ガロア理論と正 n 角形の作図

July 16, 2016

定義 (体)

四則演算 $+, -, \times, \div$ で閉じた集合 K のことを体という．

例． $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ **は体．**

体 K, L について $K \subset L$ であるとき，L は K の拡大体であるという．
これを L/K が体の拡大であるという．

定義

L を K の拡大体，$\alpha \in L$ とする．K を含み α を持つ体のうち最小のものを K に α を添加した体といい，$K(\alpha)$ と書く．

例． $\mathbb{Q}$ **に** $\sqrt{2}$ **を添加した体は**

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} | a, b \in \mathbb{Q}\}$$

である．

ガロア理論とは

ざっくり言えば「体の拡大を群を使って調べる」という理論である

ガロア理論とは

- 2 次方程式，3 次方程式，4 次方程式には解の公式が存在する
- 3 次，4 次の公式は 15 世紀に見つけられた．
- 一方，5 次方程式は一般に解けないことがアーベルによって証明された (1824 年)
- ここで方程式が解けるとは四則演算とべき根のみによって解を表せるということ

- **ガロアは与えられた代数方程式が解けるかどうかの必要十分条件を与えた** (1832 **年**).
- **そこで使われた理論を整備したものがガロア理論である.**

体の拡大を調べる上でもっとも基本的であるのが，線形代数を使うこと

L/K が体の拡大であるとき，L を K 上のベクトル空間とみることができる．このとき $\dim_K L$ を L/K の拡大次数といい，$[L : K]$ と書く．

例．$\mathbb{Q}$ 上のベクトル空間 $\mathbb{Q}(\sqrt{2})$ の基底として $\{1, \sqrt{2}\}$ がとれる．よって

$$[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = \dim_{\mathbb{Q}} \mathbb{Q}(\sqrt{2}) = 2$$

命題 (拡大次数の積の法則)

L/M, M/K がともに有限次拡大のとき
L/K も有限次拡大で，

$$[L : K] = [L : M][M : K].$$

定義

L/K を体の拡大，$\alpha \in L$ とする．

$\alpha \in L$ が K 上代数的 $\overset{\text{def}}{\iff}$ ある K 係数多項式 $f(x)$ が存在して $f(\alpha) = 0$

L/K が代数拡大 $\overset{\text{def}}{\iff}$ すべての $\alpha \in L$ に対して α は K 上代数的．

定義

α が K 上代数的であるとき，K 係数多項式 $f(x)$ で $f(\alpha) = 0$ となるもののうち次数が最小なものを α の K 上の最小多項式という．

定理

α の K の最小多項式を $f(x)$ とするとき，

$$[K(\alpha) : K] = \deg f(x)$$

例．$\sqrt{2}$ の $\mathbb{Q}$ 上の最小多項式は $x^2 - 2$ で次数は 2．$[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]$ に一致．
$\sqrt[3]{2}$ の $\mathbb{Q}$ 上の最小多項式は $x^3 - 2$ で次数は 3．よって $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$．

定義 (共役)

α の K 上の最小多項式を $f(x)$ とする．
このとき $f(x)$ の根のことを α の K 上の共役という．

例.

- $\sqrt{2}$ の最小多項式 $x^2 - 2$ の根は $\sqrt{2}, -\sqrt{2}$. よって $\sqrt{2}$ の $\mathbb{Q}$ 上の共役は $\sqrt{2}$ と $-\sqrt{2}$.
- $\sqrt[3]{2}$ の最小多項式 $x^3 - 2$ の根は $\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2$. よって $\sqrt[3]{2}$ の $\mathbb{Q}$ 上の共役は $\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2$.

定義 (ガロア拡大)

代数拡大 L/K がガロア拡大 $\overset{\text{def}}{\iff}$ 任意の $\alpha \in L$ に対して α の K 上の共役はすべて L に属する.

本当は分離拡大という条件を考えないといけないがここでは正確さを犠牲にする

- $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ はガロア拡大
- $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ はガロア拡大ではない．実際 $\sqrt[3]{2}$ の共役 $\sqrt[3]{2}\omega$ が $\mathbb{Q}(\sqrt[3]{2})$ に入っていない．

定義 (ガロア群)

L から L への全単射 σ で次の条件をみたすもの全体を $\mathrm{Gal}(L/K)$ と書き，L/K のガロア群という．

1. $\forall a \in K, \sigma(a) = a$
2. $\forall a, b \in L, \sigma(a+b) = \sigma(a) + \sigma(b)$
3. $\forall a, b \in L, \sigma(ab) = \sigma(a)\sigma(b)$

命題

$\sigma \in \mathrm{Gal}(L/K), \alpha \in L$ を K 上代数的な元とする．このとき $\sigma(\alpha)$ は α の K 上の共役である

命題

$L = K(\alpha)$ のとき，$\mathrm{Gal}(L/K)$ の元は α の行き先だけで決まる．

例． $\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$ **の元は** $\sqrt{2}$ **の行き先だけで決まり，** $\sqrt{2}$ **の行き先は** $\sqrt{2}$ **か** $-\sqrt{2}$ **である．**

$$\sigma_1(\sqrt{2}) = \sqrt{2}$$
$$\sigma_2(\sqrt{2}) = -\sqrt{2}$$

となる $\sigma_1, \sigma_2 \in \mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$ **をとれば，**

$$\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \{\sigma_1, \sigma_2\}$$

である．

なお，このような σ_2 **がとれることは自明なことではない**

定理

L/K が有限次ガロア拡大ならば

$$|\mathrm{Gal}(L/K)| = [L : K]$$

なお上の等号 $=$ を $\leq$ にかえたものはガロア拡大でなくても成立する.

定義

L/K が体の拡大のとき $K \subset M \subset L$ である体 M を L/K の中間体という．

定理 (ガロアの基本定理)

L/K を有限次ガロア拡大とする．
このとき L/K の中間体全体と
$\mathrm{Gal}(L/K)$ の部分群全体には一対一対応
がつく．

その対応関係は中間体全体を $\mathbb{M}$，部分群全体を $\mathbb{H}$ とおくとき

$$\mathbb{M} \ni \boldsymbol{M} \mapsto \{\boldsymbol{g} \in \mathbf{Gal}(\boldsymbol{L}/\boldsymbol{K}) | \forall \boldsymbol{x} \in \boldsymbol{M}, \boldsymbol{g}(\boldsymbol{x}) = \boldsymbol{x}\} \in \mathbb{H}$$
$$\mathbb{H} \ni \boldsymbol{H} \mapsto \{\boldsymbol{x} \in \boldsymbol{L} | \forall \boldsymbol{g} \in \boldsymbol{H}, \boldsymbol{g}(\boldsymbol{x}) = \boldsymbol{x}\} \in \mathbb{M}$$

である．

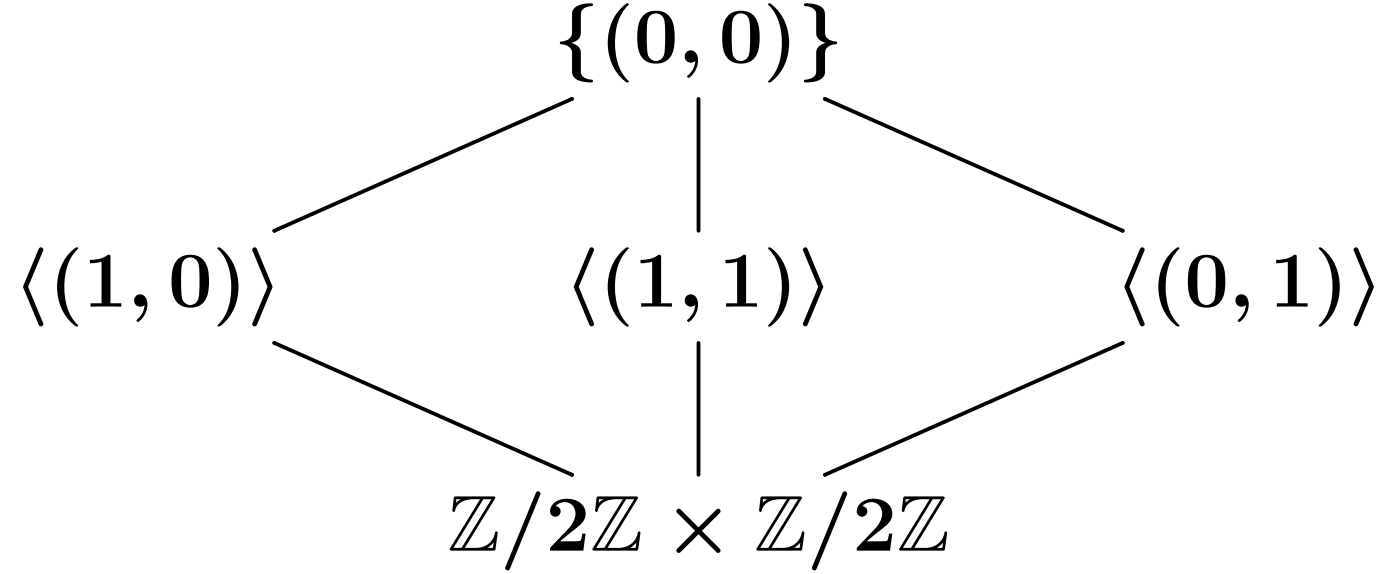
また，M, M' $(M \subset M')$ を中間体，対応する部分群を H, H' とするとき

$$[M' : M] = (H : H')$$

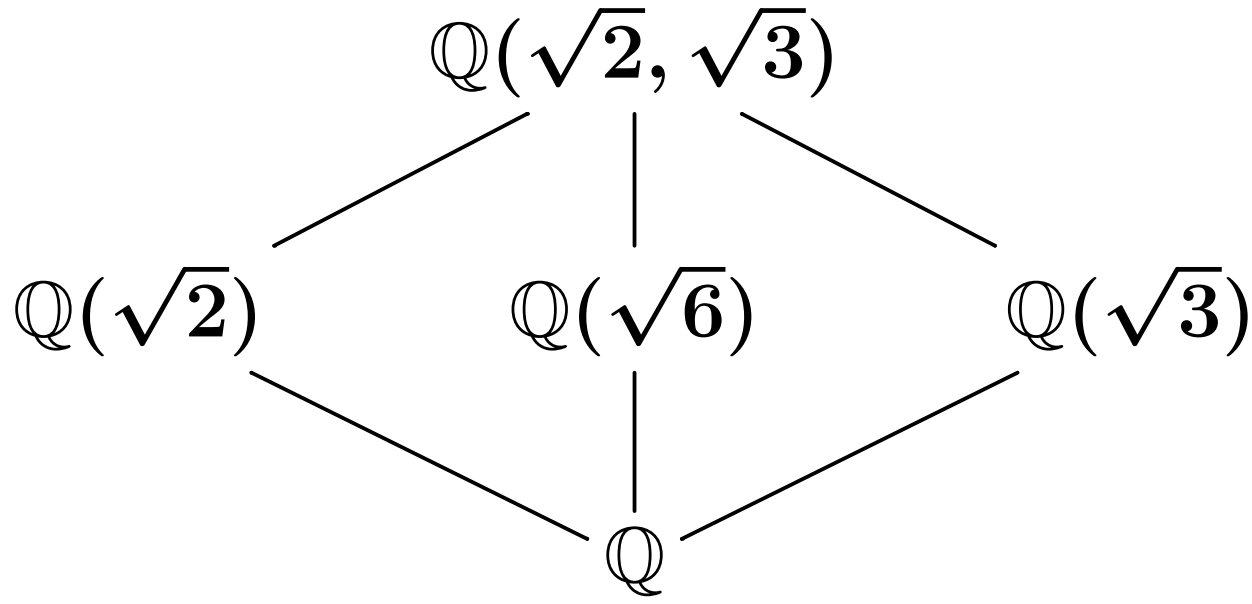
である．(つまり拡大次数と群の指数が一致する)

さらに M を中間体とし，対応する部分群を H とするとき，M/K がガロア拡大である必要十分条件は H が $\mathrm{Gal}(L/K)$ の正規部分群であることである．
そしてそのとき M/K のガロア群は $\mathrm{Gal}(L/K)/H$ に同型である．

例． $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ **とおく．**
$\mathrm{Gal}(L/\mathbb{Q})$ **は考察することにより**
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ **と同型であることがわかる．**
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ **の部分群のハッセ図は次のようになる．**



これと対応して $L/\mathbb{Q}$ の中間体は次のようになる．



このようにしてガロア群の構造を調べ，その部分群全体を求め，対応する中間体を求めることにより，中間体をすべて決定できる！

作図可能性

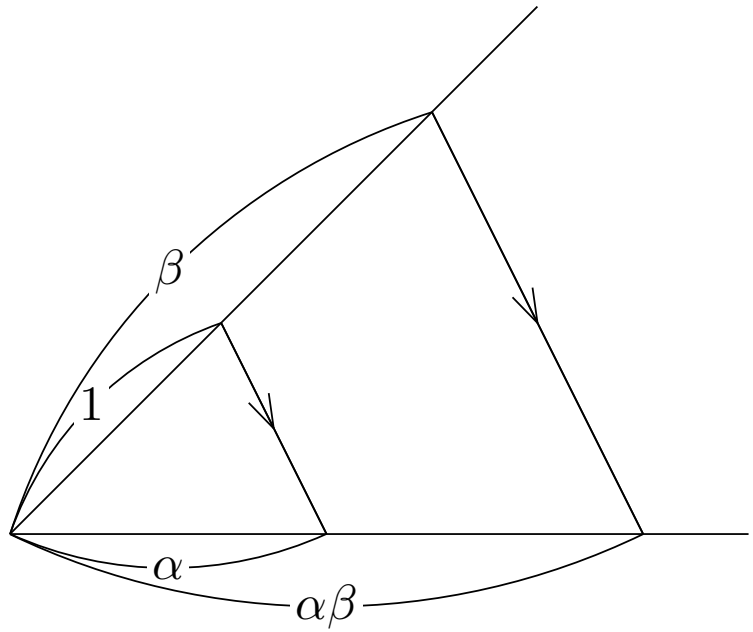
定規とコンパスだけを使って正 n 角形を作図したい．n がどんなとき可能だろう？

2 点 $(0,0),(1,0)$ から出発して次の操作 $(1),(2)$ を有限回行って得られる点を作図可能な点という．

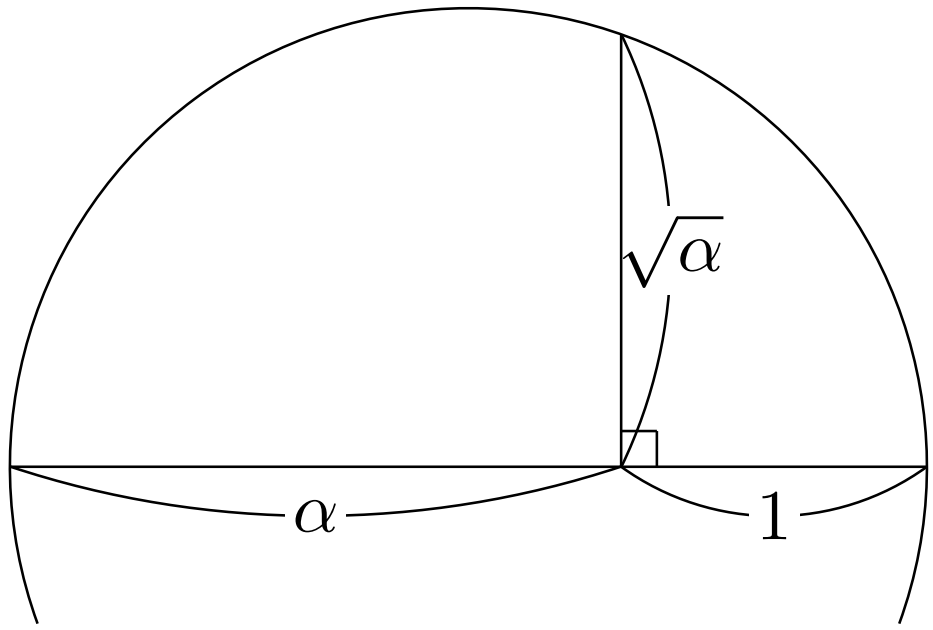
1. 与えられた 2 点を結ぶ直線を描く
2. 与えられた点を中心とし，与えられた長さを半径とする円を描く

作図可能な点の座標となる実数の集合を L と書く．

L は和，差，積，商で閉じていることが容易にわかる (よって L は体である)．
たとえば $\alpha, \beta \in L$ なら積 $\alpha\beta$ も L に入っていることは次の図からわかる．



また $\alpha \in L, \alpha > 0$ なら $\sqrt{\alpha}$ も L に属することが分かる．



また作図可能な点というのは直線と直線の交点，直線と円の交点，円と円の交点として現れる．
その座標は一次方程式，二次方程式の解であるので，結局，L は 0 と 1 から出発して和，差，積，商，平方根を有限回使って得られる実数全体となることがわかる．

これを体の言葉で言い直すと次のようになる．

定理

$\alpha \in \mathbb{R}$ とするとき，次の条件 *(1), (2)* は同値である．

1. $\alpha \in L$
2. 体の列 $K_0 = \mathbb{Q} \subset K_1 \subset K_2 \subset \cdots \subset K_n \subset \mathbb{R}$ で $i = 1, \ldots, n$ に対し $\beta_i \in K_{i-1}$ があり，$K_i = K_{i-1}(\sqrt{\beta_i})$ となるものが存在し，$\alpha \in K_n$ である．

もっと短く言うと，$\alpha \in L$ であるためには α が $\mathbb{Q}$ に 2 次拡大を積み上げた体に入っていることが必要十分である．

例． たとえば作図可能な数

$$\sqrt{2+\sqrt{3}}+\sqrt{5}$$

に対しては，次の体の列をとればよい．

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{3}) \subset \mathbb{Q}(\sqrt{3}, \sqrt{2+\sqrt{3}})$$
$$\subset \mathbb{Q}(\sqrt{3}, \sqrt{2+\sqrt{3}}, \sqrt{5})$$

例． 正五角形は作図可能である．

$$\cos\frac{2\pi}{5} = \frac{-1+\sqrt{5}}{4}$$

である．よって $\cos\frac{2\pi}{5}$ **は作図可能．**
$\sin\theta = \sqrt{1-\cos^2\theta}$ **により** $\sin\frac{2\pi}{5}$ **も作図可能．よって点** $(\cos\frac{2\pi}{5}, \sin\frac{2\pi}{5})$ **が作図可能なので正五角形は作図可能．**

$$\cos\frac{2\pi}{5} = \frac{-1+\sqrt{5}}{4}$$

の証明． $\zeta = \exp\frac{2\pi i}{5}$ **とおくと，**

$$\zeta^4 + \zeta^3 + \zeta^2 + \zeta + 1 = 0$$

である．

$$a = \zeta + \zeta^4, b = \zeta^2 + \zeta^3$$

とおくと，

$$a + b = -1, ab = -1.$$

よって a, b は 2 次方程式

$$x^2 + x - 1 = 0$$

の解．これを解くと

$$x = \frac{-1 \pm \sqrt{5}}{2}.$$

$a = \zeta + \zeta^4 = \zeta + \zeta^{-1} = \zeta + \bar{\zeta} =$
$2\mathrm{Re}\zeta = 2\cos\frac{2\pi}{5}$ なので $a > 0$. よって,

$$a = \frac{-1+\sqrt{5}}{2}.$$

したがって

$$\cos\frac{2\pi}{5} = \frac{-1+\sqrt{5}}{4}.$$

これから正 n 角形が作図可能であるための必要条件を考えよう．
$\zeta_n = \exp \frac{2\pi i}{n}$ とおく．
正 n 角形が作図可能だとすると $\mathbb{Q}$ から 2 次拡大を重ねて得られる体 K があり，
$\cos \frac{2\pi}{n} \in K$ である．
拡大次数の積の法則より，$[\mathbb{Q}(\cos \frac{2\pi}{n}) : \mathbb{Q}]$ は $[K : \mathbb{Q}]$ を割り切る．よって
$[\mathbb{Q}(\cos \frac{2\pi}{n}) : \mathbb{Q}]$ は 2 べきである．

ここで $[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\cos\frac{2\pi}{n})] = 2$ である.
よって拡大次数の積の法則より
$[\mathbb{Q}(\zeta_n) : \mathbb{Q}]$ も 2 べきである.

以上より，次の結果が得られた．

- 正 n 角形が作図可能 $\Rightarrow$ $[\mathbb{Q}(\zeta_n) : \mathbb{Q}]$ は 2 べきである

この結果を得るのにガロア理論は使っていない．この結果の逆が成立するのだが，その証明にガロア理論を使う．
しかし，逆を証明する前に $[\mathbb{Q}(\zeta_n) : \mathbb{Q}]$ は 2 べきであるという条件の必要十分条件を与えよう．

ζ_n の $\mathbb{Q}$ 上の最小多項式は次になることが知られている：

$$\Phi_n(x) = \prod_{\substack{1 \leq i \leq n \\ \gcd(i,n)=1}} (x - \zeta_n^i)$$

このことの証明は難しい．今は認めることにする．

例.

$$\begin{aligned}\Phi_4(x) &= (x-\zeta_4)(x-\zeta_4^3)\\ &= (x-i)(x+i) = x^2+1\end{aligned}$$

特に $\Phi_n(x)$ の次数は

$$\deg \Phi_n(x) = \phi(n)$$

である．ここに $\phi(n)$ はオイラーの ϕ 関数で，$1 \leq i \leq n$ で $\gcd(i, n) = 1$ をみたす i の個数を表す．

$\phi(n)$ は次の性質をみたす (証明略).

- m と n が互いに素ならば
  $\phi(mn) = \phi(m)\phi(n)$
- 素数 p と整数 $e \geq 1$ について
  $\phi(p^e) = (p-1)p^{e-1}$

では，$[\mathbb{Q}(\zeta_n) : \mathbb{Q}]$ は 2 べきであるという条件の必要十分条件を与えよう．ζ_n の $\mathbb{Q}$ 上の最小多項式が $\Phi_n(x)$ なので

$$[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \deg \Phi_n(x) = \phi(n).$$

よって $\phi(n)$ が 2 べきであることが必要十分．

$n = 2^{e_0} p_1^{e_1} \dots p_r^{e_r}$ と素因数分解するとき

$$\phi(n) = 2^{e_0 - 1} \prod_{i=1}^{r} (p_i - 1) p_i^{e_i - 1}$$

であるため，$\phi(n)$ が 2 べきであるためには，各 $i = 1, \dots, r$ について $e_i = 1$ かつ $p_i - 1$ が 2 べきであることが必要十分．

$p-1$ が 2 べきになる，つまり
$p=2^k+1$ と書ける奇素数には，フェルマー素数という名前がある．
よって，$[\mathbb{Q}(\zeta_n):\mathbb{Q}]$ は 2 べきであることは n を前スライドのように素因数分解するとき，すべての $i=1,\dots,r$ について $e_i=1$ かつ p_i がフェルマー素数であることが必要十分．

なお，フェルマー素数としては現在，次の 5 個が知られている：

$$3, 5, 17, 257, 65537.$$

これ以外にフェルマー素数が存在するかどうかは未解決問題である．

では次の結果：

- 正 n 角形が作図可能 $\Rightarrow$ $[\mathbb{Q}(\zeta_n) : \mathbb{Q}]$ は 2 べきである

の逆：

- $[\mathbb{Q}(\zeta_n) : \mathbb{Q}]$ は 2 べきである $\Rightarrow$ 正 n 角形が作図可能

を示そう．

$K = \mathbb{Q}(\zeta_n) \cap \mathbb{R}$ とおく．
このとき $\cos \frac{2\pi}{n} \in K$ である．
$[\mathbb{Q}(\zeta_n) : \mathbb{Q}]$ は 2 べきなので，拡大次数の積の法則から $[K : \mathbb{Q}]$ も 2 べきである．
また，$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ がアーベル群なので，ガロアの基本定理により，$K/\mathbb{Q}$ はガロア拡大で $\mathrm{Gal}(K/\mathbb{Q})$ は
$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ の剰余群である．
よって，$\mathrm{Gal}(K/\mathbb{Q})$ も位数 2 べきのアーベル群である．

よって有限アーベル群の基本定理により群の列

$$\mathrm{Gal}(K/\mathbb{Q}) = G_0 \supset G_1 \supset \cdots \supset G_r = \{1\}$$

であって，$|G_i/G_{i+1}| = 2$ であるものがある．$\mathrm{Gal}(K/\mathbb{Q})$ の部分群 G_i に対応する中間体を M_i とすると

$$\mathbb{Q} = M_0 \subset M_1 \subset \cdots \subset M_r = K$$

であって，$[M_{i+1} : M_i] = 2$ となる．

したがって，K は $\mathbb{Q}$ に 2 次拡大を積み上げた体である．
ゆえに $\cos \frac{2\pi}{n} \in K$ は作図可能．
よって正 n 角形は作図可能．

以上より次の定理が得られた：

定理

次の *(1), (2), (3)* は同値．

1. 正 n 角形が作図可能
2. $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$ は 2 べきである
3. $n = 2^{e_0} p_1^{e_1} \dots p_r^{e_r}$ と素因数分解するとき，すべての $i = 1, \dots, r$ について $e_i = 1$ かつ p_i がフェルマー素数である

この定理によれば $\cos \frac{2\pi}{17}$ は有理数から出発して四則演算と平方根を有限回使って書ける．実際それを書き下すとどうなるか．

こうなる：

$$\cos\frac{2\pi}{17} = \frac{-1+\sqrt{17}}{16} + \frac{1}{8}\sqrt{\frac{17-\sqrt{17}}{2}}$$
$$+\frac{1}{4}\sqrt{\frac{17+3\sqrt{17}}{4} - \frac{1}{2}\sqrt{\frac{17-\sqrt{17}}{2}} - \frac{17+\sqrt{17}}{2}}$$

参考文献

- 雪江明彦 (2010) 『代数学 2 環と体とガロア理論』 日本評論社