

復習と補遺。

命題 14.1. 体 K の有限次拡大体 L および、 L と K の中間体 M が与えられたとき、つぎの等式が成り立つ。

$$[L : K] = [L : M][M : K]$$

補題 14.1 (既約性の判定法).

- (1) 整数係数の多項式 $f \in \mathbb{Z}[X]$ にたいして、 f が $\mathbb{Q}[X]$ 上可約ならば、 f は $\mathbb{Z}[X]$ 上可約である。(ガウス)
- (2) $f \in \mathbb{Z}[X]$ に有理数解 p/q (p, q は互いに素な整数) が存在するならば、 p は f の定数項の約数であり、 q は f の最高次の係数の約数である。
- (3) $f \in \mathbb{Z}[X]$ がモニックで、かつある素数 p にたいして

$$f(X) \equiv X^d \pmod{p}$$

がなりたつとする。このとき、もし f の定数項が p^2 で割り切れなければ f は既約である。(アイゼンシュタイン)

問題 12.1 有理数 a, b で、

$$\mathbb{Q}(a\sqrt{3} + b\sqrt{6}) = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{6})$$

とならないような a, b はどのようなものか。全て求めなさい。

問題 13.1 $L = \mathbb{Q}(\sqrt[4]{2}, \sqrt{-1})$, $K = \mathbb{Q}$ とおく。このとき L と K のあいだの中間体 M で、 K 上の拡大次数が 4 であるものを二つあげなさい。

問題 13.2 前問で、 $\text{Gal}(L/K)$ は可換群だろうか、理由をつけて述べなさい。

問題 13.3 前問で、 $\text{Gal}(L/K)$ の群の構造を理由をつけて述べなさい。