第10回 代数系　JNF

例

$(x-2)^3$

$\boxed{\text{体}}$

R

可換環の一種

$0 \neq 1$ かつ $R^\times = R \setminus \{0\}$

記法　体の準同型 = 可換環の準同型

Prop　$F_1 \xrightarrow{\varphi} F_2$; 体の準同型

$\Rightarrow \ker\varphi = 0$ （つまり φ は単射）

∵ $\ker\varphi \subseteq F_1$: ideal

$\ker\varphi = (0)$ or 全体 //

$I \subseteq \mathbb{F}$: ideal

体

$I \neq \{0\} \Rightarrow \exists\, i \in I,\ i \neq 0 \quad i^{-1} i = 1 \in I$

$\Rightarrow I =$ 全体

イデアル = ker 環準同型

正規部分群 = ker 群準同型

<u>記法</u> $\mathbb{F}_1 \xhookrightarrow{\varphi} \mathbb{F}_2$: field 拡大

しばしば $\mathbb{F}_1 \subseteq \mathbb{F}_2$ を考える。

記法

$$F \subset F' \supset S$$

部分集合

$F(S) = F'$ 中で F と S を含む最小の体

$$= \bigcap_{\substack{K \text{ s.t.} \\ \boxed{F' \supseteq K \supseteq S, F}}} K$$

部分体の共通部分は体

体

K として F' をとれる

㊟ 位相sp $Y \subseteq X$

$$\overline{Y} = \bigcap_{\substack{C \supseteq Y \\ 閉}} C$$

<u>Ex</u> $\mathbb{Q}(\sqrt{2}) = \{a+b\sqrt{2} \mid a, b \in \mathbb{Q}\}$

$$\begin{array}{ccc} \mathbb{Q} & & \sqrt{2} \\ \cap & & \rotatebox{90}{$\in$} \\ & \mathbb{R}, \mathbb{C} & \end{array}$$

一般の場合

は体(有理化)

$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \{a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6} \mid a, b, c, d \in \mathbb{Q}\}$

$\parallel$

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

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

$\parallel$ $\qquad$ $\cup\!\parallel$ 明らか

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

$\cap\!\parallel$: $\sqrt{2}, \sqrt{3} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$

<u>Fact</u> $\mathbb{Q}(s_1, \dots, s_l) = \mathbb{Q}(\exists t)$

$s_i \in \overline{\mathbb{Q}}$

$\boxed{\text{単拡大定理}}$

ガロアの基本定理

線形代数 個数を数える

$\mathbb{F} \overset{\tau}{\hookrightarrow} \mathbb{F}'$ について $\mathbb{F}'$ は

$\mathbb{F}$-vector sp になる via

$f \cdot f' := \tau(f) f'$ とする.
in $\mathbb{F}'$

$f \in \mathbb{F}$

$f' \in \mathbb{F}'$

<u>Def</u> $\mathbb{F} \overset{\tau}{\hookrightarrow} \mathbb{F}'$ finite が有限次finite

$\Leftrightarrow$ $\mathbb{F}'$: f.g. $\mathbb{F}$-線型 sp.

Ex

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

$$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$$

$$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$$

$$a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$$

$$= (a + b\sqrt{2}) + (c + d\sqrt{2})\sqrt{3}$$

Prop $\mathbb{F}_1 \subseteq \mathbb{F}_2 \subseteq \mathbb{F}_3$ について

① $\mathbb{F}_1 \subseteq \mathbb{F}_3$: 有限次

$\iff$ $\mathbb{F}_1 \subseteq \mathbb{F}_2$: 有限次
$\mathbb{F}_2 \subseteq \mathbb{F}_3$

② $[\mathbb{F}_1 : \mathbb{F}_3] = [\mathbb{F}_1 : \mathbb{F}_2][\mathbb{F}_2 : \mathbb{F}_3]$

(∵) ① $\Rightarrow$: 明らか

$$\left(\begin{aligned} \mathbb{F}_3 &= \mathbb{F}_1 v_1 + \cdots + \mathbb{F}_1 v_\ell \\ &\subseteq \mathbb{F}_2 v_1 + \cdots + \mathbb{F}_2 v_\ell \subseteq \mathbb{F}_3 \end{aligned} \right)$$

$\underline{\Leftarrow}$ $\mathbb{F}_2 = \mathbb{F}_1 v_1 + \cdots + \mathbb{F}_1 v_m$

$\mathbb{F}_3 = \mathbb{F}_2 w_1 + \cdots + \mathbb{F}_2 w_n$

$$\Rightarrow \mathbb{F}_3 = \sum_{\substack{1 \le i \le m \\ 1 \le j \le n}} \mathbb{F}_1 v_i w_j$$

を言う + 線形独立性

↑ OK

↑

$$\sum_{i,j} c_{ij} v_i w_j = 0 \text{ in } \mathbb{F}_3$$

$$\|$$

$$\sum_j \Big(\underbrace{\sum_i c_{ij} v_i}_{= 0 \text{ in } \mathbb{F}_2}\Big) w_j = 0 \quad \therefore \forall c_{ij} = 0$$

応用 コンパスと定規の作図

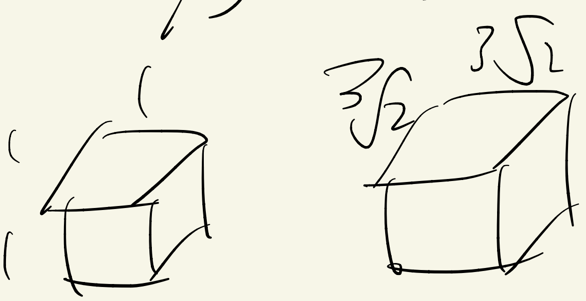
ギリシア時代

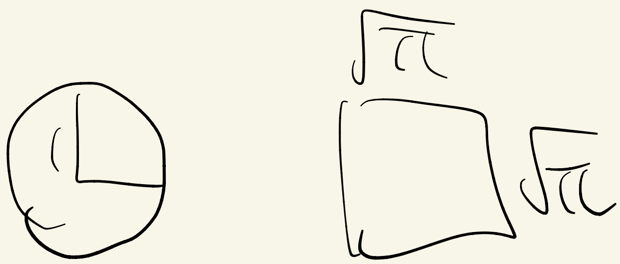
$\cancel{x^n + y^n = z^n} \quad n \geq 3$

$180^\circ / 3 = 60^\circ$

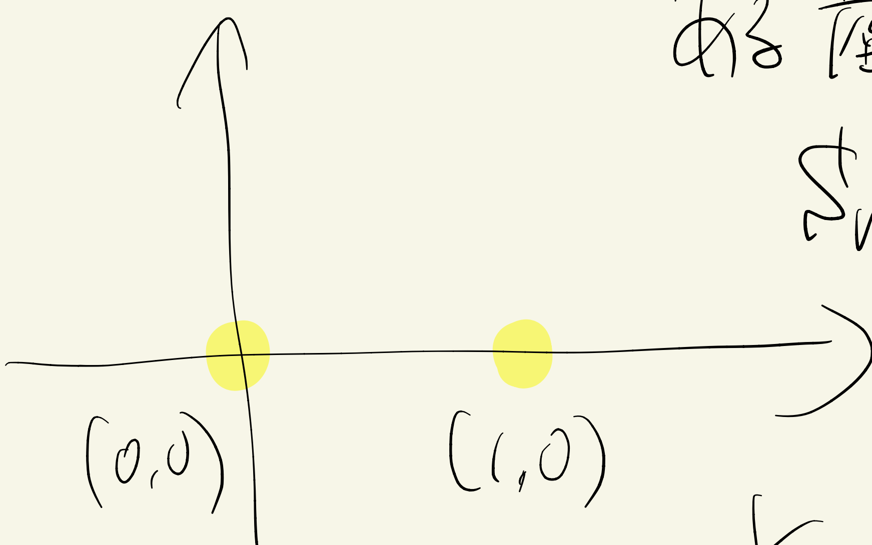
$x^y - z^w = 1$

$3^2 - 2^3 = 1$ (カタラン)





nステップ目に
ある座標を
$S_n \subseteq \mathbb{R}$



$K_n = \mathbb{Q}(S_n)$
は作図可能

$[K_n : K_{n-1}] = 1$ or 2

(各自考えよ)

$K_n = K_{n-1}$

2次方程式 $\sqrt{\ }$

2の巾 $= [K_n : \mathbb{Q}]$

$\parallel$

$[K_n : \mathbb{Q}(\sqrt[3]{2})]\underbrace{[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}]}_{3}$

$\sqrt[3]{2} \in K_n$ とする

$\mathbb{Q}(\sqrt[3]{2}) \subseteq K_n \Rightarrow$

$\parallel$

$\{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Q}\}$

Def $\mathbb{F} \subseteq \mathbb{F}'$

$$\begin{array}{c} \mathbb{F}' \\ \cup \\ \theta \end{array}$$

① θ が $\mathbb{F}$代数的

$\iff \exists f(x) \in \mathbb{F}[x],\ f(\theta) = 0$ in $\mathbb{F}'$

② $\mathbb{F} \subseteq \mathbb{F}'$ が代数的

$\iff \forall \theta \in \mathbb{F}'$ が $\mathbb{F}$代数的

Ex $\mathbb{Q} \subseteq \mathbb{R}$: not 代数的

$$\begin{array}{c} \mathbb{R} \\ \cup \\ \pi \end{array}$$

prop $F \subseteq F'$: 有限次

$\Rightarrow$ 代数拡大

(証) $n = [F' : F]$

$\theta \in F'$ について

$\underbrace{\theta^0 = 1, \theta, \dots, \theta^n}_{n+1コ}$ は F線形従属

をもつ

$$\therefore \sum_{m=0}^{n} a_m \theta^m = 0$$

$$\therefore f(\theta) = 0 \quad f(x) = \sum_{m=0}^{n} a_m x^m \quad //$$

<u>記法</u> $\mathbb{F} \subseteq \mathbb{E}$

$$\begin{array}{c} \mathbb{E} \\ \cup \\ \theta \end{array}$$

$I = \{ f(x) \in \mathbb{F}[x] \mid f(\theta) = 0 \text{ in } \mathbb{E} \}$

は $\mathbb{F}[x]$ の ideal

PID

$I \neq \{0\} \iff \theta$ が $\mathbb{F}$ 代数的

このとき $I = ({}^{\exists} f(x))$ $\mathrm{Irr}(\mathbb{F}; \theta)$

モニック, 1次以上

prop $\mathbb{F} \subseteq \mathbb{F}'$: 拡大

$\cup$

θ : 代数的

$$f(x) := \mathrm{Irr}(\mathbb{F};\theta)$$

$$\mathbb{F}(\theta) \cong \mathbb{F}[x]/(f(x))$$ 有理化の原理

Ex $\mathbb{Q}(\sqrt{2}) \cong \underline{\mathbb{Q}[x]/(x^2-2)}$

$$= \{a+bx \mid a,b \in X\}$$

① $\mathbb{F}[x] \to \mathbb{F}(\theta)$ 環準同型 ($\mathbb{F}[x]$の普遍性)

$f(x) \to f(\theta)$

$(x \mapsto \theta)$

$\therefore\ \mathbb{F}[x]/(f(x)) \hookrightarrow \mathbb{F}(\theta)$

整域 $\qquad$ 体

$f(x)$:素元(∵既約) かつ $\mathbb{F}[x]/(f(x))$は体

$$\boxed{A:\mathrm{PID} \quad \mathrm{Spec}\,A\setminus\{0\} = \{\text{極大ideal}\}}$$

$$\mathbb{F}[x] \twoheadrightarrow \mathbb{F}[\theta] = \{ f(\theta) \mid f(x) \in \mathbb{F}[x] \}$$

$$f(x) \overset{\varphi}{\longmapsto} f(\theta)$$

$\mathbb{F}$とθを
ふくむ最小の環

$$\mathbb{F}(\theta)$$

$$\mathbb{F}[x]/(f(x)) \overset{\varphi}{\simeq} \mathbb{F}[\theta] \subseteq \mathbb{F}(\theta)$$

体　　　　も体

最小性より $\mathbb{F}[\theta] = \mathbb{F}(\theta)$ //

参 今の設定で

$$[\mathbb{F}(\theta):\mathbb{F}] = \deg \mathrm{Irr}(\mathbb{F};\theta)$$

参 $\mathbb{F}_1 \subseteq \mathbb{F}_2 \subseteq \mathbb{F}_3$

$\mathbb{F}_1 \subseteq \mathbb{F}_3$：代数拡

$\mathbb{F}_1 \subseteq \mathbb{F}_2$
$\mathbb{F}_2 \subseteq \mathbb{F}_3$ ：代数

$\boxed{\Leftarrow}$

重ここをもつか
というか

$\mathbb{C}$

$\mathbb{F}[x] \ni f(x)$

$\overline{\mathbb{Q}} = \{ x \in \mathbb{C} \mid x$ は $\mathbb{Q}$ 代数的 $\}$

は体 (代数的数)

$\overline{\mathbb{Q}} = \{ \theta \in \mathbb{C} \mid \exists f(x) \in \mathbb{Q}[x],\ f(\theta) = 0 \}$

モニック

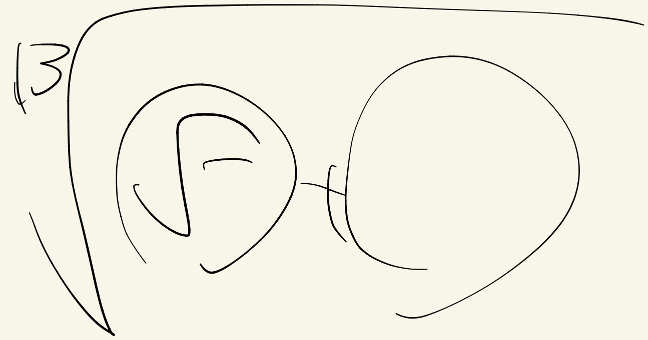
$\overline{\mathbb{Q}} \supseteq K$: 代数体

$\cup|$

$\mathbb{Q}$

有限体

$x^{13}-1=0$　　$x=\sqrt[13]{1}$



ガロア基本定理

$$\exists!$$

$$\begin{array}{ccccl} F: 体 & \longleftarrow & \mathbb{Z} & : 環準同型 \\ 1 & \longleftarrow & 1 & \end{array}$$

$\mathbb{Z}/\mathrm{Ker}$

整域

$\mathrm{Ker}=(0)$ or (p)

標数 0　　p

$\mathbb{Z}/p\mathbb{Z} =: \mathbb{F}_p$ $\cancel{\mathbb{Z}_p}$

<u>prop</u> $\mathbb{F}$：有限体 $\Rightarrow |\mathbb{F}| = p^n$

p：素数

(:) $\mathbb{Z} \hookrightarrow \mathbb{F}$ or $\mathbb{F}_p \hookrightarrow \mathbb{F}$

$\mathbb{Q}$ $\exists!$

$\mathbb{F}$ は $\mathbb{Q}$-vector sp

たので $|\mathbb{F}| = \infty$

$\mathbb{F}$ は $\mathbb{F}_p$-vector sp

$\dim = n$ $|\mathbb{F}| = p^n$

$R \rightsquigarrow \mathrm{Frac}(R) = \left(R \times (R \setminus \{0\})\right) / \sim$

整域　　商体

$$= \left\{ \frac{a}{b} \;\middle|\; \begin{array}{l} a \in R \\ b \in R\setminus\{0\} \end{array} \right\}$$

$$ad - bc = 0 \underset{\text{def}}{\iff} \overset{\shortparallel}{\frac{c}{d}}$$

<u>Ex</u> $\mathrm{Frac}(\mathbb{Z}) = \mathbb{Q}$

<u>普遍性</u>

$$\begin{tikzcd} R \arrow[r, "\forall f \,:\, \text{ring hom}"] \arrow[d, hook] & \forall S \\ \mathrm{Frac}\,R \arrow[ur, dashed, "\exists ?\, \tilde{f}"'] & \end{tikzcd} \quad : 環$$

単射

$r \mapsto r/1$

$\forall r \in R\setminus\{0\},\; f(r) \in S^{\times}$

$\mathrm{Frac}\, R = K$ （R：整域）

は R：UFD $\Rightarrow$ $R[x]$ もUFD

の proof に使ったりする

<u>prop</u> $\forall p \geq 2$：素数

$\forall n \geq 1$

$\exists \mathbb{F}$：体 s.t.

$|\mathbb{F}| = p^n$

$\because$ $f(x) \in \underline{\mathbb{F}_p[x]}$：モニックで
PID
n次，irr

$\Rightarrow$ $\mathbb{F}_p[x]/(f(x))$ がいそう。

$\underline{\text{Ex}}$ $\mathbb{F}_2[x] \ni x^2,\ x^2+1,\ x^2+x,\ x^2+x+1$

$$x^2+1 = (x+1)^2, \qquad x^2+x = x(x+1)$$

$$\mathbb{F}_4 = \mathbb{F}_2[x]\big/\left(x^2+x+1\right)$$

$\underline{\text{要5 モにいい}}$ $$a_n = \left| \left\{ \underset{\text{モニック}}{\mathbb{F}_p[x] \text{ の } n \text{次 irr}} \right\} \right|$$

$$a_n = \frac{1}{n} \sum_{d \mid n} \underline{\mu\left(\frac{n}{d}\right)}\, p^d$$

メビの関数 0, 1, −1

$$p^n - p^{n-1} - p^{n-2} - \cdots - p^0 > 0$$

$\overline{\mathbb{Q}}$, $\mathbb{C}$

$\mathbb{F}_9 = \mathbb{F}_3[x]/(f(x))$

prop p：素, $n \geq 1$ $\mathbb{F}, \mathbb{F}'$：体

$$|\mathbb{F}| = |\mathbb{F}'| = p^n \Rightarrow \mathbb{F} \simeq \mathbb{F}'$$

$\mathbb{F}^\times \simeq C_{p^n-1}$

$\forall x \in \mathbb{F}^\times \quad x^{p^n-1} = 1 \text{ in } \mathbb{F}^\times (\mathbb{F})$

$\forall x \in \mathbb{F} \quad x^{p^n} = x$

今, $\mathbb{F}^\times$ の原始根 x_0

$f(x) = \mathrm{Irr}(\mathbb{F}_p : x_0) \quad f(x) \mid x^{p^n} - x$

$$\mathbb{F} = \mathbb{F}_p[x_0] \simeq \mathbb{F}_p[x]/(f(x))$$

$\uparrow$

x_0: generator

$\mathbb{F}' \ni y$ 　 $y^{p^n} - y = 0$ をみたすので

とくに $\exists y_0 \in \mathbb{F}'^{\times}$ s.t. $f(y_0) = 0$

($\Leftarrow$ 体で d 次多項式は高々 d コの解をもつ)

$$x^{p^n} - x = \underline{f(x)} \cdots$$

$\therefore$ $\mathbb{F}$

$$\underset{\text{になる}}{\mathbb{F}' = \mathbb{F}} \supseteq \underbrace{\mathbb{F}_p[y_0]}_{p^n\text{コの元}} \simeq \boxed{\mathbb{F}_p[x]/(f(x))}$$

フィボナッチ数列への応用

$\mathbb{F}_{p^2}$

$\cup$

$\mathbb{F}_p[x]/(x^2-5)$

$a_0 = 0$

$a_1 = 1$

$a_{n+2} = a_n + a_{n+1}$

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

は $\mathbb{F}_p$ or $\mathbb{F}_{p^2}$ $(p \neq 2, 5)$ で意味を持つ

Fact x^2-5 は $\mathbb{F}_p(x)$ で可約

① if $p \equiv \pm 1 \mod 5$（重こんせ）

② 〃 既約 if $p \equiv \pm 2$ (mod 5)

系 $p \equiv \pm 1 \pmod 5$

①

$$\Rightarrow a_{n+p-1} = a_n \quad \forall n$$

in $\mathbb{F}_p$

② $p \equiv \pm 2 \pmod 5$

$$\Rightarrow a_{n+p^2-1} = a_n \quad \forall n$$

in $\mathbb{F}_p$

① $\frac{1+\sqrt{5}}{2} \in \mathbb{F}_p^\times \Rightarrow \left(\frac{1+\sqrt{5}}{2}\right)^{p-1} = 1$

② $\frac{1+\sqrt{5}}{2} \in \mathbb{F}_{p^2}^\times \quad \left(\frac{1+\sqrt{5}}{2}\right)^{p^2-1} = 1$

Ex $p=3$

a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	a_9
0	1	1	2	3	5	8	13	21	34
								0	1

Lemma $\mathbb{F}$: $\mathrm{char}\,\mathbb{F} = p \geq 2$: 体

のとき $\sigma_{\mathbb{F}} : \mathbb{F} \to \mathbb{F}$ は準同型

$$x \mapsto x^p$$

(フロベニウス)　　abelian

∵ $\sigma(a+b) = \sigma(a) + \sigma(b)$ のみ非自明

$$\begin{array}{ccc} \sigma(a+b) & & \sigma(a)+\sigma(b) \\ \| & & \| \\ (a+b)^p & & a^p + b^p \\ \| & & \\ \end{array}$$

$$a^p + \binom{p}{1} a^{p-1} b + \cdots + \binom{p}{1} a b^{p-1} + b^p$$

ここで $1 \leq k \leq p-1 \Rightarrow \binom{p}{k} \in p\mathbb{Z}$ //

Def $\mathbb{F} \subseteq \mathbb{F}'$: 体拡大

$$\mathrm{Gal}(\mathbb{F}'/\mathbb{F}) := \left\{ \begin{tikzcd} \mathbb{F}' \arrow[rr, "f", "\sim"'] & & \mathbb{F}' \\ & \mathbb{F} \arrow[ul] \arrow[ur] \arrow[u, phantom, "\circlearrowleft"] & \end{tikzcd} \right\}$$ は群

商の意味なし

注 $\mathrm{Aut}(N)$

Thm $p \geq 2$: 素数 $n \geq 1$

$$\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \simeq C_n \quad : n\text{次巡回群}$$

$$\sigma^x \mapsfrom [x]$$

(∵) σ は単射より全単射

$\sigma \in \mathrm{Gal}$ $(a \in \mathbb{F}_p \Rightarrow a^p = a)$

$\mathbb{F}_{p^n}^\times \simeq C_{p^n-1}$ より

$\mathbb{F}_{p^n} = \mathbb{F}_p[x_0]$ を考えると $\left(\begin{array}{c}\mathrm{Irr}(\mathbb{F}_p : x_0) \\ \| \\ f(x)\end{array}\right)$

σ の位数は n である $\therefore |\mathrm{Gal}| \geq n$

$\left(\sigma(x_0) = x_0^{p} \overset{\sigma}{\longmapsto} x_0^{p^2} \cdots\cdots \right)$

今、$\forall \tau \in \mathrm{Gal}$ $f(\tau(x_0)) = 0$

$$\begin{array}{c} f(\tau(x_0)) \\ \| \\ \tau(f(x_0)) \end{array}$$

$\tau \neq \tau'$ in $\mathrm{Gal} \Rightarrow \tau(x_0) \neq \tau'(x_0)$

$\tau(x_0)$ は $f(x)$ の解なので高々 n コ

$\therefore |\mathrm{Gal}| \leq n$ //

$r(A)+r(B)-n \leq r(AB)$

系② $p \equiv \pm 2 \pmod 5$

$\forall n \geq 0 \quad a_{n+2(p+1)} = a_n$ in $\mathbb{F}_p$

$a_n = \frac{1}{\sqrt{5}}(\alpha^n - \beta^n)$

$p^2-1 = (p-1)(p+1)$

証

$p \equiv \pm 2 \bmod 5$

$\Rightarrow \mathbb{F}_{p^2} \simeq \mathbb{F}_p[x]/(x^2-x-1)$

$\uparrow$

$\sqrt{5}$ の $\sigma_{\mathbb{F}_{p^2}}$ は

x^2-x-1 の解を入れかえる $\frac{\sqrt{5}\pm 1}{2}$ の最小多項式

$\alpha, \beta = \frac{\sqrt{5}\pm 1}{2}$

$\alpha^p = \beta$

$\beta^p = \alpha$

$\Rightarrow \alpha^{p+1} = \beta^{p+1} = -1$

$\therefore \alpha^{2(p+1)} = \beta^{2(p+1)} = 1$

記法 $F \subset F'$：拡大

$\mathrm{Gal}(F'/F) \supset G$：部分群

$$(F')^G = \left\{ x \in F' \;\middle|\; \begin{array}{l} \forall \tau \in G \\ \tau(x) = x \end{array} \right\}$$

は F の拡大体

F' の部分体

Def $F' \supset F$：有限次拡大が

ガロア拡大 $\overset{\text{def}}{\iff} F'^{\,\mathrm{Gal}(F'/F)} = F$

系 $p \geq 2$: 素

$n \geq 1$: $\qquad \mathbb{F}_p \subseteq \mathbb{F}_{p^n}$: ガロア拡大

① $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \langle \underset{\substack{\parallel \\ \mathrm{id.}}}{\sigma^0}, \sigma^1, \cdots, \sigma^{n-1} \rangle$

$\forall k \in \mathbb{Z}/n\mathbb{Z}$

$$x \in \mathbb{F}_{p^n} \quad \sigma^k(x) = x \iff \sigma(x) = x$$

$$\iff x^p = x$$

$$\iff x \in \mathbb{F}_p$$

$\mathbb{F}'$

$\cup|$ ガロア $\quad G \supseteq H$

$\mathbb{F}$

リード・ソロモン符号

ガロアの基本定理 (but for 代数体 i.e. $\overline{\mathbb{Q}}$の部分体)

単拡大