

§15. 補遺

次の命題は、例 7.9 の最後の方、および、補題 8.5 の証明で使われている。

命題 15.1 体 K の乗法群 $K^\times$ の有限部分群は巡回群である。

証明 A を $K^\times$ の有限部分群とし、 A に属する位数最大の元 a をひとつとる。 a で生成される巡回群 $\langle a \rangle$ が A に一致すること確かめればよい。そこで、 $\langle a \rangle$ に属さない $b \in A$ が存在するとして矛盾を導く。 a, b の位数をそれぞれ m, n とする。いま、素数 p について

$$m = p^e m', \quad n = p^f n', \quad \text{ただし, } p \text{ は } m' n' \text{ を割り切らない}$$

とすると、 $a^{p^e}, b^{n'}$ の位数はそれぞれ m', p^f でこれらは互いに素だから、積 $a^{p^e} b^{n'}$ の位数は $p^f m'$ である。よって、 m の最大性より

$$p^f m' \leq m = p^e m', \quad \therefore f \leq e$$

となる。これが任意の素数 p について成り立つから、 m は n の倍数であることがわかる。 b の位数は n であったから、とくに b は多項式 $X^m - 1$ の根である。一方、 a の位数は m であったから、 $m+1$ 個の元

$$b, 1, a, a^2, \dots, a^{m-1} \in K^\times$$

はすべて多項式 $X^m - 1$ の根となるが、体 K において m 次式は m 個より多くの根をもたないはずだから矛盾である。 $\square$

次に、分離拡大に関する重要な命題 8.10 および定理 8.11 の証明において鍵となった補題の証明を与える。

補題 15.2 (補題 8.9 再掲) 体 K 上代数的である α, β が、 $\beta \in K(\alpha)$ をみたすならば、

$$|\text{Conj}(\alpha, K)| = |\text{Conj}(\alpha, K(\beta))| |\text{Conj}(\beta, K)|$$

が成り立つ。

証明 ふたつの写像

$$F : \text{Conj}(\alpha, K(\beta)) \times \text{Conj}(\beta, K) \longrightarrow \text{Conj}(\alpha, K)$$

$$G : \text{Conj}(\alpha, K) \longrightarrow \text{Conj}(\alpha, K(\beta)) \times \text{Conj}(\beta, K)$$

を定義し、それらが互いに逆写像であること、すなわち $F \circ G$ と $G \circ F$ がそれぞれ恒等写像であることを確かめればよい。そのために、まず $\delta \in \text{Conj}(\beta, K)$ に対して、定理 6.11

より, $\sigma(\beta) = \delta$ をみたす $\sigma \in \text{Aut}(\overline{K}/K)$ が存在することに注意する. このような σ を各 δ に対して 1 つずつ選んで固定し σ_δ と表すことにする;

$$\sigma_\delta \in \text{Aut}(\overline{K}/K), \quad \sigma_\delta(\beta) = \delta \in \text{Conj}(\beta, K).$$

(1) F の定義: $\gamma \in \text{Conj}(\alpha, K(\beta))$ ならば, γ と α は $K(\beta)$ 上共役であるから, K 上でももちろん共役, よって $\text{Conj}(\gamma, K) = \text{Conj}(\alpha, K)$ が成り立つ. さらに, $\delta \in \text{Conj}(\beta, K)$ に対して, $\sigma_\delta \in \text{Aut}(\overline{K}/K)$ が上のようにして定まり, $\sigma_\delta(\gamma) \in \text{Conj}(\gamma, K) = \text{Conj}(\alpha, K)$ であるから,

$$F : \text{Conj}(\alpha, K(\beta)) \times \text{Conj}(\beta, K) \longrightarrow \text{Conj}(\alpha, K), \quad (\gamma, \delta) \mapsto \sigma_\delta(\gamma)$$

が定義できる.

(2) G の定義: $\varepsilon \in \text{Conj}(\alpha, K)$ に対して定理 6.11 を適用すれば, $\tau(\alpha) = \varepsilon$ をみたす $\tau \in \text{Aut}(\overline{K}/K)$ が存在する. このとき $\tau(\beta)$ の値は τ の選び方によらず ε のみから定まる (実際, $\tau' \in \text{Aut}(\overline{K}/K)$ も $\tau'(\alpha) = \varepsilon$ をみたすならば, $(\tau^{-1} \circ \tau')(\alpha) = \alpha$ だから, $\tau^{-1} \circ \tau'$ は $K(\alpha)$ 上で恒等写像であり, さらに $\beta \in K(\alpha)$ だから, $(\tau^{-1} \circ \tau')(\beta) = \beta$ すなわち $\tau'(\beta) = \tau(\beta)$ を得る). また, $\tau(\beta) \in \text{Conj}(\beta, K)$ に注意すれば, $\sigma_{\tau(\beta)} \in \text{Aut}(\overline{K}/K)$ が ε のみから定まるともわかる. ここで, 上の σ_δ の定義から $\sigma_{\tau(\beta)}(\beta) = \tau(\beta)$, すなわち $\sigma_{\tau(\beta)}^{-1}(\tau(\beta)) = \beta$ だから, $\sigma_{\tau(\beta)}^{-1} \circ \tau \in \text{Aut}(\overline{K}/K(\beta))$. よって

$$\sigma_{\tau(\beta)}^{-1}(\varepsilon) = \left(\sigma_{\tau(\beta)}^{-1} \circ \tau \right) (\alpha) \in \text{Conj}(\alpha, K(\beta))$$

であり

$$G : \text{Conj}(\alpha, K) \longrightarrow \text{Conj}(\alpha, K(\beta)) \times \text{Conj}(\beta, K), \quad \varepsilon \mapsto \left(\sigma_{\tau(\beta)}^{-1}(\varepsilon), \tau(\beta) \right)$$

が定義される.

(3) $F \circ G$ が恒等写像であることの証明: $\varepsilon \in \text{Conj}(\alpha, K)$ に対して, $\tau(\alpha) = \varepsilon$ をみたす $\tau \in \text{Aut}(\overline{K}/K)$ をとると

$$F(G(\varepsilon)) = F\left(\sigma_{\tau(\beta)}^{-1}(\varepsilon), \tau(\beta)\right) = \sigma_{\tau(\beta)}\left(\sigma_{\tau(\beta)}^{-1}(\varepsilon)\right) = \varepsilon$$

よって $F \circ G$ は $\text{Conj}(\alpha, K)$ 上の恒等写像である.

(4) $G \circ F$ が恒等写像であることの証明: $(\gamma, \delta) \in \text{Conj}(\alpha, K(\beta)) \times \text{Conj}(\beta, K)$ に対して, $F(\gamma, \delta) = \sigma_\delta(\gamma)$ である. いま γ に対して, $\rho(\alpha) = \gamma$ をみたす $\rho \in \text{Aut}(\overline{K}/K(\beta))$ が存在する. この ρ を用いると, $\sigma_\delta(\rho(\alpha)) = \sigma_\delta(\gamma)$ より, $\tau(\alpha) = \sigma_\delta(\gamma)$ をみたす $\tau \in \text{Aut}(\overline{K}/K)$ として $\tau = \sigma_\delta \circ \rho$ をとることができる. さらに $\rho(\beta) = \beta$ なので, $\tau(\beta) = \sigma_\delta(\rho(\beta)) = \sigma_\delta(\beta) = \delta$ となるから

$$G(F(\gamma, \delta)) = G(\sigma_\delta(\gamma)) = \left(\sigma_{\tau(\beta)}^{-1}(\sigma_\delta(\gamma)), \tau(\beta) \right) = \left(\sigma_\delta^{-1}(\sigma_\delta(\gamma)), \delta \right) = (\gamma, \delta)$$

よって $G \circ F$ は $\text{Conj}(\alpha, K(\beta)) \times \text{Conj}(\beta, K)$ 上の恒等写像である. □

最後に, 対称群の生成系に関する補題を紹介する. $\mathbb{Q}$ 上ベキ根によって解けない 5 次方程式の実例を与えた定理 14.11 の証明に, この補題が使われている.

補題 15.3 n を 3 以上の自然数とする. n 次対称群 S_n の部分群 G が以下のいずれかを満たすならば, $G = S_n$ が成り立つ.

- (1) G は互換 $(1\ 2), (1\ 3), \dots, (1\ n)$ を含む.
- (2) G は長さ 2, $n-1$, n の巡回置換を少なくともひとつずつ含む.
- (3) n は素数で, G は互換および長さ n の巡回置換を少なくともひとつずつ含む.

証明 (1) $2 \leq i < j \leq n$ なる任意の i, j について,

$$(1\ i)(1\ j)(1\ i) = (i\ j)$$

が成り立つから, G はすべての互換を含む. S_n の任意の元は互換の積で表すことができるから, $G = S_n$ を得る.

(2) G は $(i\ j), (2\ 3 \cdots n)$ を含むとしてよい. さらに G は長さ n の巡回置換 σ を含むが, $\sigma = (1 \cdots i \cdots)$ と書いたとき, $1, i$ の間隔が d であれば $\sigma^d(1) = i$ となる. いま, $\sigma^d(k) = j$ とすると, $k \neq 1$ かつ $\sigma^{-d}(i\ j)\sigma^d = (1\ k)$ であり, さらに

$$(2\ 3 \cdots n)(1\ k)(2\ 3 \cdots n)^{-1} = \begin{cases} (1\ k+1) & (k = 2, \dots, n-1), \\ (1\ 2) & (k = n) \end{cases}$$

と計算され, (1) に帰着する.

(3) G は $(i\ j), \sigma = (1\ 2 \cdots n)$ を含むとしてよい. このとき, $\sigma^{j-i}(i) = j$ が成り立つが, n は素数だから σ^{j-i} も長さ n の巡回置換であり, $\sigma^{j-i} = (i\ j \cdots)$ なる形に書かれる. これと $(i\ j)$ との積 $(i\ j)(i\ j \cdots) = (j \cdots)$ は長さ $n-1$ の巡回置換 (下線の部分が同じ) だから (2) に帰着する. □