ガロアの理論（平成２６年）

代数方程式が代数的に解けるための条件を述べた理論をガロア理論という.

1. 体の拡大

方程式を解くために, 方程式の根を体に添加していく.

x^2-2 は有理整数体 Q 上で既約で, Q$(\sqrt{2})$ 上で $(x-\sqrt{2})(x+\sqrt{2})$ と可約となる.

体 Q を体 Q$(\sqrt{2})$ に拡大することによって, 方程式は解くことが出来るようになる.

- Q$(\sqrt{2})$: Q の単拡大で, Q$(\sqrt{2})$ / Q と記す.
- $p(x) = x^2-2 = (x-\sqrt{2})(x+\sqrt{2})$ を Q 上の最小多項式という.
- $p(x) = 0$ は Q$(\sqrt{2})$ 上で解をもつから, Q$(\sqrt{2})$ を $p(x)$ の分解体という.

例　実数体 R 上の最小多項式 $p(x) = x^2 + 1 = (x-i)(x+i)$ の分解体は複素数体 C である.

（注）代数学の基本定理によって, 複素数体 C が全ての最小多項式の分解体となる.
（注）単拡大の例　・べき根拡大　・円分拡大　・クンマー拡大

2. 分解体の固定群

$\alpha_1, \alpha_2, \alpha_3$ を根とする最小多項式は,

$$p(x) = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)$$
$$= x^3-(\alpha_1+\alpha_2+\alpha_3)\,x^2 + (\alpha_1\alpha_2+\alpha_2\alpha_3+\alpha_3\alpha_1)\,x-\alpha_1\alpha_2\alpha_3$$

係数は対称式である.

- $p(x)$ は根の変換で不変である.
- ガロアは, 分解体 $Q(\alpha_1, \alpha_2, \alpha_3)$ と最小多項式 $p(x)$ を同じものと考えている.

$$Q(\alpha_1, \alpha_2, \alpha_3) = p(x)$$

- 4.で示すように, 分解体を不変にする固定群を考える.

3. 分解体と最小多項式

補助定理 1

F(α) / F を単拡大とする. α が F 上の最小多項式 m をもつとき, 次のことが成り立つ.

（1）F(α) の元は $p(\alpha)$ と一意的に表される.

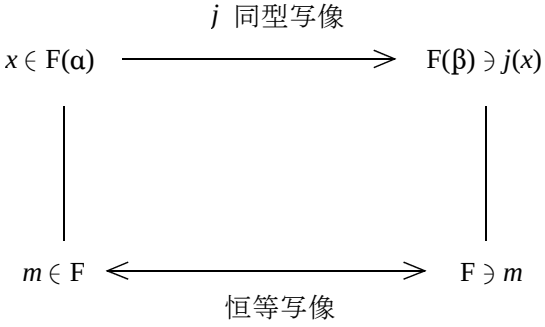
（2）$deg\ p(\alpha) < deg\ m(\alpha)$

証明　体 F(α) の元は $f(x)/g(x)$ と表され，$p(\alpha)$ が最小多項式だから
$p(\alpha) = f(\alpha)/g(\alpha)$ と一意的に表される．　$g(\alpha) \neq 0$

いま，$m(\alpha) = 0$ だから　$m \nmid g$
$\therefore\ a\,g + b\,m = 1$ なる多項式 a, b がある．
$m(\alpha) = 0$
$\therefore\ a(\alpha)\,g(\alpha) = 1$
$\therefore\ p(\alpha) = f(\alpha) / g(\alpha) = f(\alpha)\,a(\alpha)$
$p(x)$ を $m(x)$ で割ったとき，余りを $r(x)$ とすると
$p(\alpha) = m(\alpha)\,q(\alpha) + r(\alpha)$　　$deg\ r(\alpha) < deg\ m(\alpha)$　……①
$m(\alpha) = 0$
$\therefore\ r(\alpha) = p(\alpha)$　……②
①②より　　$deg\ p(\alpha) < deg\ m(\alpha)$

補助定理 2
単拡大 F(α) / F，F(β) / F について，α と β は同じ F 上の最小多項式をもつとき，α を β に写す同型写像 j がとれる．

証明



拡大体 F(α) の元 x, y は次のようにかける．
$x = x_0 + x_1\,\alpha + \cdots + x_n\,\alpha^n$
$y = y_0 + y_1\,\alpha + \cdots + y_n\,\alpha^n$
ただし　$n < deg\ m$

$j(x + y) = (x_0 + y_0) + (x_1 + y_1)\,\beta + \cdots + (x_n + y_n)\beta^n$
$= (x_0 + x_1\,\beta + \cdots ; x_n\,\beta^n) + (y_0 + y_1\,\beta + \cdots + y_n\,\beta^n)$
$= j(x) + j(y)$
$\therefore\ j(x + y) = j(x) + j(y)$

いま，$x = f(\alpha)$, $y = g(\alpha)$, $x\,y = h(\alpha)$ とおく
$f(\alpha)\,g(\alpha) - h(\alpha) = 0$　……②
F(α)：体だから　$f\,g - h \in F(\alpha)$,
m は F(α) の最小多項式だから

$f\ g\ -h$ は m で割り切れる.

$$(f\ g\ -h)\ (\alpha) = (f\ g)\ (\alpha) - h(\alpha)$$

$$= m\ (\alpha)$$

$$= 0$$

$$\therefore\ (f\ g)\ (\alpha) = h\ (\alpha) \quad \cdots\cdots\cdots\cdots\cdots\cdots ③$$

②③より　$(f\ g\ )(\alpha) = f\ (\alpha)\ g(\alpha)$

m は F(β) の最小多項式でもあるから同様にして

$$(f\ g\ )(\beta) = f\ (\beta)\ g(\beta)$$

$$j\ \{\ (xy)(\alpha)\ \} = (f\ g)\ (\beta) \qquad j : \alpha \to \beta$$

$$= f\ (\beta)\ g\ (\beta) \qquad x \to f \qquad y \to g$$

$$= j\ \{\ (x)(\alpha)\ \}\ j\ \{\ (y)(\alpha)\ \} \qquad x\ y \to f\ g$$

よって j は同形写像にとることが出来る.

補助定理 3

体　F, F'　について,

i　は F→ F' の同形写像.

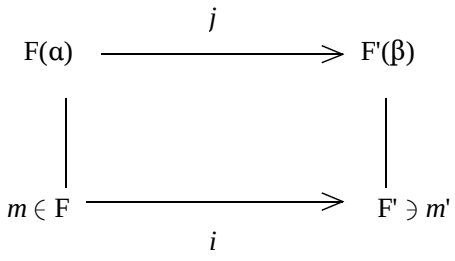
F (α), F'(β) は　F, F' の単拡大

α, β はそれぞれ　F, F'　上の最小多項式　m, m' をもち, $i\ (m) = m'$ とするとき,

(1)　j : F(α) → F'(β)

(2)　$j\ |_F = i$,　$j(\alpha) = \beta$

証明



F(α) の元は, 次数が deg m より小で　$p(\alpha)$ の形である.

ただし, p は F 上の多項式である.

$j(p(\alpha)) = (i(p))(\beta)$　とおくと,

最小多項式は

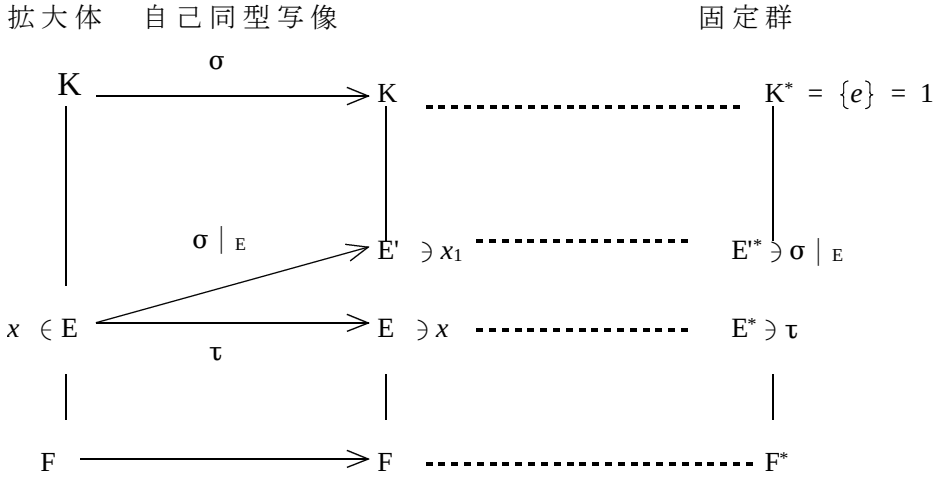
$$p(t) = k\ (\ t - \alpha\ ) \qquad k,\ \alpha \in F$$

$$i\ (p(t)) = k'\ (\ t - \beta\ ) \qquad k',\ \beta \in F'$$

$$\because\ i\ (p(t)) = i\ \{k\ (\ t-\alpha\ )\}$$
$$= i\ (k)\ i\ (\ t-\alpha\ )$$
$$= k'\ (\ t'-i(\alpha))$$
$$= k'\ (\ t-\beta\ )$$

4. 分解体と固定群の関係

ガロアは固定群の列は正規部分群の列になることを発見する.



$$\sigma\tau\sigma^{-1}(x_1) = \sigma\tau(x_1) = \sigma(x_1) = x_1$$
$$\therefore\ \sigma\ E^*\ \sigma^{-1} \subseteq E'^* \quad \cdots\cdots\cdots\cdots\cdots\cdots (1)$$

同様にして

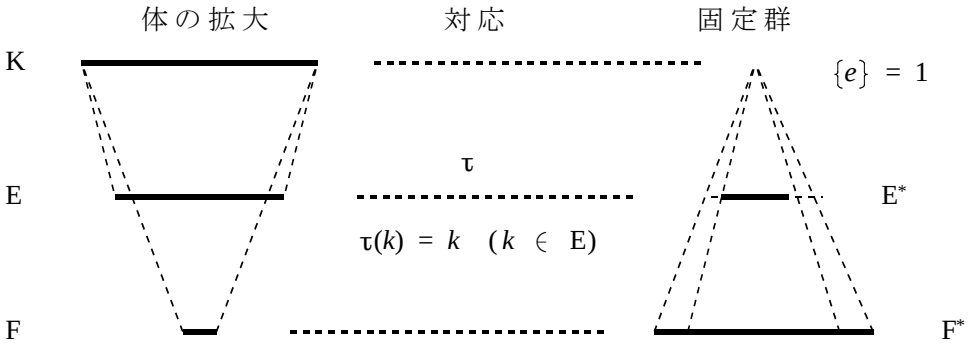
$$\sigma^{-1}\tau\sigma(x) = \sigma^{-1}\tau(x_1) = \sigma^{-1}(x_1) = x$$
$$\therefore\ \sigma^{-1}\ E'^*\ \sigma \subseteq E$$
$$\therefore\ \sigma\ E^*\ \sigma^{-1} \supseteq E'^* \quad \cdots\cdots\cdots\cdots\cdots\cdots (2)$$
$$(1)\ (2)\ \text{より} \quad \sigma\ E^*\ \sigma^{-1} = E'^*$$

補助定理 3 により, 同形写像 σ を E に制限して E' = E とすることが出来る. このとき K / F を正規拡大と定義する.

$$\sigma\ E^*\ \sigma^{-1} = E^*$$

よって $F^* \rhd E^* \rhd K^*$

5. 分解体と中間体



（注）有限鎖 $F^* \supseteq E^* \supseteq K^* = 1$ があって

（1）$F^* \rhd E^* \rhd K^* = 1$

（2）F^* / E^*, E^* / K^* がアーベル群

を満すとき，群 F^* を可解群といい，体の拡大 K / F を可解拡大という．

参考文献

Ian Stewart, Galois Theory, Chapman and Hall, London, 1973

ガロアの理論 I. スチュワート著 新関章三訳 共立出版 １９７９