「不変体の有理性問題について」

Sp: 金井さん (新潟大)

－ 巡回群を例として －

$\underline{\S 1}$: IGP & NP (Inverse Galois Problem, Noether Problem)

$\underline{\S 2}$: Stably / retract rationality.

$\underline{\S 3}$: NP for $C_n/\mathbb{Q}$ ← C_nは位数 n の巡回群.

$\underline{\S 1}$

■ IGP.

Problem

IGP(k, G) : k : a field
G : finite group

Then is there

L/G : Galois extension (s.t.) $\mathrm{Gal}(L/k) \simeq G$?

$\rightsquigarrow$ (i.e.) $\exists H \leq \mathrm{Gal}(\bar{k}/k)$ (s.t.) $\mathrm{Gal}(\bar{k}/k)/H \simeq G$?

Notation

k : a field
G : finite group
$G_k := \mathrm{Gal}(\bar{k}/k)$
$\mathbb{F}_q$: a finite field

Example 1

Cases where IGP(k, $\forall G$) does $\underline{\underline{\text{Not}}}$ hold : (k : fix したときに、Gを任意に与えたら....?)

① $k = \bar{k}$ $\rightsquigarrow$ $G_k \simeq \{1\}$

② $k = \mathbb{F}_q$ $\rightsquigarrow$ $G_k \simeq \hat{\mathbb{Z}} = \varprojlim_n \mathbb{Z}/n\mathbb{Z}$ (i.e.) L/k is cyclic group.

③ $k = \mathbb{Q}_p$ $\rightsquigarrow$ $\forall K/k$: sovable extension (i.e.) $\mathrm{Gal}(L/k)$ is solvable.

Example 2

Cases where IGP(k, $\forall G$) holds :

① $\mathbb{F}_q(t)^{ab}$ ← Abel extension

② $\bar{k}(t)$

Example 3

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

(1) G : Abel [Kronecker − Weber]

G : solvable [Shafarevich]

(2) G : simple

(i) C_p ⊂ (condition (1))

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

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

· $PSL_2(\mathbb{F}_q)$ [Zywina] $\xleftarrow{\text{!!}}$ Galouis representartion !

(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 : odd , $n \geq 3$.

· M_{23}

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

NP

Problem

$NP(k, G)$: k : a field
G : a finite group

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

Then is $k(G) := k(x_g \mid g \in G)^G$ rational $/ k$?

(i.e.) $k(G) = k(\exists t_1, \dots, \exists t_{\#G})$: purely trans.

· Noether's strategy.

$NP(k,G)$ is affirmative.
(i.e.) $k(G)$ is rational $/ k$.

$\Longrightarrow \exists \phi : k(\underbrace{t_1, \dots, t_{\#G}}_{\underline{t}}) \xrightarrow{\sim} k(G)$

$$\begin{tikzcd} & \text{func. field} & & \text{variety} \\ & k(x_g \mid g \in G) \arrow[r, leftrightarrow] \arrow[d, dash, "\text{G-ext.}"'] & & \mathbb{P}_k^{\#G} \arrow[d, dash] \\ & k(G) \arrow[r, leftrightarrow] & & \mathbb{P}_k^{\#G}/G \end{tikzcd}$$

$\overset{\phi^{-1}}{\rightsquigarrow}$ $\exists f(\underline{t}; X) \in k(\underline{t})[X]$ (s.t.) $Spl(f(\underline{t}; X)/k(\underline{t}))/k(\underline{t})$: G-ext. ------- ☆

minimal splitting field

k : Hilbert $\rightsquigarrow$ $\exists \infty a \in k^{n}$ ($n = \#G$) (s.t.) $Gal(f(a; X)/k) \simeq G$. $\Longrightarrow$ $IGP(k, G)$ holds

Remark

· k : NF (fin. ext of $\mathbb{Q}$) is Hilbert.

· $k = \bar{k}$, $k = \mathbb{F}_q$ is Not Hilbert.

· Henselian $\supset \mathbb{Q}_p$, $k[t]$ is Not Hilbert //

$f(\underline{t} : X)$ has $\underbrace{\text{"nice property"}}_{\text{"generic"}}$.

Definition [generic G/k polynomial]

$$\begin{tikzcd} & & & Spl(-) \\ L \arrow[dr, dash, "\text{G-ext}"'] & & & \\ & K \arrow[d, dash] & k(\underline{t}) \arrow[uur, dash, "\text{G-ext}"'] & \\ & k \arrow[ur, dash] & & \end{tikzcd}$$

k : infinite field.
G : finite group.

$f(\underline{t} : X) \in k(t)[X]$ is a generic G/k-polynomial

$\overset{def}{\Longleftrightarrow}$ ① : $Spl(f(\underline{t}; X)/k(\underline{t}))/k(\underline{t})$: G-ext

② : $\forall K \supset k$, $\forall L/K$: G-ext. Then $\exists a \in k^n$ (s.t.) $Spl(f(a; X)/K) = L$.

Theorem [Kyuk '84]

k : Hilbert.

$f(\underline{t};X)$ in ㊟ is a genelic G/k - palyporial.

Remark [DeMeyen '83] [Kempen '01]

1983年 De Meyer が generic G/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 : $^{\forall}H \leq G$, $k \subset K$: fix. Then, for $^{\forall}M/K$: Hilbert,

$\exists\, a \in k^n$ (s.t.) $\mathrm{Spl}(f(a;X)/K) = M$.

一方, 2001年 Kempen が ①, ② から ③ が従うことを示した.

§2

▨ Rationality Problem & NP

Problem

RP . : k : a field
G : a finite group
F/k : fin. gen. ext.

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

Is F^G rational $/ k$?

Remark

- RP for left regular action is $NP(k.G)$
  $(k(x_g \mid g \in G))$
- For $F = k(t)$, always F^G is rational $/ k$ [Lüroth's theorem]

Theorem [Kemper - Mattig '00]

$G \curvearrowright k$: trivial
k : Hilbert.

$G \curvearrowright F$: linear faithful

$f(X) \in F^G[X]$: min. poly.

$$\begin{array}{ccc} & & F \\ & & | \\ k(\underline{t}) & \xrightarrow[\phi]{\sim} & F^G \end{array}$$

Then F^G is rational $/ k$ $\Rightarrow$ $\underset{\underset{\phi^{-1}(f(X))}{\parallel}}{f(\underline{t};X)}$ is a generic G/k - paly.

Example 1 [Kummer theory]

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

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

$F := k(x)$

$\quad \sigma : x \longmapsto \zeta_n x$

$$\begin{tikzcd} k(x) \arrow[d, dash, "C_n\text{-ext.}\ \le n"] \\ k(x)^G \arrow[d, equal] \\ k(x^n) \end{tikzcd} \quad n$$

$\leftarrow \left(x^n \in k(x)^G \quad \because\ \sigma(x^n) = \zeta_n x^n = x^n \right)$

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

$\phi^{-1}(f_x(X)) = f(t;X) = X^n - t$ is a gen C_n/k-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 $\sigma \in G$, $F(V) := F(u_1, \cdots, u_n)$

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

Then

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

(proof)

$$\sigma \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix} = \underbrace{\begin{pmatrix} a_{ij}(\sigma) \end{pmatrix}}_{\substack{\| \\ A_\sigma \in GL_n(F)}} \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix}$$

We define

$$\begin{aligned} f : G &\longrightarrow GL_n(F) \\ \sigma &\longmapsto A_\sigma . \end{aligned}$$

Then we obtain

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

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

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

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

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

Remark

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

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

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

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

$\therefore$ $F(V)^G$ is rational $/ F^G$. $\square$

Corollary [No name lemma]

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

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

Corollary [Permutation NP]

$G \leq S_n$, k : a field. ← Gは faithful に作用している必要あり.

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

Then

$k(x_1,\dots,x_n)^G$ is rational $/ k$ $\Rightarrow$ $NP(k,G)$ hold.

上の Corollary で

$V = \bigoplus_{g\in G} k x_g$ …… NP

$W = \bigoplus_{i=1}^{n} k x_i$ …… Perm NP

で適用する.

Example 2 [Perm. NP]

$G = S_n$.

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

By (Cor. Perm. NP) $NP(k, S_n)$ holds.

Stably / retract rational

Definition

k : a field.
F : fin. gen. field / k

- F is stable rational / k $\overset{\text{def}}{\iff}$ $F(\exists s_1, \dots, \exists s_t)$ is rational / k
- F is retract rational / k (k : infinite field) $\overset{\text{def}}{\iff}$ $\exists$ k-alg $R \subseteq F$ (s.t.)

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

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

  $$R \underset{\phi}{\overset{\psi}{\rightleftarrows}} k[x_1 \dots x_n]\left[\frac{1}{f}\right]$$

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

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

"rational" $\Longrightarrow$ "stab. rational" $\overset{\star}{\Longrightarrow}$ "retract rational" $\Longrightarrow$ "uni rational"

$\not\Longleftarrow$ [Beaurille, Colliot, Sunsuc, Synnerton - Dyer '85]

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

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

$\not\Longleftarrow$ [Soltman '84]

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

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

$\not\Longleftarrow$ [Soltman '82]

$\mathbb{Q}(C_8)$

Definition

F, F' : fin. gen / k.

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

このとき, F と F' は stably equiv. という.

Theorem

k : infinite field

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

特に,

F : stable. rat. $/k \implies F$: ret. rat. $/k$

(proof)

後半のみを示す.

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

$$\begin{aligned} F(\exists t_1, \dots, \exists t_n) &\\ \| &\\ k(\exists x_1, \dots, \exists x_m) &\\ \wr \ \text{stable} &\\ k &: \text{retract rational } /k \end{aligned}$$

$\therefore$ F : retract rational $/k$. □

Lemma [Swan's lem]

k : a field

G : a fin group

F : k の拡大体で fin. gen.

$G \curvearrowright F$.

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

Then

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

(proof)

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

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

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

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

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

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

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

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

∴ $S[\frac{1}{s}] = R[\frac{1}{rt}]$.

$\square$

▨ A proof for ㊍ $(F \overset{\text{Stab}}{\sim} F',\ F: \text{ret. rat.} \Rightarrow F': \text{ret. rat.})$

We show that F: ret rational $/k \Longrightarrow F(x_1, \dots, x_n)$: ret rational $/k$

$\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad \wr\!\wr$

$\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad F'(y_1, \dots, y_m)$: ret rational $/k$

$\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad \Longrightarrow F'$: ret rational $/k$

F : ret rational $/k \overset{\text{def}}{\iff} \exists R_0 \subset F$: k-alg (s.t.) · $\mathrm{Quot}(R_0) = F$

· $R_0 \underset{\psi}{\overset{\phi}{\rightleftarrows}} k[x_{n+1}, \dots, x_{n'}][\frac{1}{\exists f}]$

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 $/k$.

∵ $R \subset F(x_1, \dots, x_n)$: k-algebra (s.t.) · $\mathrm{Quot}(R) = F(x_1, \dots, x_n)$

· $R \rightleftarrows k[x_1 \cdots x_n, x_{n+1} \cdots x_{n'}][\frac{1}{f}]$

∴ $F'(y_1, \dots, y_m)$ is ret. rational $/k$.

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

Then

$\mathrm{Quot}(R) = \mathrm{Quot}(A[y_1 \cdots y_m])$

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

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

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

∴ $A[\frac{1}{a}][y_1 \cdots y_m][\frac{1}{t}] = R[\frac{1}{r}][\frac{1}{a}] = R[\frac{1}{rs}] \underset{\psi}{\overset{\phi}{\rightleftarrows}} k[y_1, \dots, y_{n'}][\frac{1}{\underbrace{\phi(rs)f}_{= f'}}]$

∴ $\tilde{\psi}' : A[y_1, \dots, y_m][\frac{1}{t}] \longrightarrow A[\frac{1}{a}]$

$$\rightsquigarrow \quad \underbrace{A[\tfrac{1}{a}][y_1, \cdots, y_m][\tfrac{1}{t}]}_{\displaystyle \shortparallel \atop \displaystyle R[\tfrac{1}{rs}]} \longrightarrow A[\tfrac{1}{a}]$$

∴ $A[\frac{1}{a}] \underset{\tilde{\psi}'}{\overset{\tilde{\phi}'}{\rightleftarrows}} R[\frac{1}{rs}] \underset{\psi}{\overset{\phi}{\rightleftarrows}} k[y_1 \cdots y_m][\frac{1}{f'}]$ & $\mathrm{Quot}(A[\frac{1}{a}]) = F'$.

∴ F' is ret rational $/k$.

Theorem [Saltman '82, DeMeyer '83]

G : fin group
F : fin. gen. $/ k$: infinite.

$G \curvearrowright F$: faithful.

F^G : ret. rationals $\iff$ $\exists$ generic G/k - poly.