Frobenius 写像の周辺

越川　皓永

1　はじめに

Frobenius 写像について、有限体の Galois 理論と Frobenius 写像の持ち上げについての δ 環の理論という 2 つの点から紹介する。環や体についての知識がなくてもある程度議論を追えるようにしたつもりであるが、用語を途中で用いることもある。また、線形代数はほぼ用いない形で説明している。$\mathbf{Z}$ で整数全体の集合、$\mathbf{N}$ で 0 以上の整数全体の集合をそれぞれ表す。

2　有限体 $\mathbf{F}_p$

偶数と奇数を足すと奇数になり、偶数同士、奇数同士を足せばそれぞれ偶数になる。これは 2 で割った余りについての足し算を考えていることと同等であり、もっと一般の余りについて成立する。

素数 p を取る。自然数（あるいは整数）a を p で割った余り $\overline{a}$ は

$$0,\quad 1,\quad \dots\quad ,\quad p-1$$

という p 通りの可能性がある。もう 1 つの数 b を考えて、冒頭に述べた事実は

$$\overline{a+b}=\overline{\overline{a}+\overline{b}}$$

と書くことができる。そこで、$\overline{a}+\overline{b}$ を

$$\overline{a}+\overline{b}:=\overline{\overline{a}+\overline{b}}$$

と定義する。（記号が混乱を招くかもしれないが、この定義では $\overline{a},\overline{b}$ という $\{0,\dots,p-1\}$ の元のみが使われている。あるいは a,b の取り方に依らない定義という言い方もできる。）すると上の式を言い換えて、$\overline{a}+\overline{b}=\overline{a+b}$ が成立する。引き算 $\overline{a}-\overline{b}$ も同様に定義し、$-\overline{a}:=\overline{0}-\overline{a}$ といったものも考えられる。この余りの加法は整数の加法と同じような性質を満たし、$\overline{0}=0$ が整数の加法における 0 と同じ役割をする。専門用語を用いると、集合 $\{0,1,\dots,p-1\}$ はこの加法を用いることで可換群（あるいはアーベル群）というものになる。（定義は省略する。）

更に、乗法を

$$\overline{a}\cdot\overline{b}:=\overline{\overline{a}\cdot\overline{b}}$$

と定義すれば、

$$\overline{a}\cdot\overline{b}=\overline{a\cdot b}$$

が成立することが分かる。この乗法も整数の乗法と同じ様な性質を満たし、$\overline{1}=1$ がやはり整数の乗法における 1 と同じ役割をする。さらに、上で考えた加法も一緒に組み合わせて、分配法則が成立する。専門用語では、集合 $\{0,1,\dots,p-1\}$ に可換環と呼ばれる構造を定めたことになる。

実はここまでは、p が素数であることは重要ではない。素数であることは除法を考える際で重要となる。そもそも整数では割り算をすると一般には余りが出てしまい、余りなくしようとすれば代わりに分数を考える必要が生じる。しかし、素数 p で割った余りで考えている際には、「余り」なく割り算ができる。

命題 p を素数とする。零でない整数 $a \in \{1, \dots, p-1\}$ に対し、ある整数 $b \in \{1, \dots p-1\}$ が唯一つ存在し、$ab-1$ が p で割り切れる。

証明 p 個の数 $\overline{a \cdot 0}\,(=0), \overline{a \cdot 1}, \dots, \overline{a \cdot (p-1)}$ がすべて相異なることを示せばよい。(そうすれば $\overline{a \cdot b} = 1$ となる $b\,(\neq 0)$ が唯一つ存在することになる。)

そこで $b, b' \in \{0, 1, \dots, p-1\}$ に対し、$\overline{a \cdot b} = \overline{a \cdot b'}$ と仮定する。すると $\overline{a(b-b')} = \overline{a \cdot b - a \cdot b'} = \overline{0}$ となり、$a(b-b')$ が p で割り切れることになる。p が素数であり、a が p で割り切れないことから、(素因数分解の一意性により) $b-b'$ が p で割れ切れる。b, b' は共に 0 以上 $p-1$ 以下なので、$b = b'$ でなければならない。

もう少しだけ直接的に証明を修正することもできる：p, a に Euclid の互除法を用いると、$cp + da = 1$ となる整数 c, d を見つけることができる。このとき $b = \overline{d}$ と取ればよい。 □

上記命題の b を a^{-1} と書くことにする。そこで、$\{0, \dots, p-1\}$ の除法を、$\overline{b} \neq 0$ のときに、

$$\frac{\overline{a}}{\overline{b}} := \overline{a} \cdot \overline{b}^{-1}$$

で定める。専門用語では体（あるいは可換体）と呼ばれるものにこれでなる。

定義 有限体 $\mathbf{F}_p$ とは $\{0, 1, \dots, p-1\}$ に上記の加減剰余を定めたものである。

元が p 個のみの体が $\mathbf{F}_p$ と「同型」になることはすぐに分かることを注意しておく。

3 Frobenius 写像

有限体 $\mathbf{F}_p$ では当然

$$\underbrace{1 + \cdots + 1}_{p\text{ 個}} = \overline{p} = 0$$

が成立する。(零環でない) 可換環 A が同様の性質 $\underbrace{1 + \cdots + 1}_{p\text{ 個}} = 0$ を満たすとき、A の標数が p であるという言い方をする。

命題 A が標数 p の可換環であるとする。このとき、$a, b \in A$ に対し、

$$(a+b)^p = a^p + b^p$$

が成立する。

証明 二項定理が A でも成立するので、

$$(a+b)^p = \sum_{i=0}^{p} \binom{p}{i} a^{p-i} b^i$$

となる。ここで二項係数は整数であり、A の元ともみなしている。二項係数

$$\binom{p}{i} = \frac{p!}{i!(p-i)!}$$

では、$i \neq 0, p$ のときに分子にのみ p が現れるので、そのとき二項係数は p で割り切れる整数となっている。したがって、A においては

$$(a+b)^p = \sum_{i=0}^{p} \binom{p}{i} a^{p-i} b^i = a^p + b^p$$

と計算できる。 □

また $(ab)^p = a^p b^p$ も成立する。A の自己写像

$$F\colon A \to A; \quad a \mapsto a^p$$

は環準同型と呼ばれるものになっており、Frobenius 写像・Frobenius 自己準同型などと呼ばれる。

系 (Fermat の小定理) 任意の $a \in \mathbf{F}_p$ に対し、$a^p = a$ となる。また、零でない $a \in \mathbf{F}_p$ に対し、$a^{p-1} = 1$ となる。

標数 p の可換環 A は $\mathbf{F}_p$ を「含んで」いて、この系の主張は $\mathbf{F}_p$ の元を A の元とみなしても成立する。

証明 上の命題を繰り返し用いることにより、

$$a^p = (\underbrace{1 + \cdots 1}_{a \text{ 個}})^p = \underbrace{1^p \cdots + 1^p}_{a \text{ 個}} = \underbrace{1 + \cdots + 1}_{a \text{ 個}} = a$$

と計算できる。$a \neq 0$ ならば、a^{-1} を掛ければ、$a^{p-1} = 1$ を得る。$\mathbf{F}_p$ が体であることから a 倍写像が全単射になり、それを用いて $a^{p-1} = 1$ を示すこともできる。 □

Frobenius 写像は $\mathbf{F}_p$ に対しては恒等写像と同じになっており、この事実自体は非自明であるものの、Frobenius 写像が「新しい」写像を与えているわけではないことになる。これはもちろん特別な現象である。

1 つの例として $\mathbf{F}_p$ 係数の多項式環 $\mathbf{F}_p[X]$ を考える。これは $\mathbf{F}_p$ 係数の多項式

$$a_0 + a_1 X + \cdots + a_d X^d, \quad a_0, \ldots, a_d \in \mathbf{F}_p$$

すべての集合を考え、多項式の加法・減法・乗法を通常と同じように定義したものである。すると $\mathbf{F}_p[X]$ においては、Frobenius 写像 F は、上記命題を用いることで、

$$F(a_0 + a_1 X + \cdots + a_d X^d) = a_0 + a_1 X^p + \cdots + a_d X^{dp}$$

とも書ける。これから、$F(f(X)) = f(X)$ となるような $f(X) \in \mathbf{F}_p[X]$ は

$$f(X) = a_0, \quad a_0 \in \mathbf{F}_p$$

の形のみであることも分かる。

4 有限体 $\mathbf{F}_{f(X)}$

もう 1 つの重要な例を与える。有限体 $\mathbf{F}_p$ は整数を p で割った余りを考えることで導入された。類似のことを多項式環 $\mathbf{F}_p[X]$ について考える。零でない多項式 $f(X) \in \mathbf{F}_p[X]$ を 1 つ取る。多項式環 $\mathbf{F}_p[X]$ では余り付きの割り算を整数の場合と同じように考えることができる（多項式の「次数」があることと $\mathbf{F}_p$ が体であるこ

とが重要である）ので、$\mathbf{F}_p$ の場合と同様にして $f(X)$ による割り算の「余り」を考える。多項式 f の次数を d とすると、「余り」の可能性は

$$r_0 + r_1 X + \cdots + r_{d-1} X^{d-1}, \quad r_0, \ldots, r_{d-1} \in \mathbf{F}_p$$

と書け、p^d 通りある。これらの「余り」に対し $\mathbf{F}_p$ の場合と同様に加法・減法・乗法を定めることができる。このように定まった可換環を $\mathbf{F}_{f(X)}$ と書く。

通常と同様に、定数でない多項式の積に分解できない多項式を既約多項式と呼ぶ。すると、Euclid の互除法を用いて、$\mathbf{F}_p[X]$ の元が既約多項式の積に「一意」に分解できることが証明できる。（$\mathbf{F}_p[X]$ の可逆元は零でない定数多項式であり、「一意」性は可逆元による曖昧さを許したものである。）

命題 $f(X) \in \mathbf{F}_p[X]$ が既約多項式であるとき、可換環 $\mathbf{F}_{f(X)}$ は体である。

証明 零でない $a \in \mathbf{F}_{f(X)}$ に対し、a 倍写像

$$\mathbf{F}_{f(X)} \to \mathbf{F}_{f(X)}; \quad b \mapsto a \cdot b$$

が単射であることを示せばよい。実際、有限集合の自己写像であることから、単射ならば全単射となり、1 の逆像が a^{-1} となる。

そこで $a \cdot b = a \cdot b'$ と仮定する。既約多項式 $f(X)$ が $a(b-b')$ を割り切ることから、$f(X)$ が a または $b-b'$ を割り切るが、a, b, b' の次数は d より小さいので $b = b'$ となるしかない。

あるいは、Euclid の互除法を直接 $f(X), a$ に用いることにより

$$g_1(X) f(X) + g_2(X) a = 1$$

となる多項式 $g_1(X), g_2(X) \in \mathbf{F}_p[X]$ を見つけることができる。このとき、$g_2(X)$ を $f(X)$ で割った「余り」が a^{-1} である。 □

以下、$f(X) = a_0 + a_1 X + \cdots + a_d X^d$ は既約であると仮定する。

系 零でない $a \in \mathbf{F}_{f(X)}$ に対し、$a^{p^d-1} = 1$。

これより、F^d は $\mathbf{F}_{f(X)}$ の恒等写像となる。

証明 前証明でみたように a 倍写像が全単射となる。0 は 0 に写るので、それ以外の元の積をとると

$$\prod_{b \neq 0} b = \prod_{b \neq 0} (a \cdot b) = a^{p^d-1} \prod_{b \neq 0} b$$

となり、これから $a^{p^d-1} = 1$ を得る。 □

この証明は元の個数が p^d である有限体であれば通じることを注意しておく。

系 $X^{p^d} - X$ は $f(X)$ で割り切れる。

証明 前系より、$X^{p^d} - X = 0$ が $\mathbf{F}_{f(X)}$ で成立していることになる。これは、$\mathbf{F}_{f(X)}$ の定義より、$f(X)$ が $X^{p^d} - X$ を $\mathbf{F}_p[X]$ において割り切ることを意味する。 □

次に体 $\mathbf{F}_{f(X)}$ 係数の多項式環 $\mathbf{F}_{f(X)}[Y]$ を更に考える。この可換環においても、既約多項式分解の存在と一意性が証明できる。

系 $\mathbf{F}_{f(X)}[Y]$ において、

$$Y^{p^d} - Y = \prod_{a \in \mathbf{F}_{f(X)}} (Y - a)$$

と分解する。

証明 任意の $a \in \mathbf{F}_{f(X)}$ に対し、$Y^{p^d} - Y$ が $Y - a$ で割り切れることが $a^{p^d} = a$ より分かる。また、$Y - a$ らは互いに素な p^d 個の 1 次式である。よって、その積は $Y^{p^d} - Y$ と一致する。 □

5 原始根

命題 体 $\mathbf{F}_{f(X)}$ の 0 でない元 a に対し、$a^m = 1$ となる最小の 0 より大きい整数 m は $p^d - 1$ を割り切る。また、$p^d - 1$ の正の約数 m に対し、位数が m となる a の $\mathbf{F}_{f(X)}$ の元の個数は $\varphi(m)$ 個である。

命題中の m を a の位数という。この命題で $\varphi(m)$ は m と互いに素な 1 以上 m 未満の整数の個数を表す Euler の関数である。

証明 $p^d - 1$ を m で割った余りを r とし、$p^d - 1 = qm + r$ と書く。すると、

$$1 = a^{p^m - 1} = a^{qm} \cdot a^r = (a^m)^q \cdot a^r = a^r$$

となる。したがって、m の最小性より $r = 0$ でなければならない。

$p^d - 1$ の約数 m に対し、$\mathbf{F}_{f(X)}$ 係数多項式 $Y^m - 1$ を考える。位数 m の元 a が存在すれば、整数 $i \in \{1, \dots m\}$ に対し、$Y - a^i$ が $Y^m - 1$ を割り切るので、以前の議論と同様にして、$Y^m = 1$ を満たす元は a^i で尽くされることが分かる。(a^i は互いに相異なる。実際、$a^i = a^j$ であれば $a^{j-i} = 1$ であるが、位数が m より $i = j$ となる。) また、i が m と互いに素でなければ、a^i の位数は m より小さい m の約数になる。したがって、位数 m の元の個数は $\varphi(m)$ 以下であると分かる。

任意の 0 でない元の位数が $p^d - 1$ を割り切ることと等式

$$\sum_{m \text{ は } p^d - 1 \text{ の約数}} \varphi(m) = p^d - 1$$

を組み合わせると、どの m に対しても位数が m となる元の個数が $\varphi(m)$ とならなければいけないと分かる。 □

系 ある $\mathbf{F}_{f(X)}$ の元 α が存在し、α の位数が $p^d - 1$ となる。特に、任意の 0 でない $\mathbf{F}_{f(X)}$ の元は $\alpha^e, 1 \leq e \leq p^d - 1$ という形に唯一の方法で書ける。

α は原始根と呼ばれることがある。この系とその証明は元の個数が p^d であるどのような体にも通用することを注意しておく。

証明 位数が $p^d - 1$ となる元 α が存在することは前命題と $\varphi(p^d - 1) > 0$ より従う。すると $\alpha^e, 1 \leq e \leq p^d - 1$ の形の元はすべて相異なる。これらは $p^d - 1$ 個あるので、$\mathbf{F}_{f(X)}$ の 0 以外の元がすべて現れる。 □

系 体 $\mathbf{F}_{f(X)}$ において、$X, F(X) = X^p, \dots, F^{d-1}(X) = X^{p^{d-1}}$ は互いに相異なる。また、

$$f(Y) = a_d(Y - X)(Y - F(X)) \cdots (Y - F^{d-1}(X))$$

が $\mathbf{F}_{f(X)}[Y]$ で成立する。

証明 前半の主張を示すには、$X \neq F^i(X)$ を $i, 1 \leq i \leq d-1$ に対し示せば十分である。ある i に対し $X = F^i(X)$ と仮定する。すると $F^i(X^j) = X^j$ が任意の j に対し成立するから、任意の $a \in \mathbf{F}_{f(X)}$ に対し、$F^i(a) = a$ となる。これは位数が $p^d - 1$ の元が存在することに矛盾する。

後半の主張を示す。$\mathbf{F}_{f(X)}$ において、$f(X) = 0$ であるから、$Y - X$ が $f(Y)$ を割り切ることが分かる。また、

$$f(F^i(X)) = F^i(f(X)) = F^i(0) = 0$$

でもあるから、$Y - F^i(X)$ が $f(Y)$ を割り切ることも分かる。前半の主張と組み合わせて、

$$(Y - X)(Y - f(X)) \cdots (Y - F^{d-1}(X))$$

が $f(Y)$ を割り切ることが分かり、次数を比較することで実は等しいことも分かる。 □

6 既約多項式の存在

今までは既約多項式 $f(X)$ から始めていたが、整数 $d \geq 1$ に対し、次数 d の既約多項式が存在するかを議論する。今までの議論により、そのような既約多項式は $X^{p^d} - X$ を割り切るから、$X^{p^d} - X$ の既約因子で次数 d のものが存在するかを調べる。

補題 既約多項式 $f(X)$ が $X^{p^d} - X$ を割り切るとき、$f(X)$ の次数 d_f は d を割り切る。逆に m が d の約数で、$f(X)$ が次数 m の既約多項式のとき、$f(X)$ は $X^{p^d} - X$ を割り切る。

証明 体 $\mathbf{F}_{f(X)}$ において、F^{d_f} は恒等写像であり、d_f はそのような最小の数であった。一方、$f(X)$ が $X^{p^d} - X$ を割り切ることから、F^d も恒等写像になる。したがって、d_f は d を割り切る。

また、$f(X)$ が次数 m の既約多項式のとき、$f(X)$ は $X^{p^m} - X$ を割り切る。よって、m が d の約数であれば、$f(X)$ は $X^{p^d} - X$ も割り切る。($\mathbf{F}_{f(X)}$ において、$F^m(X) = X$ を繰り返し用いることで、$X^{p^d} = F^d(X) = (F^m)^{d/m}(X) = X$ と計算できる。) □

命題 $N(p, m)$ で次数 m の $\mathbf{F}_p$ 係数既約多項式で X^m の係数が 1 のものの個数を表すとする。そのとき、

$$\sum_{m \text{ は } d \text{ の約数}} m \cdot N(p, m) = p^d.$$

証明 前補題より、$f(X)$ が $X^{p^d} - X$ の既約因子のときに、$f(X)^2$ が $X^{p^d} - X$ を割り切らないことを示せばよい。これには、$\mathbf{F}_{f(X)}[Y]$ で $Y^{p^d} - Y$ を代数的に微分してから $Y = X$ を代入して 0 でないことを確認すればよい。(積の微分と $\mathbf{F}_{f(X)}$ において $f(X) = 0$ であることを用いている。) そして、$\mathbf{F}_{f(X)}[Y]$ において、

$$(Y^{p^d} - Y)' = p^d Y^{p^d - 1} - 1 = -1$$

と計算でき、これは 0 でない。 □

これから既約多項式の存在が導ける：

系 任意の整数 $d \geq 1$ に対し、$N(p, d)$ は 0 でない。

証明 不等式

$$\sum_{m \text{ は } d \text{ の約数}, m \neq d} m \cdot N(p, m) < p^d$$

を示せばよい。任意の整数 m に対し $m \cdot N(p,m) \leq p^m$ であることは前系より明らかであるから、

$$\sum_{m \text{ は } d \text{ の約数}, m \neq d} m \cdot N(p,m) \leq \sum_{1 \leq m < d} p^m = \frac{p^d - 1}{p-1} < p^d$$

となる。 □

Möbius の反転公式と呼ばれるものを用いると、$N(p,d)$ 自体の式を得ることもできるがここでは省略する。

7 $\mathbf{F}_{f(X)}$ の Galois 理論

次数 d の既約多項式 $f(X)$ を取る。d の約数 m に対し、

$$\mathbf{F}_{f(X),m} := \{a \in \mathbf{F}_{f(X)} \mid F^m(a) = a\}$$

と定める。この部分集合は加減剰余で閉じており、$\mathbf{F}_{f(X)} = \mathbf{F}_{f(X),d}$ の部分体と呼ばれるものになる。

命題 $\mathbf{F}_{f(X),m}$ の元の個数は p^m であり、位数が $p^m - 1$ となる元を含む。特に、$m = 1$ のとき、$\mathbf{F}_{f(X),1}$ は $\mathbf{F}_p$ と同型となる。

証明 $\mathbf{F}_{f(X),m}$ の 0 でない元の位数は $p^m - 1$ を割り切る。逆に位数が $p^m - 1$ を割り切る元は $\mathbf{F}_{f(X),m}$ に属する。したがって、$\mathbf{F}_{f(X),m}$ の元の個数は

$$1 + \sum_{n \text{ は } p^m - 1 \text{ の約数}} \varphi(n) = 1 + p^m - 1 = p^m$$

と計算できる。

$m = 1$ のときの主張は、定数多項式全体が丁度 $\mathbf{F}_{f(X),1}$ になることから従う。 □

命題 m, m' を d の約数とする。$\mathbf{F}_{f(X),m} \subset \mathbf{F}_{f(X),m'}$ となる必要十分条件は m が m' の約数になることである。

証明 m' が m の倍数のとき、$\mathbf{F}_{f(X),m} \subset \mathbf{F}_{f(X),m'}$ となることは明らかである。逆に、$\mathbf{F}_{f(X),m} \subset \mathbf{F}_{f(X),m'}$ と仮定する。位数が $p^m - 1$ の元 $a \in \mathbf{F}_{f(X),m}$ を取る。仮定より $a^{p^{m'}-1} = 1$ であり、位数が $p^m - 1$ であることから、$p^m - 1$ が $p^{m'} - 1$ を割り切る。これより m が m' を割り切ることが分かる。 □

$\mathbf{F}_{f(X)}$ の部分体は実は $\mathbf{F}_{f(X),m}$ で尽くされる。$\mathbf{F}_{f(X),m}$ 自体の定義・包含関係と合わせて、これは拡大 $\mathbf{F}_p \subset \mathbf{F}_{f(X)}$ についての Galois 理論といえるものになる。

次の補題は論理的には必要ないが、その証明と同じ手法を後で用いる。

補題 ある元 $a \in \mathbf{F}_{f(X),m}$ が m と異なる m のどの約数 n に対しても $a \notin \mathbf{F}_{f(X),n}$ を満たすと仮定する。このとき、$\mathbf{F}_{f(X),m}$ の元 b は

$$b = b_0 + b_1 a + \cdots + b_{m-1} a^{m-1}, \quad b_0, \ldots, b_{m-1} \in \mathbf{F}_p$$

という形に唯一の方法で書ける。

証明 $\mathbf{F}_p$ と a から加法、減法、乗法を用いて書ける元、つまり

$$b = b_0 + b_1 a + \cdots + b_e a^e, \quad b_0, \ldots, b_e \in \mathbf{F}_p$$

という形の元すべてのなす $\mathbf{F}_{f(X),m}$ の部分集合 $\mathbf{F}_p(a)$ を考える。これは明らかに部分環になる。また、$\mathbf{F}_p(a)$ は有限集合であるから、ある 0 でない多項式 $g(X) = c_0 + c_1X + \cdots c_eY^e \in \mathbf{F}_p[X]$ が存在して

$$0 = g(a) = c_0 + c_1a + \cdots + c_ea^e$$

となる。そのような $g(X)$ のうち次数 e が最小のものを取る。$\mathbf{F}_{f(X)}$ が体であることから、$g(X)$ は既約多項式となることが分かる。すると写像

$$\mathbf{F}_{g(X)} \to \mathbf{F}_p(a); \quad h(X) \mapsto h(a)$$

により、$\mathbf{F}_{g(X)}$ と $\mathbf{F}_p(a)$ が同型になることが分かる。よって、$\mathbf{F}_p(a)$ は元の個数が p^e の体となる。すると、すべての $\mathbf{F}_p(a)$ の元 x が $x^{p^e} = x$ を満たすことになり、$\mathbf{F}_p(a) \subset \mathbf{F}_{f(X),e}$ となるが、元の個数が等しいので $\mathbf{F}_p(a) = \mathbf{F}_{f(X),e}$ となる。包含 $\mathbf{F}_{f(X),e} = \mathbf{F}_p(a) \subset \mathbf{F}_{f(X),m}$ より、e が m の約数となる。仮定より、$e = m$ でなければならない。体 $\mathbf{F}_{g(Y)}$ と $\mathbf{F}_p(a)$ の同型があることが分かったので、主張が示された。 □

命題 M を $\mathbf{F}_{f(X)}$ の部分体とする。ある d の約数 m が存在して、$M = \mathbf{F}_{f(X),m}$ となる。

証明 α を位数 $p^d - 1$ の元とする。すると $\mathbf{F}_p(\alpha) = \mathbf{F}_{f(X)}$ である。前証明と同様の議論を体 M 係数の多項式環 $M[Y]$ を用いて行うことで、ある既約多項式 $g(Y) \in M[Y]$ と同型

$$M[Y]/(g(Y)) \to \mathbf{F}_{f(X)}; \quad h(Y) \mapsto h(\alpha)$$

が存在する。ここで、$M[Y]/(g(Y))$ は $g(Y)$ による割り算の「余り」に体の構造を入れたものである。以前と同様の議論により、「余り」の元の個数は $\#M$ のべきとなる。したがって、$\#M$ は p^d のべき根となるが、そのような数はある d の約数 m を用いて p^m と書ける。つまり、M は元の個数が p^m の体となり、任意の M の元 x に対し $x^{p^m} = x$ となる。したがって、$M \subset \mathbf{F}_{f(X),m}$ となり、元の個数が等しいから $M = \mathbf{F}_{f(X),m}$ となる。 □

$\#M$ が p^d のべき根となることを示すには、線形代数を代わりに使うことを許せば、$\mathbf{F}_{f(X)}$ が M 上のベクトル空間であり基底を持つことからも導ける。

8 有限体の一意性

任意の整数 $d \geq 1$ に対し、次数 d の既約多項式 $f(X) \in \mathbf{F}_p[X]$ が存在することを証明した。そして $\mathbf{F}_{f(X)}$ は元の個数が $q := p^d$ の体であった。実はそのような体は、p, d を固定したとき、すべて「同型」となる。結果、そのような体を単に $\mathbf{F}_q$ と書くことが多い。(ただし、一意なのはあくまで同型類なので少し曖昧さのある記号である。)

この一意性について大体のことを説明する。$f(X), g(X) \in \mathbf{F}_p[X]$ を共に次数 d の既約多項式とする。既にみたように、$f(Y), g(Y)$ は $Y^{p^d} - Y$ を $\mathbf{F}_p[Y]$ において割り切る。一方、$\mathbf{F}_{f(X)}[Y]$ において、

$$Y^{p^d} - Y = \prod_{a \in \mathbf{F}_{f(X)}} (Y - a)$$

という分解があった。これより、$g(Y)$ も $\mathbf{F}_{f(X)}[Y]$ において 1 次式の積に分解することが分かる。$g(Y)$ を割り切る 1 次式 $Y - b, b \in \mathbf{F}_{f(X)}$ を 1 つ取る。写像

$$B\colon \mathbf{F}_{g(X)} \to \mathbf{F}_{f(X)}; \quad h(X) \mapsto h(b)$$

を考える。$g(b)=0$ であることを使うと、この写像 B は加減剰余を保つ。また、$g(X)$ が既約であることから、B は単射である。元の個数がともに p^d の集合の間の写像であるから、B は全単射になること（「同型」になること）が結局分かる。また、$X, F(X), \dots, F^{d-1}(X)$ が $\mathbf{F}_{g(X)}$ において互いに相異なるので、

$$B(X)=b, \quad B(F(X))=F(b), \quad \dots \quad , \quad B(F^{d-1}(X))=F^{d-1}(b)$$

も相異なり、分解

$$g(Y)=c(Y-b)(Y-F(b))\cdots(Y-F^{d-1}(Y))$$

が $\mathbf{F}_{f(X)}[Y]$ において存在することが分かる。（ここで c は $g(Y)$ の Y^d の係数である。）つまり、$g(Y)$ を割り切る 1 次式の選び方というのは定数項での F^i によるずれだけ可能性があるということである。写像 B の定義において、b の代わりに $F^i(b)$ を用いると、B と F^i の合成 $F^i\circ B = B\circ F^i$ が得られる。結論をまとめておく：

命題 上述の意味において $\mathbf{F}_{f(X)}$ と $\mathbf{F}_{g(X)}$ は同型であり、同型は F^i によるずれを除いて一意に決まる。

最後に、元の個数が $q=p^d$ の体は $\mathbf{F}_{f(X)}$ の形の体に同型になることを注意しておく。実際、そのような体は自動的に標数 p になり、位数 p^d-1 の元 α が存在することが前と同様の議論で証明できる。すると、

$$\mathbf{F}_p[X]\to\mathbf{F}_q; \quad h(X)\mapsto h(\alpha)$$

という全射を考えることができ、前と同様の議論により、$\mathbf{F}_q$ が $\mathbf{F}_{f(X)}$ の形に書けることが分かる。

9 Frobenius 持ち上げ・δ 構造

可換環 A の標数が素数 p のときに、Frobenius 写像 $F\colon A\to A; a\mapsto a^p$ が環準同型となるのであった。標数が p でないときにも Frobenius 写像の「代わり」を用いるというアイデアはある程度古典的なものであったが、近年改めてそのアイデアに焦点が当てられている。その触り部分を紹介する。

可換環 A の自己準同型 $\varphi\colon A\to A$ を Frobenis 写像と結びつけるには少なくとも p で割った「余り」で考える必要がある。つまり、

$$\varphi(x)=x^p+(p\text{ の倍数})$$

という条件が少なくとも必要である。δ 構造というのはこの「p の倍数」部分を「p で割った」ものが満たすべき性質を公理化したものである。（技術的なことを述べれば、A に p 捩れがあると p で割ることは一意にはできない。δ 構造は p 捩れのある環に対しては、φ より多い情報を与えるものになる。）

定義 (Joyal) A を可換環とする。A の δ 構造とは写像 $\delta\colon A\to A$ であって、

$$\delta(0)=\delta(1)=0, \quad \delta(ab)=\delta(a)b^p+a^p\delta(b)+p\delta(a)\delta(b),$$
$$\delta(a+b)=\delta(a)+\delta(b)-\sum_{i=1}^{p-1}\frac{(p-1)!}{i!(p-i)!}a^ib^{p-i}$$

を満たすもののことである。可換環と δ 構造の組を δ 環と呼ぶ。

δ 環の元 a に対し, $\varphi(a)=\varphi_A(a)=a^p+p\delta(a)$ と定める。

命題 δ 環 A の元 a, b に対し、

$$\varphi(a+b) = \varphi(a) + \varphi(b), \quad \varphi(ab) = \varphi(a)\varphi(b)$$

が成立する。また、$\varphi(1) = 1$ である。つまり、$\varphi\colon A \to A$ は環準同型である。

証明 φ, δ の定義より、

$$\begin{aligned}\varphi(a+b) &= (a+b)^p + p\delta(a+b) \\ &= a^p + b^p + \sum_{i=1}^{p-1} \frac{p!}{i!(p-i)!} a^i b^{p-i} + p\delta(a) + p\delta(b) - \sum_{i=1}^{p-1} p\frac{(p-1)!}{i!(p-i)!} a^i b^{p-i} = \varphi(a) + \varphi(b)\end{aligned}$$

である。同様に、

$$\varphi(a)\varphi(b) = (a^p + p\delta(a))(b^p + p\delta(b)) = a^p b^p + p\big(\delta(a)b^p + a^p\delta(b) + p\delta(a)\delta(b)\big) = \varphi(ab)$$

となる。また、$\varphi(1) = 1 + 0 = 1$ である。 □

典型的な δ 環の例を挙げておく．まず、任意の整数 m に対し $m - m^p$ が p で割り切れるから $\delta(m) = (m - m^p)/p$ という写像 $\delta\colon \mathbf{Z} \to \mathbf{Z}$ が定まり、これが δ 構造になる。この場合、φ は恒等写像 $\varphi(m) = m$ である。これは $\mathbf{F}_p$ において Frobenius が恒等写像であり、$\mathbf{Z}$ の恒等写像がその持ち上げであるということを言い換えたものである。

次に多項式環 $\mathbf{Z}[X]$ を考える。$\mathbf{F}_p[X]$ においては $f(X)^p = f(X^p)$ であったから、$\mathbf{Z}[X]$ において

$$\delta(f(X)) = \frac{f(X^p) - f(X)^p}{p}$$

が定まる。これは δ 構造であり、$\varphi(f(X)) = f(X^p)$ となる。この例の特徴は $\delta(X) = 0$ となることである。

前の例において $\delta(X) = 0$ であったが、これはある意味で「条件」を課していることになる。$\delta(X)$ 自体を新たな変数として追加することで、この「条件」を外すことができる。正確には、無限変数多項式環

$$\mathbf{Z}[X_0, X_1, X_2, \dots]$$

を考える。ここで $X_0 = X$ である。このとき、$\delta(X_i) = X_{i+1}, i \geq 0$ となるような δ 構造が唯一存在する。また、そのとき $\varphi(X_i) = X_i^p + pX_{i+1}$ である。実際、$\varphi(X_i) = X_i^p + pX_{i+1}$ となるような環準同型 φ は唯一存在するから、そこから δ が決まり、$\delta(X_i) = X_{i+1}$ を満たす。(元 $f \in \mathbf{Z}[X_0, X_1, X_2, \dots]$ が与えられたときに $\delta(f)$ を $X_0, X_1, \dots$ を用いて一意に書くことができるわけだが、これは $\delta(X_i) = X_{i+1}$ と δ 環の公理のみから帰納的に計算することができることを注意しておく。)

系 任意の δ 環 A に対し、$\varphi \circ \delta = \delta \circ \varphi$ が成立する。

証明 元 $a \in A$ が与えられたとき、δ 構造を保つような環準同型

$$\mathbf{Z}[X_0, X_1, X_2, \dots] \to A; \quad X_i \mapsto \delta^i(a)$$

が存在する。したがって、A が $\mathbf{Z}[X_0, X_1, X_2, \dots]$ の場合だけ証明すればよい。この場合は、$p\delta \circ \varphi, p\varphi \circ \delta$ がともに $\varphi \circ \varphi - (\varphi$ の p 乗) と一致することよりよい。 □

より一般に、可換環 A が与えられたとき、上のような構成を一般化して (A と別の) 環と δ 構造を構成することができる。これはいわば「A から生成される」δ 環である。もう少し正確には δ 環の圏から可換環の圏への忘却関手の左随伴関手を与える。一方、実は右随伴関手も存在する。次はその記述を紹介する。

10　Witt ベクトルの環

A を可換環とする。A の元の列

$$a = (a_0, a_1, \dots)$$

すべてのなす集合 $A^{\mathbf{N}}$ を考える。自己写像 $\delta\colon A^{\mathbf{N}} \to A^{\mathbf{N}}$ を

$$a = (a_0, a_1, \dots) \mapsto \delta(a) = (a_1, a_2, \dots)$$

で定める。以下では、上の写像 δ が δ 構造を定めるような可換環の構造を $A^{\mathbf{N}}$ に定める。また、射影

$$p_0\colon A^{\mathbf{N}} \to A; \quad a = (a_0, a_1, \dots) \mapsto p_0(a) = a_0$$

が環準同型となるようにもする。例えば、$a+b$ の第 0 成分 $p_0(a+b) = (a+b)_0$ は $a_0 + b_0$ でなければならない。また、$a \cdot b$ の第 0 成分は $a_0 \cdot b_0$ である。次に第 1 成分について考える。$a+b$ の第 1 成分は $\delta(a+b)$ の第 0 成分でなければならない。また、$\delta(a+b)$ は δ 構造になっているのであれば、

$$\delta(a+b) = \delta(a) + \delta(b) - \sum_{i=1}^{p-1} \frac{(p-1)!}{i!(p-i)!} a^i b^{p-i}$$

を満たさなければならない。したがって、p_0 が環準同型であることも用いれば、

$$(a+b)_1 = p_0(\delta(a+b)) = \delta(a)_0 + \delta(b)_0 - \sum_{i=1}^{p-1} \frac{(p-1)!}{i!(p-i)!} a_0^i b_0^{p-i} = a_1 + b_1 - \sum_{i=1}^{p-1} \frac{(p-1)!}{i!(p-i)!} a_0^i b_0^{p-i}$$

が成立しなければならない。

これを帰納的に行う。それには次の補題がいる。

補題 整数 $m \geq 0$ に対し、ある $2(m+1)$ 変数整数係数多項式 $S_m(A_0, \dots, A_m, B_0, \dots, B_m)$ および $P_m(A_0, \dots, A_m, B_0, \dots, B_m)$ が存在し、任意の δ 環 A の元 a, b に対し、

$$\delta^{m+1}(a+b) = S_m(a, \dots, \delta^m(a), b, \dots, \delta^m(b)), \quad \delta^{m+1}(a \cdot b) = P_m(a, \dots, \delta^m(a), b, \dots, \delta^m(b))$$

が成立する。また、このような S_m, P_m はそれぞれ唯一である。

証明 2 つの変数 $X = X_0, Y = Y_0$ から「生成」される無限変数 δ 環

$$\mathbf{Z}[X_0, X_1, \dots, Y_0, Y_1, \dots]$$

を考える。(前と同様に $\delta(X_i) = X_{i+1}, \delta(Y_i) = Y_{i+1}$ である。) $\delta^m(X_0 + Y_0)$ という元は唯一の $2(m+1)$ 変数整数係数多項式 $S(X_0, \dots, X_m, X_0, \dots, X_m)$ を用いて、

$$\delta^m(X_0 + Y_0) = S(X_0, \dots, X_m, X_0, \dots, X_m)$$

と書けることが容易に分かる。この $S_m(X_0, \dots, X_m, X_0, \dots, X_m)$ が条件を満たす。同様に、$\delta^m(X_0 \cdot Y_0)$ という元は唯一の $2(m+1)$ 変数整数係数多項式 $P(X_0, \dots, X_m, X_0, \dots, X_m)$ を用いて、

$$\delta^m(X_0 \cdot Y_0) = P_m(X_0, \dots, X_m, X_0, \dots, X_m)$$

と書け、この P_m が条件を満たす。 □

整数 $m \geq 0$ に対し、$a+b, a\cdot b$ の第 m 成分までが定まっているとし、第 $m+1$ 成分を

$$(a+b)_{m+1} := S_m(a_0,\dots,a_m,b_0,\dots,b_m), \quad (a\cdot b)_{m+1} := P_m(a_0,\dots,a_m,b_0\dots,b_m)$$

で定める。これにより、2 つの写像 $+,\cdot : A^{\mathbf{N}} \times A^{\mathbf{N}} \to A^{\mathbf{N}}$ が定義された。後はこれが可換環を定め、δ が実際に δ 構造であることを確認すればよい。また可換環であることさえ確認すれば、δ が δ 構造を定めていることは上記補題と $+,\cdot$ の定め方から明らかである。可換環であることを確認するには単位元と零元も必要であるが、

$$(1,0,0,\dots), \quad (0,0,0,\dots)$$

が具体的に取れ、これが条件を満たすことは、前補題の証明で S_m および P_m を $\mathbf{Z}[X_0,X_1,\dots,Y_0,Y_1,\dots]$ を用いて構成したことから確認できる。可換環であることを確認するには結合法則や分配法則といった等式も確認する必要がある。これらの等式は代わりに

$$\mathbf{Z}[X_0,X_1,\dots,Y_0,Y_1,\dots,Z_0,Z_1,\dots]$$

を用いることで確認すればよくなり、そしてこれが δ 環であることからそれは当然成立する。また、$+$ についての逆元の存在も必要であるが、$\mathbf{Z}[X_0,X_1,\dots]$ において $\delta^m(-X_0)$ を記述する多項式を見つけて、$+,\cdot$ と同様に帰納的に $-a$ の第 m 成分を決定することができる。

以上によって、可換環 A から、$(A^{\mathbf{N}},+,\cdot,\delta)$ という δ 環が構成された。この構成は実は δ 環の圏から可換環の圏への忘却関手の右随伴関手を与える。特に、A が δ 環である場合、

$$A \to A^{\mathbf{N}}; \quad a \mapsto (a,\delta(a),\delta^2(a),\dots)$$

は環準同型となる。実際、$(+,\cdot)$ の構成はまさしくこれが成立するようになっている。

可換環 $(A^{\mathbf{N}},+,\cdot)$ はより古くから知られている Witt ベクトルの環というものと同型になっているので、これを説明する。

補題 δ 環 $\mathbf{Z}[X_0,X_1,\dots]$ において、

$$\varphi^m(X_0) = \sum_{i=0}^{m} p^i D_i(X_0,\dots,X_i)^{p^{m-i}}$$

がすべての整数 $m \geq 0$ について成立するような $D_0, D_1, D_2, \dots$ が唯一存在し、また

$$D_m(X_0,\dots,X_m) = X_m + (\text{定数項が } 0 \text{ となっている } X_0,\dots,X_{m-1} \text{ の多項式})$$

と書ける。さらに、任意の δ 環 A の元 a に対し、

$$\varphi^m(a) = D_0(a)^{p^m} + pD_1(a,\delta(a))^{p^{m-1}} + \cdots + p^m D_m(a,\delta(a),\dots,\delta^m(a))$$

が成立する。

証明 D_m の存在と性質を m についての帰納法でまとめて証明する。まず $D_0(X_0) = X_0, D_1(X_0,X_1) = X_1$ である。$D_0,\dots,D_m$ が存在したとする。このとき、後半の主張が m までについては正しい。したがって、等式

$$\varphi^m(X_0) = \sum_{i=0}^{m} p^i D_i(X_0,\dots,X_i)^{p^{m-i}}$$

に $\varphi(X_0)$ を代入することで、

$$\varphi^{m+1}(X_0) = \sum_{i=0}^{m} p^i D_i(\varphi(X_0), \dots, \delta^i(\varphi(X_0)))^{p^{m-i}}$$

となる。また、φ と δ は可換なので、

$$\delta^i(\varphi(X_0)) = \varphi(\delta^i(X_0)) = X_i^p + pX_{i+1}$$

となり、さらに

$$D_i(\varphi(X_0), \dots, \delta^i(\varphi(X_0))) = D_i(X_0, \dots, \delta^i(X_0))^p + (p \text{ の倍数})$$

となる。これより、

$$p^i D_i(\varphi(X_0), \dots, \delta^i(\varphi(X_0)))^{p^{m-i}} = p^i D_i(X_0, \dots, \delta^i(X_0))^{p^{m+1-i}} + (p^{m+1} \text{ の倍数})$$

となるから「p^{m+1} の倍数」の和を D_{m+1} とおく。D_{m+1} の X_{m+1} を含む項が X_{m+1} のみであることを確認する。上記の議論において、X_{m+1} が寄与するのは $p^m D_m(\varphi(X_0), \dots, \delta^m(\varphi(X_0))$ のみであり、さらに帰納法の仮定から、その内の $p^m \delta^m(\varphi(X_0))$ のみである。そして、

$$p^m \delta^m(\varphi(X_0)) = p^m \varphi(\delta^m(X_0)) = p^m X_m^p + p^{m+1} X_{m+1}$$

であるから、D_{m+1} に現れる X_{m+1} を含む項は X_{m+1} のみである。 □

$\delta_m(a) := D_m(a, \delta(m), \dots, \delta^m(a))$ とおく。前補題を用いると、$\delta^m(a)$ を $a, \delta(a), \dots, \delta_m(a)$ を用いて書けることが m についての帰納法で分かる。同様の理由で次の系も得られる。

系 写像

$$A^{\mathbf{N}} \to A^{\mathbf{N}}; \quad (a_0, a_1, \dots) \mapsto (D_0(a_0), D_1(a_0, a_1), D_2(a_0, a_1, a_2), \dots)$$

は全単射である。

この写像により、以前に定義した $+, \cdot$ を右に移すことで得られる可換環こそが Witt ベクトルの環と呼ばれるものと同じになる。この可換環を $W(A)$ と書くことにする。なお、単位元と零元は再び

$$(1, 0, 0, \dots), \quad (0, 0, 0, \dots)$$

となっている。

系 $m \geq 0$ を整数とする。写像

$$w_m \colon W(A) = A^{\mathbf{N}} \to A; \quad b = (b_0, b_1, \dots) \mapsto b_0^{p^m} + pb_1^{p^{m-1}} + \cdots + p^m b_m$$

は環準同型となる。

可換環の圏から可換環の圏への関手とみなしたとき、Witt ベクトルの環はこの系の性質で特徴づけられる。

証明 まず、今までの議論のように、$\Phi_m(X_0, \dots, X_m) = \varphi^m(X_0)$ とおく。すると、前補題より、

$$b = (b_0, b_1, \dots) = (D_0(a_0), D_1(a_0, a_1), \dots)$$

と書いたとき、$w_m(b) = \Phi_m(a_0, a_1, \dots, a_m)$ となる。φ^m は環準同型となっていることから、Φ_m は対応する性質を満たし、それにより w_m が環準同型になることが分かる。 □

11 p 進整数環

A が有限体 $\mathbf{F}_p$ の場合を考える。$W(\mathbf{F}_p)$ は $\mathbf{Z}_p$ とも書かれ、p 進整数環と呼ばれる。この可換環で

$$p = p(1, 0, \dots)$$

をまず計算する。そのために、代わりに $W(\mathbf{Z})$ で同じものを計算する。この場合は $w_m(p) = p \in \mathbf{Z}$ であることを使えば計算することができ、例えば最初の 2 項は

$$p = (p, 1 - p^{p-1}, \dots) \in W(\mathbf{Z})$$

となる。さらに続けると、第 3 項以降は p で割り切れることが分かる。(実は p^2 でも割り切れる。) したがって、$W(\mathbf{F}_p)$ においては

$$p = (0, 1, 0, \dots)$$

となる。($\mathbf{Z}$ は δ 環でもあるから、$\mathbf{Z} \to W(\mathbf{Z})$ を使っても計算できる。)

より一般に、$\mathbf{Z}_p = W(\mathbf{F}_p)$ では

$$p(b_0, b_1, b_2, \dots) = (0, b_0, b_1, \dots)$$

となる。すると $\mathbf{Z}_p$ の元 b に対し、$c_0\,(= b_0), c_1, \dots \in \mathbf{F}_p$ が一意的に存在し、任意の整数 $m \geq 0$ に対し、

$$b - \big((c_0, 0, \dots) + p(c_1, 0, \dots) + \cdots + p^m(c_m, 0, \dots)\big)$$

が p^{m+1} の倍数となることが分かる。逆にどのような列 $c_0, c_1, \dots \in \mathbf{F}_p$ に対しても上の意味で対応する元 $b \in \mathbf{Z}_p$ が唯一存在する。このため、$\mathbf{Z}_p$ は p 進完備であると呼ばれる。少し言い換えた説明をする。自然な写像

$$\mathbf{Z} \to \mathbf{Z}_p; \quad n \mapsto n \cdot 1$$

を考えたとき、$n \cdot 1$ に対応する $c_0, c_1, \dots$ はあるところからすべて 0 であり、0 でない部分は n を p 進法で記述したときに現れるものと一致する。つまり

$$n = c_0 + c_1 p + \cdots + c_m p^m, \quad n \cdot 1 = (c_0, 0, 0, \dots) + \cdots + p^m(c_m, 0, 0, \dots)$$

である。p 進整数環 $\mathbf{Z}_p$ 自体は $c_0, c_1, \dots$ が 0 でない項が無限個あるようなものも含めた可換環となっており、ある種の整数の拡張である。そのために $\mathbf{Z}_p$ は「$\mathbf{Z}$ の p 進完備化」と呼ばれる。整数論の研究において、p 進整数環を用いて問題の p 進的側面を調べるという手法は非常に強力なものとなっており、現代では欠かせない視点となっている。

12 おわりに

有限体の Galois 理論は、代数幾何の文脈において、有理点を Frobenius 写像の「固定点」と捉えるという視点を与え、それは Weil 予想やエタールコホモロジーといった 20 世紀の華々しい数学へと繋がった。一方、δ 環の理論が注目を惹いたのは非常に最近の p 進 Hodge 理論の研究の進展によるものである。それはプリズマティックコホモロジーという新しいコホモロジーの発見に繋がった。「Frobenius 持ち上げ」という手法は非常に注目を集めており、今後も進展が期待される。