4　体

体に関しては定義は前節で述べたがもう一度確認しておこう。

定義 4.1 集合 K が**体** (*field*) であるとは 2 種類の演算 (通常加法・乗法と呼ばれ「$+$, $\cdot$」と表される) が定義されて次の条件を満たすものをいう。

(1) 演算「$+$」に関し可換群をなす。即ち

1) 演算「$+$」は結合法則を満たす：$(a+b)+c=a+(b+c)$

2) 加法に関する単位元 (零元と呼び 0 で表す) が存在する：$\exists 0 \in R \forall a \in R; a+0=0+a=a$

3) 任意の $a \in R$ に対し逆元 $-a$ が存在する：$\exists -a \in R; a+(-a)=-a+a=0$

4) 交換法則が成り立つ：$a+b=b+a$

(2) $K=K-\{0\}$ は演算「$\cdot$」に関し群をなす：

1) 演算「$\cdot$」は結合法則を満たす：$(a\cdot b)\cdot c=a\cdot(b\cdot c)$

2) 乗法に関する単位元 (1 で表す) が存在する：$\exists 1 \in K^* \forall a \in K^*; a\cdot 1=1\cdot a=a$

3) 任意の $a \in K^*$ に対し逆元 a^{-1} が存在する：$\exists a^{-1} \in R; a\cdot a^{-1}=a^{-1}\cdot a=1$

(3) 分配法則が成り立つ：$a\cdot(b+c)=a\cdot b+a\cdot c$, $(a+b)\cdot c=a\cdot c+b\cdot c$

幾つか例をあげよう。有理数全体の集合 $\boldsymbol{Q}$ は通常の和と積に関し体をなす。同様に実数全体の集合 $\boldsymbol{R}$，複素数全体の集合 $\boldsymbol{C}$ も体をなす。

例 4.2 乗法が可換でない体 (非可換体) の例をあげよう。この例はハミルトンの 4 元数体と呼ばれる。i,j,k という 3 つのシンボルを用意する。i,j,k は

$$i^2=-1,\ j^2=-1,\ k^2=-1,\ ij=k,\ jk=i,\ ki=j,\ kj=-i,\ ji=-k,\ ik=-j$$

という関係式が成立しているとする。$\boldsymbol{H}=\{\,a+bi+cj+dk \mid\ a,b,c,d \in \boldsymbol{R}\,\}$ とし，積・和を多項式の様に積をとり，関係式を用いて i^2 等を変形したもので定義する:

$$\begin{aligned}(a+bi+cj+dk)+(a'+b'i+c'j+d'k) &= (a+a')+(b+b')i+(c+c')j+(d+d')k\\ (a+bi+cj+dk)\cdot(a'+b'i+c'j+d'k) &= (aa'-bb'-cc'-dd')+(ab'+ba'+cd'-dc')i\\ &\quad +(ac'-bd'+ca'+db')j+(ad'+bc'-cb'+da')k\end{aligned}$$

$\alpha=a+bi+cj+dk$ に対し $\widetilde{\alpha}=a-bi-cj-dk$ とおくと，$\alpha\widetilde{\alpha}=a^2+b^2+c^2+d^2(=\|\alpha\|^2$ と定義する) なので $\alpha^{-1}=\dfrac{\widetilde{\alpha}}{\|\alpha\|^2}$ となる。

演習問題 4.1　$\boldsymbol{H}$ が体になる事を示せ。

以下この講義では体は**可換体**を仮定する。

p を素数とする。$\boldsymbol{Z}_p$ は体である。この事実は命題 2.22 から従う。この体は $\boldsymbol{Q}, \boldsymbol{R}, \boldsymbol{C}$ などとは大きく違う。単位元 1 を何回か足していくと 0 になるが，この事は $\boldsymbol{Q}, \boldsymbol{R}, \boldsymbol{C}$ では決して起こらない。そこで次の定義を与える。

定義 4.3 体 F の単位元 1 を何回か加えて 0 になったとする。このとき回数の最小値をこの体の標数という。

有理数体の様に何回加えても 0 にならないとき，その体の標数は 0 と定義する。

つまり $\boldsymbol{Z}_p$ の標数は p，有理数体 $\boldsymbol{Q}$, 実数体 $\boldsymbol{R}$, 複素数体 $\boldsymbol{C}$ の標数は 0 である。

命題 4.4 体の標数は 0 でなければ素数である。

証明　体の標数を $m \neq 0$ とする。m が素数でないとき，$m = pq$ と分解できる $(p \neq 1, q \neq 1)$。このとき

$$(\underbrace{1+\cdots+1}_{p})(\underbrace{1+\cdots+1}_{q}) = \underbrace{1+1+\cdots+1}_{m} = 0$$

体なので $\underbrace{1+\cdots+1}_{p} = 0$ または $\underbrace{1+\cdots+1}_{q} = 0$ が従うが，これは m の最小性に矛盾する。 ∎

有理数体 $\boldsymbol{Q}$ にある代数方程式 $f(X) = 0$ の解 α を付け加えてできる体 $\boldsymbol{Q}(\alpha)$ を考える。

$\alpha = \sqrt{2}$ の場合を考える。有理数と $\alpha = \sqrt{2}$ の加減乗除からできる元は $a + b\alpha$ $(a, b, \in \boldsymbol{Q})$ の形をしている事を示そう。この形の元が和・差・積・逆元をとる操作で閉じている事を言えばよい。加減に関しては問題ないので，まず乗つまり積についてみる。$(a+b\alpha)(a'+b'\alpha) = aa' + (ab' + a'b)\alpha + bb'\alpha^2 = (aa' + 2bb') + (ab' + a'b)\alpha$ となるので積はまた $a + b\alpha$ の形をしている。除即ち割り算については $\dfrac{1}{a+b\alpha} = \dfrac{a-b\alpha}{a^2-2b^2}$ となる。$a^2 - 2b^2 \neq 0$ なので商も $a + b\alpha$ の形をしている。結局 $\boldsymbol{Q}(\sqrt{2}) = \left\{ a + b\sqrt{2} \,\middle|\, a, b \in \boldsymbol{Q} \right\}$ が分かる。

$\alpha = \sqrt[3]{2}$ とする。有理数と $\alpha = \sqrt[3]{2}$ の加減乗除からできる元は $a + b\alpha + c\alpha^2$ の形をしている。積は $(a+b\alpha+c\alpha^2)(a'+b'\alpha+c'\alpha^2) = (aa' + 2bc' + 2b'c) + (ab' + a'b + 2cc')\alpha + (ac' + bb' + a'c)\alpha^2$ となるので積はまた $a + b\alpha + c\alpha^2$ の形をしている。逆数は $(a+b\alpha+c\alpha^2)(x+y\alpha+z\alpha^2) = 1$ を満たす有理数 x, y, z が存在すればよい。x, y, z は連立方程式

$$\begin{cases} ax + 2cy + 2bz &= 1 \\ bx + ay + 2cz &= 0 \\ cx + by + az &= 0 \end{cases}$$

の解である。a, b, c が有理数のとき $\begin{pmatrix} a & 2c & 2b \\ b & a & 2c \\ c & b & a \end{pmatrix}$ の行列式は 0 ではないので，商も $a + b\alpha + c\alpha^2$ の形をしている。結局 $\boldsymbol{Q}(\sqrt[3]{2}) = \left\{ a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2 \,\middle|\, a, b, c \in \boldsymbol{Q} \right\}$ が分かる。

演習問題 4.2　a, b, c が有理数のとき上の行列の行列式が実際 0 にならない事を示せ。また a, b, c が実数の場合 0 になるような a, b, c を 1 組求めよ。

一般の $\boldsymbol{Q}(\alpha)$，もっと一般的に体 K に対し $K(\alpha)$ を調べるために，体 K 上の多項式環 $K[X]$ について少し調べる。

$$f(X) = a_0 + a_1 X + \cdots + a_n X^n \qquad (a_i \in K)$$

を K 係数**多項式** (*polynomial*) または K 上の多項式と呼ぶ。$a_n \neq 0$ のとき n を $f(X)$ の**次数** (*degree*) といい $\deg f(X)$ または $\deg(f)$ と表す。次数については

$$\deg(fg) = \deg(f) + \deg(g) \qquad \deg(f+g) \leqq \max\{\deg(f), \deg(g)\}$$

が成立する。

証明は省略するが，次の定理は多項式の割り算等にとって基本的である。多項式環と整数環の間には著しい平行関係があるが，その基礎には多項式と整数の間で定理 4.5 及びその類似が成立することがある。

定理 4.5 [**割り算の原理**] $f, g \in K[X]$ に対し

$$f = gq + r, \qquad \deg r < \deg g$$

となる $q, r \in K[X]$ が唯 1 つ存在する。

演習問題 ****4.3**　定理 4.5 を証明せよ。

多項式 $f, g \in K[X]$ に対し多項式 q が存在して $f = gq$ となるとき，f を g の倍数 (倍多項式というべきか)，g を f の約数 (約多項式というべきか) という。2 つの多項式の最大公約数・最小公倍数も同様に定義できる。自分の次数より小さい定数以外の次数の約数を持たない多項式を既約多項式という。既約多項式は K の選べ方で変わる。$f(X) = x^2 - 2$ は $\boldsymbol{Q}[X]$ では既約であるが，$\boldsymbol{Q}(\sqrt{2})[X]$ では $f(X) = (X - \sqrt{2})(X + \sqrt{2})$ と分解されるので既約ではない。

2 つの体 K, L が $K \subset L$ の関係にあるとき K を L の部分体，L を K の拡大体という。

命題 4.6 $f(X) \in K[X]$ に対し次の 2 つは同値である。
(1) $\alpha \in L$; $f(\alpha) = 0$
(2) $f(X)$ を $L[X]$ の中で見ると，$X - \alpha$ は $f(X)$ の約数

証明　$X - \alpha$ が $f(X)$ の約数のとき，ある多項式 $g(X) \in L[X]$ が存在して $f(X) = (X - \alpha)g(X)$ と書ける。このとき $f(\alpha) = (\alpha - \alpha)g(\alpha) = 0$ となる。逆に $f(\alpha) = 0$ とする。定理 4.5 より $f(X) = (X - \alpha)g(X) + r$ と書ける。$0 = f(\alpha) = r$ より $f(X) = (X - \alpha)g(X)$ となる。 ∎

整数における約数・倍数と体上の多項式環の間には著しい平行関係がある。ユークリッドの互除法と同様の議論で次を示す事ができる。

定理 4.7 d を $f, g \in K[X]$ の公約数とする。f, g の最大公約数が d である事と $qf + rg = d$ となる $q, r \in K[X]$ が存在する事は同値である。

演習問題 ****4.4**　　定理 4.7 を証明せよ。

命題 4.8 L を K の拡大体とする。$\alpha \in L-K$ がある多項式 $f(X) \in K[X]$ に対し $f(\alpha)=0$ が成立するとする。その様な多項式のなかで次数の最も低いものを 1 つ取ってきて固定する (それを $f(X)$ とする)。そのとき $f(X)$ は既約である。このような多項式で最高次数が 1 であるものを $f_\alpha(X)$ とすると $f_\alpha(X)$ は α によって一意的に決まる。

証明　$f(X)$ が既約でないとするとき，$f(X)=g(X)h(X)$ と書ける。ただし $\deg(g)<\deg(f)$, $\deg(h)<\deg(f)$ とする。$g(\alpha)h(\alpha)=f(\alpha)=0$ より，$g(\alpha)=0$ または $h(\alpha)=0$ が成立する。これは $f(X)$ が $f(\alpha)=0$ となる最小次数の多項式であることに矛盾する。

最高次係数が 1 である多項式が 2 つ存在したとして，それを $f(X)$,$f'(X)$ とする。このとき $g(X)=f(X)-f'(X)$ とおくと，$\deg(g)<\deg(f)$ であり，$g(\alpha)=f(\alpha)-f'(\alpha)=0$ となる。よって $g(X)=0$ でなくてはならない。 ∎

多項式 $f_\alpha(X)$ の次数が n のとき，α の (K 上の) 次数は n という。

定理 4.9 L を K の拡大体とし，$\alpha \in L-K$ とする。α の K 上の次数が n のとき

$$K(\alpha)=\left\{\, a_0+a_1\alpha+\cdots+a_{n-1}\alpha^{n-1} \,\middle|\, a_i \in K(i=0,\ldots,n-1) \,\right\}$$

と表せる。

証明　$K(\alpha)=\left\{ \dfrac{f(\alpha)}{g(\alpha)} \,\middle|\, f(X),g(X)\in K[X], g(\alpha)\neq 0 \right\}$ であるので，$K(\alpha)$ の元は $\dfrac{f(\alpha)}{g(\alpha)}$ の形をしている。$f_\alpha(X)$ と $g(X)$ に共通因数があれば $f_\alpha(X)$ の既約性からそれは $f_\alpha(X)$ である。このとき $g(\alpha)=0$ となるので，$f_\alpha(X)$ と $g(X)$ は互いに素である。定理 4.7 より $q(X)g(X)+r(X)f_\alpha(X)=1$ となる $q(X),r(X)\in K[X]$ が存在する。このとき $q(\alpha)g(\alpha)=1$。よって $\dfrac{f(\alpha)}{g(\alpha)}=f(\alpha)q(\alpha)$ と書ける。

以上により $K(\alpha)=\{\, f(\alpha) \,|\, f(X)\in K[X] \,\}$ となるが，$f(X)=q(X)f_\alpha(X)+r(X)$ ($\deg(r)<\deg(f_\alpha)=n$) と表すと $f(\alpha)=r(\alpha)$ となる。 ∎