

ガロア理論の基本定理

吉田 輝義

0.0 準備

(a) 集合と写像・体・群 ここでは集合論の公理には立ち入らないが、集合 X とは「 x が X の元である ($x \in X$ と書く)」か否かが定まっているような概念であり、普通は自然数の集合から (あるいは元を持たない空集合から) 出発していくつかの公理に基づいて構成されるものである。例えば自然数 $1, 2, \dots, n$ のみを元にもつ集合を $\{1, 2, \dots, n\}$ と表す。集合 X, Y に対し、任意の $y \in Y$ に対し $y \in X$ であるとき Y は X の部分集合であるといい $Y \subset X$ と書く。 $Y \subset X$ かつ $X \subset Y$ のとき $X = Y$ と定める。集合 Λ の各元 $\lambda \in \Lambda$ に対して X の部分集合 Y_λ が定まってい、任意の $x \in X$ はただ一つの $\lambda \in \Lambda$ に対して $x \in Y_\lambda$ となっているとき、 X は Y_λ の直和であるという。

集合 X, Y に対し、任意の $x \in X$ にある $\tau(x) \in Y$ を対応させる規則を写像 $\tau: X \rightarrow Y$ という。集合 X に対し恒等写像 $\text{id}_X: X \rightarrow X$ が任意の $x \in X$ に対し $\text{id}_X(x) = x$ で定義され、 X の部分集合 Y に対し包含写像 $\iota: Y \rightarrow X$ が任意の $y \in Y$ に対し $\iota(y) = y$ で定義される。写像 $\tau: X \rightarrow Y$ と $Z \subset X$ に対し、 $x \in Z$ に対する $\tau(x)$ からなる Y の部分集合 $\tau(Z)$ が定まる。二つの写像 $\tau: X \rightarrow Y$ と $\sigma: Y \rightarrow Z$ の合成 $\sigma\tau: X \rightarrow Z$ は $\sigma\tau(x) = \sigma(\tau(x))$ で定義される。写像 $\tau: X \rightarrow Y$ と $\sigma: Y \rightarrow X$ に対し $\sigma\tau = \text{id}_X$ かつ $\tau\sigma = \text{id}_Y$ であるとき σ, τ は互いに逆写像であるという。このとき $x = \sigma(y)$ は $\tau(x) = y$ をみたす唯一の x だから、 σ は τ によって唯一に定まるので $\sigma = \tau^{-1}$ と表す。逆写像が存在するとき τ は可逆であるといい、このとき τ^{-1} も可逆で $(\tau^{-1})^{-1} = \tau$ である。2つの可逆写像の合成は可逆である。 $\tau: X \rightarrow Y$ が可逆ならば $Y = \tau(X)$ である。包含写像 $\iota: Y \rightarrow X$ が可逆ならば $Y = X$ である。

自然数 n に対し、集合 X から $\{1, 2, \dots, n\}$ への可逆写像が存在するとき、 X は有限でその元の個数は n であるといい、 $|X| = n$ と表す。 $n \neq n'$ ならば $\{1, 2, \dots, n\}$ と $\{1, 2, \dots, n'\}$ の間には可逆写像は存在しないから、元の個数は存在すれば唯一に定まる。有限集合 X が X_λ の直和であれば、 $|X|$ は各 λ に対する $|X_\lambda|$ の和である。 $Y \subset X$ かつ $|X| \leq |Y|$ ならば $Y = X$ である。

集合 X に対して、任意の2つの元 $x, y \in X$ に対し $x + y, xy \in X$ を対応させる規則 (加法・乗法) が定まってい、(i) 相異なる2つの元 $0, 1 \in X$ が存在し、任意の $x \in X$ に対し $0 + x = x, 1x = x$, (ii) 任意の $x, y, z \in X$ に対し $(x + y) + z = x + (y + z)$, $x(yz) = (xy)z$ (結合法則), $x + y = y + x$, $xy = yx$ (交換法則), $x(y + z) = xy + xz$ (分配法則), (iii) 任意の $x \in X$ に対し $-x$ が存在して $x + (-x) = 0$, (iv) 任意の $x \neq 0$ に対し x^{-1} が存在して $xx^{-1} = 1$, という条件をみたすとき、 X を体という。このとき $0, 1$ はそれぞれ唯一に定まり、また任意の $x \in X$ に対し $-x, x^{-1}$ も唯一に定まる。体 X の部分集合 Y が、(i) $0, 1 \in Y$, (ii) $x, y \in Y$ ならば $x + y, x - y, xy \in Y$, (iii) $x \in Y$ かつ $x \neq 0$ ならば $x^{-1} \in Y$, という条件をみたすとき、 Y は X の加法・乗法によって体となり、 Y は X の部分体であるという。2つの体 X, Y の間の写像 $\tau: X \rightarrow Y$ は、(i) $\tau(0) = 0, \tau(1) = 1$, (ii) $\tau(x + y) = \tau(x) + \tau(y)$, $\tau(xy) = \tau(x)\tau(y)$ をみたすとき体の射であるといい、このとき $\tau(X)$ は Y の部分体であり、 $x \in X$ に対し $\tau(x) = 0$ ならば $x = 0$ である ($x \neq 0$ ならば $1 = \tau(1) = \tau(xx^{-1}) = 0 \cdot \tau(x^{-1}) = 0$ となり矛盾)。体の射が可逆ならば、逆写像も体の射である。体 X の部分体 Y に対し、包含写像 $\iota: Y \rightarrow X$ は体の射である。

集合 X に対して、任意の 2 つの元 $\sigma, \tau \in X$ に対して $\sigma\tau \in X$ を対応させる規則 (合成) が定まっていて、(i) ある元 $e \in X$ が存在して、任意の $\sigma \in X$ に対し $e\sigma = \sigma e = \sigma$ 、(ii) 任意の $\rho, \sigma, \tau \in X$ に対し $\rho(\sigma\tau) = (\rho\sigma)\tau$ (結合法則)、(iii) 任意の $\sigma \in X$ に対し σ^{-1} が存在して $\sigma\sigma^{-1} = \sigma^{-1}\sigma = e$ 、という 3 つの条件をみたすとき、 X を群という。このとき e は唯一つに定まり、また任意の $\sigma \in X$ に対し σ^{-1} も唯一つに定まる。群 X の部分集合 Y が、(i) $e \in Y$ 、(ii) 任意の $\sigma, \tau \in Y$ に対し $\sigma\tau, \sigma^{-1} \in Y$ をみたすならば、 Y は X の合成によって群となる。このとき Y は X の部分群であるという。

(b) 線型代数 体 K と集合 X に対して、任意の $x, y \in X$ に対し $x + y \in X$ を対応させる規則 (加法) および任意の $a \in K$ と $x \in X$ に対し $ax \in X$ を対応させる規則 (K の作用) が定まっていて、(i) ある元 $0 \in X$ が存在し、任意の $x \in X$ に対し $0 + x = x$ 、 $1x = x$ 、(ii) 任意の $x, y, z \in X$ と $a, b \in K$ に対し $(x + y) + z = x + (y + z)$ 、 $a(bx) = (ab)x$ (結合法則)、 $x + y = y + x$ (交換法則)、 $a(x + y) = ax + ay$ 、 $(a + b)x = ax + bx$ (分配法則)、(iii) 任意の $x \in X$ に対し $-x$ が存在し $x + (-x) = 0$ 、という 3 つの条件をみたすとき、 X を K ベクトル空間という。このとき 0 は唯一つに定まり、任意の $x \in X$ に対し $-x$ も唯一つに定まり、 $0x = 0$ 、 $(-a)x = -(ax)$ が従う。

S を K ベクトル空間 X の部分集合とする。 $a_1, \dots, a_n \in K$ および $x_1, \dots, x_n \in S$ に対し $a_1x_1 + \dots + a_nx_n$ の形の表示を S の K 線型結合といい、すべての a_i が 0 であるものを自明な K 線型結合という。 S の K 線型結合のうち $0 \in X$ に等しいのは自明なもののみであるとき、 S は K 線型独立であるという。 X の任意の元が S の K 線型結合で表せるとき S は X の生成系であるといい、 K 線型独立な生成系を X の K 上の基底という。 S が基底ならば X の任意の元は S の K 線型結合で一意的に表される。有限な生成系 S が存在するとき X は有限生成であるという。このとき S の部分集合 T で、生成系だがどの元を除いても生成系でなくなるものをとれば、 T は X の基底である。

定理. X が有限生成ならば任意の基底の元の個数は等しい。この個数 n を X の次元という。 S を X の K 線型独立な部分集合とすると $|S| \leq n$ であり、 $|S| = n$ ならば S は基底である。

逆に自然数 n が存在して X の任意の K 線型独立な部分集合 S に対し $|S| \leq n$ であるならば、他のどの元を加えても線型独立でなくなるような S をとれば X の生成系であるから、 X は有限生成である。このとき定理より次元は n 以下である。

例. K は $\{1\}$ を基底とする 1 次元 K ベクトル空間である。正の整数 n に対し、 K の元の n 個組 (a_1, \dots, a_n) の全体のなす集合 K^n を考える。 a_i を (a_1, \dots, a_n) の第 i 成分という。 K^n に成分ごとの加法・成分ごとの K の乗法による K の作用を定義すると、 K^n は K ベクトル空間になる。第 i 成分のみが 1 でその他の成分がすべて 0 である元を $e_i \in K^n$ と表すと、 $(a_1, \dots, a_n) = a_1e_1 + \dots + a_n e_n$ と一意的に表され、 $\{e_1, \dots, e_n\}$ は K^n の基底であるから、 K^n の次元は n である。

2 つの K ベクトル空間 X, Y の間の写像 $\tau: X \rightarrow Y$ は、任意の $x, y \in X$ と $a \in K$ に対し $\tau(x + y) = \tau(x) + \tau(y)$ 、 $\tau(ax) = a\tau(x)$ をみたすとき K 線型であるという。このとき $\tau(0) = 0$ である。 K 線型写像が可逆ならば逆写像も K 線型である。 K 線型写像 $\tau: X \rightarrow Y$ は、 $\tau(x) = 0$ となる $x \in X$ が $x = 0$ に限るとき単射であるという。単射によって K 線型独立な集合は K 線型独立な集合に写る。よって、 X, Y の次元がそれぞれ n, m で単射 $\tau: X \rightarrow Y$ が存在すれば $n \leq m$ である。 $n = m$ であれば、任意の単射 $X \rightarrow Y$ は定理より基底を基底に写すから可逆である。

0.1 拡大

定義. K を体とする. 体 F と射 $\tau: K \rightarrow F$ の組を K の拡大と呼び, F_τ と表す.

(a) 射・群 (以下現れる $(F_\tau, F'_{\tau'})$, (F_τ) は普通 $\text{Hom}(F_\tau, F'_{\tau'})$, $\text{Aut}(F_\tau)$ などと書かれる.)

定義. K の拡大 $F_\tau, F'_{\tau'}$ に対し, F_τ から $F'_{\tau'}$ への射とは, 体の射 $\rho: F \rightarrow F'$ であって $\rho\tau = \tau'$ をみたすもののことである. F_τ から $F'_{\tau'}$ への射の全体のなす集合を $(F_\tau, F'_{\tau'})$ で表す.

$$\begin{array}{ccc} F & \xrightarrow{\rho} & F' \\ & \swarrow \tau & \nearrow \tau' \\ & K & \end{array}$$

射 $\rho \in (F_\tau, F'_{\tau'})$ が可逆ならば, $\rho\tau = \tau'$ から $\tau = \rho^{-1}\rho\tau = \rho^{-1}\tau'$ であるから $\rho^{-1} \in (F'_{\tau'}, F_\tau)$ である. 拡大 F_τ に対し, (F_τ, F_τ) の可逆な射たちのなす部分集合を (F_τ) で表す. $\text{id} \in (F_\tau)$ であり, また $\rho, \rho' \in (F_\tau)$ に対して $\rho\rho', \rho^{-1} \in (F_\tau)$ だから, (F_τ) は射の合成に関して群をなす.

(b) 次数 F_τ を K の拡大とすると, F に K の τ による作用 (K の元 x を $\tau(x)$ 倍で作用させる) を定めると, F は K ベクトル空間となる. 拡大の間の射は単射の K 線型写像になる.

定義. 拡大 F_τ は, τ による作用で F が有限生成 K ベクトル空間となるとき有限拡大といい, その次元を F_τ の次数といって $[F_\tau]$ で表す. 次数が 1 ならば τ は可逆だから $F = \tau(K)$ である.

射 $\rho \in (F_\tau, F'_{\tau'})$ は単射の K 線型写像だから, $F_\tau, F'_{\tau'}$ が有限拡大で $[F_\tau] = [F'_{\tau'}]$ であれば可逆である. とくに有限拡大 F_τ に対し $(F_\tau) = (F_\tau, F_\tau)$ である.

(c) ガロア拡大の定義

命題 1. (デデキント) K の拡大 $F_\tau, F'_{\tau'}$ に対し, F_τ が有限拡大ならば $|(F_\tau, F'_{\tau'})| \leq [F_\tau]$. とくに $|(F_\tau)| \leq [F_\tau]$.

証明. 一般に有限生成 K ベクトル空間 V と K の拡大 F_τ に対して, V から F への K 線型写像全体のなす集合を $\text{Hom}_K(V, F)$ で表す. これに加法と F の作用を $(\rho + \rho')(x) = \rho(x) + \rho'(x)$, $(a\rho)(x) = a\rho(x)$ で定めれば F ベクトル空間になる. また $\{e_1, \dots, e_n\}$ が V の基底ならば, $\rho_i \in \text{Hom}_K(V, F)$ を $\rho_i(a_1e_1 + \dots + a_n e_n) = \tau(a_i)$ で定めれば任意の ρ は $\rho = \rho(e_1)\rho_1 + \dots + \rho(e_n)\rho_n$ と一意的に表されるから $\{\rho_1, \dots, \rho_n\}$ は $\text{Hom}_K(V, F)$ の基底である. そこで, $(F_\tau, F'_{\tau'})$ が $\text{Hom}_K(F, F')$ の部分集合として F' 線型独立であることを示せば定理より命題が従う.

$(F_\tau, F'_{\tau'}) = \{\rho_1, \rho_2, \dots\}$ とし, $\{\rho_1, \dots, \rho_k\}$ が F' 線型独立なことを k に関する帰納法で示す. $a_1\rho_1 + \dots + a_k\rho_k = 0$ (*) を F' 線型結合とする. $k = 1$ なら $\rho_1 \neq 0$ だからよい. 任意の $x, y \in F$ に対し $a_1\rho_1(xy) + \dots + a_k\rho_k(xy) = 0$ だから, 写像として $a_1\rho_1(x)\rho_1 + \dots + a_k\rho_k(x)\rho_k = 0$. (*) の $\rho_k(x)$ 倍を引いて, $a_1(\rho_1(x) - \rho_k(x))\rho_1 + \dots + a_{k-1}(\rho_{k-1}(x) - \rho_k(x))\rho_{k-1} = 0$. よって帰納法の仮定より係数はすべて 0 で, x は任意だから $a_i(\rho_i - \rho_k) = 0$ を得るが, $a_i \neq 0$ とすると a_i^{-1} をかけて $\rho_i \neq \rho_k$ に矛盾するから $a_i = 0$ ($1 \leq i \leq k-1$). よって $k = 1$ の場合より a_k も 0. \square

定義. 有限拡大 F_τ は, $|(F_\tau)| = [F_\tau]$ のときガロア拡大という.

(d) ガロア拡大の構成

定義. K の拡大 F_τ に対し, L を $\tau(K)$ を含む F の部分体とする. τ を K から L への射と考えた K の拡大 L_τ を F_τ の部分拡大といい, 包含写像 $\iota: L \rightarrow F$ で定まる拡大 F_ι を F/L で表す.

一般に $(F_\tau) = (F/\tau(K))$ であり, F_τ が有限拡大ならば $[F_\tau] = [F/\tau(K)]$. また G を (F_τ) の部分群とすると, G の任意の元の作用で動かないような F の元全体のなす F の部分集合 $F^G = \{ \text{任意の } \rho \in G \text{ に対し } \rho(x) = x \text{ なる } x \in F \}$ は各 ρ が体の射だから F の部分体となり, $\tau(K)$ を含むから, 部分拡大 F_τ^G が定まる. 定義より直ちに $G \subset (F/F^G)$.

命題 2. (アルティン) (F_τ) の有限な部分群 G に対し, F/F^G はガロア拡大で $G = (F/F^G)$.

証明. $G = \{\rho_1, \dots, \rho_n\}$ ($\rho_1 = \text{id}$) とし, $x \in F$ に対して $\rho(x) = (\rho_1(x), \dots, \rho_n(x)) \in F^n$ と書く. $\rho \in G$ と $\mathbf{x} = (x_1, \dots, x_n) \in F^n$ に対し $\rho(\mathbf{x}) = (\rho(x_1), \dots, \rho(x_n))$ と定めると $\rho(a\mathbf{x}) = \rho(a)\rho(\mathbf{x})$ であり, $\rho(\rho(\mathbf{x}))$ は $\rho(\mathbf{x})$ の成分の順序を置換したものになるから, $a_1\rho(x_1) + \dots + a_k\rho(x_k) = 0$ (*) ならば $\rho(a_1)\rho(x_1) + \dots + \rho(a_k)\rho(x_k) = 0$ (†).

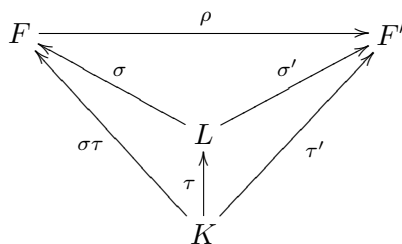
$L = F^G$ とおく. F の任意の L 線型独立な部分集合 $\{x_1, \dots, x_k\}$ に対して F^n の部分集合 $\{\rho(x_1), \dots, \rho(x_k)\}$ が F 線型独立なこと (従って $k \leq n$) を k に関する帰納法で示す. (*) を F 線型結合とする. $k = 1$ なら $\rho(x_1) \neq 0$ だからよい. まず $a_k \neq 0$ と仮定する. すべての a_i を a_i/a_k で置き換えて $a_k = 1$ としよ. すると任意の $\rho \in G$ に対し $\rho(a_k) = 1$ だから, (*) から (†) を引いて $(a_1 - \rho(a_1))\rho(x_1) + \dots + (a_{k-1} - \rho(a_{k-1}))\rho(x_{k-1}) = 0$. よって帰納法の仮定より係数はすべて 0 で, ρ は任意だから $a_i \in L$ ($1 \leq i \leq k-1$). ここで (*) の第 1 成分を見ると $a_1x_1 + \dots + a_kx_k = 0$ で, $\{x_1, \dots, x_k\}$ が L 線型独立かつ $a_k = 1$ だったから矛盾. 従って $a_k = 0$ だから, 帰納法の仮定より a_i はすべて 0. よって F/L は有限拡大で定理より $[F/L] \leq n = |G|$. 一方 $G \subset (F/L)$ と命題 1 より $|G| \leq (F/L) \leq [F/L]$ なので, $|(F/L)| = [F/L]$ かつ $G = (F/L)$. □

0.2 拡大の塔

L_τ が K の拡大, F_σ が L の拡大ならば, $\sigma\tau: K \rightarrow F$ は拡大 $F_{\sigma\tau}$ を定める. これを拡大の塔 L_τ, F_σ という: $K \xrightarrow{\tau} L \xrightarrow{\sigma} F$. L_τ が F_τ の部分拡大ならば $L_\tau, F/L$ は拡大の塔である.

(a) 塔と射・群 K の任意の拡大 F'_τ と $\rho \in (F_{\sigma\tau}, F'_\tau)$ に対して $\sigma' = \rho\sigma: L \rightarrow F'$ とおくと L の拡大 $F'_{\sigma'}$ が得られ, $\rho \in (F_\sigma, F'_{\sigma'})$. また $\sigma'\tau = \rho\sigma\tau = \tau'$ だから $\sigma' \in (L_\tau, F'_\tau)$. 逆に $\sigma' \in (L_\tau, F'_\tau)$ かつ $\rho \in (F_\sigma, F'_{\sigma'})$ であれば, $\rho\sigma\tau = \sigma'\tau = \tau'$ より $\rho \in (F_{\sigma\tau}, F'_\tau)$. 以上により次が示された:

補題 a. 塔 L_τ, F_σ と K の任意の拡大 F'_τ に対し, $(F_{\sigma\tau}, F'_\tau)$ は各 $\sigma' \in (L_\tau, F'_\tau)$ に対する $(F_\sigma, F'_{\sigma'})$ の直和である. とくに $F'_\tau = F_{\sigma\tau}$ を考えれば, (F_σ) は $(F_{\sigma\tau})$ の部分群である.



(b) 塔と次数・ガロア拡大の特徴づけ

補題 b. 塔 L_τ, F_σ に対し, $F_{\sigma\tau}$:有限拡大 $\iff L_\tau, F_\sigma$:有限拡大. このとき $[F_{\sigma\tau}] = [F_\sigma][L_\tau]$.

証明. (\implies): 定理およびその直後の注意による ($S \subset L$ が K 線形独立なら $\sigma(S) \subset F$ も K 線形独立; L 線形独立な $S \subset F$ は K 線形独立). (\impliedby): $\{a_i\}$ を F の L 上の基底, $\{b_j\}$ を L の K 上の基底とする. 任意の F の元は $\{a_i\}$ の L 線形結合で表して各係数を $\{b_j\}$ の K 線形結合で表せば $\{a_i\sigma(b_j)\}$ の K 線形結合で一意的に表されるから, $\{a_i\sigma(b_j)\}$ は F の K 上の基底である. \square

命題 3. 有限拡大 F_τ に対し $G = (F_\tau)$ とおくと, F_τ :ガロア拡大 $\iff F^G = \tau(K)$.

証明. (\implies): $L = F^G$ とおくと $L_\tau, F/L$ は塔だから補題 b より $[F_\tau] = [F/L][L_\tau]$. 一方 $G \subset (F/L)$ と命題 1 より $[F_\tau] = |G| \leq |(F/L)| \leq [F/L]$ だから $[L_\tau] = 1$, よって $L = \tau(K)$.

(\impliedby): 命題 2 より $F/\tau(K)$ はガロア拡大だから, $|(F_\tau)| = |(F/\tau(K))| = [F/\tau(K)] = [F_\tau]$. \square

(c) 塔とガロア拡大

補題 c. 有限拡大の塔 L_τ, F_σ に対し, $F_{\sigma\tau}$ がガロア拡大ならば, F_σ もガロア拡大である.

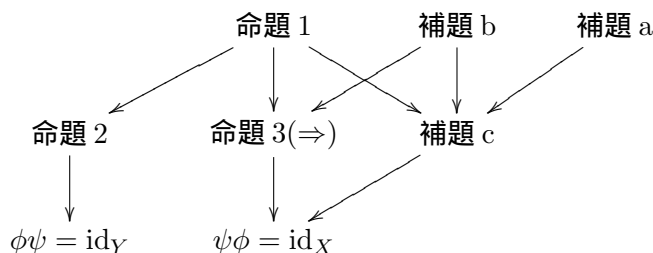
証明. 補題 b より $|(F_{\sigma\tau})| = [F_{\sigma\tau}] = [F_\sigma][L_\tau]$. 一方補題 a を $F_{\tau'} = F_{\sigma\tau}$ に適用すると, $|(F_{\sigma\tau})|$ は各 $\sigma' \in (L_\tau, F_{\sigma\tau})$ に対する $|(F_\sigma, F_{\sigma'})|$ の和で, これが $[F_\sigma][L_\tau]$ となるには, 命題 1 より $|(L_\tau, F_{\sigma\tau})| = [L_\tau]$ かつすべての σ' で $|(F_\sigma, F_{\sigma'})| = [F_\sigma]$ が必要である. とくに $\sigma' = \sigma$ として $|(F_\sigma)| = [F_\sigma]$. \square

(d) 基本定理

基本定理. ガロア拡大 F_τ の部分拡大全体のなす集合を X とし, (F_τ) の部分群全体のなす集合を Y とすれば, 次は互いに逆写像である (ϕ は補題 a の後半により定まる):

$$\phi : X \ni L_\tau \mapsto (F/L) \in Y, \quad \psi : Y \ni G \mapsto F_\tau^G \in X.$$

証明. $\psi\phi = \text{id}_X$ は補題 c と命題 3(\implies) より従う. $\phi\psi = \text{id}_Y$ は命題 2 である. \square



謝辞. 勝良健史氏, 谷口隆氏, 三枝洋一氏, 山本修司氏のコメントに感謝します. (2011/6/4)