今日のテーマ:**ガロア拡大とガロア群**

前回に述べた系 7.11 は破壊力のある定理である。ただし、$K$ が無限この元をもたなければならないことが少し面倒な条件であった。じつは、有限個の元しかもたない体 (**有限体**と呼ばれる) は構造がよくわかっていて、その理論を用いて $K$ が有限体の場合を別途調べることにより、系 7.11 の仮定を除くことができる。この講義ではその部分は少し省略して、はじめから系 7.11 が有限の仮定無しでつかえることを承知して先に進むことにする。

**定理 8.1.** $K$ の有限次代数拡大体 $L = K(\alpha_1, \alpha_2, \ldots, \alpha_t)$ が $K$ 上ガロア拡大であるための必要十分条件は、生成元 $\alpha_1, \ldots, \alpha_t$ がすべて $K$ 上分離的であり、なおかつそれらの $K$ 上の共役がすべて $L$ 内に存在することである。

このとき $L$ は $K$ 上一つの元で生成される。($L$ は $K$ 上 **単純拡大** (**単拡大**もしくは**単生成**) という言い方もされる。)

**定義 8.2** (体の $K$ 同型, ガロア群)**.**

(1) 体 $K$ の有限次拡大 $L_1, L_2$ に対して、 $L_1$ から $L_2$ への $K$-同型とは、環は和、積および $K$ の元 を保つもののことをいう。つまり、写像 $\varphi : L_1 \to L_2$ が $K$-同型であるとは、次の条件を同時に満足するときにいう。
   (a) $\varphi$ は環の準同型である。
   (b) $\varphi|_K = \mathrm{id}_K$ .

(2) 体 $K$ の有限次ガロア拡大 $L$ に対して、
   $\mathrm{Hom}_K^{\mathrm{alg}}(L, L)$ は写像の合成について群をなす。この群を $L$ の $K$ 上の**ガロア群**とよび、
$$\mathrm{Gal}(L/K)$$
   で書き表す。

体の有限次ガロア拡大が与えられると、ガロア群がひとつ定まる。この群を詳しく調べることにより、体の拡大の様子が手に取るようにわかる。これがガロア理論の真骨頂である。

ガロア群を計算するときには、

(1) ガロア群の元になりそうなものをすべて挙げる。
(2) それらがガロア群の元になるか、それらで足りているかを元の数の勘定で確認する。

のステップで行うことが多い。その意味で次の命題は基本的である。

**命題 8.3.** 体 $K$ の有限次ガロア拡大 $L$ に対して、
$$|G| = [L : K]$$

**例 8.4.** $\mathbb{Q}(\sqrt{11})$ は $\mathbb{Q}$ 上のガロア拡大であって、そのガロア群の元は $\sqrt{11}$ の行き先 ($\sqrt{11}$ or $-\sqrt{11}$) で定まる。その結果、
$$\mathrm{Gal}(\mathbb{Q}(\sqrt{11}))/\mathbb{Q}) \cong C_2 \quad (2\text{ 次の巡回群})$$

**例 8.5.** $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ は $\mathbb{Q}$ 上のガロア拡大であって、そのガロア群の元は $\sqrt{2}$ と $\sqrt{3}$ の行き先 (それぞれ $\sqrt{2}$ or $-\sqrt{2}$ と $\sqrt{3}$ or $-\sqrt{3}$) で定まる。その結果、
$$\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3}))/\mathbb{Q}) \cong C_2 \times C_2 \quad (2\text{ つの }2\text{ 次の巡回群の直積。})$$

**問題 8.1.** $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ を求めよ。

**定義 8.6.** 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**中間体**と呼ぶ。

**補題 8.7.** 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 $H = \mathrm{Gal}(L/M)$ は ガロア群 $G = \mathrm{Gal}(L/K)$ の部分群とみなすことができる。