数理解析研究所講究録 1274 巻 2002 年 157-162

Distribution of units of an algebraic number field

名城大学理工学部 北岡良之 (Yoshiyuki Kitaoka)

Department of Mathematics, Meijo University

F を代数体としその整数環を o_F、単数群を $o_F^\times$ とする。知りたいのはその分布である。もっともこれは漠然とした問いであり定式化の仕方でいろいろなアプローチがあろう。私がこれを気にしだしたのは別の問題をやっていて比較的自由に扱える体を欲しくなり実2次体上の ray class field を候補としたのであるがその拡大次数すら本当に具体的には書き下せないことを改めて実感したことによる。従ってここでのアプローチは類体論と解析数論を念頭に置くこととし F の整イデアル $\mathfrak{n}$ に対し $E(\mathfrak{n}) := \{u \bmod \mathfrak{n} \mid u \in o_F^\times\}$、$I(\mathfrak{n}) := [(o_F/\mathfrak{n})^\times : E(\mathfrak{n})]$、と置き $I(\mathfrak{n})$ を調べることである。それは F の導手が $\mathfrak{n}$ の ray class field の F 上の拡大次数の分岐部分である。Lenstra は F の素イデアル $\mathfrak{p}$ で以下の条件を満たすものの集合が Dirichlet 式密度をもつことを示した。

F のガロア拡大 K と、$Gal(K/F)$ の共役類の集合 C を与えた時 $I(\mathfrak{p})$ が任意にあらかじめ与えられた数を割り、$\mathfrak{p}$ の Frobenius automorphism が C にはいる。

従って1次の素イデアル以外は無視されるが以下の我々の見方だと2次以上の素イデアルも対象となる。

講演のときはガロア拡大を仮定したがここではそれを外す。

代数体 $F \subset K$ を固定し K は $\mathbb{Q}$ 上のガロア拡大であり $o_F^\times$ は無限群と仮定する。K は F の $\mathbb{Q}$ 上のガロア閉包とは限っていない。$\eta \in Gal(K/\mathbb{Q})$ を任意に固定する。K_n で K に $o_K^\times$ の全ての n 乗根を添加した体とする。

$$E(\mathfrak{n}) := \{u \bmod \mathfrak{n} \mid u \in o_F^\times\},\ I(\mathfrak{n}) := [(o_F/\mathfrak{n})^\times : E(\mathfrak{n})]$$

と置く。そうすると

Distribution of units

Lemma 1 *Let $g(x)$ be a polynomial in $\mathbb{Z}[x]$ such that*

$$W_1(g(x)) := \{\epsilon^{g(\eta)} \mid \epsilon \in o_F^\times\}$$

is a finite group. We fix a primitive polynomial $g(x)$ of minimal degree. Then it divides $x^d - 1$ for $d := [\langle\eta\rangle : \langle\eta\rangle \cap Gal(K/F)]$.

が成り立ち $g(x)$ をここでのものとし $d := [\langle\eta\rangle : \langle\eta\rangle \cap Gal(K/F)]$ に対し

$$h(x) := (x^d - 1)/g(x)\,(\in \mathbb{Z}[x]), \quad \delta_1 := \#W_1(g(x))$$

と置く時、K の素イデアル $\mathfrak{P}$ の Frobenius automorphism $((K/\mathbb{Q})/\mathfrak{P})$ が η になるとき $\mathfrak{P}$ の下にある F の素イデアルや素数 p を η に対応するということにすると ($p \nmid 2dK$ は仮定)

Lemma 2 *If a prime number p ($\nmid 2dK$) corresponds to η, then δ_1 divides $h(p)$.*

Lemma 3 *Let m be a natural number and p a prime number corresponding to η and we take a prime ideal $\mathfrak{P}_m$ of K_m lying above p and put $\mathfrak{p} = \mathfrak{P}_m \cap F$. Then we have*

$$\frac{mh(p)}{\delta_1} \mid I(\mathfrak{p}) \iff \begin{cases} m \mid \delta_1 g(p) \text{ and} \\ \sqrt[m]{\epsilon}^{\delta_1 g(p)} \equiv 1 \bmod \mathfrak{P}_m \text{ for } {}^\forall\epsilon \in o_F^\times. \end{cases}$$

が成り立つことは容易にわかる。

Lemma 4 *Let m be a natural number and $\mathfrak{p}$ a prime ideal of F corresponding to η and we take a prime ideal $\mathfrak{P}_m$ of K_m lying above $\mathfrak{p}$ such that $\rho := ((K_m/\mathbb{Q})/\mathfrak{P}_m)$ is identical with η on K, and let p be a prime number lying below $\mathfrak{p}$. If $p \nmid m$ moreover, then we have*

$$\frac{mh(p)}{\delta_1} \mid I(\mathfrak{p}) \iff \sqrt[m]{\epsilon}^{\delta_1 g(\rho)} = 1 \text{ for } {}^\forall\epsilon \in o_F^\times.$$

さて自然数 δ_0 を

$$\sqrt[\delta_0]{\epsilon}^{\delta_1 g(\rho)} = 1 \text{ for } {}^\forall\epsilon \in o_F^\times \text{ and for } {}^\forall\rho$$

を満たす最大のものにとる（存在証明は必要）。ただし, ρ は $\rho_{|K} = \eta$ を満たす $\mathbb{C}$ の同型写像である。そうすると、

$$\ell(p) := \delta_0 h(p)/\delta_1 \mid I(\mathfrak{p})$$

であり $g(x)$, δ_1, $h(x)$ は F の $\mathbb{Q}$ 上のガロア閉包 F_0 や $\eta_{|F_0}$ にのみに依っているが δ_0, $\ell(p)$ は K に依っている。

これらのことに注意し、 K_η で η で固定される K の部分体とおき、自然数 m に対して

$$H_m(\eta) := \{\rho \in Gal(K_m/\mathbb{Q}) \mid \rho_{|K} = \eta \text{ and } \sqrt[m]{\epsilon}^{\delta_1 g(\rho)} = 1 \text{ for } {}^\forall\epsilon \in o_F^\times\}$$

と置くと

Proposition 1 *Let m be a natural number. Denoting a prime ideal of F (resp. K_η) by $\mathfrak{p}$ (resp. $\mathfrak{p}_\eta$) and a prime number lying below them by p, we have*

$$\begin{aligned} & \#\{\mathfrak{p} \mid p \le x,\ p \nmid 2mdK,\ mh(p)/\delta_1 \mid I(\mathfrak{p}),\ \textit{and } \mathfrak{p} \textit{ corresponds to } \eta\ \} \\ = \quad & [\{\sigma \in Gal(K/F) \mid \sigma\eta = \eta\sigma\} : Gal(K/F) \cap \langle\eta\rangle]^{-1} \times \\ & \#\left\{ \mathfrak{p}_\eta \;\middle|\; \begin{array}{l} p \le x,\ p \nmid 2mdK,\ \textit{and } ((K_m/K_\eta)/\mathfrak{P}_m) \in H_m(\eta) \\ \textit{for some ideal } \mathfrak{P}_m \textit{ of } K_m \textit{ lying above } \mathfrak{p}_\eta \end{array} \right\}. \end{aligned}$$

がわかり Chebotarev の定理から

Theorem 1 *Let m be a natural number. Denoting a prime ideal of F by $\mathfrak{p}$ and a prime number lying below it by p, we have*

$$\begin{aligned} & \#\{\mathfrak{p} \mid p \le x,\ p \nmid 2mdK,\ mh(p)/\delta_1 \mid I(\mathfrak{p}),\ \textit{and } \mathfrak{p} \textit{ corresponds to } \eta\ \} \\ \sim \quad & [\{\sigma \in Gal(K/F) \mid \sigma\eta = \eta\sigma\} : Gal(K/F) \cap \langle\eta\rangle]^{-1} \frac{\#H_m(\eta)}{[K_m : K_\eta]} \mathrm{Li}(x). \end{aligned}$$

を得、次の予想に至る。

Conjecture. *Let δ be a natural number. Setting*

$$\kappa(\eta;\delta) := [\{\sigma \in Gal(K/F) \mid \sigma\eta = \eta\sigma\} : Gal(K/F) \cap \langle\eta\rangle]^{-1} \sum_{m=1}^{\infty} \frac{\mu(m)\#H_{\delta m}(\eta)}{[K_{\delta m} : K_\eta]},$$

and denoting a prime number and a prime ideal of F by $p, \mathfrak{p}$ $(\mathfrak{p} \mid p)$ we have

$$\begin{aligned} & \#\{\mathfrak{p} \mid p \le x,\ p \nmid 2dK,\ I(\mathfrak{p}) = \delta h(p)/\delta_1,\ \textit{and } \mathfrak{p} \textit{ corresponds to } \eta\ \} \\ \sim \quad & \kappa(\eta)\mathrm{Li}(x). \end{aligned}$$

Distribution of units

これは一般化されたリーマン予想を仮定すれば $K = F$ が実二次体のとき、または $\eta \in Gal(K/F)$ のときは正しい。後者は Lenstra の結果に帰着される。上のように定式化してしまえば **Conjecture** に至る諸結果の証明は分岐理論の簡単な演習である。

$\kappa(\eta;\delta) > 0$ を調べるために次のことを使う。

$$[K_m : K] = [K_b : K][K_a : K],\ K_a \cap K_b = K,\ [K_b : K] = b^r\varphi(b),$$

但し、$m = ab$ は $(b, 2adK) = 1$, を満たし $r = \dim_{\mathbb{Q}}(o_K^{\times} \otimes_{\mathbb{Z}} \mathbb{Q})$ であり φ は オイラーの関数である。従って, K_a と K_b は線形無関連であり $\delta = \gamma_1\gamma_2$ が $(\gamma_2, 2dK) = 1$, $\gamma_1 \mid (2dK)^{\infty}$ なら

$$[K_{\delta ab} : K_\eta] = [K_{\gamma_1 a} : K_\eta][K_{\gamma_2 b} : K],\ \#H_{\delta ab}(\eta) = \#H_{\gamma_1 a}(\eta)\#H_{\gamma_2 b}(\eta),$$

から

$$\begin{aligned} & [\{\sigma \in Gal(K/F) \mid \sigma\eta = \eta\sigma\} : Gal(K/F) \cap \langle\eta\rangle]\kappa(\eta) \\ = & \sum_{a \mid 2dK} \frac{\mu(a)\#H_{\gamma_1 a}(\eta)}{[K_{\gamma_1 a} : K_\eta]} \times \sum_{(b,2dK)=1} \frac{\mu(b)\#H_{\gamma_2 b}(\eta)}{[K_{\gamma_2 b} : K]} \\ = & \sum_{a \mid 2dK} \frac{\mu(a)\#H_{\gamma_1 a}(\eta)}{[K_{\gamma_1 a} : K_\eta]} \times \prod_{p \nmid 2dK} \left(1 - \frac{\#H_{\hat{p}}(\eta)}{\hat{p}^r\varphi(\hat{p})}\right), \end{aligned}$$

が従う。但し、$\hat{p} = p^{\nu_p(\gamma_2)+1}$ である。

$\#H_p(\eta)$ を具体的に求めることは易しくはないがほとんど全ての素数 p に対し $(\deg g(x))/p(p-1)$ 以下であることは次のようにわかり、$\kappa(\eta)$ が絶対収束することがわかる。$\epsilon_1, \epsilon_2, \cdots, \epsilon_r$ を K の基本単数とし $\{u_i = \epsilon_i^{c_i} \mid 1 \le i \le R\}$ が F の基本単数とする (1 の冪根の違いは除く)。素数 p がどの c_i も割らないとする。そのとき $A := (a_{ij})$ を

$$\epsilon_i^{\eta} = \alpha_i \prod_{j=1}^{r} \epsilon_j^{a_{ij}}$$

で定める。但し、α_i は K の 1 の冪根である。そうすると $g(x) = \sum_{t=0}^{n} g_t x^t$ で g_t を定め $g_A(c) := \sum_{t=0}^{n} g_t \sum_{k=0}^{t-1} c^{t-k-1}A^k$ と置くと

$$\begin{aligned} & \#H_p(\eta) \\ = & \sum_{\substack{c \bmod p \\ g(c) \not\equiv \bmod p}} \#\{\boldsymbol{b} \bmod p \mid \text{first } R \text{ entries of } g_A(c)\boldsymbol{b} \equiv 0 \bmod p\}. \end{aligned}$$

となり、更に p が A の位数を割らなければ基本単数を取り直して

$$A \equiv \begin{pmatrix} c1_s & 0 \\ 0 & A_0 \end{pmatrix} \bmod p$$

と出来る。ここで s は c の $A \bmod p$ における重複度であり c は $A_0 \bmod p$ の固有値ではなく

$$g_A(c) \equiv \begin{pmatrix} g'(c)1_s & 0 \\ 0 & (c-A_0)^{-1}(g(c)-g(A_0)) \end{pmatrix} \bmod p$$

となり $g(x)h(x) = x^d - 1$ からもし $g(c) \equiv 0 \bmod p, p \nmid d$ なら $g'(c) \not\equiv 0 \bmod p$ で $g_A(c) \not\equiv 0 \bmod p$ を得 $\#H_p(\eta) \leq (\deg g(x))/p(p-1)$ がわかり所期の評価を得る。

$\kappa(\eta;\delta) > 0$ は

$$\sum_{a|2dK} \frac{\mu(a)\#H_{\gamma_1 a}(\eta)}{[K_{\gamma_1 a} : K_\eta]} \neq 0$$

かつ $\#H_{\hat{p}} \neq [K_{\hat{p}} : K]$ ($p \nmid 2dK$) と同値である。特に

Theorem 2 *$\kappa(\eta;\delta_0)$ is positive.*

更にいくつか知りたいことがあるが δ_0、 $H_m(\eta)$ の決定は単数群へのガロア群の表現が関連していて興味がある。F はとめておいて L を K を含む $\mathbb{Q}$ 上のガロア拡大とし ρ を $Gal(L/\mathbb{Q})$ の元で $\eta = \rho_{|K}$ とするとき $\delta_0 := \delta_0(\rho, L/F)$ と $\delta_0(\eta, K/F)$ との関係はどうなるのだろうか。一般に ray class field を決めるのは大変であるが $\delta_0 h(p)/\delta_1$ に対応する体について何かわからないだろうか。

注 $g(x)$ は F が $\mathbb{Q}$ 上ガロア拡大のときは具体的にわかり、更に F が実のときは $Gal(F/\mathbb{Q}) \neq \langle\eta\rangle$ なら $h(x) = 1$ そうでなければ $h(x) = x - 1$ となる。従って F の素イデアルを導手とする ray class field は F の Hilbert 類体 ($Gal(F/\mathbb{Q}) \neq \langle\eta\rangle$ の場合) か Hilbert 類体と $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$ の合成体 ($Gal(F/\mathbb{Q}) = \langle\eta\rangle$ の場合) を含み (δ_0, δ_1 を無視すれば) それらがきっかり一致する素イデアルが密度正を持って存在するというのが予想 (+ Th.2) である。この場合類体として本質的に新しいものがないことを示唆しているともみれる。

References

[CKY] Y-M. J. Chen, Y. Kitaoka and J. Yu, *Distribution of units of real quadratic number fields,* Nagoya Math. J., **158**(2000), 167-184

[H] C. Hooley, *On Artin's Conjecture,* J. reine angew. Math., **225**(1967), 209-220.

[IK] M. Ishikawa and Y. Kitaoka, *On the distribution of units modulo prime ideals in real quadratic fields,* J. reine angew. Math., **494**(1998), 65-72.

[K1] Y. Kitaoka, *Distribution of units of a cubic field with negative discriminant* , J. of Number Theory, **91**(2001), 318-355.

[K2] Y. Kitaoka, *Distribution of units of an algebraic number field. submitted.*

[L] H. W. Lenstra, Jr., *On Artin's conjecture and Euclid' algorithm in global fields,* Inventiones math. , **42**(1977), 201-224.

[M] K. Masima, *On the distribution of units in the residue class field of real quadratic fields and Artin's conjecture* (in Japanese), RIMS *Kokyuroku*, **1026**(1998), 156-166.

[R] H. Roskam, *A quadratic analogue of Artin's conjecture on primitive roots,* J. of Number Theory, **81**(2000), 93-109.