16. 1 の冪根・円分体・円分多項式

16–1. **1 の冪根.**

- $\zeta \in \overline{K}$: 1 **の** n **乗根 (**n**-th root of unity)** $\overset{\leftarrow}{\iff} \zeta^n = 1$
- $\zeta \in \overline{K}$: 1 **の原始** n **乗根 (primitive** n**-th root of unity)**
  $\overset{\leftarrow}{\iff} \zeta^n = 1$ かつ $(0 < \forall k < n : \zeta^k \neq 1) \iff (\zeta^m = 1 \iff n|m)$
- $\mathrm{ch}(K) \nmid n$ なら $\overline{K}$ 内に 1 の原始 n 乗根が存在
- $\mathrm{ch}(K) = p > 0$ の時は、$\overline{K}$ 内にも 1 の原始 p 乗根は存在**しない**
- $\zeta_n \in \overline{K}$: 1 の原始 n 乗根の一つとするとき、
  - $\mu_n = \mu_n(\overline{K}) := \{x \in \overline{K} \,|\, x^n = 1\}$: 1 の n 乗根全体は $\overline{K}^\times$ の部分群で、$\mu_n = \langle \zeta_n \rangle \simeq \boldsymbol{Z}/n\boldsymbol{Z}$
  - $\mu_n(K) := \mu_n \cap K^\times$ は μ_n の部分群
  - $\mu_n^* := \{\zeta_n^k \,|\, (k,n) = 1\}$: 1 の原始 n 乗根全体で、$\#\mu_n^* = \varphi(n)$
- $\boldsymbol{C}$ 内では $e^{\frac{2\pi i}{n}}$: 1 の原始 n 乗根の一つ
- $\boldsymbol{Q}(\zeta_n)$: 第 n **円分体 (cyclotomic field)**

16–2. **円分多項式.** $n \geq 1$ に対し、

- $\Phi_n(X) := \prod_{\zeta \in \mu_n^*} (X - \zeta) \in \boldsymbol{Z}[X]$: 第 n **円分多項式 (cyclotomic polynomial)**
- $\deg \Phi_n = \varphi(n) = \#(\boldsymbol{Z}/n\boldsymbol{Z})^\times, \quad X^n - 1 = \prod_{d|n} \Phi_d(X)$
- **定理**: $\Phi_n(X)$: $\boldsymbol{Z}$ 上既約 (従って $\boldsymbol{Q}$ 上でも既約)
- ζ_n : 1 の原始 n 乗根に対し、円分体 $\boldsymbol{Q}(\zeta_n)$ は $\boldsymbol{Q}$ 上 $\varphi(n)$ 次の正規拡大

16–3. **参考: Möbius の反転公式.** 正整数 $n \geq 1$ に対し、

- $\mu(n) := \begin{cases} 1 & (n = 1) \\ (-1)^k & (n \text{ が相異なる } k \text{ 個の素因子の積のとき}) \\ 0 & (n \text{ が平方因子を持つとき } (\exists p : p^2 | n)) \end{cases}$: **Möbius の** μ **関数**
- $\sum_{d|n} \mu(d) = \begin{cases} 1 & (n = 1) \\ 0 & (n > 1) \end{cases}$
- (Möbius の反転公式) $f, g : \boldsymbol{N} \to \boldsymbol{C}$ に対し、
  $$\left(\forall n \geq 1 : \sum_{d|n} f(\frac{n}{d}) = g(n) \right) \Rightarrow \left(\forall n \geq 1 : f(n) = \sum_{d|n} \mu(d) g(\frac{n}{d}) \right)$$
- $\Phi_n(X) = \prod_{d|n} (X^{\frac{n}{d}} - 1)^{\mu(d)}$

17. 多項式の既約性

R : 単項 ideal 整域 (PID)、$Q := \mathrm{Frac}(R)$: R の商体、$\pi \in R$: R の素元とする。
($R = \boldsymbol{Z}, Q = \boldsymbol{Q}, \pi = p$: 素数 を想定して良い。)

17–1. **Gauß の補題.** $f(X) = \sum_{i=0}^{n} a_i X^i \in R[X]$ に対し、

- f : **原始的 (primitive)** $\overset{\leftarrow}{\iff} (a_0, \ldots, a_n) = (1)$ (互いに素)
- $f, g \in R[X]$: 原始的 $\Rightarrow fg$: 原始的
- **定理**(Gauß の補題): $f \in R[X]$ が R 上既約 $\Rightarrow f$: Q 上でも ($Q[X]$ 内でも) 既約

17–2. **Eisenstein の既約性判定法.** $f(X) = \sum_{i=0}^{n} a_i X^i \in R[X]$: monic $(a_n = 1)$ に対し、

- $(0 \leq \forall i \leq n-1 : \pi | a_i)$ かつ $\pi^2 \nmid a_n \Rightarrow f$: $R[X]$ 内で (従って $Q[X]$ 内でも) 既約