ガロア理論

松本　眞

平成 18 年 11 月 22 日

目 次

基本的参考文献

体とガロア理論　藤崎源二郎、岩波書店

Seminaire de Geometrie Algebrique A. Grothendieck, Societe Mathematique de France

1　有限次ガロア理論

1.1　拡大体

定義 1.1. L を体とする。$K \subset L$ が L の部分体であるとは、L の演算（和、差、積）の K への制限によって、K が体となることをいう。このとき、L を K の

拡大体という。

例 1.2.

$$\mathbb{Q} \subset \mathbb{Q}[\sqrt{2}] \subset \mathbb{R} \subset \mathbb{C}$$

は全て体であり、部分体ー拡大体である。

$$\mathbb{Q} \subset \mathbb{Q}[\sqrt[3]{3}] \subset \mathbb{R}$$

も全て体である。

定義 1.3. $K \subset L$ を体の拡大、$\alpha \in L$ とする。$K[\alpha] \subset L$ で、α の多項式（係数は K）として書けるような L の部分集合を表す。

定義 1.4. $K[t]$ で、K 係数一変数多項式環を表す。

命題 1.5. $K \subset L \ni \alpha$ のとき、

$$s_\alpha : K[t] \to L, t \mapsto \alpha$$

なる環順同型写像で、K に制限すると恒等写像になるものが唯一つ存在する。

証明. $s_\alpha(f(t)) := f(\alpha)$ と置けばよいし、そう置くしかない。例えば $f(t) = a_2t^2 + a_1t^1 + a_0$ ならば、環準同型の定義から $s_\alpha(f(t)) = s_\alpha(a_2t^2 + a_1t^1 + a_0) = s_\alpha(a_2)s_\alpha(t)^2 + s_\alpha(a_1)s_\alpha(t) + s_\alpha(a_0)$. K の元である a_0, a_1, a_2 は仮定より s_α で不変、また $s_\alpha(t) = \alpha$ なのでこの式は $a_2\alpha^2 + a_1\alpha + a_0 = f(\alpha)$ となる。

これで、環準同型ならば $f(t) \mapsto f(\alpha)$ しかないとわかった。逆に、これが環準同型になることは各自確かめよ。 □

定義 1.6. 上で、s_α の像集合 $\mathrm{Im}(s_\alpha)$ は、「K 係数で α の多項式としてかけるような L の元の全体」である。これを $K[\alpha] \subset L$ で表す。

「環準同型の像は部分環」なので、$K[\alpha]$ は L の部分環である。「整域の部分環は整域」なので、部分整域である。

定理 1.7. (環準同型定理)

$h : R \to R'$ を環準同型とする。その像 $\mathrm{Im}h$ は R' の部分環であり、その核 $\mathrm{Ker}h = h^{-1}(0)$ は R のイデアルである。そして、

$$\bar{h} : R/\mathrm{Ker}h \to \mathrm{Im}h$$

なる自然な環同型が存在する。自然、とは、次の図式が可換になること。

$$\begin{array}{ccc} R & \to & R' \\ \downarrow & \circlearrowleft & \cup \\ R/\mathrm{Ker}h & \to & \mathrm{Im}h. \end{array}$$

この定理を s_α に対して適用すれば、

命題 1.8. 環同型

$$K[t]/\mathrm{Ker}s_\alpha \cong K[\alpha]$$

が存在する。ここで、左辺における t の同値類 $\bar{t}$ は、右辺において α にうつされる。

定理 1.9. 体 K 上の一変数多項式環 $K[t]$ は、単項イデアル整域である。

定義 1.10. $\mathrm{Ker}s_\alpha$ は $K[t]$ のイデアルであるから、上の定理により単項イデアルである。すなわち、ある多項式（$\varphi_\alpha(t)$ と記す）が存在して、

$$\mathrm{Ker}s_\alpha = (\varphi_\alpha(t))$$

とできる。$\varphi_\alpha(t) = 0$ のとき、α を K 上超越的であるという。$\varphi_\alpha(t) \neq 0$ のとき、α を K 上代数的であるという。

$\varphi_\alpha(t)$ の定数倍を調節して最高次の係数を 1 としたもの（monic 多項式という）を、α の最小多項式という。

以上から、次を得る。

定理 1.11. $\alpha \in L \subset K$ に対し、環同型

$$K[t]/\varphi_\alpha(t) \cong K[\alpha] \subset L$$

が存在する。もし、α が K 上代数的なら、$K[\alpha]$ は体である。K 上超越的なら、$K[\alpha]$ は多項式環 $K[t]$ と同型である。

証明. 前半はすでに示されている。「代数的なら体」というのは、次の二つの補題の帰結である。超越的なら、$\varphi_\alpha(t) = 0$ より、左辺が多項式環と同型になる。 □

補題 1.12. $f(t) \in K[t]$ を 0 でない多項式とする。$K[t]/(f(t))$ が整域となる必要十分条件は、$f(t)$ が既約多項式であることである。また、このとき、自動的に体となる。

証明. $f(t) = g(t)h(t)$ と非自明に因数分解されるならば、$K[t]/(f(t))$ の中で $[g(t)][h(t)] = 0$ となり、零因子がある。よって、対偶を取って「整域ならば $f(t)$ は既約」が言えた。次に、$f(t)$ が既約であるとする。0 でない多項式 $[g(t)] \in K[t]/f(t)$ をとる。$g(t)$ と $f(t)$ は互いに素なので、

$$a(t)g(t) + b(t)f(t) = 1$$

なる多項式 $a(t), b(t)$ が存在する。この式を $\mod f(t)$ で見ると、

$$[a(t)][g(t)] = 1,$$

すなわち $[g(t)]$ は積に関して可逆である。これで「$f(t)$ が既約ならば体」が言えた。「体ならば整域」はほぼ自明。 □

補題 1.13. K を体、L を K を含む整域とする（特に体なら十分）。このとき、K 上代数的な元 $\alpha \in L$ の最小多項式は既約多項式である。

証明. 整域の部分環は整域なので、$K[\alpha] \cong K[t]/(\varphi_\alpha(t))$ は整域。よって $\varphi_\alpha(t)$ は既約。 □

次の補題は、最小多項式を求めるときに便利である。

補題 1.14. $\alpha \in L$ の K 上の最小多項式は、次のようにして求まる。

$1, \alpha, \alpha^2, \ldots$ が K 上いつ線形従属になるか求める。いつまでたっても線形従属にならないならば、どんな次数の非零多項式に α を代入しても 0 とはならないから、$\mathrm{Ker} s_\alpha = 0$、すなわち α は超越元。

ある次数 n で、初めて $1, \alpha, \alpha^2, \ldots, \alpha^n$ が一次従属になったとする。このとき

$$a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0$$

となる $a_i \in K$ たち（全てが零、ではない）がある。n の最小性より $a_n \neq 0$、そして α は $n-1$ 次式以下の多項式の根にならない。よって、上の式が α の最小多項式を与えており、これは n 次である。

補題 1.15. K 係数 monic 既約多項式 $f(t)$ に対して $f(\alpha) = 0$ であるなら、$f(t)$ は α の最小多項式である。

証明. $f(\alpha) = 0$ ならば $f(t) \in \mathrm{Ker} s_\alpha = (\varphi_\alpha(t))$, よって $\varphi(t)$ は $f(t)$ を割り切る。$f(t)$ は既約なので、$\varphi_\alpha(t)$ は $f(t)$ に一致するか、定数であるしかない。$t = \alpha$ を代入すると零になるのだから、定数はありえない。 □

定義 1.16. 上の補題により、既約多項式 $f(t)$ の根は、どれも $f(t)$ を最小多項式にしている。このように、最小多項式を同一にしているような元を共役元という。

共役関係は、同値関係である。

例 1.17. $\sqrt{2}, -\sqrt{2}$ は $\mathbb{Q}$ 上共役である。

$t^3 - 2$ は $\mathbb{Q}$ 上既約である（下の例参照）から、それらの三つの根（うち二つは複素数）は $\mathbb{Q}$ 上共役である。

例 1.18. t^3-2 は、$\mathbb{Q}$ 上既約多項式である。なんとなれば、もし非自明な分解をもてば、一次と二次に分解するしかなく、それは t^3-2 に有理数解が存在することを意味し、それは矛盾（$(a/b)^3=2$ とおいて、分母を払い、素因数分解して 2 の重複度を考える）。

これにより、

$$\mathbb{Q}[t]/(t^3-2) \cong \mathbb{Q}[\sqrt[3]{2}].$$

1.2 体上有限次元の環

定義 1.19. K を体とし、$L \supset K$ を、K を部分環としてもつ可換環とする。このとき、L は K 上の線形空間の構造をもつ。L が有限次元 K 線形空間のとき、L を K 上有限次元の環という。その次元を $[L:K]$ であらわす。特に L が体のとき、L は K の有限次拡大体であるといい、その次元を拡大次数という。

補題 1.20. $K \subset L$, $L \subset M$ が有限次拡大体であるとき、

$$[M:L][L:K] = [M:K].$$

証明. M の L 上の基底が $m_1, \ldots, m_s$ で、L の K 上の基底が $l_1, \ldots, l_t$ のとき、$m_i l_j$ $(i=1,\ldots,s, j=1,\ldots,t)$ が M の K 上の基底となることより従う。 □

補題 1.21. $g(t) \in K[t]$ としたとき、$K[t]/(g(t))$ は K 上有限次元の環であり、その次元は $\deg(g(t))$ である。したがって、$\alpha \in L \supset K$ を拡大体の元で代数的なものとするとき、

$$[K[\alpha]:K] = \deg(\varphi_\alpha(t)).$$

証明. $K[t]/(g(t))$ の代表元として、$g(t)$ の次数以下の次数の多項式の集合をとることができる。これは、$f_1(t) \equiv f_2 \mod g(t)$ と、f_1, f_2 を $g(t)$ で割った余りが一致していることとが同値であることに起因する。$g(t)$ の次数以下の次数の多項式の集合は、基底

$$1, t, t^2, \ldots, t^{\deg(g(t))-1}$$

をもつ K 上の $\deg(g(t))$ 次元のベクトル空間である。 □

定理 1.22. $\sqrt[3]{2}$ は、定規とコンパスでは作図できない。（与えられた立方体の、二倍の体積を持つ立方体の辺の長さは定規とコンパスでは作図できない。ギリシャ以来 2000 年を超える間未解決問題であった。）

証明. 概略のみ。「作図可能」とは何か、を定式化する必要がある。1cm の距離に二点をうち、そこから定規で線を結び、コンパスで円を書き、直線または円の交点を求めることができる。xy 平面にこれらの図を書いていく。これら

の点の、x, y 座標を $\mathbb{Q}$ に添加した体を考える。すなわち、最初に求めた交点の座標を (α_1, α_2) とすると、$K_1 := \mathbb{Q}[\alpha_1]$, $K_2 := K_1[\beta_1]$ とおく。以後、二番目に求めた交点を $K_3 := K_2[\alpha_2]$, $K_4 := K_3[\alpha_4]$ とする。交点は、それまでに求めた点の座標を係数に用いた二次方程式の解として求まるので、K_{i+1} は K_i のたかだか 2 次拡大である。したがって $[K_{i+1} : K_i] = 1, 2$。よって $K_0 := \mathbb{Q}$ とおくと $[K_n : K_0]$ は 2 のべき乗。

今、仮に $\sqrt[3]{2}$ が作図可能であったとすると、座標 $(\sqrt[3]{2}, 0)$ が作図できる。これを作図する方法に上の議論を適用すると、$\sqrt[3]{2} \in K_n$ なる状況になる。しかし、このとき

$$K_n \supset \mathbb{Q}[\sqrt[3]{2}] \supset \mathbb{Q}$$

となり、

$$[K_n : \mathbb{Q}] = [K_n : \mathbb{Q}[\sqrt[3]{2}]][\mathbb{Q}[\sqrt[3]{2}] : \mathbb{Q}] = [K_n : \mathbb{Q}[\sqrt[3]{2}]] \times 3$$

は 3 の倍数となる。素因数分解の一意性より、2 の冪が 3 で割り切れることはないのでこれは矛盾。 □

定理 1.23. 角 $\pi/3$(60 度) の三等分 $\pi/9$(20 度) は、定規とコンパスで作図できない。

証明. これもギリシャ以来の未解決問題であった、「角の三等分」問題である。

作図可能であったとしよう。

$$\cos 3\theta + i \sin 3\theta = (\cos\theta + i \sin\theta)^3$$

より

$$\cos 3\theta = (cos\theta)^3 - 3\cos\theta \sin^2\theta 4\cos^3\theta - 3\cos\theta.$$

$\theta = \pi/9$、$\alpha = \cos\theta$

$$1/2 = 4\alpha^3 - 3\alpha,$$

よって $\beta = 2\alpha$ とおくと

$$\beta^3 - 3\beta - 1 = 0.$$

ここで、$t^3 - 3t - 1$ は $\mathbb{Q}$ 上の既約多項式である。可約だとすれば一次式と二次式の積であり、有理数解 n/m をもつはずであるが、代入して分母をはらい、m, n の素因数に着目すると有理数解の非存在がわかる。

よって、$\mathbb{Q}[\beta] = \mathbb{Q}[\alpha]$ は $\mathbb{Q}$ の三次拡大なので、α は作図できず、したがって所望の角は作図できない。 □

1.3 代数閉包の存在

命題 1.24. $K \subset L \subset M$ を体の拡大とする。M/K が有限次拡大なら、M/L, L/K も有限次拡大である。

証明. L/K について：有限次元線形空間の部分空間は有限次元線形空間だから。M/L について：M の K 上の線形空間としての生成元をとると、L 上でも生成元になっている。有限生成の線形空間は有限次元だから。 □

定義 1.25. $K \subset L$ を体の拡大とする。L が K 上の代数拡大であるとは、L のどの元も K 上代数的であること。

命題 1.26. $K \subset L$ を体の拡大とする。$\alpha \in L$ が K 上代数的 $\Leftrightarrow$ $K[\alpha]$ が K 上有限次元の線形空間

証明は、補題 1.14 より従う。

系 1.27. 有限次拡大は、代数拡大である。
$\alpha_1, \alpha_2, \ldots, \alpha_n$ が代数的ならば、$K[\alpha_1, \ldots, \alpha_n$ は K 上有限次拡大。
K 上代数的な L の元で生成される整域は、有限次拡大体である。

定義 1.28. Ω を体とする。Ω が代数閉体であるとは、以下の同値な条件のいずれか（したがって全て）を満たすことである。

1. Ω 係数の多項式は、一次式の積に分解する。
2. Ω 係数の一次以上の多項式は、Ω 内に根を持つ。
3. Ω の代数拡大体は、Ω 自身に限る。

これらの条件の同値性はやさしい。1 から 2 はあきらか。2 から 3 は、既約多項式が一次式しかないので、代数的な元はすべて Ω に属することからわかる。3 から 1 は、２次以上の既約多項式があったら代数拡大が作れてしまうことから従う。

定理 1.29. 任意の体 K に対し、K を含む代数閉体が存在する。
しかも、K 上代数拡大体となるようなものが存在する。

証明. Zorn の補題を使う。K の濃度を超える集合 $X(2^K$ など) を用意する。K が有限のときには X を連続無限集合とする。単射 $K \to X$ を一つ固定し、K を X の部分集合とみなす。X の部分集合 L とそこに入っている二項演算 $+, \times$ であって、L は K の代数拡大体となるもの、の全体の集合を $\mathcal{F}$ とする。その元 $(L, +, \times), (L', +', \times')$ に対し、順序を L が L' の部分体である $\Leftrightarrow$ $L \leq L'$ で定義することができる。$\mathcal{F}$ は、帰納的順序集合である (全順序部分集合があった

ら、それらの合併は $\mathcal{F}$ に属する上界である）。Zorn の補題により極大元が存在するのでそれを Ω とする。Ω は代数拡大の合併だから、その濃度は K の濃度以下である（有限の場合は、可算無限集合以下である）。Ω が代数閉でなければ、既約多項式 $f(t) \in \Omega[t]$ が存在する。$\Omega[t]/(f(t))$ に同型な体を、$\mathcal{F}$ の中に見出すことができる。（濃度が X の方が高いので。）これは、極大性に矛盾。

したがって、Ω は代数閉体である。作り方から、代数拡大でもある。 □

定義 1.30. K を部分体として含む代数拡大体で、代数閉体であるものが存在する。これを K の代数閉包という。

例 1.31. $\mathbb{C}$ は代数閉体であり、$\mathbb{R}$ の代数閉包である。$\mathbb{Q}$ の代数閉包ではない。$e \in \mathbb{C}$ は $\mathbb{Q}$ 上代数的でないため。

1.4 分離拡大

定義 1.32. 体 K の単位元 1 をとる。$1+1+\cdots+1=0$ と、何回足したら 0 にもどるかを考える。いつまでたっても 0 にもどらないなら K の標数は 0 といい、p 回目で初めて 0 になるとき、K の標数は p であるという。

命題 1.33. 整数環 $\mathbb{Z}$ から K に、$1_{\mathbb{Z}}$ を 1_K に送るような環準同形が唯一つある。その核は $\mathbb{Z}$ のイデアルであり、$\mathbb{Z}$ が単項イデアル整域であるからそれは単項イデアル (p) である。準同型定理により $\mathbb{Z}/(p) \subset K$ とみなせるから、(p) は素イデアル。よって、p は 0 または素数。これが K の標数に他ならない。

例 1.34. p が素数のとき、$\mathbb{F}_p := \mathbb{Z}/(p)$ は p 元体と言われる有限体で、標数は p である。上の命題により、標数 p の体は全て $\mathbb{F}_p$（と同型な体）を含む。

p 元体を係数とする有理式体 $\mathbb{F}_p(t)$ は、標数が p の無限体である。

標数 0 の体は、$\mathbb{Q}$ と同型な部分体を含む。

$\mathbb{F}_p$, $\mathbb{Q}$ はそれより真に小さい部分体を含まない。これらを素体という。

定義 1.35. $L = K[\alpha]$ のように、一個の代数的元により K 上生成される体を K の単拡大という。

命題 1.36. 有限次拡大体は単拡大の有限回の繰り返しによって得られる。（非自明な単拡大を行うたびに、拡大次数は上がるから。）

定義 1.37. L, M を K を部分体として含む体とする。

$$\mathrm{Hom}_K(L, M) := \{h : L \to M \mid \ h|_K = \mathrm{id}\}$$

と定義する。すなわち、h は L から M への環準同型で、K 上では恒等写像となるものの全体である。

補題 1.38. $L = K[\alpha]$ を単拡大とし、$\Omega \supset K$ を代数閉体とする。このとき、集合

$$\mathrm{Hom}_K(L, \Omega)$$

は $\varphi_\alpha(t)$ の Ω における根の集合 (すなわち α の共役元の集合) と一対一に対応する。特に、その元の個数は $\varphi_\alpha(t)$ の次数を超えない。

証明. $L = K[\alpha] = K[t]/\varphi_\alpha(t)$ から Ω への環準同型 σ に対し、$[t]$ の行き先にを対応づける写像を考える。$[t]$ は $\varphi_\alpha(t)$ の根だから、行き先も $\varphi_\alpha(t)$ の根でなければならない。逆に、$\beta \in \Omega$ を根とすると、その最小多項式は $\varphi_\alpha = \varphi_\beta$ であるから、$s_\beta : K[t] \to \Omega$ の核は φ_α で生成され、$s_\beta : K[t]/\varphi_\beta(t) \to \Omega$ を与える。$[t]$ の行き先を決めれば $K[t]$ からの写像が決定するから、φ_α の根と $\mathrm{Hom}_K(L, \Omega)$ の元は一対一に対応する。 □

命題 1.39. L/K を拡大体、$\alpha \in L$ を K 上代数的な元とする。α が K 上分離的であるとは、次の同値な条件のどれか一つ（したがって全て）をみたすこと。

1. $\varphi_\alpha(t)$ が、Ω 内で重根を持たない。
2. $K \subset \Omega$ を代数閉体としたとき、α と共役な元が Ω 内に $[K[\alpha] : K]$ 個存在する。
3. $\#\mathrm{Hom}_K(K[\alpha], \Omega) = [K[\alpha] : K]$.

証明. 重根を持たなければ、相異なる根が $\deg \varphi_\alpha$ 個あるわけで、この数は $[K[\alpha] : K]$ だから、1 と 2 は同値。2 と 3 の同値性はすでに見た。 □

上の定義は代数閉体の取り方に依存する定義に見えるが、実は依存しない。$K[\alpha]$ は代数拡大体だから、K 上の環準同型 $\sigma : K[\alpha] \to \Omega$ の像は K 上代数的である。

定義 1.40. Ω 内で K 上代数的な元の全体を $\bar{K}$ とかき、Ω における K の代数閉包という。Ω が代数閉体であることにより、$\bar{K}$ は代数閉体である。なんとなれば、$\bar{K}$ 係数の定数でない多項式は Ω 内で根を持つが、それは $\bar{K}$ 上代数的で、したがって K 上代数的であるからである。

命題 1.41. L/K を代数拡大体、$\sigma : K \to \Omega$ を環準同型（体の埋め込み）とする。このとき、環準同型 $\sigma' : L \to \Omega$ であって、σ を拡張するものが存在する。

証明. $L = K[\alpha]$ と単拡大になっている場合は、K 上の最小多項式を用いて

$$L \cong K[t]/\varphi_\alpha(t)$$

である。補題 1.38 で同じ議論が使われているが、$\sigma(\varphi_\alpha(t)) \in \Omega[t]$ の根を β とすると、$\sigma' : [t] \mapsto \beta$ とすることで σ の延長が得られる。

L/K が有限次拡大体の場合は、単拡大を繰り返すことで上に帰着される。無限次代数拡大体の場合は、Zorn の補題を使う。L の部分体 $M \supset K$ と、σ の延長 $\sigma_M : M \to \Omega$ の組の集合を考える。$(M, \sigma_M) \geq (M', \sigma_{M'})$ を「$M \supset M'$ かつ σ_M は $\sigma_{M'}$ の延長」で定義する。

帰納的順序集合となるので極大元がある。それが L に一致しなければ、L 内に非自明な単拡大がとれて、ちょっと大きくできるので矛盾。 □

定義 1.42. L を K を部分体として含む体とし、$\sigma : K \to M$ を体の埋め込みとする。

$$\mathrm{Hom}_{K,\sigma}(L, M) := \{h : L \to M | h|_K = \sigma\}$$

と定義する。すなわち、h は L から M への環準同型で、K 上では σ となるものの全体である。

特に、σ が恒等写像のとき、

$$\mathrm{Hom}_K(L, M) := \mathrm{Hom}_{K,\sigma}(L, M)$$

と記す。

先の補題は、L/K が代数拡大で M が代数閉体ならここで定義された集合は空でないことを示している。

補題 1.43. Ω_1 を K の代数閉包とし、$\sigma : K \to \Omega_2$ を体の埋め込みで、Ω_2 は $\sigma(K)$ の代数閉包であるとする。すると、σ の延長である体同型 $\Omega_1 \to \Omega_2$ が存在する。

証明. 先の補題から、環準同型は存在する。Ω_2 が代数拡大であるから、全射でなければ、Ω_1 の代数拡大が存在して矛盾。 □

命題 1.44. Ω を K を部分体とする代数閉体、$L' \supset L \supset K$ を代数拡大体とする。

$$\mathrm{Hom}_K(L', \Omega) \to \mathrm{Hom}_K(L, \Omega)$$

は全射であり、右側の集合の元 σ に対してその逆像は

$$\mathrm{Hom}_{L,\sigma}(L', \Omega)$$

である。この集合のサイズは σ によらないので、

$$\#\mathrm{Hom}_K(L', \Omega) = \#\mathrm{Hom}_{L,\sigma}(L', \Omega) \times \#\mathrm{Hom}_K(L, \Omega).$$

証明. 全射性はすでに示した拡張可能性である。逆像がこうなるのは、時間をかけて定義を読み直せば自明である。最後の、σ に関する非依存性については、$\mathrm{Hom}_{L,\sigma_1}(L',\Omega)$ と $\mathrm{Hom}_{L,\sigma_2}(L',\Omega)$ の間に全単射をつくればよい。像はどうせ $\bar{K}$ 内に入るので、$\Omega = \bar{K}$ の場合に示せばよい。このとき、体同型 $\sigma_2 \circ \sigma_1^{-1} : \sigma_1(L) \to \sigma_2(L)$ を延長する体同型 $\tau : \Omega \to \Omega$ が存在するので、前者の元に τ をほどこすことで後者への前単射が作れる。 □

補題 1.45. Ω を K を部分体とする代数閉体、L/K を有限次拡大体とすると、

$$\mathrm{Hom}_K(L,\Omega) \leq [L:K].$$

証明. 命題1.44により、単拡大についてのみ示せばよいが、それは補題1.38で示した。 □

定義 1.46. $K \subset \Omega$ を、体と代数閉体とする。有限次拡大体 L/K が分離拡大であるとは、K 上恒等写像であるような L から Ω への環準同型の集合

$$\mathrm{Hom}_K(L,\Omega)$$

の元の個数が、拡大次数 $[L:K]$ に一致すること。

次は、すでに示したこと (1.39) の言い換えである。

命題 1.47. K 上代数的な元 α が分離的である必要十分条件は、$K[\alpha]$ が K の分離拡大であることである。

命題 1.48. 代数拡大 L/K に対して、以下は同値。

1. L/K は分離的
2. 任意の中間体 M に対して L/M, M/K がそれぞれ分離的
3. L の任意の元は分離的
4. L/K は K 上分離的な元で生成される

証明. $[L:K] = [L:M][M:K]$ と $\#\mathrm{Hom}_K(L,\Omega) = \#\mathrm{Hom}_M(L,\Omega)\#\mathrm{Hom}_K(M,\Omega)$ と $\#\mathrm{Hom}_K(L,\Omega) \leq [L:K]$ から、「L/K が分離的 $\Leftrightarrow$ 等号成立 $\Leftrightarrow$ どの中間拡大でも等号成立」である。これにより 1 と 2 は同値。2 から 3 は直前の補題から自明。3 から 4 も自明。4 から 1 だが、分離元による単拡大は分離拡大だからこれを繰り返し使えばよい。α が K 上分離的なら、$M \supset K$ 上分離的であることは、M 上の最小多項式は K 上の最小多項式の約数であることから従う。 □

注意 1.49. 体の拡大についてのある性質 P が、次の性質を持つとする。「$L/M/K$ が体の拡大で、L/M と M/K が P を満たすならば、　L/K も P を満たす。また逆に、L/K が P なら L/M, M/K も P。」

有限次拡大、分離拡大、代数拡大はこの P の性質をもつ。

あとで出てくる、正規拡大はこの性質を持たない。

注意 1.50. K が標数 0 であるとき、全ての代数拡大は分離拡大である。これは、K 上の既約多項式 $f(t)$ はみな重根を持たないからである。証明は、「重根を持つこと」と「$f(t), f'(t)$ が互いに素でないこと」は同値である（ライプニッツ公式から従う）。よって、$f(t)$ が既約なのに重根をもつには、$f'(t) = 0$ しかない。これは、各項の t の冪が標数 p の倍数であるときにしかおきない。(標数 0 のときには起きない。)

有限体 $\mathbb{F}_q$（q は p の冪）の場合も、全ての代数拡大は分離拡大である。上のように、既約多項式で $f'(t) = 0$ となるものがないことを言えばよいが、p 乗写像 $\mathbb{F}_q \to \mathbb{F}_q$ が単射環準同型、したがって有限性より同型となる。すると、$f(t)$ の係数は全て何かの p 乗元であり、$f(t) = g(t)^p$ となってしまい、$\mathbb{F}_q$ 上既約でなくなるからである。

$K = \mathbb{F}_p(T)$ は、非分離拡大をもつ。

$$K[t]/(t^p - T)$$

がその一例である。（各自確かめよ。）

つまり、標数 0 の体を扱う限りは、みな分離的であるので心配しなくてよい。

1.5　正規拡大

定義 1.51. $\sigma : K \to \Omega$ を代数閉体への埋め込みとする。代数拡大 L/K が正規拡大であるとは、

$$\mathrm{Hom}_{K,\sigma}(L, \Omega)$$

のどの元をとっても、それによる L の像が代わらないこと。

この定義も σ, Ω の取り方によらないことは補題 1.43 より従う。

例 1.52. $\mathbb{Q}[\sqrt{2}]/\mathbb{Q}$ は正規拡大である。$\sqrt{2}$ の共役元は、$\pm\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$ しかないからである。

$\mathbb{Q}[\sqrt[3]{2}]/\mathbb{Q}$ は正規拡大でない。$\sqrt[3]{2}$ の共役元には、複素数 $\omega\sqrt[3]{2}$ があり、これは $\mathbb{Q}[\sqrt[3]{2}] \subset \mathbb{R}$ に入らないからである。

命題 1.53. 代数拡大 L/k が正規拡大であることと、以下は同値。

- L の任意の元に対し、その K 上の共役元は全て L に属する。より正確に言うと、$L \subset \Omega$ と代数閉体に埋め込んだとき、L の元の K 上の共役元となる Ω の元は、L に入る。

1.6 有限次ガロア理論

定義 1.54. 代数拡大 L/K が正規かつ分離のとき、ガロア拡大という。有限次拡大のときは、有限次ガロア拡大という。

定義 1.55. $L \supset K$ を体の拡大とする。K 上恒等的な L の体自己同型のなす群を $\mathrm{Aut}(L/K) := \{\sigma : L \to L | \sigma|_K = \mathrm{id}\}$ とおく。

その部分群 H に対して、H による固定体を

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

とおく。

定理 1.56. (ガロア理論の基本定理) L/K を有限次ガロア拡大とする。このとき、$G(L/K) := \mathrm{Aut}(L/K)$ とおき、L/K のガロア群と呼ぶ。

$G(L/K)$ の部分群が包含関係に関してなす順序集合を $\mathcal{G}$, L/K の中間体が包含関係に関してなす順序集合を $\mathcal{F}$ とする。

$\mathcal{G}$ と $\mathcal{F}$ の間に、次の 1 対 1 対応が存在する。左から右へは $H \mapsto L^H$, 右から左へは $M \mapsto G(L/M)$. これらは、包含関係を反転する。

包含関係を反転するのは、定義から良く考えれば容易に従う。互いに逆写像であることを示せばよいが、いくつかの補題を要する。

補題 1.57. L/K を有限次拡大体とする。以下は同値。

1. L/K はガロア拡大
2. $K = L^{\mathrm{Aut}(L/K)}$
3. $K = L^H$, ここに $H < \mathrm{Aut}(L/K)$ はある部分群

証明. 1 から 2: $K \subset L^{\mathrm{Aut}(L/K)}$ は自明。もしこの集合が異なるとして、右に入るが左に入らない元 α を持ってくる。L を含む代数閉体 Ω をとり、$\mathrm{Hom}_K(L, \Omega)$ を考えると、L 上の恒等写像 $\iota : L \to \Omega$ のほかに、α を α 以外の共役元（分離拡大だから存在する）に送るような埋め込み $\tau : L \to \Omega$ が存在する。正規だから ι と τ の像は一致するので、$\tau^{-1} \circ \iota \in \mathrm{Aut}(L/K)$ が存在し、α を固定しないので $\alpha \in L^{\mathrm{Aut}(L/K)}$ に矛盾。

2 から 3 は自明。

3 から 1:任意の $\alpha \in L$ に対し、その H 軌道 $S := \{\sigma(\alpha)|\sigma \in H\} \subset L$ を考え、それらを根とする多項式

$$\prod_{s\in S}(t-s)$$

の係数は、H によって固定されるために $L^H = K$ に入る。したがって、α の K 上の共役元は全て S に入るので、正規拡大である。また、最小多項式は上の多項式の約数で、重根を持たないので分離的である。 □

この補題により、基本定理で右→左→右と移すと元に戻ることがわかる。なぜなら、$M \mapsto \mathrm{Aut}(L/M) \mapsto L^{\mathrm{Aut}(L/M)}$ が M に戻ると分かったからである。L/M がガロア拡大になることは、分離性は補題から従い、正規性は「像集合が埋め込み方によらない」という性質なので L/K の正規性から従う。

補題 1.58. L/K を有限次代数拡大とし、Ω を K を含む代数閉体とする。

$$\#\mathrm{Aut}(L/K) \leq \#\mathrm{Hom}_K(L,\Omega) \leq [L:K]$$

が成立する。

左の等号が成立する必要十分条件は、L/K が正規拡大であることである。右の等号が成立する必要十分条件は、L/K が分離拡大であることである。

証明. 右の不等号はすでに示した。等号成立は分離性の定義である。左の不等号であるが、$\mathrm{Aut}(L/K)$ は $\mathrm{Hom}_K(L,\Omega)$ に右作用する。$\sigma \in \mathrm{Aut}(L/K)$ が $f : L \to \Omega$ を $f \circ \sigma : L \to \Omega$ に移す。f は単射なので、この作用は固定点を持たない。よって、

$$\{f \circ \sigma | \sigma \in \mathrm{Aut}(L/K)\} \subset \mathrm{Hom}_K(L,\Omega)$$

の左辺の集合は $\mathrm{Aut}(L/K)$ と 1 対 1 に対応する。よって不等号が従う。等号成立のとき、右辺の元は全て $f \circ \sigma$ と書けるのだから、これらによる L の像は全て $f(L)$ に一致する。 □

補題 1.59. L を体とし、$H < \mathrm{Aut}(L)$ を有限部分群とする。$L/(L^H)$ はガロア拡大であり、$[L : L^H] \leq \#H$ である。

次の証明にはギャップがあった。

証明. ガロア拡大であることはすでにみた。H の位数に関する帰納法を用いる。$H = \{1\}$ の時には自明。そうでないとする。$M := L^H$ とおく。H が非自明に作用する L の元 α に対し、$H \cdot \alpha$ は M 上の α の共役の全てである（重複があるかも）。それらを根とする多項式は M 係数となるからである。そこで、H_α を α のスタビライザーとすると、H の真部分群であり

$$L^{H_\alpha} \supset K[\alpha].$$

帰納法の仮定により

$$[L : L^{H_\alpha}] \leq \#H_\alpha.$$

一方、α の共役元の個数は $H \cdot \alpha$ の個数、すなわち H/H_α の個数を超えないから

$$[K[\alpha] : K] \leq \#(H/H_\alpha)$$

これらをあわせると証明したい不等式を得る。

はずだったが、$L^{H_\alpha} = K[\alpha]$ がいえないと、あわせても証明したい不等式が得られない。 □

ちょっと嫌な証明だが、次の証明にする。

証明. $[L : M] > \#(H)$ として矛盾を導く。

$$H = \{\sigma_1 = \mathrm{id}, \sigma_2, \ldots, \sigma_n\}$$

とする。仮定より、$x_1, x_2, \ldots, x_{n+1} \in L$ なる、M 上一次独立な元が取れる。

$$v_i := (\sigma_1(x_i), \sigma_2(x_i), \ldots, \sigma_n(x_i))$$

なる L 上の n 次元ベクトルを $i = 1, 2, \ldots, n+1$ で考えると、$n+1$ 本あるから一次従属である。すなわち、全部が 0 ではない $r_i \in L$ が存在して

$$r_1 v_1 + \cdots + r_{n+1} v_{n+1} = 0$$

となる。i の順序を取り替えて、$r_i \neq 0$ なる r_i は頭のほうに持ってくる。そして、r_1 で全体を割ることで $r_1 = 1$ としてよい。

このとき、第一成分に着目すると、x_i の L 係数一次結合となっている。x_i の M 係数一次結合は独立性より 0 にならないから、r_l の中で M に入らないものがある。r_2 であるとしても一般性を失わない。M に入らないのだから、ある H の元で動かされる。σ_2 であるとしてよい。上の等式に σ_2 を施すと

$$\sigma_2(r_1)\sigma_2(v_1) + \cdots + \sigma_2(r_{n+1})\sigma_2(v_{n+1}) = 0$$

となるが、$\sigma_2(v_i)$ は v_i の成分を置換するだけだから

$$\sigma_2(r_1)v_1 + \cdots + \sigma_2(r_{n+1})v_{n+1} = 0$$

となる。元の等式から引くと

$$(r_1 - \sigma_2(r_1))v_1 + (r_2 - \sigma_2(r_2))v_2 + \cdots + (r_{n+1} - \sigma_2(r_{n+1}))v_{n+1} = 0$$

である。$r_1 = 1$ より、v_1 の係数は 0。σ_2 の決め方から、v_2 の係数は非零。すると、0 でない係数が一個減った線形関係式が得られる。これを繰り返すと矛盾する。（あるいは、最初から、0 でない係数が最小個となるような線形関係式からスタートすれば、ただちに矛盾する。） □

系 1.60. L を体とし、$H < \mathrm{Aut}(L)$ を有限部分群とする。$L/(L^H)$ はガロア拡大であり、$G(L/L^H) = H$ である。

証明. ガロア拡大であることは、先に示した。$G(L/L^H) \geq H$ も自明である。等号を示す。上で示した補題と、その前に示した補題により

$$[L : L^H] \leq \#H \leq \#G(L/L^H) \leq \#\mathrm{Hom}_{L^H}(L, \Omega) \leq [L : L^H]$$

より、全てに等号が成立する。 □

これにより、ガロア理論の基本定理の証明は終わる。左→右→左でもとにもどることを言えば良いわけだが、$H \mapsto L^H \mapsto G(L/L^H) = H$ だからである。

2 無限次ガロア理論

無限次ガロア拡大の理論は、有限次ガロア拡大の理論に毛が生えた程度のものであるが、その毛は「位相群」なので、なれないと難しいと感じられるかも知れない。

2.1 無限次ガロア理論の基本定理

定義 2.1. 体の拡大 L/K がガロア拡大であるとは、分離的かつ正規であることである。

このとき、L/K のガロア群 $G(L/K)$ を

$$G(L/K) := \mathrm{Aut}(L/K)$$

で定義する。

$G(L/K)$ には profinite 位相とよばれる位相が入る（後述）。

定理 2.2. L/K の任意の中間体の集合を $\mathcal{F}$ とし、包含関係による順序を入れる。$G(L/K)$ の任意の閉部分群の集合を $\mathcal{G}$ とし、包含関係による順序を入れる。次の対応により、$\mathcal{F}$ と $\mathcal{G}$ の間には順序を反転する 1 対 1 対応が存在する。

$$H \in \mathcal{G} \mapsto L^H \in \mathcal{F}, \quad F \in \mathcal{F} \mapsto G(L/H).$$

2.2 profinite 位相

一般に、L/K がガロア拡大、F が中間体であるとする。代数閉体への埋め込み $\sigma : K \to \Omega$ を一つ取り、F の K 上の Ω への埋め込みの全てを考えてそれらが生成する Ω の部分体 M を考える。それぞれの埋め込みは L の埋め込みに延長でき、L/K は正規だから L の像はかわらない。

このことから、K 上の L の Ω への埋め込みを任意に一つとると、M はその像の部分体になっていることがわかる。その L における逆像を、F の (L における) ガロア閉包という。ここでは $\tilde{F}$ で表わす。ガロア拡大の部分拡大なので分離的であり、また構成法から正規であるので K 上のガロア拡大となる。

$$\rho_F : G(L/K) \to \mathrm{Aut}(\mathrm{Hom}_K(F, \Omega))$$

であり、この核は $G(L/F)$ に他ならない。そして、この作用は推移的である。(延長可能性 (命題 1.41 と、上に述べたような「Ω の中で考えてから引き戻す」議論による。)

特に、F が K 上のガロア拡大であるときは、

$$1 \to G(L/F) \to G(L/K) \to G(F/K) \to 1$$

なる短完全列を得る。右の射の全射性は、$G(F/K) \cong \mathrm{Hom}_K(F, \Omega)$ と推移性から従う。

$G(L/K)$ に入れる位相とは、任意の**有限次**中間拡大 F/K に対し、ρ_F を連続にし、かつ $G(L/K)$ を位相群とするような最弱の位相である。

この位相は、少なくとも次の性質：

1. $G(L/F)$ は e を含む開集合
2. $g \in G(L/K)$ に対し、$gG(L/F)$ は g を含む開集合

を持つが、逆に、$gG(L/F)$ を g の開近傍系 (F は有限次中間拡大を全て走る) と定義することができる（開近傍系の公理を満たす、ここでは略)。

この位相は、自然な同一視

$$G(L/K) = \varprojlim_{F:\text{有限次ガロア}/K} G(F/K)$$

において、右辺の $G(F/K)$ に離散位相をいれて得られる射影極限の位相に一致する。射影極限の位相の定義は、$G(L/K) \to G(F/K)$ を任意の F に対して連続にするような最弱の位相であり、F のガロア閉包 $\tilde{F}$ が K 上有限次ガロア拡大であることから従う。

難しい位相のようだが、感覚的には次の通りである。e の開近傍とは、有限次拡大 F 上で id となるような $G(L/K)$ の全体である。F が大きくなるにつれ

て、この開近傍は小さくなる。二つの元が近いとは、その差（比）がより小さな開近傍に入っているということである。

定理 2.3. 上の位相で、$G(L/K)$ はコンパクトハウスドルフ位相群である。

位相群になることのチェックは難しくないが、面倒である（略）。コンパクトハウスドルフであることは、「コンパクトハウスドルフ群の射影極限はコンパクトハウスドルフ」という一般論から従う（略）。コンパクト性の証明は、本質的にチコノフの定理を使うことになりやさしくない。

2.3 無限次ガロア理論の基本定理の証明

定理 2.4. L/K をガロア拡大とし、$\mathcal{G}^o \subset \mathcal{G} = G(L/K)$ を開部分群の全体、$\mathcal{F}^f \subset \mathcal{F}$ を有限次中間拡大体の全体とすると、これらの間に順序を反転する 1 対 1 対応がある。

H が開部分群ということは、ある有限次ガロア拡大 M があって $G(L/M) \subset H$。$L^{G(L/M)} = M$ となることは、$L - M$ の任意の元を取ってきたときそれを動かす $G(L/K)$ の元があることから従う。（延長定理を用いる。）

したがって、$L^H \subset L^{G(L/M)} = M$ となる。M/K に対して有限次ガロア理論を用いると、$G(M/K)$ の部分群と M/K の中間体の間に 1 対 1 対応がある。ということは、$G(M/K)$ を含む $G(L/K)$ の部分群 H と、M/K の中間体 F の間に 1 対 1 対応がある。この対応がどうやって与えられたかを思い出すと、$H \mapsto L^H$、$F \mapsto G(L/F)$ が互いに逆写像であることがわかる。

証明. 無限次ガロア理論の基本定理の証明

中間体 $F \mapsto G(L/F) \mapsto L^{G(L/F)}$ が F に戻ることは、$L - F$ の任意の元に対してそれを動かす $G(L/F)$ の元が存在することから従った。

$G(L/F)$ が閉部分群であること：位相群の一般論で、開部分群は閉部分群でもある。(剰余類に分解すると、各剰余類は開だからそれらの合併も開。開部分群の補集合は、したがって開。) F は有限次拡大 F_i の合成として得られる。$G(L/F) = \cap G(L/F_i)$ であり、閉部分群の共通部分だから閉。

問題は逆向きの対応である。

$$H \mapsto L^H \mapsto G(L/L^H) =: H'$$

とおいたとき、H' が H の位相的閉包になることを示せば十分である。$H \subset H'$ でかつ H' が閉であることはすでに示したから、位相的閉包 $\bar{H} = H'$ を示せばよい。

いま一般に、任意の部分群 $H < G(L/K)$ と任意の有限次ガロア拡大 M に対し、H_M で H の作用を M に制限したものとすると $H_M \subset G(M/K)$ は部分群であり、$G(L/K) \to G(M/K)$ の像である。

任意の M に対して

$$H_M = H'_M$$

であることを示そう。H_M の定義から $M^{H_M} = M \cap L^H$ である。一方、すでに言った「簡単な向き」から $L^H = L(G(L/L^H)) = L^{H'}$ だから、$M^{H'_M} = M \cap L^{H'} = M^{H_M}$. 有限次ガロア理論の基本定理により $H_M = H'_M$ である。

さて、H_M の $G(L/K) \to G(M/K)$ における逆像は $H \cdot G(L/M)$ である。よって、$H \cdot G(L/M) \supset H'$ がわかる。ここで M をどんどん大きくして左辺の共通部分をとったもの

$$\cap_M (H \cdot G(L/M)) \supset H'$$

が、H の閉包であることを言えば証明は終わる。$H \cdot G(L/M)$ は部分群であり、$G(L/M)$ が開であることから開部分群であり、したがって閉部分群である。それらの共通部分は閉部分群である。

これが閉包に一致しないとすると、閉包に含まれていて左辺には含まれないある $g \in G(L/K)$ が存在する。閉包に含まれるから g のどんな開近傍 $g \cdot G(L/M')$ も H と交わる。$G(L/M')$ を移行すると、左辺に g が入っていることを示している。これは矛盾である。

以上により、無限次ガロア理論の基本定理は証明された。 □

2.4 実例：有限体の場合

p を素数とし、有限体 $K = \mathbb{F}_q$, $q = p^f$ を考える。K の n 次拡大体 L を考えると、q 乗写像 $K \to K, x \to x^q$ は単位環準同型であり、核は自明なので単射であり、有限集合だから全射でもある。これをフロベニウス写像といい Frob であらわす。$(\mathbb{F}_q)^\times$ の元は $x^{q-1} = 1$ を満たし、$x = 0$ をも加えれば $x^q = x$ を満たす。したがって

$$\mathrm{Frob} \in \mathrm{Aut}(L/K).$$

さて、Frob が生成する部分群 $H < \mathrm{Aut}(L/K)$ を考えると、$L^H = K$ である。なぜなら、Frob が固定する元は $x^q - x = 0$ の根であり、それはたかだか q 個しかないが、それらは K の元で尽くされているからである。よって、補題 1.57 により、L/K はガロア拡大であり、また、有限次ガロア理論の基本定理により、$H = G(L/K)$ に他ならない。

定理 2.5. $K = \mathbb{F}_q$ を q 元体、L/K を任意の有限次拡大体とし、その拡大次数を n とする。これはガロア拡大であり、ガロア群はフロベニウス Frob で生成され、$(\mathbb{Z}/n, +)$ に同型である。

ガロア拡大であるから、ガロア群の位数と拡大次数は等しい。n 元からなる一元生成の群は、$\mathbb{Z}/n$ に他ならない。

定理 2.6. $K = \mathbb{F}_q$ とし、$\bar{K}$ をその一つの代数閉包とする。これは K のガロア拡大であり、$\mathrm{Frob} \in G(\bar{K}/K)$ の生成する部分群の位相的閉包は $G(\bar{K}/K)$ に一致する。

命題 2.7. 任意の素数 p、自然数 f に対して p^f 元からなる体が存在し、同型を除いて一意である。

このような体を K とおく。素体の理論により K は $\mathbb{F}_p$ を部分体としてもつ。$\mathbb{F}_p$ 上の有限次拡大である。Ω を $\mathbb{F}_p$ の代数閉包とすると、K は Ω にある $\sigma : K \to \Omega$ により埋め込める。このとき、$q = p^f$ 乗フロベニウスは $\mathrm{Frob}_q \in G(\Omega/\sigma(K))$ に入り、その固定体は $\sigma(K)$ であることを上で見た。フロベニウスの選び方は $q = p^f$ にしかよらない。したがってその固定体も q にしかよらない。任意の K が、同じフロベニウスの固定体と同型なのだから、互いに同型である。

存在の方は、q 乗フロベニウスの Ω における固定体を取ればよい。$t^q - t = 0$ を Ω において解くわけだが、重根がない（微分して gcd をとると $(t^q - t, -1) = 1$ だから）。よって、q 元からなる体となる。

ガロア理論の基本定理により、$\mathbb{Z}/n$ の部分群と、$\mathbb{F}_{q^n}/\mathbb{F}_q$ の中間体は 1 対 1 対応する。$\mathbb{Z}/n$ の部分群は $d\mathbb{Z}/n,\ d|n$ の形をしている。これに対応する中間体は $\mathbb{F}_{q^d}$ である。

逆に、中間体はこの形のものに限られる。

定義 2.8. $\mathbb{Z}/n$ は、n の整除の関係に関して射影系をなす。この射影的極限を

$$\hat{\mathbb{Z}} := \mathrm{proj}\lim \mathbb{Z}/n$$

と書く。

命題 2.9. K を有限体とするとき、

$$G(\bar{K}/K) \cong \hat{\mathbb{Z}}.$$

証明は、各有限次拡大についての射影極限をとることによる。