代数学続論
体と Galois 理論

目次

1　体の拡大

以降の議論では特に述べない限り体は可換体とする。可換体は以下のように言い換えられる。

$\Leftrightarrow$ 可換整域で (0) と (1) 以外のイデアルがない。

$\Leftrightarrow$ クルル次元が 0 の可換整域。

$\Leftrightarrow$ 可換整域で 0 以外の元は可逆。

ただし Krull 次元とは環の素イデアルの包含関係による順序の鎖の長さの上限のことである。

K:体とするとき $K^\times$:可逆元の集合とし、上の同値からこれは $K^\times = K - \{0\}$ としたものと等しい。

例 1.1. $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}\,(p:\text{素数}), \mathbb{Q}_p\,(p\text{ 進体})$

例 1.2. *K;* 体としたとき

$K(x)$:有理関数体 $=$ { 多項式/多項式 $(\neq 0)$| 多項式 $\in K[x]$

$K[[x]]$:形式的冪級数体 $\{\sum_{i\in\mathbb{Z}, i\leq n} c_i x^i | c_i \in K, \in \mathbb{Z}\}$

$\mathbb{Q}$ に α を添加した体 $\Leftrightarrow \mathbb{Q}(\alpha)\,(\alpha \in \mathbb{C}) = (\alpha$ を含む最小の体 $\subset \mathbb{C}) = \{f(\alpha) | f \in \mathbb{Q}(x), (f$ の分母$)(\alpha) \neq 0\} = \{\alpha$と有理数からできる元全体 $\}$

Fact 1.3. R:可換環 $\supset I$: イデアル のとき、R/I:体 $\Leftrightarrow$ I:極大イデアル

例 1.4. $R = K[x], I = (f)$ とするとき *Fact* から

I が極大 $\Leftrightarrow$ I:素イデアル $\Leftrightarrow$ f:既約

よって $K[x]/(f)$ が体 $\Leftrightarrow$ f が既約

Rem 1.5. $\mathbb{Z}/\mathbb{Z} = 0$ は零環で体ではない。$\mathbb{F}_1$:一元体 $\subset \mathbb{Z}$ は実際にはない。

定義 1.6. K, L:体 $K \subset L$ とする。

(K の体構造) = (L の体構造を K に制限したもの) であるとき K は L の 部分体 (subfield)、L は K の 拡大体 (extension field) といい、体の拡大 (field extension) L/K とも言う。つまり、以下の図が可換であるということ。

定義 1.7. 体の準同型とは環としての準同型のこと。

Note 1.8. 体の準同型は全て単射。

Proof. K, L:体 , $\phi : K \longrightarrow L$:準同型とするとき $\ker(\phi)$ は K のイデアルであるから体であることより $\ker(\phi) = (0)$ または $(1) = K$ となる。$\ker(\phi) = K$ のとき $\phi(K) = 0$ から準同型であるための $\phi(1) = 1$ を満たしていないからこれは不適。したがって $\ker(\phi) = (0)$ より ϕ は単射。 □

hom : $\phi : K \longrightarrow L$ があると単射より K は L の部分体 $\phi(K)$ と同一視できる。これより L が K を含んでいなくても K の拡大体と見ることができる。

L/K が拡大のときとくに L は K 上のベクトル空間とみなせるため $\dim_K(L)$ が定義できる。 $(\in \mathbb{Z}_{\geq 1} \cup \{\infty\})$

定義 1.9. $[L : K] := \dim_K(L)$ と書きこれを L/K の 拡大次数 (extension degree)という。この値により拡

大は有限次拡大、無限次拡大に分けられる。

例 1.10. $K(x)/K$ とするとき x が不定元なのでこれは無限次拡大。

$K[x]/(f)$ で $f = a_0 + a_1 x + \cdots + a_n x^n$ で既約とすると $a_n = 1$ とできて、$x^n \equiv -(a_0 + \cdots + a_{n-1}x^{n-1}), (\mod (f))$ となり n 次以上の多項式の次数を下げられるので結局基底は $1, x, \cdots x^{n-1}$ より $[K(x)/(f) : K] = n$ となるのでこれは有限次拡大。

定義 1.11. 体 L に対しその自己同型写像の集合を

$$\mathrm{Aut}(L) := \{ \text{ 体の自己同型 } |\sigma : L \longrightarrow L\}$$

と書きこれは写像の合成について群になっている。また、拡大 L/K に対して K の拡大体としての同型写像 ($K-$ 同型写像) の集合を

$$\mathrm{Aut}_K(L) := \{\sigma \in \mathrm{Aut}(L) | \sigma_K = \mathrm{id}_K\}$$

と書きこれは $\mathrm{Aut}(L)$ の部分群になる。

群になることは写像の結合法則、 id_L が単位元、逆元は同型写像より逆写像を考えればよい。

定義 1.12. L/K が拡大、 $K \subset M \subset L$ で M が L の部分体であるとき M は L/K の中間体 (intermediate field)という。これを $L/M/K$ とかくこともある。

また、 $L/M/K$ のとき $\mathrm{Aut}_K(L) \supset \mathrm{Aut}_M(L)$ が得られる。一般に $\mathrm{Aut}_K(M)$ は包含関係が言えない。

定義 1.13. L:体 $H(\subset \mathrm{Aut}(L))$:部分集合の 2 つに対し

$$L^H := \{x \in L |^{\forall} \sigma \in H, \sigma(x) = x\}$$

は L の部分体になり、L の H による固定部分体という。このような元を H により固定される元ともいう。

部分体になることは $\sigma \in H \subset \mathrm{Aut}(L)$ は同型写像より加法乗法を保存し、 $1, 0$ は常に動かないことからわかる。

Rem 1.14. $H_1 \subset H_2 \subset \mathrm{Aut}(L) \Longrightarrow L^{H_1} \supset L^{H_2}$ が成り立つ。これは H_2 により固定される元は包含関係より H_1 によっても固定されるからである。

Rem 1.15. $L/M/K$ のとき $[L : K] = [L : M][M : K]$ が成り立つ。何れかが無限次元であれば成立する。

有限次元の場合は次のようになる。L を M 上のベクトル空間と見たとき、その基底は $[L : M]$ 個でその係数は M の元であるから M を K 上のベクトル空間と見たときの $[M : K]$ 個の基底で書かれるため L を K 上のベクトル空間と見たときはその基底の積で書かれるからである。

一般に $V : M-\mathrm{vect.sp}, M/K$:拡大のとき V を K 上のベクトル空間と見れて $\dim_K(V) = \dim_M(V) \cdot [M : K]$ となる。

2 Galois 理論の基本定理