有限体のガロア理論/ 1 の冪根

ここで、有限体の場合のガロア理論についてまとめておこう。
次のことは本講では言わずもがなであろう。

補題 12.1. 体 K 上の一変数 d 次多項式の根は d 個以下である。

代数学 II で学んだ有限生成アーベル群の基本定理から直ちに:

命題 12.2. 体 K に対して、$K^\times$ の有限部分軍は必ず巡回群である。

系 12.3. 有限体 K の元の個数が q であるとき、K の各元は $X^q - X$ の根である。$X^q - X$ の根の個数はたかだか q 個であるから、K は $X^q - X$ の最小分解体である。

命題 12.4. 有限体 K の元の個数が q であるとき、q はある素数 p の冪である。逆に、素数 p の冪 q に対して、元の個数が q であるような体が存在して、同型を覗いて一意的である。この体のことを $\mathbb{F}_q$ と書く。

命題 12.5. 素数 p を固定する。可換環 A において、 $p_A = 0_A$ であるとき、

$$A \ni x \mapsto x^p \in A$$

は環の準同型である。これを A のフロベニウス自己準同型写像と呼ぶ。

一般に体 K に対して、K に含まれる最小の部分体が存在する。(K の標数が 0 なら $\mathbb{Q}$, K の標数が p なら $\mathbb{F}_p$ である。) その体を**素体**と呼ぶ。

---

1 の冪根

1 の冪根は度々出てきた。標数 $p > 0$ の場合には 1 の冪根とはすなわち $\cup_n \mathbb{F}_{p^n}$ の元のことである。標数 0 場合には基本的には $\mathbb{C}$ の中で考えれば十分である。

定理 12.6. 正の整数 n に対して、$z^n = 1$ を満たす複素数 z はちょうど n 個存在する。それらは

$$\exp(\frac{2\pi k\sqrt{-1}}{n}) \qquad (k = 0, 1, 2, \ldots, n-1)$$

であり、これらを複素平面上で順に線分で結ぶと単位円に内接し、1 をひとつの頂点とする正 n 角形ができる。

命題 12.7. 一般に、体 K と正の整数 n に対して、

$$\{x \in K; x^n = 1\}$$

は乗法に関して群をなし、その位数は n 以下である。

定義 12.8. 体 K に対して、n 乗して初めて 1 になるような K の元を (K における)1 の**原始 n 乗根**と呼ぶ。

命題 12.9. $\mathbb{C}$ における 1 の原始 n 乗根を ζ_n と書くと、$\mathbb{Q}(\zeta_n)$ は $\mathbb{Q}$ のガロア拡大であり、ガロア群 $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ は $\mathbb{Z}/n\mathbb{Z}$ の乗法群 $(\mathbb{Z}/n\mathbb{Z})^\times$ と同型である。

ガロア群がアーベル群 (可換群) であるとき、アーベル拡大と呼ばれる。上の $\mathbb{Q}(\zeta_n)$ は $\mathbb{Q}$ のアーベル拡大の一例である。実はつぎの驚くべき定理が成り立つ。

定理 12.10 (クロネッカー・ウエーバー)**.** $\mathbb{Q}$ のアーベル拡大は必ずある円分体 $\mathbb{Q}(\zeta_n)$ の部分体である。

上記定理は**類体論**の成果の一つである。(というより、類体論により整理され、さらなる拡張の方向が探られた。) 類体論のおかげで、アーベル拡大 (とくに $\mathbb{Q}$ の有限次代数拡大 K のアーベル拡大) については、上記定理の他にもいろいろなことがわかっている。それでは、非アーベル拡大についてはどうかという疑問が当然生じるが、それについては現代でも活発に研究が行われているところである。