

今日のテーマ: ガロア対応

体 K のガロア拡大 L を考えると、 L は K 上のひとつの元だけで生成され(系 6.9), ガロア群 $\text{Gal}(L/K) = \text{Hom}_K(L, L)$ の元の個数は拡大次数 $[L : K]$ と一致するのです。(補題 7.2, 命題 7.3 の内容。命題 8.4 としてまとまっている。)

定義 9.1. 体 K とその拡大体 L が与えられたとき、 L の部分体 M で、 K を部分体として含むもののことを L と K のあいだの中間体と呼ぶ。

補題 9.2. 体 K の有限次ガロア拡大 L が与えられているとする。このとき、 K と L の中間体 M に対し、

- (1) L は M の有限次ガロア拡大でもある。
- (2) ガロア群 $H = \text{Gal}(L/M)$ は ガロア群 $G = \text{Gal}(L/K)$ の部分群とみなすことができる。

定義 9.3. 体 K の有限次ガロア拡大 L が与えられているとする。このとき、ガロア群 $G = \text{Gal}(L/K)$ の部分群 H に対して、

$$L^H = \{x \in L; \sigma(x) = x \quad (\forall \sigma \in H)\}$$

とおく。これは K と L の中間体であり、これを H の固定体(もしくは不変体)と呼ぶ。

補題 9.4. 体 K の有限次ガロア拡大 L が与えられているとする。このとき、ガロア群 $G = \text{Gal}(L/K)$ の部分群 H に対して、

- (1) $M = L^H$ は K と L の中間体である。
- (2) $|L : K| = |H|$.

定理 9.5. 体 K の有限次ガロア拡大体 L が与えられたとき、 $G = \text{Gal}(L/K)$ の部分群 H と、 K と L のあいだの中間体とは上の二つの補題にある対応で一対一に対応する。

系 9.6. 体 K と体 K の有限次ガロア拡大体 L が与えられたとき、 K と L のあいだの中間体は有限個しかない。

問題 9.1. $L = \mathbb{Q}(\sqrt{3} + \sqrt{5})$ と $K = \mathbb{Q}$ のあいだの中間体で、 L と K とも異なるものをひとつ挙げよ。理由も書くこと。

問題 9.2. 前問で、中間体をすべて挙げよ。