数理解析研究所講究録
第 759 巻 1991 年 152-161

Hilbert の既約性定理のある類似と代数体の分布

防衛大　山村　健　(Ken Yamamura)

1 Introduction

n を 3 以上の自然数とする。ここで、次のことを主張する。

(P)　n 次の有理整係数の monic 多項式の最小分解体を取ると、それが Q の S_n-拡大（Galois 群が n 次対称群 S_n に同型な Galois 拡大）で、そのただ 1 つの 2 次部分体上不分岐であるようなものになる割合が大きい。

(F)　n 次代数体の Galois 閉包を取ると、上のような体となる割合が大きい。

「割合」とは密度の意味で、(P) ではすべての係数の絶対値が一定値 N 以下の多項式全体に対する比率の（$N \to \infty$ としたときの）極限であり、(F) では判別式の絶対値が一定値 X 以下の体全体に対する比率の（$X \to \infty$ としたときの）極限である。また、「大きい」というのは不明確な表現だが、予想としては、割合がそれぞれ、(P) の場合は 0.5 より、(F) の場合は 0.6 より大きい。

この小文で、上の主張の根拠、背景について述べ、また主張の内容を正確に formulate し、$n = 3$ の場合にはそれが証明されていることを報告する。

2 The generic situation

(P) の多項式は、n 次一般多項式からその係数の parameter をすべて有理整数でおきかえる特殊化によって生じる。「n 次の有理整係数の monic 多項式の最小分解体が Q の S_n-拡大となる割合は 1 である。」というのが Hilbert の既約性定理の定量化版を一般多項式に適用した特別な場合である。Hilbert の既約性定理は「特殊化による Galois 群の保存」を主張す

るが、我々はさらに「不分岐性の保存」も考察しようというわけである。まず、generic situation を見直すことから始める。

さて、

$$f(X,t) = X^n + t_1X^{n-1} + \cdots + t_n$$

を n 次の一般多項式とし、特殊化

$$t = (t_1, \cdots, t_n) \to a = (a_1, \cdots, a_n) \in \mathbf{Z}^n$$

を考える。したがって、$f(X,t)$ は $k = \mathbf{Q}(t_1, \cdots, t_n)$ 上の多項式とみなす。$f(X,t)$ の最小分解体を K とおくと、$\mathrm{Gal}(K/k) = S_n$ である。n 次交代群 A_n に対応する体を F とする。分岐について考えるために、$O_k = \mathbf{Z}[t_1, \cdots, t_n]$ とおき、O_k の K および F における整閉包をそれぞれ O_K および O_F とおく。このとき、次のことが容易にわかる。

定理 1．O_K/O_F はすべての高さ 1 の素 ideal で不分岐である。

我々はこれを「A_n-部分の不分岐性」と呼び、Galois 群に加えて、これの特殊化による保存について考察する。表題の「Hilbert の既約性定理のある類似」をはっきりさせるために、定理と類似を列挙しよう：

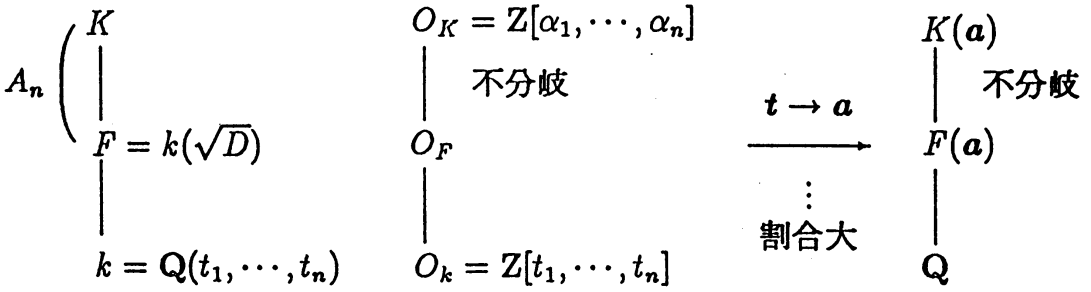
定理（定量化版）：（密度の意味で）ほとんどすべての特殊化は Galois 群を保存する。

我々の類似：大きな割合の特殊化が Galois 群に加えて、A_n-部分の不分岐性を保存する。

定理 1 は共役差積

$$D(K/F) = O_K : \{\beta \in O_K \mid \text{任意の} \alpha \in O_K \text{に対して、} T_{K/F}(\alpha\beta) \in O_F\}$$

を用いると、簡単に $D(K/F) = O_K$ と表わされる。



3 Preliminaries

この節では、$f(X)$ を $\mathbf{Z}$ 上の monic 既約多項式、Kをその最小分解体、$F = \mathbf{Q}(\sqrt{D})$ (Dは $f(X)$ の判別式) とし、K/Fが (すべての有限素点で) 不分岐となるための条件について述べる。(以下、無限素点の分岐は考えない。) そのためにまず、pを素数とし、

(ur,p) K/Fは p 上のすべての素点で不分岐

となるための十分条件を列挙する :

(i) $f(X) \bmod p$は重根を持たないか、または、ただ1つの重根を持ち、その重複度は2。

(ii) $f(X) \bmod p$ と $f'(X) \bmod p$ の最大公約数の次数は高々1。

(iii) $p^2 \nmid D$.

(iv) $p \nmid D$.

容易にわかるように

$$\text{(i)} \Longrightarrow \text{(iii)} \Longrightarrow \text{(ii)} \Longrightarrow \text{(i)} \Longrightarrow \text{(ur, p)}$$

である。ここで、注意すべきことは、これらの条件はすべて$f(X)$ の係数の mod p 冪に関する合同条件であることである。これらをまとめると次の定理が得られる :

定理2. 次の条件 (1)-(4) のうちの1つが成り立てば、Kは F上不分岐な ($D(K/F) = O_K$なる) $\mathbf{Q}$ の S_n-拡大である。

(1) すべての素数 p に対して、(i) が成立。

(2) $(D, R_1) = 1$.

(3) Dは squarefree.

(4) Dは素数。

(2) で、R_1は $f(X)$ と $f'(X)$ の終結式 (行列式) の (最後の2行2列を除いて得られる行列の) 小行列式である。

注意. 不分岐性に関する条件がすべての素数 p に対して満たされると、同時に、$\mathrm{Gal}(K/\mathbf{Q}) = S_n$ がしたがう。定理の条件 (2) および (3) はそれぞれ、すべての素数 p に対して、(ii) および (iii) が成立するということと同値である。既約多項式の判別式は必ずある素数 p で割れるので、すべての素数 p に対して、(iv) が成立することはない。

上の定理に対応して、n 次体の Galois 閉包を取ったとき、上のような $\mathbf{Q}$ の S_n-拡大が生じるための条件については、次が成り立つ：

定理３． Eを n 次体とし、Dをその判別式とする。このとき、次の条件 (a)-(c) のうちの１つが成り立てば、Eの Galois 閉包はその２次部分体上不分岐な $\mathbf{Q}$ の S_n-拡大である。

(a) すべての素数 p に対して、p は Eで不分岐であるか、または、ただ１つの分岐素因子を持ち、その分岐指数は２で、剰余次数は１。

(b) Dは squarefree.

(c) Dは素数。

4 The rate of the preservation of the unramifiedness of the A_n-part

主張 (P) の「割合」を formulate するために、まず、n 次の有理整係数 monic 多項式 $f(X, \boldsymbol{a})$ を$\boldsymbol{a}$と同一視することにより、$\mathbf{Z}^n$の元とみなし、$\mathbf{Z}^n$の部分集合 $\mathcal{A}$ に対して、密度$\delta(\mathcal{A})$ を次のように定義する。

$$\delta(\mathcal{A}) = \lim_{N\to\infty} \frac{\#\mathcal{A}(N)}{\#\mathbf{Z}^n(N)},$$

ただし、

$$\mathcal{A}(N) = \{\boldsymbol{a} = (a_1, \cdots, a_n) \in \mathcal{A} \mid |a_i| \leq N\}.$$

さて、$\mathbf{Z}^n$の部分集合 $\mathcal{A}_{S_n}$をつぎのように定義する：

$$\mathcal{A}_{S_n} = \{\boldsymbol{a} \in \mathbf{Z}^n \mid G(\boldsymbol{a}) = S_n\}.$$

ここで、$G(\boldsymbol{a})$ は $f(X, \boldsymbol{a})$ の Galois 群を表わす。このとき、Hilbert の既約性定理は簡単に、$\delta(\mathcal{A}_{S_n}) = 1$ と表現できる。したがって、密度を考え

るとき、$G(\boldsymbol{a}) \neq S_n$なる多項式はneglectしてよい。我々が、考察の対象とするのは以下の部分集合である：

$$\mathcal{A}_{ur,n} = \{\boldsymbol{a} \in \mathcal{A}_{S_n} \mid K(\boldsymbol{a})/F(\boldsymbol{a}) \text{は不分岐}\},$$

$$\mathcal{A}_{i,n} = \{\boldsymbol{a} \in \mathcal{A}_{S_n} \mid f(X,\boldsymbol{a}) \text{は定理の条件}\ (i)\ \text{をみたす}\}\ (1 \leqq i \leqq 4).$$

ここで、$K(\boldsymbol{a})$は$f(X,\boldsymbol{a})$の最小分解体、$F(\boldsymbol{a}) = \mathbf{Q}(\sqrt{D(\boldsymbol{a})})$, $D(\boldsymbol{a})$は$f(X,\boldsymbol{a})$の判別式である。

主要課題. 各$\mathcal{A}_{*,n}$は密度を持つか？　もし持つなら、それを求めよ。

この問題を考えるために、$\mathcal{A}_{*,n}(* \neq 4)$の各元の条件を素数$p$に限定したものを$\mathcal{A}^{(p)}_{*,n}$で表わす。このとき、次が成り立つ。

命題. 任意の素数pに対して、$\mathcal{A}^{(p)}_{i,n}(i = 1,2,3)$は密度を持ち、

$$\begin{aligned}
\delta(\mathcal{A}^{(p)}_{1,n}) &= \frac{z_n(p) + u^{(1)}_n(p)}{p^n} = 1 - \frac{2p^{n-2} + (-1)^n(p-1)}{p^{n-1}(p+1)},\\
\delta(\mathcal{A}^{(2)}_{2,n}) &= \delta(\mathcal{A}^{(2)}_{3,n}) = \frac{z_n(2)}{2^n} = \frac{1}{2},\\
\delta(\mathcal{A}^{(p)}_{2,n}) &= \delta(\mathcal{A}^{(p)}_{1,n})\ (p \neq 2),\\
\delta(\mathcal{A}^{(p)}_{3,n}) &= \frac{z_n(p) + u^{(1)}_n(p)(1-p^{-1})}{p^n}\\
&= 1 - \frac{3p^{n-1} - p^{n-2} + (-1)^n(p-1)}{p^{n-1}(p+1)}\ (p \neq 2).
\end{aligned}$$

ここで、$z_n(p)$, および、$u^{(1)}_n(p)$は$\mathbf{F}_p$上のn次monic多項式のうち重根を持たないものの個数、および、ただ1つの重根を持ち、その重複度が2であるものの個数を表わす：

$$\begin{aligned}
z_n(p) &= p^n - p^{n-1},\\
u^{(1)}_n(p) &= \frac{p^n - p^{n-1} + (-1)^{n-1}(p^2-p)}{p+1}.
\end{aligned}$$

予想1. $\mathcal{A}^{(p)}_{ur,n}$は密度を持ち、その密度$\delta(\mathcal{A}^{(p)}_{ur,n})$は$p$の有理式となる。$\mathcal{A}_{ur,n}$および$\mathcal{A}_{i,n}(i = 1,2,3,4)$は密度を持ち、その密度$\delta(\mathcal{A}_{*,n})(* \neq 4)$はすべての素数$p$にわたる$\delta(\mathcal{A}^{(p)}_{*,n})$の積となる：

$$\delta(\mathcal{A}_{*,n}) = \prod_p \delta(\mathcal{A}^{(p)}_{*,n})\ (* \neq 4).$$

また、

$$\delta(\mathcal{A}_{4,n}) = 0.$$

上の予想で、$\delta(\mathcal{A}_{*,n})$ が $\delta(\mathcal{A}^{(p)}_{*,n})$ の積になるという根拠は、前節で述べた不分岐性のための条件が係数に関する mod p 冪に関する合同条件で、したがって、異なる p に対しては独立であるということによる。これは、自然数の分布、例えば、squarefree な自然数の集合 S_f の密度が

$$\lim_{n\to\infty} \frac{\#S_f(n)}{n} = \prod_p (1-\frac{1}{p^2}) \ (S_f(n) = \{m \in S_f \mid m \leqq n\})$$

のような Euler 積になることの類似の高次元版とみなすと理解しやすいであろう。

予想 1 の大部分が $n = 3$ の場合は正しいことが証明された：

定理 4. $\mathcal{A}^{(p)}_{ur,3}, \mathcal{A}_{ur,3}, \mathcal{A}_{1,3}, \mathcal{A}_{2,3}$ は密度を持ち、

$$\delta(\mathcal{A}^{(p)}_{ur,3}) = 1 - \frac{p^2+1}{p^4+p^3+p^2+p+1},$$

$$\delta(\mathcal{A}_{ur,3}) = \prod_p \delta(\mathcal{A}^{(p)}_{ur,3}) = 0.7059\cdots,$$

$$\delta(\mathcal{A}_{1,3}) = \prod_p \delta(\mathcal{A}^{(p)}_{1,3}) = \prod_p (1-\frac{1}{p^2}) = \frac{6}{\pi^2} = 0.6079\cdots,$$

$$\delta(\mathcal{A}_{2,3}) = \prod_p \delta(\mathcal{A}^{(p)}_{2,3}) = \frac{4}{\pi^2} = 0.4052\cdots.$$

定理の証明は誤差項の初等的な評価による。その際、判別式の性質、および素数定理を用いた。

また、Ekedahl 氏は東大における 11 月のセミナーで、$\mathcal{A}_{1,n}$ に関する予想が一般の n に対して正しいことを証明したと発表した：

定理. (T.Ekedahl)　すべての $n \geqq 3$ に対して、

$$\delta(\mathcal{A}_{1,n}) = \prod_p \delta(\mathcal{A}^{(p)}_{1,n}).$$

残念ながら、彼は証明については触れなかったので、筆者は個人的に彼から聞いた idea の一部を頼りに、$n = 4$ の場合しかこれを確認できなかった。

さて，予想が正しいと仮定して、$\delta(\mathcal{A}_{ur,n})$ はどれくらい大きいのであろうか？ $\delta(\mathcal{A}^{(p)}_{ur,n})$ の大きさについては、次が成り立つ：

命題. 4以上の任意の自然数 n と任意の素数 p に対して、

$$\underline{\delta}(\mathcal{A}^{(p)}_{ur,n}) = \liminf_{N\to\infty} \frac{\#\mathcal{A}^{(p)}_{ur,n}(N)}{\#\mathbb{Z}^n(N)} > L_{n,p}$$

なる explicit に定まる p の有理式 $L_{n,p}$が存在して、

$$L_n = \prod_p L_{n,p} > 0.51$$

が成り立つ。また、極限

$$L_\infty = \lim_{n\to\infty} L_n = 0.5172\cdots$$

が存在し、しかも任意の $n \geqq 4$ に対して

$$|L_n - L_\infty| < 0.01$$

が成り立つ。

注意. この命題から、任意の n に対して、

$$\delta(\mathcal{A}_{ur,n}) > 0.5$$

である、したがって、(極限的には) 少なくとも半分の特殊化が A_n-部分の不分岐性を保存すると期待される。また、上からの評価については、かなりあらい評価で、

$$\overline{\delta}(\mathcal{A}^{(p)}_{ur,n}) = \limsup_{N\to\infty} \frac{\#\mathcal{A}^{(p)}_{ur,n}(N)}{\#\mathbb{Z}^n(N)} < U_{n,p} < L_{n,p} + \frac{1}{p^2(p+1)}$$

なる explicit に定まる p の有理式 $U_{n,p}$が存在して、

$$U_n = \prod_p U_{n,p} < 0.6051$$

が成り立つ。また、極限

$$U_\infty = \lim_{n\to\infty} U_n = 0.5908\cdots$$

が存在し、しかも任意の $n \geqq 5$ に対して

$$|U_n - U_\infty| < 0.01$$

が成り立つ。これらのことから、ほとんどすべての n について、$\delta(\mathcal{A}_{ur,n})$ の値はほとんど同じではないかと思われる。

5 The distribution of algebraic number fields

さて、主張 (P) を formulate しよう。(r,s) を $r+2s=n$ なる負でない有理整数の組とし、$\mathcal{F}(X)$ で実素点の個数が r で、虚素点の個数が s の n 次体で、その判別式の絶対値が X 以下のものの共役類全体を表わす。このとき、

$$N_{(r,s)}(X)=\#\mathcal{F}(X)$$

$$N_{ur,(r,s)}(X)=\#\{\{E\}\in\mathcal{F}(X)\mid E\text{の Galois 閉包が } \mathbf{Q}\text{ の } S_n\text{-拡大でその 2 次部分体上不分岐}\}$$

$$N_{sf,(r,s)}(X)=\#\{\{E\}\in\mathcal{F}(X)\mid E\text{ の判別式は squarefree}\}$$

$$N_{pr,(r,s)}(X)=\#\{\{E\}\in\mathcal{F}(X)\mid E\text{の判別式は素数}\}$$

とおく。

予想２．各 (r,s) に対して、極限

$$\rho_{*,(r,s)}=\lim_{X\to\infty}\frac{N_{*,(r,s)}(X)}{N_{(r,s)}(X)}$$

が存在して、その値は（nが一定のとき）(r,s) のえらびかたによらない。また、

$$1>\rho_{ur,(r,s)}>\rho_{sf,(r,s)}>\rho_{pr,(r,s)}=0.$$

Davenport と Heilbronn による 3 次体の分布に関する結果を使うとこの予想が $n=3$ の場合はおおむね正しいことが証明される：

定理５．

$$\rho_{ur,(3,0)}=\rho_{ur,(1,1)}=\frac{\zeta(3)}{\zeta(2)}=0.7307\cdots,$$

$$\rho_{sf,(3,0)}=\rho_{sf,(1,1)}=\frac{2\zeta(3)}{3\zeta(2)}=0.4801\cdots.$$

ここで、$\zeta(s)$ は Riemann zeta である。

さて、一般の n について、$\rho_{ur,(r,s)},\rho_{sf,(r,s)}$はどれくらい大きいのであろうか？　代数体の分布に関する次の conjectural asymptotic law

$$\#\{E(\subset\mathbf{C})\mid[E:\mathbf{Q}]=n,E\text{の判別式の絶対値}\leqq X\}\sim\frac{X}{\zeta(n)}$$

(これは $n=2$ および、$n=3$ のとき正しい。ここでは、共役な体は別なものとして数えていることに注意。) を説明する heuristic principle と同じ idea から次のことが期待される：

$$\rho_{ur,(r,s)} \geqq \frac{\prod_p (1+p^{-1})}{\prod_p (1+p^{-1}+\cdots+p^{-(n-1)})} = \frac{\zeta(n)}{\zeta(2)} > \frac{1}{\zeta(2)} = \frac{6}{\pi^2} = 0.6079\cdots,$$

$$\rho_{sf,(r,s)} \geqq \frac{1}{1+2^{-1}} \cdot \frac{\prod_p (1+p^{-1})}{\prod_p (1+p^{-1}+\cdots+p^{-(n-1)})} = \frac{2\zeta(n)}{3\zeta(2)} > \frac{4}{\pi^2} = 0.4052\cdots.$$

これらのもとになる idea は、次のようである。E を n 次体とし、その判別式を D とする。まず、$p > n$ ならば、

$$p^0, p^1, \cdots, p^{n-1} \parallel D$$

のいずれかである。しかも、それぞれそうなる頻度は均等であると思われる。$p \leqq n$ のときも「平均的」には (つまり E が動くとき)、これと同等のことが成り立つとみなせる。つまり、代数体の判別式は、平均的には、各素数について、上のように均等に分布していると考えられる。したがって、判別式の絶対値が一定数以下の n 次体の個数を数える数列の母関数は平均的には

$$\prod_p (1+p^{-s}+\cdots+p^{-(n-1)s})$$

であると考えられる。これから、上の asymptotic law がしたがう。また、E が 3 節の定理 3 の条件 (a) をみたす n 次体を動くときは、$p > n$ ならば、$p^0 \parallel D$, または $p^1 \parallel D$ であるから、上と同様な考え方により、$\rho_{ur,(r,s)}$ についての不等式がしたがう。

参考文献

[1] H. Davenport and H. Heilbronn, *On the density of discriminants of cubic fields II, Proc. Roy. Soc. London* A **322**(1971), 405–420.

[2] J. P. Serre, *Une ≪formul de masse≫ pour les extensions totalement ramifiées des degré donné d'un corps local, C. R. Acad. Sc. Paris* **286**(1978), 1031–36.

[3] B. L. van der Waerden, *Die Seltenheit der Gleihungen mit Affect, Math. Ann.* 109(1934), 13–16.

[4] D. J. Wright, *Distribution of discriminants of abelian extensions, Proc. London Math. Soc.* (3) 58(1989), 17–50.

[5] K. Yamamura, *Some analogue of Hilbert's irreducibility theorem and the distribution of algebraic number fields,* to appear in *J. Fac. Sci. Univ. Tokyo* 38(1991).