- 円分拡大と巡回拡大（応用として，正 5 角形と正 17 角形の作図法）.
- PID 上有限生成加群の構造定理.

予想（ガロアの逆問題）：有限群 G について $\mathrm{Gal}(K/\mathbb{Q}) \cong G$ なるガロア拡大 $(\overline{\mathbb{Q}} \supsetneq) K/\mathbb{Q}$ が存在する.

定義：$n \geq 1$ とし，$\zeta_n = \exp(2\pi\sqrt{-1}/n)$ とする．以下を n 次の円分多項式という.

$$\Phi_n(x) = \prod_{0 \leq k < n, \gcd(n,k)=1} (x - \zeta_n^k).$$

事実：$\Phi_n(x)$ は $\mathbb{Z}[x]$ のモニック $\varphi(n)$ 次既約多項式.

系：任意の $n \geq 1$ について，$\mathbb{Q} \subseteq \mathbb{Q}(\zeta_n)$ はガロア拡大で,

$$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times, \quad (\sigma_x : \mathbb{Q}(\zeta_n) \to \mathbb{Q}(\zeta_n), \zeta_n \mapsto \zeta_n^x) \leftarrow\!\shortmid x.$$

注意：$\exists n \geq 1, \mathbb{Q} \subseteq K \subseteq \mathbb{Q}(\zeta_n)$ となる体 K を円体という．同値な条件として「$K/\mathbb{Q}$ が有限次ガロア拡大で $\mathrm{Gal}(K/\mathbb{Q})$ が可換群（i.e., アーベル拡大）」が知られている（Kronecker-Weber の定理）.

例：$\sqrt{5} = \zeta_5 - \zeta_5^2 - \zeta_5^3 + \zeta_5^4$.

注意：p が奇素数なら，$\sqrt{p} \in \mathbb{Q}(\zeta_p)$ は $W_p^2 = (-1)^{\frac{p-1}{2}} p$ から従う．これと $\sqrt{2} \in \mathbb{Q}(\zeta_8)$ より，$d \in \mathbb{Z}$ については確かに $\mathbb{Q}(\sqrt{d})$ は円体になっていることが分かる.

定理（Kummer 拡大）：$\mathbb{Q}(\zeta_n) \subseteq K \subseteq L \subseteq \overline{\mathbb{Q}}$ とする．L/K がガロア拡大で $\mathrm{Gal}(L/K) \cong C_n$ ならば $\exists a \in L, L = K(a)$ かつ $a^n \in K$.

証明：$\mathrm{Gal}(L/K) = \{\tau^0, \tau^1, \cdots, \tau^{n-1}\}$ とする．$\tau : L \xrightarrow{\sim} L$ を K 線形写像と思ったときの固有値の集合を R とする．$\tau^n = \mathrm{id}_L$ より $\forall r \in R, r^n = 1$ で（よって $R \subseteq K$），$\mathrm{ord}\,\tau = n$ より $0 < \exists k < n, \gcd(k,n) = 1, \zeta_n^k \in R$. R が $K^\times$ の部分群であることは簡単に確認できるので，$R = \{\zeta_n^k \mid 0 \leq k < n\}$ が分かった.

τ の ζ_n 固有ベクトル $a \in L \setminus \{0\}$ が目的のものであることを示す.

- $b := a^n$ について，$\tau(b) = \tau(a)^n = b$ なので $b \in L^{\mathrm{Gal}(L/K)} = K$.
- $\tau^i(a) = \zeta_n^i a$ なので $a, \tau(a), \cdots, \tau^{n-1}(a)$ はすべて異なる.

よって $\mathrm{Gal}(L/K(a)) = \{\tau^0\}$ なので $K(a) = L$（ここでガロア理論の基本定理を用いた）.

応用（フェルマー素数と作図可能性）：奇素数 $p \geq 3$ について，正 p 角形が作図可能 $\Leftrightarrow \exists k \geq 0, p = 2^{2^k} + 1$.

証明：まず $p = 2^n + 1$（$n \geq 1$）なら $n = 2^k$（$k \geq 0$）でなければならないことを注意する．また「正 p 角形が作図可能 $\Leftrightarrow \cos\dfrac{2\pi}{p} = \dfrac{1}{2}(\zeta_p + \zeta_p^{-1})$ が作図可能」も注意する.

$(\Rightarrow)$：$\mathbb{Q}(\zeta_p) \supsetneq \mathbb{Q}\left(\cos\dfrac{2\pi}{p}\right) \supseteq \mathbb{Q}$ を考えることにより，$\left[\mathbb{Q}\left(\cos\dfrac{2\pi}{p}\right) : \mathbb{Q}\right] = \dfrac{\varphi(p)}{2} = \dfrac{p-1}{2}$.

よって $\dfrac{p-1}{2} = 2^k$ でなければならない.

($\Leftarrow$):$\mathbb{Q}(\zeta_p) \supsetneq \mathbb{Q}\left(\cos\dfrac{2\pi}{p}\right) \supset \mathbb{Q}$ から $\mathbb{Q}\left(\cos\dfrac{2\pi}{p}\right)/\mathbb{Q}$ はガロア拡大で $\mathrm{Gal}\left(\mathbb{Q}\left(\cos\dfrac{2\pi}{p}\right)/\mathbb{Q}\right) \cong C_{2^{2^k-1}}$ が分かる．C_{2^n} には $G_0 = C_{2^n} \trianglerighteq G_1 \trianglerighteq G_2 \trianglerighteq \cdots \trianglerighteq G_n = \{e\}$ で $\forall i, [G_i : G_{i+1}] = 2$ となる正規部分群の列が取れるため，Kummer 拡大を繰り返し，各ステップで $\sqrt{\text{何とか}}$ を付加する拡大で $\mathbb{Q}$ から $\mathbb{Q}\left(\cos\dfrac{2\pi}{p}\right)$ に到達できる．

例（正 5 角形の作図法）：$G := \mathrm{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q} \cong (\mathbb{Z}/5\mathbb{Z})^\times (\cong C_4 = \mathbb{Z}/4\mathbb{Z})$ だが，2 が $(\mathbb{Z}/5\mathbb{Z})^\times$ の原始根であることより，G の生成元として

$$\tau : \mathbb{Q}(\zeta_5) \to \mathbb{Q}(\zeta_5), \quad \zeta_5 \mapsto \zeta_5^2$$

が取れる．$C_4 \trianglerighteq C_2 \trianglerighteq C_1$ を注意する（ここで $C_2 = \{[0],[2]\}, C_1 = \{[0]\}$）．ガロア理論の基本定理より $K := \mathbb{Q}(\zeta_5)^{C_2}$ は，$\mathbb{Q}$ のガロア拡大で，$\mathrm{Gal}(K/\mathbb{Q}) \cong C_4/C_2 \cong C_2$ となっている．

$\Phi_4(x) = x^4 + x^3 + x^2 + x + 1$ より

$$\mathbb{Q}[x]/\Phi_4(x) \cong \mathbb{Q}(\zeta_5) = \{A + B\zeta_5 + C\zeta_5^2 + D\zeta_5^3 \mid A, B, C, D \in \mathbb{Q}\}$$

だが，$\mathbb{Q}(\zeta_5) = \{p\zeta_5 + q\zeta_5^2 + r\zeta_5^3 + s\zeta_5^4 \mid p, q, r, s \in \mathbb{Q}\}$ でもある．

$\tau^2(p\zeta_5 + q\zeta_5^2 + r\zeta_5^3 + s\zeta_5^4) = p\zeta_5^4 + q\zeta_5^3 + r\zeta_5^2 + s\zeta_5$ より，$K = \{y(\zeta_5 + \zeta_5^4) + z(\zeta_5^2 + \zeta_5^3) \mid y, z \in \mathbb{Q}\}$ である．Kummer 拡大に関する定理の証明より，τ の -1 固有ベクトル $a \in K$ は $a^2 \in \mathbb{Q}$ で $K = \mathbb{Q}(a)$ となる（$C_4/C_2 = \{[0] + C_2, [1] + C_2\}$ に注意）．固有空間への射影を考えれば（参考：広義固有空間を用いた JNF の存在定理の証明），

$$a := \zeta_5 + \zeta_5^4 - \tau(\zeta_5 + \zeta_5^4) = \zeta_5 + \zeta_5^4 - (\zeta_5^2 + \zeta_5^3)$$

がそのような元の 1 つと分かる．以下より $K = \mathbb{Q}(\sqrt{5})$.

$$a^2 = \zeta_5^2 + \zeta_5^3 + \zeta_5^4 + \zeta_5 + 2(1 - \zeta_5^3 - \zeta_5^4 - \zeta_5 - \zeta_5^2 + 1) = -1 + 2 \cdot (2 - (-1)) = 5.$$

例（正 17 角形の作図法）：$G := \mathrm{Gal}(\mathbb{Q}(\zeta_{17})/\mathbb{Q} \cong (\mathbb{Z}/17\mathbb{Z})^\times (\cong C_{16} = \mathbb{Z}/16\mathbb{Z})$ だが，3 が $(\mathbb{Z}/17\mathbb{Z})^\times$ の原始根であることより，G の生成元として

$$\tau : \mathbb{Q}(\zeta_{17}) \to \mathbb{Q}(\zeta_{17}), \quad \zeta_{17} \mapsto \zeta_{17}^3$$

が取れる．$C_{16} \trianglerighteq C_8 \trianglerighteq C_4 \trianglerighteq C_2 \trianglerighteq C_1$ を注意する．ここで

$$C_8 = \{[0],[2],[4],[8],[10],[12],[14]\}, \quad C_4 = \{[0],[4],[8],[12]\}, \quad C_2 = \{[0],[8]\}, \quad C_1 = \{[0]\}.$$

ガロア理論の基本定理より $K_1 := \mathbb{Q}(\zeta_{17})^{C_8}, K_2 := \mathbb{Q}(\zeta_{17})^{C_4}, K_3 := \mathbb{Q}(\zeta_{17})^{C_2}$ について，

$$\mathbb{Q} =: K_0 \subsetneq K_1 \subsetneq K_2 \subsetneq K_3 \subsetneq K_4 := \mathbb{Q}(\zeta_{17})$$

であり，K_i/K_{i-1} は $\mathrm{Gal}(K_i/K_{i-1}) \cong C_2$ となる Kummer 拡大になっている．

Step 1：まず K_1 の生成元を求めよう．$b \in \mathbb{Q}(\zeta_{17}) = \{A_1\zeta_{17} + \cdots + A_{16}\zeta_{17}^{16} \mid A_i \in \mathbb{Q}\}$ について，$b \in K_1 \Leftrightarrow b = \tau^2(b)$ を計算すると

$$S = \zeta_{17} + \zeta_{17}^9 + \zeta_{17}^{13} + \zeta_{17}^{15} + \zeta_{17}^{16} + \zeta_{17}^8 + \zeta_{17}^4 + \zeta_{17}^2,$$
$$T = \zeta_{17}^3 + \zeta_{17}^{10} + \zeta_{17}^5 + \zeta_{17}^{11} + \zeta_{17}^{14} + \zeta_{17}^7 + \zeta_{17}^{12} + \zeta_{17}^6$$

について，$K_1 = \{pS + qT \mid p, q \in \mathbb{Q}\}$ だが，$\mathrm{Gal}(K_1/\mathbb{Q}) \cong C_{16}/C_8 = \{[0] + C_8, [1] + C_8\}$ かつ $\tau(S) = T$ なので，$(S-T)^2 \in \mathbb{Q}$ かつ $\mathbb{Q}(S-T) = K_1$ である．$(S-T)^2 = 17$ が分かるので，$K_1 = \mathbb{Q}(\sqrt{17})$. なお $S + T = -1$ より $S = \frac{-1 \pm \sqrt{17}}{2}, T = \frac{-1 \mp \sqrt{17}}{2}$.

Step 2：K_2 の K_1 上の生成元を求めよう．$b \in \mathbb{Q}(\zeta_{17}) = \{A_1\zeta_{17} + \cdots + A_{16}\zeta_{17}^{16} \mid A_i \in \mathbb{Q}\}$ について，$b \in K_2 \Leftrightarrow b = \tau^4(b)$ を計算すると

$$U = \zeta_{17} + \zeta_{17}^{13} + \zeta_{17}^{16} + \zeta_{17}^{4}, \quad V = \zeta_{17}^{9} + \zeta_{17}^{15} + \zeta_{17}^{8} + \zeta_{17}^{2},$$
$$W = \zeta_{17}^{3} + \zeta_{17}^{5} + \zeta_{17}^{14} + \zeta_{17}^{12}, \quad X = \zeta_{17}^{10} + \zeta_{17}^{11} + \zeta_{17}^{7} + \zeta_{17}^{6}$$

について，$K_2 = \{rU + sV + tW + uX \mid r, s, t, u \in \mathbb{Q}\}$ だが，$\mathrm{Gal}(K_2/K_1) \cong C_8/C_4 = \{[0] + C_4, [2] + C_4\}$ かつ $\tau^2(U) = V$ なので，$(U-V)^2 \in K_1$ かつ $K_1(U-V) = K_2$ である．$(U-V)^2 = -9S - 8T = 8 - S = \frac{17 \mp \sqrt{17}}{2}$ が分かるので，$K_2 = \mathbb{Q}(\sqrt{17})(\sqrt{34 \mp 2\sqrt{17}})$.

なお $(W-X)^2 = -8S - 9T = S + 9 = \frac{17 \pm \sqrt{17}}{2}, W + X = T = \frac{-1 \mp \sqrt{17}}{2}$. ただし $(U-V)(W-X) = 2S - 2T = \pm 2\sqrt{17}$ より，$U - V = \pm\sqrt{\frac{17 \mp \sqrt{17}}{2}}, W - X = 2\sqrt{17}\sqrt{\frac{2}{17 \mp \sqrt{17}}}$.

Step 3：K_3 の K_2 上の生成元を求めよう．$b \in \mathbb{Q}(\zeta_{17}) = \{A_1\zeta_{17} + \cdots + A_{16}\zeta_{17}^{16} \mid A_i \in \mathbb{Q}\}$ について，$b \in K_3 \Leftrightarrow b = \tau^8(b)$ を計算すると

$$\alpha = \zeta_{17} + \zeta_{17}^{16}, \quad \beta = \zeta_{17}^{13} + \zeta_{17}^{4}, \quad \gamma = \zeta_{17}^{9} + \zeta_{17}^{8}, \quad \delta = \zeta_{17}^{15} + \zeta_{17}^{2},$$
$$\varepsilon = \zeta_{17}^{3} + \zeta_{17}^{14}, \quad \lambda = \zeta_{17}^{5} + \zeta_{17}^{12}, \quad \mu = \zeta_{17}^{10} + +\zeta_{17}^{7}, \quad \nu = \zeta_{17}^{11} + +\zeta_{17}^{6}$$

について，$K_3 = \{i_1\alpha + \cdots + i_8\nu \mid i_1, \cdots, i_8 \in \mathbb{Q}\}$ だが，$\mathrm{Gal}(K_3/K_2) \cong C_4/C_2 = \{[0] + C_2, [4] + C_2\}$ かつ $\tau^4(\alpha) = \beta$ なので，$(\alpha - \beta)^2 \in K_2$ かつ $K_2(\alpha - \beta) = K_3$ である．$(\alpha - \beta)^2 = -4U - 3V - 6W - 4X = -3(U+V) - U - 4(W+X) - 2W = -3(S+T) - T - U - 2W$ が分かり，これは

$$3 + \frac{1 \pm \sqrt{17}}{2} - \frac{1}{4}((-1 \pm \sqrt{17}) \pm \sqrt{34 \mp 2\sqrt{17}}) - (2\sqrt{17}\sqrt{\frac{2}{17 \mp \sqrt{17}}} + \frac{-1 \mp \sqrt{17}}{2})$$
$$= \frac{17}{4} \mp \frac{1}{4}\sqrt{17} - 4\frac{\sqrt{17}}{\sqrt{34 \mp 2\sqrt{17}}} \mp \frac{\sqrt{34 \mp 2\sqrt{17}}}{4}.$$

なので $K_3 = \mathbb{Q}(\sqrt{17})(\sqrt{34 \pm 2\sqrt{17}})(\sqrt{\frac{17}{4} \mp \frac{1}{4}\sqrt{17} - 4\frac{\sqrt{17}}{\sqrt{34 \mp 2\sqrt{17}}} \mp \frac{\sqrt{34 \mp 2\sqrt{17}}}{4}})$（注：計算に誤りがあるかもしれません）．

ジョルダン標準形の存在証明（付録）：ここでは線形代数の先にある代数学の知識も認めると，どんな感じで証明できるのか雰囲気をみてみよう．以下を仮定する．

$(*)$　体 $\mathbb{F}$ 成分の $n \times n$ 行列 A は固有多項式 $\det(xE_n - A)$ が $\mathbb{F}[x]$ で 1 次式に分解している．

Step 1：$V = \mathbb{F}^n$ は $x\boldsymbol{v} = A\boldsymbol{v}$ とすることで $\mathbb{F}[x]$ 加群になる．$(n =) \dim_{\mathbb{F}} V < \infty$ なので，V は有限生成 $\mathbb{F}[x]$ 加群だが，$\mathbb{F}[x]$ はネーター環なので，V は有限表示 $\mathbb{F}[x]$ 加群である．よって適当な

$\mathbb{F}[x]$ 成分 $a \times b$ 行列 M が存在して，以下の $\mathbb{F}[x]$ 加群同型が成り立つ

$$V \cong \mathrm{Coker}(M) := \mathrm{Coker}(\mathbb{F}[x]^b \to \mathbb{F}[x]^a, \boldsymbol{f} \mapsto M\boldsymbol{f}).$$

Step 2：$\mathbb{F}[x]$ は PID（単項イデアル整域）なので，スミス標準形（単因子標準形）がとれる．

$$PMQ = D = \begin{pmatrix} f_1(x) & & & O \\ & \ddots & & \\ & & f_r(x) & \\ O & & & O \end{pmatrix}$$

ここで P, Q は $\det P, \det Q \in \mathbb{F} \setminus \{0\}$ となる $\mathbb{F}[x]$ 成分の $a \times a, b \times b$ 行列である（これは $\exists R \in M_a(\mathbb{F}[x]), PR = RP = E_a, \exists S \in M_b(\mathbb{F}[x]), QS = SQ = E_b$ と同値である．このような P, Q はユニモジュラー行列ともよばれる）．$f_1, \cdots, f_r$ は「最高次の係数が 1 の多項式で $f_i(x)$ は $f_{i+1}(x)$ を割り切る（$1 \leq i < r$）」という条件で M から一意的に定まる．

Step 3：$f(x) = x^m + a_1 x^{m-1} + \cdots + a_m \in \mathbb{F}[x]$ について，行列 $C(f(x)) \in M_m(\mathbb{F})$ を

$$C(f(x)) = \begin{pmatrix} 0 & & O & -a_m \\ 1 & \ddots & & \vdots \\ & \ddots & 0 & -a_2 \\ O & & 1 & -a_1 \end{pmatrix}$$

と定義する（$m \geq 2$ のとき．$m = 1$ のときは $C(f(x)) = (-a_1)$ であり，$m = 0 \Leftrightarrow f(x) = 1$ のときは $C(f(x))$ は 0×0 行列と思う）．$\det(xE_m - C(f(x))) = f(x)$ となることは難しくない．$C(f(x))$ は $f(x)$ のフロベニウス同伴行列とよばれる．

Step 4：$\mathrm{Coker}(M) \cong \mathrm{Coker}(D) \cong \bigoplus_{i=1}^r \mathbb{F}[x]/\langle f_i(x)\rangle \bigoplus \mathbb{F}[x]^{\oplus(a-r)}$ だが，$\dim_{\mathbb{F}} V < \infty$ より $a = r$．よって $\mathbb{F}[x]$ 加群として $V \cong \bigoplus_{i=1}^r \mathbb{F}[x]/\langle f_i(x)\rangle$ なので，ある $R \in GL_n(\mathbb{F})$ が存在して

$$R^{-1}AR = \bigoplus_{i=1}^{r} C(f_i(x))$$

となる．両辺の固有多項式をとると，仮定 $(*)$ と $\mathbb{F}[x]$ が UFD（一意分解整域）であることより，各 $f_i(x)$ も実は $\mathbb{F}[x]$ 中で 1 次式の積に分解されていることがわかる．以上より $f(x) = (\lambda - \gamma_1)^{\delta_1} \cdots (\lambda - \gamma_u)^{\delta_u}$ の形（ここで $u \geq 0, \delta_j \geq 1, 1 \leq j \neq k \leq u \Rightarrow \gamma_j \neq \gamma_k$）について $\mathbb{F}[x]/\langle f(x)\rangle$ を考察すればよい．さらに CRT（中国剰余定理）を適用すると

$$\mathbb{F}[x]/\langle f(x)\rangle \cong \bigoplus_{j=1}^{u} \mathbb{F}[x]/\langle (\lambda - \gamma_j)^{\delta_j}\rangle$$

なので，$f(x) = (x - \alpha)^m$ の場合に帰着される

Step 5：$W := \mathbb{F}[x]/\langle f(x)\rangle = \mathbb{F}[x]/\langle (x-\alpha)^m\rangle$ は，基底

$$\{(x-\alpha)^k + \langle (x-\alpha)^m\rangle \mid 0 \leq k < m\}$$

をもつが，これについての $x-\alpha$ の行列表示は $J(0;m)$ である．よってこの基底に関する x の行列表示は $J(\alpha;m)$ となる．以上より x の行列表示がジョルダン細胞の直和になるような V の基底が存在する

注：Step 2 は既習のランク標準形の一般化になっている．ランク標準形とは

$$\forall M\colon \mathbb{F} \text{ 成分 } a\times b \text{ 行列}, 0\leq \exists r\leq \min(a,b), \exists P\in GL_a(\mathbb{F}), \exists Q\in GL_b(\mathbb{F}), PMQ=\begin{pmatrix} E_r & O \\ O & O \end{pmatrix}.$$

だった．Step 2 については行・列基本変形とユークリッドの互除法の組合せで，P,Q を具体的に求めるアルゴリズムが存在する（ランク標準形は行・列基本変形のみで P,Q が求まるのでした）．

注：以上で $\mathbb{F}[x]$ を $\mathbb{Z}$ に置き換えると，有限生成アーベル群（$=\mathbb{Z}$ 加群）の構造定理（の一意性を除いた部分）がえられる（Step 1,2 のみで十分）．