- 有限体の応用．
- 1 のべき根について（平方剰余の相互法則）．
- クンマー拡大とその応用．

命題：p が素数で $n \geq 1$ とする．体 $\mathbb{F}, \mathbb{F}'$ が $|\mathbb{F}| = |\mathbb{F}'| = p^n$ ならば $\mathbb{F} \cong \mathbb{F}'$.

証明：$\mathbb{F}^\times \cong C_{p^n-1}$ だったことを思い出す（有限アーベル群の構造定理を仮定して証明した）．よって $\forall x \in \mathbb{F}^\times, x^{p^n-1} = 1$ なので $\forall x \in \mathbb{F}^\times, x^{p^n} = x$. $\mathbb{F}^\times$ の原始根 x_0 を選び，$f(x) = \mathrm{Irr}(\mathbb{F}_p; x_0)$ とする．$f(x) | x^{p^n} - x$ である．$\mathbb{F} = \mathbb{F}_p[x_0] \cong \mathbb{F}_p[x]/(f(x))$ で，$\forall y \in \mathbb{F}', y^{p^n} - y = 0$ でもあるので，$\exists y_0 \in \mathbb{F}', f(y_0) = 0$. $\mathbb{F}' \supseteq \mathbb{F}_p[y_0] \cong \mathbb{F}_p[x]/(f(x))$ なので，$\mathbb{F}' = \mathbb{F}_p[y_0] \cong \mathbb{F}_p[x]/(f(x)) \cong \mathbb{F}$.

記法：位数 p^n の有限体を $\mathbb{F}_{p^n}$ とか $\mathrm{GF}(p, n)$ のように書く．これは同型を除いて一意的だが，上の命題で自然な同型を選ぶことはできない（と思う）．

応用（フィボナッチ数列の周期）：$a_0 = 0, a_1 = 1, a_{n+2} = a_n + a_{n+1}$（$n \geq 2$）で定まる数列 $(a_n)_{n \geq 0}$ を（この講義では）フィボナッチ数列という．一般項の公式

$$a_n = \frac{1}{\sqrt{5}} \left(\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right)$$

は，素数 $p \neq 2, 5$ について $\mathbb{F}_p$ または $\mathbb{F}_{p^2}$ で意味を持つ．

事実：素数 $p \neq 2, 5$ について，$x^2 - 5$ が $\mathbb{F}_p[x]$ で既約 $\Leftrightarrow p \equiv \pm 2 \pmod 5$.

証明：平方剰余の相互法則（後述）から従う．

系：素数 p について

(1) $p \equiv \pm 1 \pmod 5$ ならば $\forall n \geq 0, a_{n+p-1} = a_n$.
(2) $p \equiv \pm 2 \pmod 5$ ならば $\forall n \geq 0, a_{n+p^2-1} = a_n$.

補題：体 $\mathbb{F}$ の標数が素数 p のとき，$\sigma_{\mathbb{F}} : \mathbb{F} \to \mathbb{F}, x \mapsto x^p$ は準同型（フロベニウス射）．

証明：$\sigma_{\mathbb{F}}(a+b) = \sigma_{\mathbb{F}}(a) + \sigma_{\mathbb{F}}(b)$ のみ非自明で，これは $0 < \forall i < p, \binom{p}{i} \in p\mathbb{Z}$ から従う．

定義：拡大 $\mathbb{F} \subseteq \mathbb{F}'$ について，

$$\mathrm{Gal}(\mathbb{F}'/\mathbb{F}) := \{ f : \mathbb{F}' \xrightarrow{\sim} \mathbb{F}' \mid f|_{\mathbb{F}} = \mathrm{id}_{\mathbb{F}} \}$$

は群（ここで / は慣習的に使われるもので，商とは関係がない）．

定理：素数 $p \geq 2$ と $n \geq 1$ について，$\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \cong C_n, \sigma_{\mathbb{F}_{p^n}}^x \mapsto x$（群同型）．

証明：$\sigma_{\mathbb{F}_{p^n}}$ は単射なので全単射（つまり $\sigma_{\mathbb{F}_{p^n}} \in \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$）．また $\mathbb{F}_{p^n}^\times \cong C_{p^n-1}$ だったから，$\sigma_{\mathbb{F}_{p^n}}$ の位数は n である．よって $|\mathrm{Gal}| \geq n$. さらに $\mathbb{F}_p[x]/(f(x)) \cong \mathbb{F}_{p^n} = \mathbb{F}_p(\theta)$ とすると，$\tau \in \mathrm{Gal}$ について $f(\tau(\theta)) = 0$ かつ $\tau \neq \tau'$ ならば $\tau(\theta) \neq \tau'(\theta)$ なので $|\mathrm{Gal}| \leq n$.

記法：拡大 $\mathbb{F} \subseteq \mathbb{F}'$ と部分群 $G \subseteq \mathrm{Gal}(\mathbb{F}'/\mathbb{F})$ について

$$\mathbb{F}'^G := \{x \in \mathbb{F}' \mid \forall \tau \in G, \tau(x) = x\}.$$

定義：有限次拡大 $\mathbb{F} \subseteq \mathbb{F}'$ がガロア拡大 $\Leftrightarrow \mathbb{F}'^{\mathrm{Gal}(\mathbb{F}'/\mathbb{F})} = \mathbb{F}$.

系：素数 $p \geq 2$ と $n \geq 1$ について，拡大 $\mathbb{F}_p \subseteq \mathbb{F}_{p^n}$ はガロア拡大.

注意：ガロア理論の基本定理とは，ガロア拡大 $\mathbb{F} \subseteq \mathbb{F}'$ について，中間体 $\mathbb{F} \subseteq M \subseteq \mathbb{F}'$ と $\mathrm{Gal}(\mathbb{F}'/\mathbb{F})$ の部分群とを 1 対 1 対応つけるものである.

応用（フィボナッチ数列の周期の精密化）：素数 $p \equiv \pm 2 \pmod 5$ について，$\forall n \geq 0, a_{n+2(p+1)} = a_n$.

証明：このとき $\mathbb{F}_{p^2} \cong \mathbb{F}_p[x]/(x^2 - x - 1)$ で $\sigma_{\mathbb{F}_{p^2}}$ は $x^2 - x - 1 = 0$ の解を入れかえる．つまり解を $\alpha, \beta \in \mathbb{F}_{p^2}$ とすると，$\alpha^p = \beta, \beta^p = \alpha$ なので $\alpha^{p+1} = \beta^{p+1} = -1$.

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.

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

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

証明：$f(x) = \mathrm{Irr}(\mathbb{Q}; \zeta_n)$ とする．任意の素数 $p \not| n$ について $f(\zeta_n^p) = 0$ を言えばよい．今

$$\Delta = \prod_{0 \leq i < j < n} (\zeta_n^i - \zeta_n^j)$$

について，$\Delta^2 = \pm n^n$ は初等的である．$\mathbb{Q}[x]$ で $f(x) | x^n - 1$ より，$f(x) \in \mathbb{Z}[x]$ が分かる（ガウスの補題．まだ証明していない）．$f(x^p) \equiv f(x)^p \pmod p$ より $f(\zeta_n^p) \in p\overline{\mathbb{Z}}$．これより $\exists x \in \overline{\mathbb{Z}}, px = \pm n^n$．よって $x \in \overline{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}$ で矛盾が生じた.

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，

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

定理（Wedderburn）：有限斜体 D は可換（つまり体）である.

証明：$Z = \{x \in D \mid \forall a \in D, ax = xa\}$ は D の部分体なので，適当な素数 p と $m \geq 1$ について $Z = \mathbb{F}_{p^m}$ とする．$\dim_Z D = n$（注：左次元）が $n > 1$ として矛盾を導く.

$a \in D \setminus Z$ について，$C(a) := \{x \in D \mid xa = ax\} (\supsetneq Z)$ は D の真の部分斜体なので，$\dim_Z C(a) =: d_a$ について $1 < d_a < n$．また連鎖律より $d_a | n$．群 $D^\times$ の類等式

$$q^n - 1 = q - 1 + \sum_a \frac{q^n - 1}{q^{d_a} - 1}$$

から（ここで $q = p^m$）$\Phi_n(q) | q - 1$ が導かれるが，これは矛盾.

定義（ルジャンドル記号）：奇素数 $p \geq 3$ と $n \in \mathbb{F}_p^\times$ について

$$\left(\frac{n}{p}\right) = \begin{cases} 1 & \exists x \in \mathbb{F}_p^\times, x^2 = n \\ -1 & o.w. \end{cases}$$

補題（オイラー基準）：$\left(\dfrac{n}{p}\right) = n^{\frac{p-1}{2}}$ （$\mathbb{F}_p^\times$ 中の等式）

定義（ガウス和）：奇素数 $p \geq 3$ について，$W_p = \displaystyle\sum_{x \in \mathbb{F}_p^\times} \left(\frac{x}{p}\right) \zeta_p^x$.

定理：$W_p^2 = (-1)^{\frac{p-1}{2}} p$.

証明:$W_p^2 = \displaystyle\sum_{x,y \in \mathbb{F}_p^\times} \left(\frac{xy}{p}\right) \zeta_p^{x+y} = \sum_{x,y \neq 0} \left(\frac{x^2 y}{p}\right) \zeta_p^{x+xy} = \sum_{x \neq 0} \left(\frac{-1}{p}\right) \zeta_p^0 + \sum_{y \neq 0,-1} \left(\frac{y}{p}\right) \sum_{x \neq 0} \zeta_p^{x(y+1)} = \left(\frac{-1}{p}\right) p$.

系（平方剰余の相互法則）：奇素数 $p \neq \ell$ について $\left(\dfrac{\ell}{p}\right)\left(\dfrac{p}{\ell}\right) = (-1)^{\frac{p-1}{2}\frac{\ell-1}{2}}$.

証明：$\left(\dfrac{W_p^2}{\ell}\right) = \left(\dfrac{-1}{\ell}\right)^{\frac{p-1}{2}} \left(\dfrac{p}{\ell}\right) = (-1)^{\frac{p-1}{2}\frac{\ell-1}{2}} \left(\dfrac{p}{\ell}\right)$. $\bmod\ \ell$ で $W_p^\ell = \displaystyle\sum_{m \neq 0} \left(\frac{m}{p}\right)^\ell \zeta_p^{\ell m} = \sum_{m \neq 0} \left(\frac{\ell^{-1} m}{p}\right) \zeta_p^m = \left(\frac{\ell}{p}\right) W_p$. よって $\left(\dfrac{W_p^2}{\ell}\right) = W_p^{2 \cdot \frac{\ell-1}{2}} = \left(\dfrac{\ell}{p}\right)$.

注意：奇素数 $p \geq 3$ について，$\left(\dfrac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

証明：$2 = (\zeta_8 + \zeta_8^{-1})^2$ より $\left(\dfrac{2}{p}\right) = 2^{\frac{p-1}{2}} = (\zeta_8 + \zeta_8^{-1})^{p-1} \equiv \dfrac{\zeta_8^p + \zeta_8^{-p}}{\zeta_8 + \zeta_8^{-1}} \pmod{p}$.

系：素数 $p \neq 2, 5$ について

$$\left(\frac{5}{p}\right) = \begin{cases} 1 & p \equiv \pm 1 \pmod{5} \\ -1 & p \equiv \pm 2 \pmod{5} \end{cases}.$$

系：奇素数 $p \geq 3$ について，$\exists x \in \mathbb{Z}, \exists y \in \mathbb{Z}, x^2 + y^2 = p \Leftrightarrow p \equiv 1 \pmod{4}$.

証明：$(\Rightarrow)$：明らか.
$(\Leftarrow)$:$(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}}$ より $\exists z \in \mathbb{F}_p^\times, z^2 = -1$. 鳩の巣原理より $-\sqrt{p} < \exists x, \exists y < \sqrt{p}, x + yz = 0$ かつ $(x,y) \neq (0,0)$. 今，$x^2 + y^2 = (x+iy)(x-iy) \in p\mathbb{Z}$ かつ $0 < x^2 + y^2 < 2p$.

注意：今回，$\mathbb{Z}[x]$ の 2 次式 $x^2 + ax + b$ がどの $\mathbb{F}_p[x]$ で分解するかが分かったが，これの一般化はいつかの例が知られている.

例：「$\sqrt[3]{2}$ について」以下が知られている（『数論を学ぶ人のための相互法則入門』平松豊一著）.

$$\exists x_1 \neq \exists x_2 \neq \exists x_3 \in \mathbb{F}_p^\times, x_1^3 = x_2^3 = x_3^3 = 2 \Leftrightarrow \exists x \in \mathbb{Z}, \exists y \in \mathbb{Z}, p = x^2 + 27y^2 \Leftrightarrow a(p) = 2.$$

ここで，形式的べき級数として

$$\sum_{n\geq 1} a(n)q^n := q\prod_{n\geq 1}(1-q^{6n})(1-q^{18n}).$$

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」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．

$(\Leftarrow)$：$\mathbb{Q}(\zeta_p)\supsetneq\mathbb{Q}\left(\cos\dfrac{2\pi}{p}\right)\supseteq\mathbb{Q}$ 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．