東海大学紀要情報通信学部
Vol.10,No.1,2017,pp.105-113

トピックス

大学初年次における数学教材の提案（その 11）
～有限体入門～

貴田 研司[*1]

Suggestion about Mathematical Material for Freshman Education Vol.11
~ Introduction to Finite Field ~

by

Kenshi KIDA[*1]

(received on May 26, 2017 & accepted on Jul.13, 2017)

あらまし

有限体の標数および素体がどのようになっているかを述べ，さらに素体上の多項式の最小分解体として捉えることによって，その存在と一意性について解説する．そしてさらに，多項式環の剰余環として有限体を構成する方法についても言及していく．

Abstract

First, we describe characteristics and prime fields of finite fields, then explain the existence and uniqueness of finite fields as minimal decomposition fields of polynomials over prime fields. Further, we present the method of composition of finite fields as factor rings of polynomial rings.

キーワード: 有限体, ガロア体, 標数, 素体, 符号理論
Keywords: *Finite Field, Galois Field, Characteristic, Prime Field, Coding Theory*

1. はじめに

大学初年次の代数学では，群，環，体などの代数系について学ぶ．体は有限集合のとき有限体（またはガロア体）という．ガロア体という名称は，これを最初に考えたガロアの名前に因むものである．そうでないときは無限体と呼ばれる．有限体は必ず可換体である（ウェダーバーンの定理）ことが知られている．

有理整数環 $\mathbf{Z}$ は単項イデアル整域であり，$m \in \mathbf{Z}$ 対して

剰余環 $\mathbf{Z}/m\mathbf{Z}$ が体 $\Leftrightarrow$ $m\mathbf{Z}$ が素イデアルである，すなわち極大イデアルである．$\Leftrightarrow$ m が素数である．

が成り立つ．よって p が素数のとき $\mathbf{Z}/p\mathbf{Z} = \mathbf{F}_p$ は有限体であるが，特に $p = 2, 3$ の場合の演算表を示すと次のようになる．

例 1 $\mathbf{Z}/2\mathbf{Z} = \{\overline{0}, \overline{1}\}$

+	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$

×	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$

*1 高輪教養教育センター 准教授
Liberal Arts Education Center, Takanawa Campus,
Associate Professor

例 2　$\mathbf{Z}/3\mathbf{Z}=\{\overline{0},\ \overline{1},\ \overline{2}\}$

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

$\times$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{1}$

本論文においては，有限体の標数および素体について述べ，さらにその存在と一意性について解説する．そして，具体的に有限体を構成する方法についても紹介する[1)2)3)4)5)6)7)8)9)10)11)12)13)]．

2. 有限体の性質

体 K の単位元 1_K に対して，n 回加えると 0 になる，すなわち $1_K+1_K+\cdots+1_K=n\cdot 1_K=0$ となるような自然数 n の中で最小の数を K の標数といい，$\mathrm{char}(K)$ と表す．ただし K にこのような自然数 n が存在しないときは，$\mathrm{char}(K)=0$ と定義することにする．標数が 0 ではない場合，その標数 p は素数であることがわかっている．また，標数が素数 p の体 K の元 a, b に対して

$$(a+b)^p=a^p+b^p \quad \text{そして} \quad (a+b)^{p^n}=a^{p^n}+b^{p^n}$$

が成り立つことがわかる．

さらに体 K のすべての部分体の共通部分からなる体を，体 K の素体といい，K の素体は K の最小の部分体である．例えば，有理数体 $\mathbf{Q}$，実数体 $\mathbf{R}$，複素数体 $\mathbf{C}$ の標数は 0 であり，素数 p に対して $\mathbf{Z}/p\mathbf{Z}=\mathbf{F}_\mathbf{p}$ の標数は p である．これらについて以下のことが知られている．

定理（標数と素体）[3)]

体 K の単位元を 1_K，素体を $\mathbf{F}$ するとき，次の(0-1),(0-2),(0-3)は互いに同値である．

(0-1)　$\mathrm{char}(K)=0$

(0-2)　$n\in\mathbf{Z}$ に対して，$n\cdot 1_K=0$ ならば $n=0$

(0-3)　$\mathbf{F}\cong\mathbf{Q}$

また，素数 p に対して，次の(P-1),(P-2),(P-3)は互いに同値である．

(P-1)　$\mathrm{char}(K)=p$

(P-2)　$p\cdot 1_K=0$

(P-3)　$\mathbf{F}\cong\mathbf{Z}/p\mathbf{Z}=\mathbf{F}_\mathbf{p}$　　■

もちろん有限体Kの標数は素数pであり，その素体$\mathbf{F_p}$はKの部分体であるから，Kは$\mathbf{F_p}$上の線形空間と見なすことができる．言い換えればKの$\mathbf{F_p}$上の次元がnのとき，Kの一組の基底を$\mathbf{v_1}$，$\mathbf{v}_2$，$\cdots$，$\mathbf{v}_n$とすれば，Kの任意の元は

$$c_1\mathbf{v_1}+c_2\mathbf{v}_2+\cdots+c_n\mathbf{v}_n \qquad \left(c_1, c_2, \cdots, c_n \in \mathbf{F_p}\right)$$

の形に一意的に表される．よって，Kの元の個数はp^nであることがわかる．よって

定理（有限体の元の個数）

有限体Kについて$\dim_{\mathbf{F}_p} K=[K:\mathbf{F_p}]=n$のとき，$K$の元の個数は$p^n$に等しい．■

となる．

さて，有限体の乗法群の構造について述べると次のようになる．

補題

体Kの0と異なる元全体のつくる乗法群K^*において，その有限部分群はすべて巡回群である．■

定理（有限体の乗法群）

標数が素数の有限体K，その素体を$\mathbf{F_p}$として，Kを$\mathbf{F_p}$上の線形空間と見て$\dim_{\mathbf{F}_p} K=n$とすれば，Kの元の個数はp^nであり，乗法群K^*の元の個数はp^n-1で巡回群である．■

この巡回群K^*の生成元のことを，有限体Kの原始元ということもある．

次に，有限体の存在と一意性については以下の通りである．

定理（有限体の存在と一意性）[4)]

任意の素数pと自然数nに対して，元の個数がp^nとなる有限体Kが存在する．このようなKは素体$\mathbf{F_p}$上の多項式$x^{p^n}-x$の最小分解体に同型である．したがって，同型を度外視して一意的に定まる．■

（証明）

$\overline{\mathbf{F_p}}$を$\mathbf{F_p}$の代数的閉包とし，$K=\left\{\alpha\in\overline{\mathbf{F_p}}\ ;\ \alpha^{p^n}=\alpha\right\}$とおけば，$K$が体になることが容易に確かめられる．$K$は多項式$f(x)=x^{p^n}-x$の解の全体であり，形式的微分$f'(x)=p^n x^{p^n-1}-1=-1\neq 0$と$f(x)$の共通の解は存在しない。よって，$f(x)$は重解を持たないので，$K$の元の個数は$p^n$である．

【証明終】

この結果から元の個数が$q=p^n$の有限体はすべて同型であるが，これを$GF(q)$と表すことがある．

3. 有限体の構成

可換体 R について多項式環 $R[x]$ は単項イデアル整域であり，R 上の多項式 $f(x)$ に対して

剰余環 $R[x]/(f(x))$ が体 $\Leftrightarrow (f(x))$ が素イデアルである，すなわち極大イデアルである．$\Leftrightarrow f(x)$ が R 上既約である．

が成り立つ．実際に，元の個数が p^n の有限体を作るときは，以下の結果

定理（有限体の構成方法）[5)6)7)]

$p(x)$ を $\mathbf{F}_p$ 上の n 次既約多項式とすれば，$\mathbf{F}_p[x]/(p(x))$ は $\mathbf{F}_p$ の n 次拡大体で，元の個数が p^n の有限体である．

■

ということに基づく．まず最初に $\mathbf{F}_p$ 上の既約な n 次多項式 $f(x)$ を一つ選び，剰余環 $F=\mathbf{F}_p[x]/(p(x))$ として構成して行く．このとき x の剰余類を $\alpha=\overline{x}=x+(p(x))$ とおくと

$$p(\alpha)=p(x)+(p(x))=0 \qquad (*)$$

であり，$(*)$ を用いて計算することにより，F の元は一意的に

$$c_0+c_1\alpha+c_2\alpha^2+\cdots+c_{n-1}\alpha^{n-1} \quad \left(c_0, c_1, c_2, \cdots, c_{n-1}\in\mathbf{F}_p\right) \qquad (**)$$

の形に表される．

したがって，α の冪もまたすべて $(**)$ の形に表されることがわかる．

ところが，α は一般には，巡回群 F^* の生成元ではなく，α の冪は F^* のすべての元を尽くすとは限らないことには注意が必要となる．

有限体 $GF(p^n)$ を取り扱う場合には，それと同型な体 $\mathbf{F}_p[x]/(p(x))$ のうちで，根 $\overline{x}=\alpha$ が巡回群 F^* の生成元であるような $\mathbf{F}_p$ 上の n 次既約多項式 $p(x)$ を選ぶことによって，有限体 F を構成する方が都合がよい．

もしも $p(x)$ が，上述のように都合よく選ばれているならば

$$F=\left\{0, \alpha, \alpha^2, \cdots, \alpha^{q-1}(=1)\right\} \quad \left(\text{ただし}, q=p^n\right)$$

であるから，α の冪を，$(*)$ を用いて計算することにより，すべてを $(**)$ の形に書き表すことにする．このとき F のおのおのの元は，一方では指数による表示，一方では $(**)$ の形の表示と，二通りに表示される．

$$\begin{cases} 0=0 \\ \alpha=\alpha \\ \cdots\cdots\cdots \\ \alpha^{n-1}=\alpha^{n-1} \\ \alpha^n=c_{n,0}+c_{n,1}\alpha+\cdots\cdots+c_{n,n-1}\alpha^{n-1} \\ \cdots\cdots\cdots \\ \alpha^{q-2}=c_{q-2,0}+c_{q-2,1}\alpha+\cdots\cdots+c_{q-2,n-1}\alpha^{n-1} \\ \alpha^{q-1}=1 \end{cases}$$

Fの元を，上のように二通りに表示しておくと，Fの演算のうち，和では右の表示，積では左の表示を用いることにより，演算を簡便化することができる．

また，$\mathbf{F}_p[x]$のモニックなn次既約多項式のうち，$GF(p^n)^*$の生成元を根にもつものを原始既約多項式ということがある．

以下に，有限体の構成についての例を挙げることにする．

例1（$GF(2^2)$）[6)8)]

$\mathbf{F}_2=\mathbf{Z}/2\mathbf{Z}=\{\overline{0},\ \overline{1}\}$上の2次多項式で既約であるものは$x^2+x+1$だけである．実際にこれ以外の3つは

$$x^2=x\cdot x,$$
$$x^2+1=(x+1)\cdot(x+1),$$
$$x^2+x=x\cdot(x+1)$$

と，積として表される．また，x^2+x+1が因数分解できたとしてみると

$$x^2+x+1=(ax+b)\cdot(cx+d)\qquad (a,b,c,d\in\mathbf{F}_2)$$
$$=acx^2+(ad+bc)x+bd$$

であるから

$$\begin{cases}ac=1\\ad+bc=1\\bd=1\end{cases}$$

でなければならない．よって，$ac=1$より$a=1,\ c=1$が得られ，$bd=1$より$b=1,\ d=1$が得られる．ところが，このとき$ad+bc=2=0$となり矛盾が生じる．したがって，x^2+x+1は$\mathbf{F}_2$上で既約であることがわかる．

よって，x^2+x+1で生成されるイデアル$I=(x^2+x+1)$は，極大イデアルであり

$$\mathbf{F}_2[x]/I=\{k_0+k_1x+I\ ;\ k_0,k_1\in\mathbf{F}_2\}=\{I,1+I,x+I,1+x+I\}$$

は元の個数が$2^2=4$の有限体$GF(4)$である．ここで

$$I=0,\ 1+I=1,\ x+I=\alpha$$

とおくと，αは$x^2+x+1=0$の$\mathbf{F}_2[x]/I$における解であるから

$$\alpha^2+\alpha+1=0\Leftrightarrow\alpha^2=-\alpha-1\Leftrightarrow\alpha^2=\alpha+1$$

となる．するとαの冪は

$$\alpha^2=\alpha+1,$$
$$\alpha^3=(\alpha+1)\alpha=\alpha^2+\alpha=(\alpha+1)+\alpha=2\alpha+1=1$$

なので，αが$GF(2^2)$の原始元であることがわかる．

よって，$GF(4)=\{0,\ 1,\ \alpha,\ \alpha+1\}$となっている．

演算表は次の通りになる．

$+$	0	1	α	$\alpha+1$
0	0	1	α	$\alpha+1$
1	1	0	$\alpha+1$	α
α	α	$\alpha+1$	0	1
$\alpha+1$	$\alpha+1$	α	1	0

$\times$	0	1	α	$\alpha+1$
0	0	0	0	0
1	0	1	α	$\alpha+1$
α	0	α	$\alpha+1$	1
$\alpha+1$	0	$\alpha+1$	1	α

例２（$GF(3^2)$）[7)]

まず，$\mathbf{F}_3[x]$の中から

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

を選んでみる．

これについて

$$f(0)=1,\ f(1)=1+1=2,\ f(2)=4+1=2$$

であるから，$\mathbf{F}_3$の中に解をもたないので，$f(x)$は$\mathbf{F}_3[x]$において既約な2次多項式である．

よって，$\mathbf{F}_3[x]/(x^2+1)$は元の個数が$3^2=9$であるような有限体$GF(9)$である．$\beta=\bar{x}$とおくと，これは$x^2+1=0$の$\mathbf{F}_3[x]/(x^2+1)$における解であるから

$$\beta^2+1=0 \Leftrightarrow \beta^2=-1$$
$$\Leftrightarrow \beta^2=2$$

が成り立つ．すると

$$\beta^3=2\beta,$$
$$\beta^4=2\beta^2=2\cdot 2=4=1$$

であるから，βは$GF(3^2)$の原始元ではないことがわかる，

原始既約多項式を見つけるために，$\mathbf{F}_3[x]$の中から改めて

$$p(x)=x^2+2x+2$$

を選ぶことにする．これについて

$$p(0)=2,\ p(1)=1+2+2=5=2,\ p(2)=4+4+2=10=1$$

であるから，$x^2+2x+2=0$ は $\mathbf{F}_3$ の中には解をもたない．したがって，$p(x)$ は $\mathbf{F}_3[x]$ において既約な2次多項式であることがわかる．

よって，$\mathbf{F}_3[x]/(x^2+2x+2)$ は元の個数が $3^2=9$ の有限体 $GF(9)$ である．ここで $\theta=\bar{x}$ とおくと $x^2+2x+2=0$ の $\mathbf{F}_3[x]/(x^2+2x+2)$ における解であるから

$$\begin{aligned}\theta^2+2\theta+2=0 &\Leftrightarrow \theta^2=-2\theta-2\\ &\Leftrightarrow \theta^2=\theta+1\end{aligned}$$

であることを用いて θ の冪を計算すると以下のように

$$\begin{aligned}\theta^2&=\theta+1,\\ \theta^3&=\theta^2+\theta=2\theta+1,\\ \theta^4&=2\theta^2+\theta=2(\theta+1)+\theta=3\theta+2=2,\\ \theta^5&=2\theta,\\ \theta^6&=2\theta^2=2(\theta+1)=2\theta+2,\\ \theta^7&=2\theta^2+2\theta=2(\theta+1)+2\theta=4\theta+2=\theta+2,\\ \theta^8&=\theta^2+2\theta=(\theta+1)+2\theta=3\theta+1=1\end{aligned}$$

となるから，θ は $GF(3^2)$ の原始元であることがわかる．よって，上の計算結果から

$$\begin{aligned}GF(9)&=\{0,\ 1,\ \theta,\theta^2,\ \theta^3,\ \theta^4,\theta^5,\ \theta^6,\ \theta^7\}\\ &=\{0,\ 1,\ \theta,\theta+1,2\theta+1,\ 2,2\theta,\ 2\theta+2,\ \theta+2\}\\ &=\{0,\ 1,\ 2,\theta,1+\theta,\ 2+\theta,2\theta,\ 1+2\theta,\ 2+2\theta\}\end{aligned}$$

と書くことができる．この演算表は以下の通りとなる．

+	0	1	2	θ	$1+\theta$	$2+\theta$	2θ	$1+2\theta$	$2+2\theta$
0	0	1	2	θ	$1+\theta$	$2+\theta$	2θ	$1+2\theta$	$2+2\theta$
1	1	2	0	$1+\theta$	$2+\theta$	θ	$1+2\theta$	$2+2\theta$	2θ
2	2	0	1	$2+\theta$	θ	$1+\theta$	$2+2\theta$	2θ	$1+2\theta$
θ	θ	$1+\theta$	$2+\theta$	2θ	$1+2\theta$	$2+2\theta$	0	1	2
$1+\theta$	$1+\theta$	$2+\theta$	θ	$1+2\theta$	$2+2\theta$	2θ	1	2	0
$2+\theta$	$2+\theta$	θ	$1+\theta$	$2+2\theta$	2θ	$1+2\theta$	2	0	1
2θ	2θ	$1+2\theta$	$2+2\theta$	0	1	2	θ	$1+\theta$	$2+\theta$
$1+2\theta$	$1+2\theta$	$2+2\theta$	2θ	1	2	0	$1+\theta$	$2+\theta$	θ
$2+2\theta$	$2+2\theta$	2θ	$1+2\theta$	2	0	1	$2+\theta$	θ	$1+\theta$

×	0	1	2	θ	$1+\theta$	$2+\theta$	2θ	$1+2\theta$	$2+2\theta$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	θ	$1+\theta$	$2+\theta$	2θ	$1+2\theta$	$2+2\theta$
2	0	2	1	2θ	$2+2\theta$	$1+2\theta$	θ	$2+\theta$	$1+\theta$
θ	0	θ	2θ	$1+\theta$	$1+2\theta$	1	$2+2\theta$	2	$2+\theta$
$1+\theta$	0	$1+\theta$	$2+2\theta$	$1+2\theta$	2	θ	$2+\theta$	2θ	1
$2+\theta$	0	$2+\theta$	$1+2\theta$	1	θ	$2+2\theta$	2	$1+\theta$	2θ
2θ	0	2θ	θ	$2+2\theta$	$2+\theta$	2	$1+\theta$	1	$1+2\theta$
$1+2\theta$	0	$1+2\theta$	$2+\theta$	2	2θ	$1+\theta$	1	$2+2\theta$	θ
$2+2\theta$	0	$2+2\theta$	$1+\theta$	$2+\theta$	1	2θ	$1+2\theta$	θ	2

（**例 2** の追記）[7)]

例 2 で示した β は $GF(3^2)$ の原始元ではなかった．しかし，$\mathbf{F}_3[x]/(x^2+1)$ の元は

$$k_0+k_1\beta \qquad (k_0, k_1 \in \mathbf{F}_3)$$

の形に一意的に表されるので

$$GF(3^2)=\{0, 1, 2, \beta, 1+\beta, 2+\beta, 2\beta, 1+2\beta, 2+2\beta\}$$

となっている．　そこで $\beta^2=-1=2$ を用いて積を計算すると，乗積表は以下の通りになる．

×	0	1	2	β	$1+\beta$	$2+\beta$	2β	$1+2\beta$	$2+2\beta$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	β	$1+\beta$	$2+\beta$	2β	$1+2\beta$	$2+2\beta$
2	0	2	1	2β	$2+2\beta$	$1+2\beta$	β	$2+\beta$	$1+\beta$
β	0	β	2β	2	$2+\beta$	$2+2\beta$	1	$1+\beta$	$1+2\beta$
$1+\beta$	0	$1+\beta$	$2+2\beta$	$2+\beta$	2β	1	$1+2\beta$	2	β
$2+\beta$	0	$2+\beta$	$1+2\beta$	$2+2\beta$	1	β	$1+\beta$	2β	2
2β	0	2β	β	1	$1+2\beta$	$1+\beta$	2	$2+2\beta$	$2+\beta$
$1+2\beta$	0	$1+2\beta$	$2+\beta$	$1+\beta$	2	2β	$2+2\beta$	β	1
$2+2\beta$	0	$2+2\beta$	$1+\beta$	$1+2\beta$	β	2	$2+\beta$	1	2β

4. おわりに

有限体は,ガロア体と呼ぶことからもわかるように,初めてこの概念を公表したのはガロアによるものである.その後,デデキントが多項式環における剰余環として有限体を構成した.このことまでを,この論文では紹介した.さらに,有限体のガロア群も興味ある問題である.また近年では,有限体は符号理論の数学的基礎として,重要な役割を果たしている.

参考文献

1) 岩永恭雄「代数学の基礎」日本評論社, 2002
2) 廣瀬健「情報数学」コロナ社, 1985
3) 菅野恒雄「代数学II―群・体―」森北出版, 1976
4) 永尾汎「代数学」朝倉書店, 1983
5) 金子晃「応用代数講義」サイエンス社, 2006
6) 平松豊一「情報の数理　応用代数学」裳華房, 1997
7) 増田真郎「応用のための代数系入門」サイエンス社, 1981
8) 細井勉「情報科学のための代数系入門」産業図書, 1982
9) 橘貞雄, 神藏正, 衛藤和文共著「応用代数学入門」冨山房インターナショナル, 2007
10) 尾関和彦「情報技術のための離散数学入門」共立出版, 2004
11) 杉原厚吉, 今井敏行共著「工学のための応用代数学」共立出版, 1999
12) 小倉久和, 高濱徹行共著「情報の論理数学入門」近代科学社, 1991
13) 伊理正夫, 藤重悟共著「応用代数」コロナ社, 1988