有限次Galois拡大 L/K を $K=L^G$, $G\subset \mathrm{Aut}(L)$, $|G|<\infty$ で作れること

← 最小分解体とは別の作り方

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

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

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。

$(*)_n$ $\sigma_1,\dots,\sigma_n$ は G から $K^\times$ への互いに異なる群の準同型で、

$a_1,\dots,a_n\in K$ かつ $a_1\sigma_1(x)+\cdots+a_n\sigma_n(x)=0$ $(x\in G)$ ならば $a_1=\cdots=a_n=0$.

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

$n\geq 2$ 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 G から $K^\times$ への互いに異なる群の準同型であり、

$a_1,\dots,a_n\in K$ かつ $a_1\sigma_1(x)+\cdots+a_n\sigma_n(x)\overset{(*)}{=}0$ $(x\in G)$ と仮定する。

$\sigma_1\neq\sigma_n$ なので、ある $y\in G$ が存在して $\sigma_1(y)\neq\sigma_n(y)$ となる。

つづく

任意に $x \in G$ をとる。(☆)より、

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

(☆)で x を yx におきかえると、

差をとるとキャンセル

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

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

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 を体 L の自己同型群の部分群であるとき、

（この G は Artin の補題の G として使われないことに注意せよ。）

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 (G, K) が $(L^\times, L)$ 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。

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(G, K)が$(L, L^\times)$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。

σ は n 個

$n = |G|$ 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。$k = \dfrac{\alpha}{\gamma_1} \neq 0$ 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、

$$\sum_{\sigma \in G} \gamma_\sigma \sigma(\beta) = \sum_{\sigma \in G} \gamma_\sigma \sum_{i=1}^{r} a_i \sigma(\beta_i) = \sum_{i=1}^{r} a_i \sum_{\sigma \in G} \sigma(\beta_i) \gamma_\sigma = 0 \leftarrow$$

これが $\forall \beta \in L$ 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

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

標数 0 では自明

(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。

□