体論 NO.13 練習問題

$\alpha = \sqrt[3]{11}, \omega = \dfrac{-1+\sqrt{-3}}{2}$ とおくとき、

(1) $X^3 - 11$ は $\mathbb{Q}$ 上既約だろうか?
(2) α の $\mathbb{Q}$ 上の共役をすべて求めなさい。
(3) $\mathbb{Q}(\alpha)$,$\mathbb{Q}(\omega)$ のそれぞれは $\mathbb{Q}$ のガロア拡大であるか、理由をつけて述べなさい。
(4) $\mathbb{Q}(\alpha, \omega)$ は $\mathbb{Q}$ 上のガロア拡大だろうか?
(5) $[\mathbb{Q}(\alpha, \omega) : \mathbb{Q}]$ を求めなさい。
(6) $\mathbb{Q}(\alpha + \omega) = \mathbb{Q}(\alpha, \omega)$ であることを示しなさい。

[解答]
(1) $f(X)$ は $\mathbb{Q}$ 上既約である。これを証明しよう。背理法で f が $\mathbb{Q}$ 可約だとする。 命題 5.1(ガウスの補題) により $\mathbb{Z}$ 上でも可約である。f は 3 次だから 1 次の $\mathbb{Z}$ 係数の因数を持つことになる。命題 5.4 により X^3-11 の因数はモニック。ゆえに、$f(a)=0$ なる整数 a が存在することになる。$\mathbb{Z}\ni x\mapsto x^3\in\mathbb{Z}$ は単調増加かつ、$0^3=0<11<27=3^3$ により、 $0<a<3$. つまり $a=1$ or 2 であるが、これらは $f(a)=0$ を満たさないから矛盾。
[別解] f が $\mathbb{Z}$ 上で可約ならば、$\mathbb{F}_7$ 上でも可約なはず。すなわち X^3-11 は $\mathbb{F}_7$ 上で根を持つことになる。ところが $\{a^3; a\in\mathbb{F}_7\}=\{0,1,-1\}\not\ni 11(=4)$ (in $\mathbb{F}_7$.) ゆえ、矛盾。
(2)

$$X^3-11=(X-\alpha)(X-\alpha\omega)(X-\alpha\omega^2)$$

かつ、X^3-11 は $\mathbb{Q}$ 上既約であるから、$\alpha,\alpha\omega,\alpha\omega^2$ が α の $\mathbb{Q}$ 上の共役である。
(3) $\mathbb{Q}(\alpha)\subset\mathbb{R}$ かつ $\alpha\omega\notin\mathbb{R}$ により、α の共役の一つ $\alpha\omega$ は $\mathbb{Q}(\alpha)$ に含まれない。ゆえに、$\mathbb{Q}(\alpha)$ は $\mathbb{Q}$ の正規拡大ではない。もちろん、ガロア拡大でもない。
ω の $\mathbb{Q}$ 上の最小多項式は $X^2+X+1=(X-\omega)(X-\omega^2)$ であるから、ω の $\mathbb{Q}$ 上の共役は ω,ω^2 の二つ。これらは $\mathbb{Q}(\omega)$ に含まれるから、$\mathbb{Q}(\omega)$ は $\mathbb{Q}$ 上の正規拡大である。$\omega\neq\omega^2$ だから ω は $\mathbb{Q}$ 上分離的でもある。ゆえに、 $\mathbb{Q}(\omega)$ は $\mathbb{Q}$ のガロア拡大である。
(4)
(3) と同様の考察により、$\mathbb{Q}(\alpha,\omega)$ は $\mathbb{Q}$ のガロア拡大であることがわかる。
(5)

$$[\mathbb{Q}(\alpha,\omega):\mathbb{Q}]=[\mathbb{Q}(\alpha,\omega):\mathbb{Q}(\alpha)][\mathbb{Q}(\alpha):\mathbb{Q}]=3[\mathbb{Q}(\alpha,\omega):\mathbb{Q}(\alpha)].$$

$\omega\in\mathbb{Q}(\alpha)$ か否かによって、 $[\mathbb{Q}(\alpha,\omega):\mathbb{Q}(\alpha)]$ は 2 か 1 かのいづれかである。他方、

$$[\mathbb{Q}(\alpha,\omega):\mathbb{Q}]=[\mathbb{Q}(\alpha,\omega):\mathbb{Q}(\omega)][\mathbb{Q}(\omega):\mathbb{Q}]=2[\mathbb{Q}(\alpha,\omega):\mathbb{Q}(\omega)].$$

ゆえ、$[\mathbb{Q}(\alpha,\omega):\mathbb{Q}]$ は 2 の倍数でなければならない。ゆえに、$[\mathbb{Q}(\alpha,\omega):\mathbb{Q}]=6$.
(もしくは: $\omega\notin\mathbb{R}$ かつ $\mathbb{Q}(\alpha)\subset\mathbb{R}$ ゆえ $\omega\notin\mathbb{Q}(\alpha)$. よって、$[\mathbb{Q}(\alpha,\omega):\mathbb{Q}(\alpha)]=2$. とやってもよい。)
(6) $L=\mathbb{Q}(\alpha,\omega)$ とおこう。 L の元は必ず

$$1,\alpha,\alpha^2,\omega,\alpha\omega,\alpha^2\omega \tag{B}$$

の線形結合で書けることがすぐに分かる。(5) により、これら 6 つの元は一次独立でなければならない。すなわち、これら 6 つの元は L の $\mathbb{Q}$ 上のベクトル空間としての基底である。$\mathrm{Gal}(L/\mathbb{Q})$ の元は α の行き先 ($\alpha,\alpha\omega,\alpha\omega^2$ の 3 とおり) と ω,ω^2 の行き先 (2 とおり) の都合 6 通りで定まる。(命題 9.4 により、これら 6 つの可能性はすべてガロア群の元として実現されねばならない。)
ガロア群の元 σ が $\alpha+\omega$ を動かさないとすると、

$$\sigma(\alpha)+\sigma(\omega)=\alpha+\omega.$$

ただし、

$$\sigma(\alpha)=\alpha \text{ or } \alpha\omega \text{ or } \alpha\omega^2.$$
$$\sigma(\omega)=\omega \text{ or } \omega^2.$$

(B) の 6 つの元が一次独立なことから、必然的に $\sigma(\alpha)=\alpha$ かつ $\sigma(\omega)=\omega$ がわかる。すなわち、$\sigma=\mathrm{id}$. よって、$M=\mathbb{Q}(\alpha+\omega)$ にガロア対応で対応する $\mathrm{Gal}(L/\mathbb{Q})$ の部分群 (M の固定群) は $\{\mathrm{id}\}$ で、これは $\mathbb{Q}(\alpha,\omega)$ の固定群と等しい。ガロア対応が全単射的であること (ガロア理論の基本定理) から、

$$\mathbb{Q}(\alpha+\omega)=\mathbb{Q}(\alpha,\omega).$$