4　標数　素体

4.1　標数　素体

補題 4.1. 任意の環準同型写像 $f : R \longrightarrow S$ にたいして $\ker(f)$ は R のイデアルになる。
　とくに、 S が整域のとき $\ker(f)$ は素イデアルである。

Proof. $G = \ker(f)$ とおく。$x, y \in G, f(x+y) = f(x) + f(y) = 0 + 0 = 0$ より加法について、$r \in R, x \in G, f(rx) = f(r)f(x) = r \cdot 0 = 0$ よりスカラー倍について閉じている。したがって R が環であることから $G = \ker(f)$ が R の部分加法群担っていることがわかる。そして $r \in R, x \in G, f(rx) = f(r)f(x) = 0$ より $rx \in G$ より $\ker(f)$ は R のイデアルになる。
　S が整域のとき $x, y \in R$ にたいして $xy \in G$ であるとする。このとき $f(xy) = f(x)f(y) = 0$ で S が整域より $f(x) = 0$ または $f(y) = 0 \Rightarrow x \in G$ または $y \in G$ より $\ker(f)$ は素イデアルになる。 □

補題 4.2. $\mathbb{Z}$ は単項イデアル整域であり素イデアルは (0) もしくは $(p), (p$ は素数$)$ である。

Proof. $\mathbb{Z}$ はかけて 0 になるような元は 0 のみなので整域。
　$\mathbb{Z}$ の任意のイデアル I をとり ${}^{\forall}m \in I$ に対して I 内の絶対値が最小で 0 でない元を n とすると、$m = k \cdot n + r, (0 \leq r < n)$ となる $k, r \in \mathbb{Z}$ が存在する。そして $m, kn \in I$ から $r = m - kr \in I$ となるが n の最小性から $r = 0$ となるので ${}^{\forall}m \in I, m = kn$ と表せる。よって $I = (n)$ であるから任意のイデアルは単項イデアルになる。逆に任意の元 n の倍数の集合 $n\mathbb{Z} := \{nk | k \in \mathbb{Z}\}$ は $\mathbb{Z}$ 加群であって $\mathbb{Z}$ の部分整域なので n によって生成される単項イデアル $n\mathbb{Z} = (n)$ となる。これより $\mathbb{Z}$ は単項イデアル整域である。
　このときイデアルは $(0), (p), (m)$ の 3 つに分けられる。ただしここで $p > 0$ は素数であり $m > 0$ は合成数である。もし負の数による単項イデアルであったとしても絶対値の等しい値をとることで正の値にできる。
　$xy \in (0) \Rightarrow xy = 0$ のとき整域より $x = 0$ または $y = 0$ となるので (0) は素イデアル。$xy \in (p) \Rightarrow {}^{\exists}k \in \mathbb{Z}, xy = pk$ となる。$k = k_1 \cdot k_2$ となる $k_1, k_2 \in \mathbb{Z}$ に対して $x = pk_1 \in (p), y = k_2$もしくは $x = k_1, y = pk_2 \in (p)$ であるから (p) は素イデアル。(m) に関しては $m = m_1 \cdot m_2$ となる $m_1, m_2 \in \mathbb{Z} - \{1\}$ に対して $m_1 m_2 \in (m)$ だが $m_1, m_2 \notin (m)$ より素イデアルではない。 □

定義 4.3. K:可換体 (可換環でもよい) に対して以下のような自然な環準同型写像 ϕ を考える。

$$\begin{aligned} \phi : \mathbb{Z} &\longrightarrow K \\ n &\longmapsto n \cdot 1_K = \underbrace{1_K + \cdots + 1_K}_{n} \end{aligned}$$

ここで補題 (4.2) から $\mathbb{Z}$ は単項イデアル整域であるから補題 (4.1) から $\ker(\phi)$ は素イデアルなので p を素数として $\ker(\phi) = (0)$ もしくは (p) となる。
　この 0 もしくは p を K の 標数 (characteristic)といい $\mathrm{char}(K), \mathrm{Ch}(K)$ と書く。これは $\ker(\phi) = (p)$ のときこの p は $p \cdot 1_K = 0$ となるような最小の正整数である。

Proof. ϕ が環準同型写像になってることを確かめる。
　この ϕ はまず $n = m$ のとき $\phi(n) = n \cdot 1_K = m \cdot 1_K = \phi(m)$ より写像になっている。そして $\phi(1) = 1 \cdot 1_K = 1_K, \phi(n+m) = (n+m) \cdot 1_K = \underbrace{1_K + \cdots + 1_K}_{n+m} = n \cdot 1_K + m \cdot 1_K = \phi(n) + \phi(m), \phi(n)\phi(m) =$

$(n\cdot 1_K)(m\cdot 1_K)=(\underbrace{1_K+\cdot+1_K}_{n})(\underbrace{1_K+\cdot+1_K}_{m})=\underbrace{1_K+\cdot+1_K}_{nm}=\phi(nm)$ であるから準同型写像になっている。

そして $\ker(\phi)=(p)=\{pl|l\in\mathbb{Z}\}$ から絶対値が p 以下の元は $\ker(\phi)$ に含まれないので p が $\ker(\phi)$ の 0 ではない元で絶対値が最小であるから $\phi(p)=0$ より p は $p\cdot 1_k=0$ となる最小の正整数。 □

定義 4.4. 任意の体 K は $\mathbb{Q}$ または $\mathbb{F}_p$ と同型な体を含む。この $\mathbb{Q},\mathbb{F}_p$ と同型な体のことを 素体 (prime field) という。

つまり素体とは真の部分体を含まない体とも言える。

Proof. 上記の設定で $\ker(\phi)=(0)$ のとき単射であるから $\mathrm{Im}(\phi)\cong\mathbb{Z}$ となり $\ker(\phi)=(p)$ のとき準同型定理から $\mathrm{Im}(\phi)\cong\mathbb{Z}/(p)=\mathbb{F}_p$ となる。よって K は体であるから $\mathbb{Z}$ を含む最小の体が $\mathbb{Q}$ で $\mathbb{F}_p$ は p 元体であることより $K\supset\mathrm{Im}(\phi)\cong\mathbb{Q}$ もしくは $\mathbb{F}_p$ より素体を含む。 □

系 4.5. $\mathrm{char}(K)=0$ の体 K の元は無限個存在する。

Proof. $\mathrm{char}(K)=0$ のとき $\mathbb{Q}$ と同型な体を含むので元の個数は少なくとも $\mathbb{Q}$ 以上であり $|\mathbb{Q}|=\infty$ より成立。 □

系 4.6. 有限体 K における素体は $\mathbb{F}_p$ と同型で K は $\mathbb{F}_p$ の有限次拡大であり拡大次数を n としたら $K\cong\mathbb{F}_p^n$ がなりたつ。そして有限体の元の個数は素数冪、つまり $|K|=p^n$ となる。$q=p^n$ として $K=\mathbb{F}_q$ とも書く。

Proof. 上記の系で K の元の個数が有限ならば $\mathrm{char}(K)\neq 0$ より $\mathrm{char}(K)=p>0$ であるので素体は $\mathbb{F}_p$ と同型。簡単のために素体を $\mathbb{F}_p$ と書くこととすると $K\supset\mathbb{F}_p$ であり $\mathbb{F}_p$ は K の演算で閉じているから K は $\mathbb{F}_p$ の拡大体。無限次拡大とすると基底が無限個あることになりそれは有限体であることに反するので $K/\mathbb{F}_p$ は有限次拡大。よって有限次拡大より拡大次数を n とすると $K\cong\mathbb{F}_p^n$ が成り立ち、$|K|=|\mathbb{F}_p^n|=|\mathbb{F}_p|^n=p^n$ より有限体の元の個数は素数冪になる。 □

4.2 Frobenius 自己準同型

定義 4.7. K が可換体で $\mathrm{char}(K)=p>0$ のとき以下は体の準同型でありこれを K の Frobenius 自己準同型という。

$$\begin{aligned}\phi:K&\longrightarrow K\\ a&\longmapsto a^p\end{aligned}$$

Proof. K が可換体であるから $\phi(ab)=(ab)^p=a^pb^p=\phi(a)\phi(b)$ より積に関しては準同型が成立。

同様に可換であるので $\phi(a+b)=(a+b)^p=\sum_{i=0}^{p}{}_pC_ia^ib^{p-i}$ となる。$0<i<p$ のとき ${}_pC_i=p!/i!(p-i)!=p\cdot(p-1)\cdots(p-i+1)/i\cdot(i-1)\cdots 2\cdot 1$ より p が係数にあるので $\mathrm{char}(K)=p>0$ よりその項は 0 になる。したがって $i=0,p$ の項だけ残るので $\phi(a+b)=(a+b)^p=a^p+b^p=\phi(a)+\phi(b)$ となるから結果として ϕ は体の自己準同型になっている。 □

定義 4.8. 体 K が 完全体 (perfect field) とは $\mathrm{char}(K)=0$ または $\mathrm{char}(K)=p>0$ で Frobenius$\phi:K\longrightarrow K$ が同型 (もともと体の準同型より全射であるということ)

($\Leftrightarrow$ K の非自明な非分離拡大が存在しない) これは示さない。

命題 4.9. 有限体は完全体。

Proof. 系 (4.6) より有限体 $K = \mathbb{F}_q$ にたいして Frobenius $\phi : \mathbb{F}_q \longrightarrow \mathbb{F}_q$ は単射で有限集合より全射だから同型写像となるので有限体は完全体。 □