

- 巡回群を例として -

§1 : IGP & NP (Inverse Galois Problem, Noether Problem)

§2 : Stably / retract rationality.

§3 : NP for C_n/\mathbb{Q} ← C_n は位数 n の巡回群.§1

■ IGP.

ProblemIGP(\mathbb{K}, G) : \mathbb{K} : a field
 G : finite group

Then is there

 L/\mathbb{K} : Galois extension (s.t.) $\text{Gal}(L/\mathbb{K}) \cong G$?→ (i.e.) $\exists H \leq \text{Gal}(\overline{\mathbb{K}}/\mathbb{K})$ (s.t.) $\text{Gal}(\overline{\mathbb{K}}/\mathbb{K})/H \cong G$?Notation \mathbb{K} : a field G : finite group $G_{\mathbb{K}} := \text{Gal}(\overline{\mathbb{K}}/\mathbb{K})$ \mathbb{F}_q : a finite fieldExample 1Cases where IGP($\mathbb{K}, \forall G$) does Not hold: (\mathbb{K} : fix したときに、 G を任意に与えたら.....?)① $\mathbb{K} = \overline{\mathbb{K}} \rightsquigarrow G_{\mathbb{K}} \cong \{1\}$ ② $\mathbb{K} = \mathbb{F}_q \rightsquigarrow G_{\mathbb{K}} \cong \hat{\mathbb{Z}} = \varprojlim_n \mathbb{Z}/n\mathbb{Z}$ (i.e.) L/\mathbb{K} is cyclic group.③ $\mathbb{K} = \mathbb{Q}_p \rightsquigarrow \forall K/\mathbb{K}$: solvable extension (i.e.) $\text{Gal}(L/\mathbb{K})$ is solvable.Example 2Cases where IGP($\mathbb{K}, \forall G$) holds:① $\mathbb{F}_q(t)^{\text{ab}}$ ← Abel extension② $\overline{\mathbb{K}}(t)$

Example 3

Cases where IGP (\mathbb{Q}, G) holds :

(1) G : Abel [Kronecker - Weber]

G : solvable [Shafarevich]

(2) G : Simple

(i) $C_p \subset$ (condition (1))

(ii) A_n ($n \geq 5$) [Hilbert] NP は $n \geq 6$ 未解決

(iii) groups of Lie type / \mathbb{F}_q

• $PSL_2(\mathbb{F}_q)$ [Zywina] $\xleftarrow{!!}$ Galois representation!

(iv) Sporadic group except for M_{23} . ("rigidity criterion" : Monster [Tompson]
others [Malle])

Example 4

Open cases :

• $PSL_2(\mathbb{F}_{p^n})$ for $p=2, n \geq 9, p:\text{odd}, n \geq 3$.

• M_{23}

• $SPU_3(\mathbb{F}_q)$ for $q \neq 3, 5$.

NP

Problem

NP(\mathbb{k}, G) : \mathbb{k} : a field
 G : a finite group
 $G \curvearrowright \mathbb{k}(x_g \mid g \in G)$ as $h \cdot (x_g) := x_{hg}$ for $\forall h, g \in G$.
 $G \curvearrowright \mathbb{k}$: trivial.

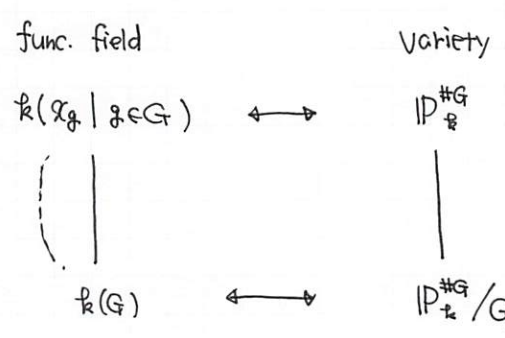
Then is $\mathbb{k}(G) := \mathbb{k}(x_g \mid g \in G)^G$ rational / \mathbb{k} ?
 (i.e.) $\mathbb{k}(G) = \mathbb{k}(\exists t_1, \dots, \exists t_{\#G})$: purely trans.

Noether's strategy.

NP(\mathbb{k}, G) is affirmative.
 (i.e.) $\mathbb{k}(G)$ is rational / \mathbb{k} .

$\Rightarrow \exists \phi : \mathbb{k}(t_1, \dots, t_{\#G}) \xrightarrow{\sim} \mathbb{k}(G)$
 !!
 \pm

$\xrightarrow{\phi^{-1}} \exists f(\pm; X) \in \mathbb{k}(\pm)[X]$ (s.t.) $\text{Spl}(f(\pm; X) / \mathbb{k}(\pm)) / \mathbb{k}(\pm)$: G -ext. $\text{minimel splitting field}$ ★



\mathbb{k} : Hilbert $\xrightarrow{\sim} \exists \infty a_i \in \mathbb{k}^{\#G}$ (s.t.) $\text{Gal}(f(a_i; X) / \mathbb{k}) \cong G$. \Rightarrow IGP(\mathbb{k}, G) holds

Remark

- \mathbb{k} : NF (fin. ext of \mathbb{Q}) is Hilbert.
- $\mathbb{k} = \overline{\mathbb{k}}$, $\mathbb{k} = \mathbb{F}_q$ is Not Hilbert.
- Henselian $\supset \mathbb{Q}_p$, $\mathbb{k}[t]$ is Not Hilbert

$f(\pm; X)$ has "nice property"
 "generic"

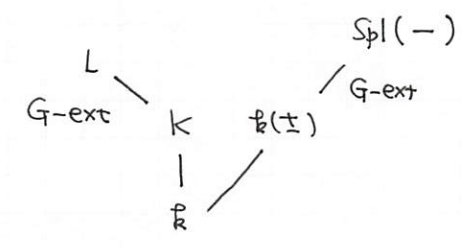
Definition [generic G/\mathbb{k} polynomial]

\mathbb{k} : infinite field.
 G : finite group.

$f(\pm; X) \in \mathbb{k}(\pm)[X]$ is a generic G/\mathbb{k} -polynomial

def \Leftrightarrow ① : $\text{Spl}(f(\pm; X) / \mathbb{k}(\pm)) / \mathbb{k}(\pm)$: G -ext

② : $\forall K \supset \mathbb{k}, \forall L/K : G$ -ext. Then $\exists a_i \in \mathbb{k}^n$ (s.t.) $\text{spl}(f(a_i; X) / K) = L$.



Theorem [Kyuk '84]

\mathbb{k} : Hilbert.

$f(\pm; X)$ in \otimes is a generic G/\mathbb{k} -polyomial.

Remark [DeMeyer '83] [Kemper '01]

1983年 De Meyer が generic G/\mathbb{k} -poly. を定義していたときは, 以下の条件も含まれていた:

③: $\forall H \leq G, \mathbb{k} \subset K: \text{fix}$. Then, for $\forall M/K: \text{Hilbert}$,

$$\exists a_1 \in \mathbb{k}^n \text{ (s.t.) } \text{Spl}(f(a_1; X)/K) = M.$$

-方, 2001年 Kemper が ①, ② から ③ が従うことを示した.

§2

▣ Rationality Problem & NP

Problem

RP : \mathbb{k} : a field
 G : a finite group
 F/\mathbb{k} : fin. gen. ext.

$G \curvearrowright \mathbb{k}$: trivial & $G \curvearrowright F$ as automorphism (i.e. $G \leq \text{Aut}_{\mathbb{k}}(F)$)

Is F^G rational / \mathbb{k} ?

Remark

• RP for left regular action is NP(\mathbb{k}, G)
 ($\mathbb{k}(xg \mid g \in G)$)

• For $F = \mathbb{k}(t)$, always F^G is rational / \mathbb{k} [Lüroth's theorem]

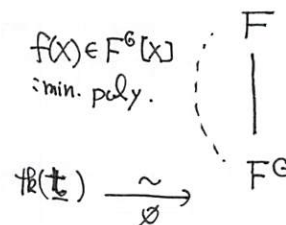
Theorem [Kemper - Mattig '00]

$G \curvearrowright \mathbb{k}$: trivial
 \mathbb{k} : Hilbert.

$G \curvearrowright F$: linear faithful

Then F^G is rational / $\mathbb{k} \Rightarrow \underbrace{f(\pm; X)}$ is a generic G/\mathbb{k} -poly.

$$\parallel \varnothing^{-1}(f(x))$$



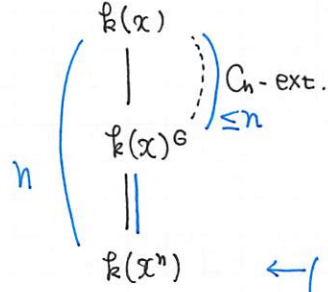
Example 1 [Kummer theory]

$k \ni \xi_n := e^{\frac{2\pi}{n}i}$

$G := C_n = \langle \sigma \rangle$

$F := k(x)$

$\sigma : x \mapsto \xi_n x$



$\leftarrow \begin{cases} x^n \in k(x)^G \\ \sigma(x^n) = \xi_n x^n = x^n \end{cases}$

$f_x(X) = X^n - x^n$ is irreducible / $k(x^n)$

$\phi^{-1}(f_x(X)) = f(t; X) = X^n - t$ is a gen C_n/\mathbb{Q} -poly.

Proposition [Endo-Miyata '73 Proposition 1.1]

F : a field

$G \curvearrowright F$: faithful.

$V := \bigoplus_{i=1}^n F u_i$: F -vector space.

$G \curvearrowright V$: semi linear (i.e.) for $\sigma \in G$, $F(V) := F(u_1, \dots, u_n)$

$\sigma(a u_i) := \sigma(a) \sum_{j=1}^n a_{ij}(\sigma) u_j$ ($a, a_{ij} \in F$)

Then

$F(u_1, \dots, u_n)^G$ is rational / $FG \leftarrow$ If F^G is rational / k , then $F(u_1, \dots, u_n)^G$ is rational / k

(proof)

$\sigma \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix} = \underbrace{\begin{pmatrix} a_{1j}(\sigma) \\ \vdots \\ a_{nj}(\sigma) \end{pmatrix}}_{A_\sigma \in GL_n(F)} \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix}$

We define

$f : G \longrightarrow GL_n(F)$
 $\sigma \longmapsto A_\sigma$

Then we obtain

$\sigma\tau \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix} = (A_\sigma \cdot \sigma(A_\tau)) \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix} = f(\sigma) \sigma f(\tau) \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix}$

① $f(\sigma\tau) = f(\sigma) \cdot \sigma f(\tau) \leftarrow$ cocycle condition

② $Z^1(G, GL_n(F)) := \{f \in \text{Map}(G, A) \mid f(\sigma\tau) = f(\sigma) \sigma f(\tau)\}$

Fact: [Hilbert 90 for $GL_n(F)$]

$H^1(G, GL_n(F)) = 1$

Remark

$$H^1(G, A) = \Sigma^1(G, A) / \sim, \text{ where } f \sim g \stackrel{\text{def}}{\iff} \exists a \in A \text{ (s.t.) } (g\sigma)^{-1} a g(\sigma) \quad (\sigma \in G)$$

By Hilb 90, we have $f \sim 1$ (identity matrix). $\rightsquigarrow \exists P \in GL_n(F)$ (s.t.) $f(\sigma) = (\sigma(P))^{-1} P$.

We put

$$\begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} := P \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix}.$$

Then

$$\sigma \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} = \sigma \left(P \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix} \right) = \sigma(P) \left(\sigma \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix} \right) = \sigma(P) f(\sigma) \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix} = P \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix} = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}.$$

① $\sigma v_i = v_i$ for any σ . (i.e.) $F(V)^G = F(u_1, \dots, u_n)^G = F(v_1, \dots, v_n)^G = F(v_1, \dots, v_n)^G$.

② $F(V)^G$ is rational / F^G . □

Corollary [No name lemma]

$W \subseteq V$: faithful $F(G)$ -submodule.

Then $F(V)^G$ is rational / $F(W)^G$

Corollary [Permutation NP]

$G \leq S_n$, \mathbb{k} : a field. \rightsquigarrow G is faithful に作用してはいる必要あり.

$G \curvearrowright \mathbb{k}(x_1, \dots, x_n)$ as $\sigma(x_i) = x_{\sigma(i)}$

Then $\mathbb{k}(x_1, \dots, x_n)^G$ is rational / $\mathbb{k} \implies NP(\mathbb{k}, G)$ holds.

上の Corollary ②

$V = \bigoplus_{g \in G} \mathbb{k} x_g \dots NP$

$W = \bigoplus_{i=1}^n \mathbb{k} x_i \dots \text{Perm NP}$

② 適用可.

Example 2 [Perm. NP]

$G = S_n$.

$\mathbb{k}(x_1, \dots, x_n)^{S_n} = \mathbb{k}(s_1, \dots, s_n)$ (s_i は i 次斉次基本対称式)

By (Cor. Perm. NP) $NP(\mathbb{k}, S_n)$ holds.

Stably / retract rational

Definition

k : a field.

F : fin. gen. field / k

F is **stable rational** / $k \stackrel{\text{def}}{\iff} F(\exists s_1, \dots, \exists s_t)$ is rational / k

F is **retract rational** / k (k : infinite field) $\stackrel{\text{def}}{\iff} \exists k\text{-alg } R \subseteq F$ (s.t.)

(i) $F = \text{Quot}(R)$

(ii) $\exists f \in k[x_1, \dots, x_n]$

$$R \begin{matrix} \xrightarrow{\psi} \\ \xleftarrow{\phi} \end{matrix} k[x_1, \dots, x_n] \left[\frac{1}{f} \right]$$

(s.t.) $\phi \circ \psi = \text{id}_R$.

F is **uni rational** / $k \stackrel{\text{def}}{\iff} F \subset \exists E$: rational / k .

"rational" \implies "stab. rational" $\stackrel{\star}{\implies}$ "retract rational" \implies "uni rational"

~~\iff~~

~~\iff~~

~~\iff~~

[Beurille, Colliot, Susuc, Symerton - Dyer '85]

[Saltman '82]

$\mathbb{Q}(C_8)$

$F = \mathbb{Q}(V)$

$V: x^2 + 3y^2 = t^3 - 2$

[Saltman '84]

$\mathbb{Q}(C_{47})$: Not stab. rat.

(c.f.) "Not rational" [Swan '69]

Definition

$F, F' : \text{fin. gen} / \mathbb{k}$.

$$F \stackrel{\text{stab}}{\sim} F' \stackrel{\text{def}}{\iff} F(\exists x_1, \dots, \exists x_n) = F(\exists y_1, \dots, \exists y_m)$$

このとき, F と F' は **stably equiv.** といふ.

Theorem

$\mathbb{k} : \text{infinite field}$

$$F \stackrel{\text{stab}}{\sim} F' \text{ ならば, } F : \text{ret. rational} / \mathbb{k} \stackrel{\text{iff}}{\iff} F' : \text{ret. rational} / \mathbb{k}.$$

特に, $F : \text{stable. rat.} / \mathbb{k} \implies F : \text{ret. rat.} / \mathbb{k}$

(proof)

後半のみを示す

仮定より $F \stackrel{\text{stab}}{\sim} F(\exists t_1, \dots, \exists t_n) : \text{rational} / \mathbb{k}$

$$\parallel$$

$$\mathbb{k}(\exists x_1, \dots, \exists x_m)$$

\hookrightarrow stable

$$\mathbb{k} : \text{retract rational} / \mathbb{k}$$

① $F : \text{retract rational} / \mathbb{k}$.



Lemma [Shan's lem]

$\mathbb{k} : \text{a field}$

$G : \text{a fin group}$

$F : \mathbb{k}$ の拡大体 \mathbb{k} の fin. gen.

$G \curvearrowright F$.

$R, S : \text{fin. gen sub } \mathbb{k}\text{-alg of } F \text{ (s.t.) } R, S \text{ are closed under the action of } G, \text{ Quot}(R) = \text{Quot}(S)$

Then $\exists r \in R^G, \exists s \in S^G \text{ (s.t.) } R[\frac{1}{r}] = S[\frac{1}{s}]$

(proof)

$$S := \mathbb{k}[\exists a_1, \dots, \exists a_n]$$

Then $a_i = \frac{x_i}{c_i}$ for some $x_i \in R, c_i \in R$ since $\text{Quot}(R) = \text{Quot}(S)$

$$C := c_1 \cdots c_n, r := \prod_{c \in G} \sigma(c) \in R^G.$$

$$\rightsquigarrow S \subset R[\frac{1}{r}].$$

Similarly $\exists s \in S^G \text{ (s.t.) } R[\frac{1}{r}] \subset S[\frac{1}{s}]$.

③ $R[\frac{1}{r}][\frac{1}{s}] = S[\frac{1}{s}]$

$\exists t \in R$ (s.t.) $S = \frac{t}{r^n}$ ($\exists n \in \mathbb{N}$) ④ $S \subset R[\frac{1}{r}]$.

Then $t = sr^n \in R^0$.

⑤ $S[\frac{1}{s}] = R[\frac{1}{rt}]$.

□

▣ A proof for ③ ($F \stackrel{\text{stab}}{\sim} F'$, $F = \text{ret. rat.} \Rightarrow F' : \text{ret. rat.}$)

We show that $F : \text{ret rational} / \mathbb{k} \Rightarrow F(x_1, \dots, x_n) : \text{ret rational} / \mathbb{k}$
 $F'(y_1, \dots, y_m) : \text{ret rational} / \mathbb{k}$
 $\Rightarrow F' : \text{ret rational} / \mathbb{k}$

$F : \text{ret rational} / \mathbb{k} \stackrel{\text{def}}{\iff} \exists R_0 \subset F : \mathbb{k}\text{-alg (s.t.)} \cdot \text{Quot}(R_0) = F$
 $\cdot R_0 \xrightleftharpoons[\psi]{\phi} \mathbb{k}[x_{n+1}, \dots, x_n][\frac{1}{\phi}]$

We put $R := R_0[x_1, \dots, x_n]$, where $F(x_1, \dots, x_n) = F'(y_1, \dots, y_m)$

Then $F(x_1, \dots, x_n)$ is ret. rational / \mathbb{k} .

⑥ $R \subset F(x_1, \dots, x_n) : \mathbb{k}\text{-algebra (s.t.)} \cdot \text{Quot}(R) = F(x_1, \dots, x_n)$
 $\cdot R \xrightleftharpoons[\psi]{\phi} \mathbb{k}[x_1, \dots, x_n, x_{n+1}, \dots, x_n][\frac{1}{\phi}]$

⑦ $F'(y_1, \dots, y_m)$ is ret. rational / \mathbb{k} .

We take $A \subset F' : \text{fin. gen. } \mathbb{k}\text{-alg (s.t.)} \text{Quot}(A) = F'$.

Then $\text{Quot}(R) = \text{Quot}(A[y_1, \dots, y_m])$

By Swan's lemma $R[\frac{1}{t}] = A[y_1, \dots, y_m][\frac{1}{t}]$ for some $r \in R$, $t \in A[y_1, \dots, y_m]$.

$\rightsquigarrow \exists \psi' : A[y_1, \dots, y_m] \rightarrow A : \text{map as } \mathbb{k}\text{-alg (s.t.) } \psi'(t) \neq 0$.

$a := \psi'(t) \in A (\subset R[\frac{1}{t}]) = \frac{s}{re}$ for some $s \in R$, $e \in \mathbb{N}$

⑧ $A[\frac{1}{a}][y_1, \dots, y_m][\frac{1}{t}] = R[\frac{1}{t}][\frac{1}{a}] = R[\frac{1}{rs}] \xrightleftharpoons[\psi]{\phi} \mathbb{k}[y_1, \dots, y_m][\frac{1}{\underbrace{\psi(rs)}_r}]$

⑨ $\tilde{\psi}' : A[y_1, \dots, y_m][\frac{1}{t}] \rightarrow A[\frac{1}{\psi}]$

$$\rightsquigarrow \underbrace{A[\frac{1}{a}][y_1, \dots, y_m][\frac{1}{f}]}_{\parallel} \rightarrow A[\frac{1}{a}]$$

$$R[\frac{1}{rs}]$$

$$\textcircled{1} A[\frac{1}{a}] \xrightleftharpoons[\tilde{\varphi}_i]{\tilde{\varphi}_i'} R[\frac{1}{rs}] \xrightleftharpoons[\psi]{\phi} k[y_1, \dots, y_m][\frac{1}{f'}] \quad \& \quad \text{Quot}(A[\frac{1}{a}]) = F'$$

② F' is int rational / k .

Theorem [Saitman '82, Remayer '83]

G : fin group

F : fin. gen. / k : infinite.

$G \curvearrowright F$: faithful

FG : int. rationals $\iff \exists$ generic G/k -poly.