

§15. 補遺

次の命題は、補題 8.5 の証明の最初の部分で使われている。

命題 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 に一致することを確かめればよい。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、 n は m の約数であることがわかる。そこで、 $c = a^{m/n}$ とおくと c の位数は n である。いま、ある $j \in \mathbf{Z}$ について $c = b^j$ だとすると、 j, n は互いに素となり（だって b, c はどっちも位数 n だもん）、したがって $b \in \langle c \rangle \subset \langle a \rangle$ となって b のとり方に矛盾する。とくに、 c は $1, b, b^2, \dots, b^{n-1}$ のどれとも異なる。さらに、これら $n+1$ 個の元

$$c, 1, b, b^2, \dots, b^{n-1} \in A \subset K^\times$$

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

次に、やり残してあった補題の証明を与える。

補題 8.9 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 定理 6.12 より、 $\delta \in \text{Conj}(\beta, K)$ に対して、 $\sigma(\beta) = \delta$ をみたす $\sigma \in \text{Aut}(\bar{K}/K)$ が存在する。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；

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

補題を示すためには、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。

(1) F の定義: $\delta \in \text{Conj}(\beta, K)$ に対して, $\sigma_\delta \in \text{Aut}(\overline{K}/K)$ が上のようにして定まり, $\gamma \in \text{Conj}(\alpha, K(\beta))$ ならば, $\sigma_\delta(\gamma) \in \text{Conj}(\gamma, K) = \text{Conj}(\alpha, K)$ 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 6.12 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 のみから定まることもわかる。ここで, 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, $\sigma_{\tau(\beta)}^{-1} \circ \tau \in \text{Aut}(\overline{K}/K(\beta))$ 。よって定理 6.12 から

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

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。 \square