代数学 III 要約 NO.12

今日のテーマ

$\boxed{\text{ガロアの基本定理 (1)}}$

この講義では、体と言えば $\mathbb{Q}$ を含むものをさすことに注意しておく。

定理 12.1 (ガロアの基本定理). L が K のガロア拡大のとき、$G = \mathrm{Gal}(L/K)$ とおくと、

$$\mathcal{G} = \{\ G \text{ の部分群}\}$$

と

$$\mathcal{F} = \{\ L \text{ と } K \text{ の中間体}\}$$

のあいだには一対一対応がつく。その対応は、

$$\Phi(H) = L^H$$

$$\Psi(M) = \mathrm{Gal}(L/M)$$

で与えられる。

実際には、上の対応は更に詳しく分かっていて、一方がよい性質を持てば他方もそうなる、という具合なのであるが、まずは二つのものが対応するという上の定理が基本だろう。

系 12.1. L が K のガロア拡大ならば、 L と K のあいだの中間体は有限個しかない。

例 12.1. $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ と $\mathbb{Q}$ のあいだの中間体は
$\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$, $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, $\mathbb{Q}(\sqrt{2}, \sqrt{5})$, $\mathbb{Q}(\sqrt{3}, \sqrt{5})$, $\mathbb{Q}(\sqrt{2}, \sqrt{15})$, $\mathbb{Q}(\sqrt{3}, \sqrt{10})$, $\mathbb{Q}(\sqrt{5}, \sqrt{6})$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(\sqrt{5})$, $\mathbb{Q}(\sqrt{6})$, $\mathbb{Q}(\sqrt{15})$, $\mathbb{Q}(\sqrt{10})$, $\mathbb{Q}$ の 14 つである。

ガロアの基本定理は、体論の様々なことがらの見通しをよくする。

例 12.2. $\mathbb{Q}$ 上の $x = \sqrt{2} + \sqrt{3} + \sqrt{5}$ の最小多項式の次数は 8 であると予想できるが、その証明はいままで (半ば暗黙のうちに) 先伸ばしにして来た。実際 8 であることを確かめるのには、$[\mathbb{Q}(x) : \mathbb{Q}] = 8$ を言えばよい。それには $L = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ なる体を補助的に考えて、$[L : \mathbb{Q}] = 8$ および $\mathbb{Q}(x) = L$ の二つを言うことになる。前者は比較的容易である。そして、それを証明しておけば $\mathrm{Gal}(L/\mathbb{Q})$ の構造が ($C_2 \times C_2 \times C_2$ と同型である、生成元、実際の作用等) わかる。そして、x が、id を除くガロア群のどの元でも不変でないことから、$\mathbb{Q}(x)$ は L と一致することがわかる。これらのことはほとんど暗算でできるほど容易な計算で確かめられる。これが基本定理の威力である。

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。