数理解析研究所講究録
1160巻 2000年 61-65

実2次体の単数の分布について

北岡良之
(YOSHIYUKI KITAOKA)

(名大・多元数理科学研究科)

§1

F を代数体とし、漠然とはしているが、F の単数がどう分布するかを知りたいとしよう。そのための定式化の一方法として、原始根に関する Artin 予想に対する Hooley の方法を取り上げてみる。

自然数 $f_1, \cdots, f_g$ が $f_1 \le \cdots \le f_g$、$\sum_{i=1}^{g} f_i = [F:\mathbf{Q}]$ を満たすとしこれらの組を $T = (f_1, \cdots, f_g)$ と書くことにする。
F の素イデアル $\mathfrak{p}$ に対し $p\mathbf{Z} = \mathfrak{p} \cap \mathbf{Z}$ で素数 p を定め、p が F で次数 f_i の素イデアル $\mathfrak{p}_i$ 達の積に分解する、すなわち $(p) = \mathfrak{p}_1 \cdots \mathfrak{p}_g$ となる時 $\mathfrak{p}$ の型は $T = (f_1, \cdots, f_g)$ であると定義する(不分岐な素イデアルのみ考えている)。自然数 $f\,(= {}^{\exists} f_i)$ に対し

$$P_{T,f}(x) := \{F\text{の素イデアル}\ \mathfrak{p} \mid \mathfrak{p}\ \text{の型} = T, \mathfrak{p}\ \text{の次数} = f, N_{F/\mathbf{Q}}(\mathfrak{p}) \le x^f\},$$

$$E(\mathfrak{p}) := \{u \mod \mathfrak{p} \in (o_F/\mathfrak{p})^\times \mid u \equiv {}^{\exists}\mathrm{unit} \mod \mathfrak{p}\},$$

$$I(\mathfrak{p}) := [(o_F/\mathfrak{p})^\times : E(\mathfrak{p})]$$

とおく。ここで $I(\mathfrak{p})$ と F の類数の積は $\bmod\ \mathfrak{p}$ で定義された F 上の ray class field の拡大次数であることに注意しておく。このとき次のような何かある都合のいい関数 "$\ell_{T,f}$" があるものとする。

$$\text{仮定：}\quad \ell_{T,f}(\mathfrak{p}) | I(\mathfrak{p}) \quad \text{if} \quad \mathfrak{p} \in P_{T,f}(\infty).$$

このとき

$$P_{T,f}(x,n) := \#\{\mathfrak{p} \in P_{T,f}(x) \mid n | I(\mathfrak{p})/\ell_{T,f}(\mathfrak{p})\},$$
$$N_{T,f}(x) := \#\{\mathfrak{p} \in P_{T,f}(x) \mid I(\mathfrak{p}) = \ell_{T,f}(\mathfrak{p})\}$$

の漸近挙動はどうなるのだろうか？

これは $I(\mathfrak{p})$ の理論的最小値 $\ell_{T,f}(\mathfrak{p})$ が存在し、比 $I(\mathfrak{p})/\ell_{T,f}(\mathfrak{p})$ が n の倍数、$I(\mathfrak{p}) = \ell_{T,f}(\mathfrak{p})$ となる $\mathfrak{p}$ がそれぞれ密度を持って存在するかどうかを問うている。これがわかったからといって単数の分布がわかったとはとても言えないが、少なくとも多少はああそんなものかという気にはなるだろう。F が実二次体の時には ε を F の基本単数として

$$\ell_{T,f}(\mathfrak{p}) := \begin{cases} 1 & \text{if } T=(1,1), f=1 \\ p-1 & \text{if } T=(2), f=2, N_{F/\mathbf{Q}}(\varepsilon)=1 \\ (p-1)/2 & \text{if } T=(2), f=2, N_{F/\mathbf{Q}}(\varepsilon)=-1 \end{cases}$$

が都合のよい関数となることを報告するのが講演の目的であった。

戦略としてまず条件 $n|I(\mathfrak{p})/\ell_{T,f}(\mathfrak{p})$ を何かある体の Frobenius 写像 の言葉で記述し Chebotarev の密度定理を使って $P_{T,f}(x,n)$ を処理する。

次にそれを使って $N(T,f)(x)$ の漸近挙動を調べる。そのために

$$N_{T,f}(x,\eta) := \#\{\mathfrak{p} \in P_{T,f}(x) \mid q \nmid I(\mathfrak{p})/\ell_{T,f}(\mathfrak{p}) \text{ for } {}^{\forall}q \le \eta\}$$
$$M_{T,f}(x,\eta_1,\eta_2) := \#\{\mathfrak{p} \in P_{T,f}(x) \mid q | I(\mathfrak{p})/\ell_{T,f}(\mathfrak{p}) \text{ for } \eta_1 < {}^{\exists}q \le \eta_2\}$$

とおく。但し、q は素数を表すものとする。このとき $\xi < x$ に対し次の簡単な（定義からすぐにわかる）不等式が基本となる。

$$N_{T,f}(x,\xi) - M_{T,f}(x,\xi,\infty) \le N_{T,f}(x,\infty) = N_{T,f}(x) \le N_{T,f}(x,\xi)$$

ここで $N_{T,f}(x,\xi)$ が $N_{T,f}(x)$ の主要項に、$M_{T,f}(x,\xi,\infty)$ が誤差項になるように ξ を取りたい（実際、実二次体のときはそれが可能である）。

$N_{T,f}(x,\xi)$ から以下の方針で主要項を取り出す。ξ 以下のすべての素数で割れないということは $Q(\xi) := \prod_{q\le\xi} q$ と互いに素ということと同じである (q は素数を表すものとする)。従って

$$\begin{aligned}
N_{T,f}(x,\xi) &= \#\{\mathfrak{p}\in P_{T,f}(x) \mid (I(\mathfrak{p})/\ell_{T,f}(\mathfrak{p}), Q(\xi)) = 1\} \\
&= \sum_{\substack{\mathfrak{p}\in P_{T,f}(x) \\ (I(\mathfrak{p})/\ell_{T,f}(\mathfrak{p}),Q(\xi))=1}} 1 = \sum_{\mathfrak{p}\in P_{T,f}(x)} \sum_{n|(I(\mathfrak{p})/\ell_{T,f}(\mathfrak{p}),Q(\xi))} \mu(n) \\
&= \sum_{n|Q(\xi)} \mu(n) \sum_{\substack{\mathfrak{p}\in P_{T,f}(x) \\ n|I(\mathfrak{p})/\ell_{T,f}(\mathfrak{p})}} 1 = \sum_{n|Q(\xi)} \mu(n) P_{T,f}(x,n)
\end{aligned}$$

となる。ここで前の $P_{T,f}(x,n)$ の処理とあわせて (すべてがうまくいけば) $N_{T,f}(x)$ の漸近式が得られる。

§2

上の戦略が実二次体 F については一般化されたリーマン予想を仮定するとうまくいくことを示す。$\ell_{T,f}(\mathfrak{p})$ を前節のように定義する。$T=(1,1), f=1$ のとき、即ち分解する素数については既に真島一成君が数理研で報告したので残りの場合即ち $T=(2), f=2$ の時を扱う。

定理.

$$N_{T,f}(x) = c_0\mathrm{Li}(x) + O(x\log(\log x)/(\log x)^2)$$

が *generalized Rieman Hypothesis* を仮定して成り立つ。ここで c_0 は具体的に与えられる正の定数である。

証明は $P_{T,f}(x,n)$ の記述さえできれば後は Hooley のやり方をまねればよい。それについては square-free な自然数 n を $F \not\subset \mathbf{Q}(\zeta_{2n})$ となるものとする (ζ_m は 1 の原始 m 乗根)。このとき $\eta\in Gal(F(\zeta_{2n})/\mathbf{Q})$ を$\eta(\zeta_{2n}) = \zeta_{2n}^{-1}, \eta|_F \neq id.$ で定める。また

$$K_n = \begin{cases} F(\zeta_{2n},\ \sqrt[2n]{\varepsilon}) & \text{if } N_{F/\mathbf{Q}}(\varepsilon)=1, \\ F(\zeta_{2n},\ \sqrt[n]{\varepsilon}) & \text{if } N_{F/\mathbf{Q}}(\varepsilon)=-1 \end{cases}$$

で n にのみ依る体 K_n を定め、共役類 C を

$$C = \{\rho \in Gal(K_n/\mathbf{Q}) \mid \rho = \eta \text{ on } F(\zeta_{2n}), \rho^2 = id.\}$$

とする。この時 C は $Gal(K_n/\mathbf{Q})$ の中心に属す。条件 n が $I((p))/\ell_{T,f}((p))$ を割ることと $F \not\subset \mathbf{Q}(\zeta_{2n})$ かつ p の上にある K_n の素イデアル $\mathfrak{P}$ に対するフロベニウス写像が C に属することは同値である。(p は F で不分解の時のみ考えている。) 従って

Chebotarev Density Theorem. $\pi_C(x, K_n)$ で x 以下の素数で K_n で不分岐かつ対応するフロベニウス写像が C に属するものの個数とすると $G.R.H.$ の仮定の下に

$$|\pi_C(x, K_n) - \frac{\#(C)}{[K_n : \mathbf{Q}]}\mathrm{Li}(x)| < \kappa \frac{\#(C)}{[K_n : \mathbf{Q}]}\sqrt{x}\log(dK_n x^{[K_n:\mathbf{Q}]})$$

が成り立つ。ここで κ は絶対定数であり dK_n は K_n の判別式の絶対値である。

を使うことによって $d(n) = \#(C)/[K_n : \mathbf{Q}]$ とおくと定理の c_0 は$\sum_{n=1}^{\infty} \mu(n)d(n)$ であることがわかる。ここで具体的に

$$d(n) = \begin{cases} (2n\varphi(n))^{-1} & \text{if } N_{F/\mathbf{Q}}(\varepsilon) = -1, 2 \nmid n, F \not\subset \mathbf{Q}(\zeta_n), \\ (n\varphi(2n))^{-1} & \text{if } \begin{cases} N_{F/\mathbf{Q}}(\varepsilon) = 1, 2|n, \sqrt{\varepsilon} \in F(\zeta_{2n}), \\ \eta(\sqrt{\varepsilon})\sqrt{\varepsilon} = 1, F \not\subset \mathbf{Q}(\zeta_{2n}), \end{cases} \\ (2n\varphi(n))^{-1} & \text{if } N_{F/\mathbf{Q}}(\varepsilon) = 1, 2 \nmid n, \sqrt{\varepsilon} \in F(\zeta_{2n}), F \not\subset \mathbf{Q}(\zeta_{2n}), \\ (2n\varphi(2n))^{-1} & \text{if } N_{F/\mathbf{Q}}(\varepsilon) = 1, \sqrt{\varepsilon} \notin F(\zeta_{2n}), F \not\subset \mathbf{Q}(\zeta_{2n}), \\ 0 & \text{if otherwise.} \end{cases}$$

である。これを使えば、例えば $N_{F/\mathbf{Q}}(\varepsilon) = -1$ かつ dF が偶数の時には

$$c_0 = \prod_p (1 - 1/p(p-1)) \quad (= \text{Artin's constant})$$

となる。

ところで F が実二次体の場合, もし p が remain prime なら F に 1 の p 乗根を添加した体が $\ell_{T,f}(\mathfrak{p})$ $(T=(2), f=2)$ を, もし p が分解するなら F 自身が $\ell_{T,f}(\mathfrak{p})$ $(=1)$ $(T=(1,1), f=1)$ を与えると見て良いと思うが一般の体ではどうなるのだろうか? 即ち $\ell_{T,f}(\mathfrak{p})$ に対応すると思われる拡大体は何であろうか?