

1 のべき根

定理 12.1. 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

$$\exp\left(\frac{2\pi k\sqrt{-1}}{n}\right) \quad (k = 0, 1, 2, \dots, n-1)$$

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 12.2. 一般に、体 K と正の整数 n に対して、

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

は情報に関して群をなし、その位数は n 以下である。

定義 12.3. 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 12.4. \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 $\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ は $\mathbb{Z}/n\mathbb{Z}$ の乗法群 $(\mathbb{Z}/n\mathbb{Z})^\times$ と同型である。

命題 12.5. p が素数の時、 $(\mathbb{Z}/p\mathbb{Z})^\times$ は巡回群である。

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 12.6 (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。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く。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。