 \in \mathbb{Q}[x]$ の分解体である。$g(x) = x^3 - 2 \in \mathbb{Q}[x]$ の分解体を得るためには、$\mathbb{Q}$ に $\sqrt[3]{2}$ と $\sqrt{3}i$ の両方を付加する必要がある。これは、$x^3 - 2 = 0$ の解が $\omega = (-1 + \sqrt{3}i)/2$ を用いて $\sqrt[3]{2}\omega^k (k = 0, 1, 2)$ と表されるからである。

定義 **2.20.** (代数的閉体、代数的閉包)

任意の $\mathbb{F}[X]$ に属する多項式 f の根がすべて $\mathbb{F}$ の元であるとき、$\mathbb{F}$ を代数的閉体という。体 $\mathbb{F}$ の拡大体のうち、代数的閉体であり最小のものを代数的閉包という。

例 **2.21.**

代数学の基本定理より、$\mathbb{C}[X]$ に属する多項式のすべての根は $\mathbb{C}$ の元である。よって $\mathbb{C}$ は代数的閉体である。また、$\mathbb{R}$ の代数的閉包は $\mathbb{C}$ である。

定義 **2.22.** (標数)

体 $\mathbb{F}$ の単位元 1 に対し、$n \cdot 1 = 0$ となる正整数 n が存在するとき (na は a の n 個の和)、そのような n のうち最小の n を $\mathbb{F}$ の標数 (charasteristic) という。そのような n が存在しない場合、標数は 0 であるという。

定理 **2.23.**

体の標数は 0 または素数である。

(証明)

体 $\mathbb{F}$ の標数 c が合成数であると仮定する。すると、$c = mn$ (m, n : 2 以上の自然数) と書き表せる。このとき $m \cdot 1 \neq 0$ かつ $n \cdot 1 \neq 0$ であるが、$(m \cdot 1)(n \cdot 1) = (mn) \cdot 1 = 0$ となる。体は整域なので $m \cdot 1 = 0$ または $n \cdot 1 = 0$ とならなければならないが、これは矛盾である。■

3 有限体

$\mathbb{F}_q$ を要素数が q 個の有限体とする。明らかに有限体の標数は 0 になり得ない。そこで、この有限体の標数を p とする。すると、$\mathbb{F}_q$ は素数体 $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ を含んでいる。よって $\mathbb{F}_q$ は $\mathbb{F}_p$ の拡大体であるから、$\mathbb{F}_p$ 上の有限次元のベクトル空間でもある。このベクトル空間の次元を f とする。

基底を選ぶことにより、f 次元ベクトル空間の元と $\mathbb{F}_p$ の元の f 個の組の間に 1 対 1 対応をつけることができる。これにより、$\mathbb{F}_q$ にはちょうど p^f 個の元があること、すなわち、q は標数 p のべきで表されなければならないことが従う。

これから、任意の素数のべき $q = p^f$ に対して q 個の要素からなる体が存在することを示し、それが同型写像による変換を除いて一意であることを示していく。

そのまえに、はじめに体の乗法に関する位数の性質を調べていく。

3.1 有限体の乗法的生成元とその存在

$\mathbb{F}_q$ には $q-1$ 個の非零要素があり、定義より乗法に関して Abel 群になっている。これらの要素からなる群を $\mathbb{F}_q^*$ と表記する。定理 1.8 より、すべての $a \in \mathbb{F}_q^*$ の位数は $q-1$ の約数である。

定義 **3.1.** (生成元)

有限体 $\mathbb{F}_q$ の生成元 (generator) とは、群 $\mathbb{F}_q^*$ の元 g であり、その位数が $q-1$ のものである。

定理 3.2.

1. すべての有限体に生成元が存在する。
2. g が $\mathbb{F}_q^*$ の生成元であるとき、g^j が生成元であることは $\gcd(j, q-1) = 1$ であることと同値である。
3. $\mathbb{F}_q^*$ には $\varphi(q-1)$ 個の生成元が存在する。正整数 n に対し、$\varphi(n)$ で 1 から n までの n と互いに素な正整数の個数を表す (Euler のトーシェント関数)。

(証明)

$a \in \mathbb{F}_q^*$ の位数が d であると仮定する。定理 1.8 より、d は $q-1$ の約数である。また、定理 1.8 の証明に出てきたように、$a, a^2, \cdots, a^d = 1$ はすべて相異なる。

ここで、a^j の位数が d であることと $\gcd(j, d) = 1$ であることは同値であることを示す。$a, a^2, \cdots, a^d$ はそれぞれ方程式 $x^d = 1$ を満たす。そして、$x^d - 1$ の根の個数は高々 d 個なので、a のべきが多項式 $x^d - 1$ のすべての根である。よって、位数 d の元はすべて a のべきの形で表されているはずである。しかし、$a, \cdots, a^d$ の中には位数が d でない元も存在する。$\gcd(j, d) = d' > 1$ であったとすると、$(a^j)^{d/d'} = 1$ となるので、a^j の位数は d/d' 以下となる。逆に、$\gcd(j, d) = 1$ であれば、不定方程式 $ju - dv = 1$ を満たす整数 u, v が存在する。よって $a = a^{ju-dv} = (a^j)^u$ は a^j のべきである。よって a^j の位数を d_2 とすると、a の位数 d は d_2 以下である。また、これまでの議論より d_2 は d 以下なので $d = d_2$ となる。よって a^j と a の位数は等しい。よって主張が示された。

上記の主張は、有限体上に位数 d の元 a が存在すれば、位数 d の元はちょうど $\varphi(d)$ 個存在することを示している。よって、$q-1$ のそれぞれの約数 d に対して、

- 位数 d の元は存在しない。
- 位数 d の元がちょうど $\varphi(d)$ 個存在する。

のいずれかが成り立つはずである。

次に、正整数 N に対して成り立つ等式

$$\sum_{d|N} \varphi(d) = N \tag{1}$$

を示す。ここで、和は N の約数全体について取っている。

まず、集合 $\{0, 1, \cdots, N-1\}$ を、N との最大公約数の値で分割する。つまり、集合 $S_k = \{j | 0 \leq j < N, \gcd(N, j) = k\}$ として先述の集合を分割する。今、式 (1) の和は N の約数全体について取っているので、約数 d について $N = d' \cdot d$ と表される整数 d' が存在する。このとき、集合 S_d は $\varphi(d')$ 個の元からなることがわかる。これは、$^\forall j \in S_d$ について、$j = j'd$ $(0 \leq j' < d')$ と表され、$\gcd(d', j') \leq \gcd(d \cdot d', j') = \gcd(N, j') = 1$ となるからである。よって、$\{0, 1, \cdots, N-1\} = \bigcup_{d|N} S_d$ で、$|S_d| = \varphi(N/d)$ なので

$$N = \sum_{d|N} \varphi(N/d) = \sum_{d|N} \varphi(d)$$

が成立する。

最後に定理を示す。$\mathbb{F}_q^*$ の任意の元の位数 d は $q-1$ の約数である。そして位数 d の元は 0 個もしくは $\varphi(d)$ 個存在する。式 (1) より、$\sum_{d|q-1} \varphi(d) = q-1$ となる。これは $\mathbb{F}_q^*$ の要素数と一致する。よって、$\mathbb{F}_q$ の元を位数によって分割すると、任意の元が $q-1$ の約数の位数を持つには、$q-1$ の約数 d に対してその位数の元がちょうど $\varphi(d)$ 個ある必要がある。特に、位数 $q-1$ の元はちょうど $\varphi(q-1)$ 個存在する。そして最初に見たように、g が位数 $q-1$ の元であるとき、g^j の位数が $q-1$ であることの必要十分条件は $\gcd(j, q-1) = 1$ が成り立つことである。よって定理が示された。■

系 3.3.

任意の素数 p に対して、$\{g^n \bmod p \mid n \in \mathbb{Z}\} = (\mathbb{Z}/p\mathbb{Z})^*$ となる整数 g が存在する。

3.2 要素数が素数のべきの有限体の存在とその一意性

この節では、要素数が素数 p のべきで表される有限体の存在と、それが同型写像による変換を除いて一意であることを示す。存在は、要素数を $q = p^f$ としたときに多項式 $x^q - x$ の分解体が要素数 q の有限体になることを用いて示す。

定理 3.4.

p を素数、f を正の整数とする。F_q は $q = p^f$ 個の要素からなる体だとする。このとき、任意の $\mathbb{F}_q$ の元は多項式 $x^q - x$ の根であり、$\mathbb{F}_q$ は多項式の根の集合である。逆に、任意の素数のべき $q = p^f$ に対して、$x^q - x \in \mathbb{F}_p[X]$ の分解体は q 個の要素からなる体である。

(証明)

$\mathbb{F}_q$ が有限体であると仮定する。任意の非零の元の位数が $q-1$ の約数であることより、すべての非零の元は方程式 $x^{q-1} = 1$ を満たす。この方程式の両辺に x を乗ずることで、$\mathbb{F}_q$ の任意の元が方程式 $x^q = x$ を満たす。代数学の基本定理より、多項式 $x^q - x$ は高々 q 個の根しか持たないため、この多項式の根の集合は $\mathbb{F}_q$ に一致する。よって $\mathbb{F}_q$ は $x^q - x \in \mathbb{F}_p[X]$ の分解体である。

逆に $q = p^f$ とし、$\mathbb{F}$ を $x^q - x \in \mathbb{F}_p$ の分解体とする。このとき、$x^q - x$ の微分は $(q \cdot 1)x^{q-1} - 1 = -1$ となる。これは q が p の倍数であるからである。よって、$x^q - x$ はその微分と共通する根を持たない。よって、$x^q - x$ は多重根を持たないため、$\mathbb{F}$ は少なくとも $x^q - x$ の q 個の根を持たなければならない。しかし、q 個の根からなる集合は体になっている。

これを示すために、標数 p の体 $\mathbb{K}$ について、$^\forall a, b \in \mathbb{K}$ に対して $(a+b)^p = a^p + b^p$ となることを示す。二項定理により $(a+b)^p = \sum_{j=0}^{p}(\binom{p}{j} \cdot 1)a^j b^{p-j}$ となるが、$0 < j < p$ のときは $\binom{p}{j}$ が p で割れるため、途中の項が消える。よって主張が示される。

この定理を繰り返し使っていくと、$a^p + b^p = (a+b)^p, a^{p^2} + b^{p^2} = (a^p)^p + (b^p)^p = (a^p + b^p)^p = (a+b)^{p^2}, \cdots, a^q + b^q = (a+b)^q$ が得られる。よって、a, b が多項式 $x^q - x$ の根であるとき、$a+b, ab$ も $x^q - x$ の根であることがわかる。よって、$x^q - x$ の分解体は q 個の根からなる体である。■

定理 3.5.

$\mathbb{F}_q$ を $q = p^f$ 個の要素からなる有限体とし、$\sigma : \mathbb{F} \ni a \mapsto a^p \in \mathbb{F}$ とする。このとき、σ は $\mathbb{F}_q$ の自己同型写像になっている。$\sigma(a) = a$ となる $\mathbb{F}_q$ の元は体 $\mathbb{Z}/p\mathbb{Z}$ の元に対応している。σ^f は恒等写像になり、$j < f$ ならば σ^j は恒等写像にはならない。

(証明)

写像 σ は明らかに乗算について準同型になっている。また、定理 3.4 の証明から σ は和についても準同型であることがわかる。ここで、$\sigma^j(a) = a^{p^j}$ となっていることに注意すると、$\sigma^j(a) = a$ となる要素は多項式 $x^{p^j} - x$ の根である。$j = 1$ のとき、これは体 $\mathbb{Z}/p\mathbb{Z}$ の p 個の元であることが Fermat の小定理より従う。$\sigma^f(a) = a$ となる要素は多項式 $x^q - x$ の根であり、それは $\mathbb{F}_q$ の任意の元である。よって、σ^f は恒等写像になっていて、σ は全単射である必要がある ($\sigma^{-1} = \sigma^{f-1}$ である)。$j < f$ のとき、$\mathbb{F}_q$ のすべての元が $x^{p^j} - x$ の根になることはないため、σ^j は恒等写像になり得ない。よって定理が示された。■

定理 3.6.

$\mathbb{F}_q$ を $q = p^f$ 個の要素からなる有限体とする。α が $\mathbb{F}_q$ の任意の元であるとき、α と $\mathbb{F}_p$ 上共役な元は $\sigma^j(\alpha) = \alpha^{p^j}$ と書かれるものである。

(証明)

$d = [\mathbb{F}_p(\alpha) : \mathbb{F}_p]$ とする。すなわち、$\mathbb{F}_p(\alpha)$ は $\mathbb{F}_{p^d}$ と同型であるとする。このとき、α は多項式 $x^{p^d} - x$ の

根だが、任意の $j < d$ に対して $x^{p^j} - x$ の根ではない。よって、$\alpha, \alpha^p, \alpha^{p^2}, \cdots, \alpha^{p^{d-1}}$ は $\mathbb{F}_q$ ですべて異なる元である。あとは、α が $f(x) \in \mathbb{F}_p[X]$ の根であるとき、α^p も $f(x)$ の根であることを示せば良い。今 $f(x) = \sum a_j x^j, a_j \in \mathbb{F}_p$ と表されているとする。このとき $0 = f(\alpha) = \sum a_j \alpha^j$ である。両辺を p 乗し、関係式 $(a+b)^p = a^p + b^p$ を使うことにより $0 = \sum (a_j \alpha^j)^p$ が得られる。今、Fermat の小定理より $a_j^p = a_j$ であるから、$0 = \sum a_j (\alpha^p)^j = f(\alpha^p)$ となる。よって定理が示された。

3.3 具体的な構成

ここでは、具体的に $\mathbb{F}_q$ を構成することを考えていく。

例 3.7.

$\mathbb{F}_9$ を構成することを考える。それには、$\mathbb{F}_3$ 上のモニックな既約多項式であって $\mathbb{F}_3$ 上に解を持たないものを用いる。総当たりでそのような多項式を探すと、x^2+1 と $x^2 \pm x - 1$ が該当するものであることがわかる。x^2+1 の根を α とすると (当然これは i であるから、α ではなく i と呼ぶことにする)、$\mathbb{F}_9$ のすべての元は $a + bi$ の形で書くことができる $(a, b \in \{-1, 0, 1\})$。この表現を用いるときの演算はガウスの整数の演算とほとんど同じようにできるが、係数が $\mathbb{F}_3$ で閉じているという点だけが異なる。

いま、$\mathbb{F}_3$ に付加した i は位数が 4 であるため、$\mathbb{F}_9^*$ の生成元になっていないということに注意する必要がある。しかし、i の代わりに $x^2 - x - 1$ の根 α を付加すると、

$$\alpha^1 = \alpha, \alpha^2 = \alpha + 1, \alpha^3 = -\alpha + 1, \alpha^4 = -1, \alpha^5 = -\alpha, \alpha^6 = -\alpha - 1, \alpha^7 = \alpha - 1, \alpha^8 = 1$$

となるので、この α は $\mathbb{F}_9^*$ の生成元になっている。このように、既約多項式 $f(x)$ の任意の根が体の非零要素からなる群の生成元になっているとき、$f(x)$ は原始的である (primitive) という。定理 3.2 より、$\mathbb{F}_9^*$ には $\varphi(9-1) = 4$ 個の生成元が存在する。そのうち 2 つは $x^2 - x - 1$ の根で、もう 2 つは $x^2 + x - 1$ の根である。残りの 2 つの非零要素は $x^2 + 1$ の根 $(\pm i = \pm(\alpha + 1))$ であり、残りの 2 つは $\mathbb{F}_3$ の非零要素である ± 1 である。これらは 1 次元のモニックな既約多項式 $x \pm 1$ の根である。

$q = p^f$ のとき、$\mathbb{F}_q$ の任意の要素 α はある次数 d の最小多項式の根になっていることを思い出す。そのとき、$\mathbb{F}_p(\alpha)$ は拡大次数が d の拡大体であり、$\mathbb{F}_q$ に含まれている。つまり、$\mathbb{F}_p(\alpha)$ は $\mathbb{F}_{p^d}$ と同型である。$\mathbb{F}_{p^f}$ は $\mathbb{F}_{p^d}$ を含んでいるため、$\mathbb{F}_{p^d}$ 上のある次元 f' のベクトル空間である。また、$\mathbb{F}_{p^f}$ の元の個数は $(p^d)^{f'}$ でなければならないこと、すなわち $f = df'$ でなければならないことがわかる。よって、d は f の約数である。逆に、任意の f の約数 d に対して、$\mathbb{F}_{p^d}$ は $\mathbb{F}_q$ に含まれている。これは、$x^{p^d} = x$ の根は $x^{p^f} = x$ の根でもあることから従う。(これを確かめるには、$y^{p^d} = y$ で $y = x^{p^d}$ と置くことで関係式 $x^{p^{2d}} = x^{p^d} = x$ が得られ、繰り返し適用することで $x^{p^{dd'}} = x^{p^f} = x$ となることを用いれば良い。) 以上の議論により、次の定理が示された。

定理 3.8.

$\mathbb{F}_{p^f}$ の部分体は、f の約数 d を用いて $\mathbb{F}_{p^d}$ と書かれる。$\mathbb{F}_{p^f}$ の元が $\mathbb{F}_p$ に付加されると、これらの部分体のうちのどれかが得られる。

以上の定理より、次の公式が用意に示される。この公式は、与えられた次数にある既約多項式の個数を与えるものである。

定理 3.9.

p : 素数、f : 正の整数とする。任意の $q = p^f$ に対し、多項式 $x^q - x \in \mathbb{F}_p[x]$ は $\mathbb{F}_p[x]$ に属する f の約数の次数であるモニックな既約多項式すべてによって因数分解できる。

(証明)

$\mathbb{F}_p$ に次数 d (f の約数) のモニックな既約多項式 $f(x)$ の根 α を付加すると、$\mathbb{F}_{p^d}$ と同型な体が得られる。先述のように $\mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^f}$ である。α は $x^q - x$ の根であるから、$f(x)$ は $x^q - x$ を割り切る必要がある。逆に、$g(x)$ が $x^q - x$ を割り切る多項式であるとする。このとき、$g(x)$ は $\mathbb{F}_q$ に根を持つ必要がある ($\mathbb{F}_q$ が $x^q - x$

の根の集合であるため)。よって、定理 3.8 より、これらの根を $\mathbb{F}_p$ に付加すると $\mathbb{F}_q$ の部分体が得られるため、$g(x)$ は f の約数の次数を持たなければならない。よって、$x^q - x$ を割り切るモニックな既約多項式の次数は f の約数に限られる。また、$x^q - x$ は多重根を持たないことは以前に確かめているので、$x^q - x$ はそれらの既約多項式の積として書かれることがわかる。よって主張が示された。■

系 3.10.

f が素数であるとき、$\mathbb{F}_p[x]$ に属する相異なる次数 f のモニックな既約多項式の個数は $(p^f - p)/f$ で与えられる[*1]。

(証明)

n を、次数 f のモニックな既約多項式の個数であるとする。定理 3.9 より、次数 p^f の多項式 $x^{p^f} - x$ は、n 個の次数 f の多項式と p 個の次数 1 の既約多項式 $x - a$ $(a \in \mathbb{F}_p)$ の積で書き表される。よって、次数について等式 $p^f = nf + p$ が成立し、定理の主張が得られる。■

一般に、f が素数でないときのことを考える。n_d を、$\mathbb{F}_p[x]$ に属する次数 d のモニックな既約多項式の個数とする。系 3.10 と同じような議論をすることにより、$n_f = (p^f - \sum dn_d)/f$ であることが確かめられる。ここで、和は $d < f$ を満たす f の約数について取っている。

定理 3.11.

p : 素数、f : 正の整数、$q = p^f$ とする。$f(x)$ を $\mathbb{F}_p[x]$ に属する次数 f の既約多項式であるとする。このとき、$\mathbb{F}_q$ の 2 つの元の積と商は $O(\log^2 q)$ bit の演算で求まる。N が正の整数であるとき、$a \in \mathbb{F}_q$ に対して a^N は $O(\log N \log^2 q)$ bit の演算で求まる。

4　多項式に対する Euclid の互除法のアルゴリズム

この節では、2 つの 1 変数多項式の最大公約数を求めるアルゴリズムについて述べる。

定義 4.1. (最大公約数)

2 つの多項式 $f, g \in \mathbb{F}_p[x]$ の**最大公約数**とは、2 つの多項式を割り切るモニックな既約多項式のうち、次数が最大のものである。f, g を割り切る他の多項式 $h(x)$ があったとき、$h(x)$ は f, g の最大公約数を割り切る。

例 4.2.

$f(x) = x^4 + x^3 + x^2 + 1, g(x) = x^3 + 1 \in \mathbb{F}_2[x]$ とする。このとき、$\gcd(f, g)$ を Euclid の互除法のアルゴリズムで求め、$\gcd(f, g)$ を $u(x)f(x) + v(x)g(x)$ の形で表す。

$$\begin{aligned} x^4 + x^3 + x^2 + 1 &= (x + 1)(x^3 + 1) + (x^2 + x) \\ x^3 + 1 &= (x + 1)(x^2 + x) + (x + 1) \\ x^2 + x &= x(x + 1) \end{aligned}$$

よって、$\gcd(f, g) = x + 1$ である。この式を逆からたどっていくことで、$x + 1$ を $f(x)$ と $g(x)$ の線形結合として表すことができる。

$$\begin{aligned} x + 1 &= g(x) + (x + 1)(x^2 + x) \\ &= g(x) + (x + 1)(f(x) + (x + 1)g(x)) \\ &= (x + 1)f(x) + x^2 g(x) \end{aligned}$$

[*1] $(p^f - p)/f$ は、Fermat の小定理より $p^f \equiv p \pmod{f}$ であるから整数になることに留意する。

次に、多変数の多項式で Euclid の互除法を行うときに備えて、Euclid の互除法の多項式の除算を 1 ステップずつ行っていく事を考える。

例 4.3.

$f(x) = x^3 - 2x^2 + 5, g(x) = 2x^2 + 3x - 4 \in \mathbb{F}_{11}[x]$ とする。このとき、f, g が互いに素であることを示し、$u(x)f(x) + v(x)g(x) = 1$ となる多項式 $u(x), v(x)$ を求める。

$$\begin{aligned} f(x) &= x^3 - 2x^2 + 5 \\ &= (-5x)g(x) + (2x^2 + 2x + 5) \\ &= (-5x + 1)g(x) + (-x - 2) \\ g(x) &= 2x^2 + 3x - 4 \\ &= (-2x)(-x - 2) + (-x - 4) \\ &= (-2x + 1)(-x - 2) + (-2) \\ (-x - 2) &= (-x - 2) \cdot 1 \end{aligned}$$

よって $\gcd(f, g) = 1$ である。Euclid の互除法のステップを逆からたどっていくことで、

$$\begin{aligned} 1 &= 5g(x) + (-10x + 5)(x + 2) \\ &= 5g(x) + (-10x + 5)((-5x + 1)g(x) - f(x)) \\ &= (10x - 5)f(x) + (50x^2 - 35x + 10)g(x) \\ &= (-x - 5)f(x) + (-5x^2 - 2x - 1)g(x) \end{aligned}$$

となるので、$u(x) = -x - 5, v(x) = -5x^2 - 2x - 1$ であることが確認できる。

参考文献

[1] Neal Koblitz, “Algebraic Aspects of Cryptography”, Springer, 1998.

[2] 雪江明彦,『代数学 1 群論入門』, 日本評論社, 2010.

[3] 雪江明彦,『代数学 2 環と体とガロア理論』, 日本評論社, 2010.