資料08-2

有限次Galois拡大 L/K を $K=L^G$ (G は $\mathrm{Aut}(L)$ の有限部分群) で作れること

← 最小分解体とは別の作り方

後で $X=L^\times$, $\sigma_i \in \mathrm{Aut}(L)$ の場合に Artinの補題を使う.

Artinの補題 群 X から体 L の乗法群 $L^\times$ への互いに異なる群の準同型たち $\sigma_1,\dots,\sigma_n$ は L 上一次独立である.

(注意 X から L への写像全体の集合は L 上のベクトル空間とみなされる.)

$$\begin{array}{ccc} X & \xrightarrow{\sigma_i} & L^\times \subset L \\ \Psi & & \Psi \\ x & \longmapsto & \sigma_i(x) \end{array}$$

証明 次の $(*)_n$ を $n=1,2,\dots$ に関する数学的帰納法で示せばよい.

$(*)_n$ $\begin{cases} \sigma_1,\dots,\sigma_n \text{ は P から } L^\times \text{ への互いに異なる群の準同型で,} \\ a_1,\dots,a_n\in L \text{ かつ } a_1\sigma_1(x)+\cdots+a_n\sigma_n(x)=0 \ (x\in X) \text{ ならば } a_1=\cdots=a_n=0. \end{cases}$

$(*)_1$ を示そう. $a_1\sigma_1(x)=0$ $(x\in X)$ と $\sigma_1(x)\in L^\times$ $(x\in X)$ より $a_1=0$.

$n\geqq 2$ であるとし, $(*)_{n-1}$ が成立していると仮定する. $(*)_n$ を示せばよい.

$\sigma_1,\dots,\sigma_n$ は X から $L^\times$ への互いに異なる群の準同型であり,

$a_1,\dots,a_n\in L$ かつ $a_1\sigma_1(x)+\cdots+a_n\sigma_n(x)\overset{(☆)}{=}0$ $(x\in X)$ と仮定する.

$\sigma_1\neq\sigma_n$ なので, ある $y\in X$ が存在して $\sigma_1(y)\neq\sigma_n(y)$ となる.

つづく

任意に $x\in X$ をとる. (☆)より,

$$0=\sigma_n(y)(a_1\sigma_1(x)+\cdots+a_n\sigma_n(x)) = a_1\sigma_n(y)\sigma_1(x)+\cdots+a_{n-1}\sigma_n(y)\sigma_{n-1}(x)+\underbrace{a_n\sigma_n(y)\sigma_n(x)}.$$

(☆)で x を yx におきえると,

差をとるとキャンセル

$$0=a_1\sigma_1(yx)+\cdots+a_n\sigma_n(yx) = a_1\sigma_1(y)\sigma_1(x)+\cdots+a_{n-1}\sigma_{n-1}(y)\sigma_{n-1}(x)+\overbrace{a_n\sigma_n(y)\sigma_n(x)}.$$

これらの差を考えると, $0=\underbrace{a_1(\sigma_n(y)-\sigma_1(y))}_{\in L}\sigma_1(x)+\cdots+\underbrace{a_{n-1}(\sigma_n(y)-\sigma_{n-1}(y))}_{\in L}\sigma_{n-1}(x).$

ゆえに, $(*)_{n-1}$ より, $a_1\underbrace{(\sigma_n(y)-\sigma_1(y))}_{\neq 0}=0,\ \ldots,\ a_{n-1}(\sigma_n(y)-\sigma_{n-1}(y))=0$. 特に, $a_1=0$.

$a_1=0$ と(☆)と $(*)_{n-1}$ より, $a_2=\cdots=a_n=0$. □

$\boxed{\text{注意}}$ G が体 L の自己同型群の部分群であるとき,
各 $\sigma\in G$ は $L^\times$ から $L^\times$ への群の準同型写像を与え,
σ から定まる $L^\times$ から $L^\times$ への群の準同型写像から
もとの σ は 0 を 0 にうつすという拡張で一意に決まるので,
Artinの補題を $X=L^\times$ の場合に適用することによって,
G は L 上一次独立な集合になっていることがわかる. □

$\sigma\in\mathrm{Aut}(L)$ ならば
$x,y\in L^\times$ について,
$\sigma(x),\sigma(y)\in L^\times$ でかつ
$\sigma(xy)=\sigma(x)\sigma(y)$.
($\sigma: L^\times\to L^\times$
群の準同型とみなせる.)

ここがポイント

$\boxed{\text{Artinの定理}}$ Gは体Lの自己同型群の有限部分群であるとし,

Lの部分体KをK $= L^G = \{\beta \in L \mid \sigma(\beta) = \beta\ (\sigma \in G)\}$ と定める.

このとき, L/K は有限次Galois拡大であり, $[L:K] = |G|$.

(Galois拡大 L/K のKからLを作るのではなく, LからKを作る話)

$G = \mathrm{Gal}(L/K)$ にもなる.

$\boxed{\text{証明}}$ まずトレース写像 $T: L \to K$ を定義しよう.

$\boxed{0}$ $\beta \in L$ に対して, $T(\beta) \in L$ を $T(\beta) = \sum_{\sigma \in G} \sigma(\beta)$ と定める.

このとき, 任意の $\sigma \in G$ に対して, $\sigma(T(\beta)) = \sum_{\tau \in G} \sigma\tau(\beta) = \sum_{\rho \in G} \rho(\beta) = T(\beta)$ なので,

$T(\beta) \in L^G = K$ となる.

σはK上の線形写像である.

$\sigma \in G$, $a \in K$, $\beta \in L$ について, $\sigma(a\beta) = \sigma(a)\sigma(\beta) = a\sigma(\beta)$ なので,

Gの元はK上でのLの体の自己同型になっている.

これで, K上の線形写像 $T = \sum_{\sigma \in G} \sigma : L \to K$ が得られたことになる.

前ページを参照.

Artinの補題の $X = L^\times$ の場合より

Artinの補題より, GはL上一次独立な集合になる (前ページの注意を参照).

特に, $T = \sum_{\sigma \in G} \sigma \neq 0$ なので, ある $\alpha \in L$ が存在して $T(\alpha) \neq 0$. ← このαを次ページで使う.

$\boxed{1}$ $[L:K] \leqq |G|$ を示そう。 $n = |G|$ とおく。

任意に $\beta_1, \cdots, \beta_{n+1} \in L$ をとる。 $\beta_1, \cdots, \beta_{n+1}$ が K 上一次従属であることを示せばよい。

$n=|G|$ 連立の $x_1, \cdots, x_{n+1}$ に関する一次方程式 $\sum_{i=1}^{n+1} \sigma^{-1}(\beta_i) x_i = 0 \quad (\sigma \in G)$ の　σ は n 個

非自明な解 $(x_1, \cdots, x_{n+1}) = (\gamma_1, \cdots, \gamma_{n+1})$, $\gamma_i \in L$ が存在する。（非自明な解は どれかが 0 でない解）

$\gamma_1 \neq 0$ と仮定してよい。 $k = \frac{\alpha}{\gamma_1} \neq 0$ とおくと, $(k\gamma_1, \cdots, k\gamma_{n+1})$ も非自明な解になり, $k\gamma_1 = \alpha$ なので, $\gamma_1 = \alpha$ と仮定できる。

このとき, $\sum_{i=1}^{n+1} \sigma^{-1}(\beta_i)\gamma_i = 0$ の両辺に σ を作用させると, $\sum_{i=1}^{n+1} \beta_i \sigma(\gamma_i) = 0 \quad (\sigma \in G)$,

これを $\sigma \in G$ について足し上げると, $\sum_{i=1}^{n+1} \beta_i T(\gamma_i) = 0$ が得られ, $T(\gamma_1) = T(\alpha) \neq 0$ と $T(\gamma_i) \in K$ より, $\beta_1, \cdots, \beta_{n+1}$ が K 上一次従属であることがわかる。

$\boxed{\text{注意}}$ 特にこれで L/K は有限次拡大であることがわかった。

$\boxed{2}$ $[L:K] \geqq |G|$ を示そう。

$[L:K] < |G|$ と仮定して矛盾を導こう。

$[L:K] = r < |G|$ であると仮定し、L の K 上での基底 $\beta_1, \dots, \beta_r$ をとる。

r 連立の $|G|$ 個の x_σ $(\sigma \in G)$ たちに関する一次方程式 $\sum_{\sigma \in G} \sigma(\beta_i) x_\sigma = 0$ $(i = 1, \dots, r)$ の非自明な解 $(x_\sigma)_{\sigma \in G} = (\gamma_\sigma)_{\sigma \in G}$, $\gamma_\sigma \in L$ が存在する。

任意に $\beta \in L$ をとる。$\beta = \sum_{i=1}^{r} a_i \beta_i$, $a_i \in K$ と書ける。

このとき、$\sigma(a_i \beta_i) = \sigma(a_i)\sigma(\beta_i) = a_i \sigma(\beta_i)$ と $\sum_{\sigma \in G} \sigma(\beta_i) \gamma_\sigma = 0$ $(i = 1, \dots, r)$ より、

$$\sum_{\sigma \in G} \gamma_\sigma \sigma(\beta) = \sum_{\sigma \in G} \gamma_\sigma \sum_{i=1}^{r} a_i \sigma(\beta_i) = \sum_{i=1}^{r} a_i \sum_{\sigma \in G} \sigma(\beta_i) \gamma_\sigma = 0 \quad \leftarrow \text{これが } \forall \beta \in L \text{ について成立}$$

となり、ある $\sigma \in G$ が存在して $\gamma_\sigma \neq 0$ となっているので、

G が L 上一次従属になって (Artinの補題に) 矛盾する。

$\boxed{3}$ L/Kが分離的であることを示そう。 θのK上での最小多項式が重根を持たないという意味

標数0では自明

$\theta \in L$を任意にとる。 θがK上分離的であることを示せばよい。

(L/Kが分離的であることの定義(の1つ)は、Lの任意の元のK上での最小多項式が重根を持たないことである。)

ポイント

L/Kは有限次拡大なのでθはK上代数的である。

Lに含まれるθのK上での共役元で互いに異なるもの全体を$\theta_1, \dots, \theta_r$と書く。

任意の$\sigma \in G$について、$\sigma(\theta_i)$もθのK上での共役元になるので、

σは集合$\{\theta_1, \dots, \theta_r\}$に作用している: $\{\sigma(\theta_1), \dots, \sigma(\theta_r)\} = \{\theta_1, \dots, \theta_r\}$ $(\sigma \in G)$.

$f(x) = \prod_{i=1}^{r}(x - \theta_i) = \sum_{i=0}^{r} c_i x^i$ $(c_i \in L)$とおく。 $f(x)$は重根を持たない。

このとき、任意の$\sigma \in G$について、$\sum_{i=0}^{r} \sigma(c_i) x^i = \prod_{i=1}^{r}(x - \sigma(\theta_i)) = \prod_{i=1}^{r}(x - \theta_i) = f(x)$

なので$\sigma(c_i) = c_i$となり、$c_i \in K$, $f(x) \in K[x]$となることがわかる。

θのK上での最小多項式は$f(x)$を割り切るので重根を持たない。

これでθがK上分離的であることが示された。

$\boxed{4}$ L/K が正規拡大であることを示そう.

上に続けて, $\theta \in L$ の K 上でのすべての共役元が L に含まれることを示せばよい.

(L/K が正規であることの定義(の1つ)は, Lの任意の元の K上での最小多項式のすべての根(K上でのすべての共役元)が L に含まれることである)

しかし, θ の K 上での最小多項式が $f(x)$ を割り切ることが示されているので, θ の K 上での任意の共役元は $\theta_i \in L$ のどれかに一致する

これで L/K が正規拡大であることも示された.

Galois拡大 = 分離的かつ正規な拡大

$\boxed{5}$ 以上によって, L/K が有限次Galois拡大であり, $[L:K] = |G|$ となることが示された. (有限次拡大 L/K が Galois拡大であることの定義は L/K が分離的かつ正規であることである.)

□

$\boxed{\text{注意}}$ Artinの定理の状況のもとで, $G \subset \mathrm{Gal}(L/K)$, $[L:K] = |\mathrm{Gal}(L/K)|$ なので, $\mathrm{Gal}(L/K) = G$ となることもわかる.

□