

Ideal Class Groups and Diophantine Equations

学習院大理 中野 伸 (Shin Nakano)

§ 0.

有限次代数体 K の ideal 類群を $C(K)$ で表わし、素数 ℓ に対して

$$C_{\ell}(K) = \{ c \in C(K) ; c^{\ell} = 1 \}, \quad \rho_{\ell}(K) = \dim C_{\ell}(K)$$

とおく. ここで $\dim$ は $\mathbb{Z}/\ell\mathbb{Z}$ -space としての次元を意味する. 本稿で扱うテーマは $C(K)$ の ℓ -rank、すなわち $\rho_{\ell}(K)$ の (下からの) 評価である. 詳しくいえば、いろいろな条件 (例えば $\mathbb{Q}$ 上の次数や無限素点の分布など) の付いた代数体 K で $\rho_{\ell}(K)$ が大きいものを作るのが目標である.

一般に、 $[K:\mathbb{Q}]$ の約数である素数 ℓ に対する $\rho_{\ell}(K)$ (あるいはもっと深く $C(K)$ の ℓ -part) は詳しく調べることができる. それは、種の理論やそれに付随する手法が有効だからである. この場合については § 1 で少しふれる. 一方、 $[K:\mathbb{Q}]$ を割らない素数 ℓ について $\rho_{\ell}(K)$ の良い評価を与えることは易しくないようである. しかし、ある種の不定方程式を通して、この問題にアプローチすることが可能である (§ 2, § 3). 特に、 $\ell = 2$ で K が 3 次体の場合、対応する不定方程式はひとつの楕円曲線を定義する. そこでは、楕円曲線の有理点

のなす群 (Mordell-Weil群) と $C_2(K)$ との関係を見ることが興味深くまた重要である。§ 4 では、このような方法で得られた 3 次巡回体に関する Washington の結果を紹介し、§ 5 でその精密化について報告する。§ 5 の考察は、お茶の水女子大学の川内真由美氏との共同研究によるものである。

§ 1.

まず、 $K^\times/K^{\times, \ell}$ の部分群 $H_\ell(K)$ を次のように定義する；

$$H_\ell(K) = \{ a \in K^\times/K^{\times, \ell} ; (a) = \mathcal{O}^\ell, \text{ for some ideal } \mathcal{O} \text{ of } K \}.$$

$a \in H_\ell(K)$ に対し $\mathcal{O}^\ell = (a)$ なる K の ideal $\mathcal{O}$ をとり、その class を対応させることにより、 $H_\ell(K) \rightarrow C_\ell(K)$ なる全射準同型が定義できる。その核は、 K の単数群を U_K と書けば、 $U_K K^{\times, \ell}/K^{\times, \ell}$ となる。それを $U_\ell(K)$ で表わせば、最も基本的な完全系列

$$(1) \quad 1 \longrightarrow U_\ell(K) \longrightarrow H_\ell(K) \longrightarrow C_\ell(K) \longrightarrow 1$$

を得る。ここで r_K を K の単数群の rank、 w_K を K に属する 1 のべき根の個数とすると、 ℓ が w_K の約数であるかないかにしたがって $\dim U_\ell(K) = r_K + 1$ または r_K となるから、次の等式を得る。

$$\rho_\ell(K) = \begin{cases} \dim H_\ell(K) - r_K - 1 & (\ell | w_K) \\ \dim H_\ell(K) - r_K & (\ell \nmid w_K). \end{cases}$$

したがって、いかにして $H_\ell(K)$ が多くの独立な元を持つようになるかが問題となる。

ここで、まず初めに $[K:Q] = \ell$ の場合を考える。素数 p が K/Q で分岐する、すなわち $(p) = \mathfrak{p}^k$ ならば $p \in H_\ell(K)$ とみなせる。さらにそのような素数全体は、例外的なケースを除いて $K^\times/K^{\times\ell}$ において $\mathbb{Z}/\ell\mathbb{Z}$ 上独立となる。したがって、その個数を t とすると $\dim H_\ell(K) \geq t$ 。

$$\therefore \rho_\ell(K) \geq t - r_K - 1 \quad \text{or} \quad t - r_K.$$

これにより $\rho_\ell(K)$ がいくらでも大きい ℓ 次体 K をたくさん作ることができる。 $\ell \nmid [K:Q]$ のときも同様の議論が成り立つ。このような考察は類体論との組合せによって種の理論へと展開し、 $C(K)$ の ℓ -part についてのより精密な議論を可能にする（詳しくは Gras[2], Ishida[4], Yahagi[15]などを参照）。

§ 2.

次に $\ell \nmid [K:Q]$ の場合にも有効であるような一つの方法をあげよう。そこでは、ある種の不定方程式が重要な役割を果たす。

$f(X) \in \mathbb{Z}[X]$ を monic な既約多項式、 θ をそのひとつの根とし $K = \mathbb{Q}(\theta)$ とする。いま、不定方程式

$$(2) \quad f(X) = \pm Y^\ell$$

の s 個の解 $(X, Y) = (A_i, C_i) \ (1 \leq i \leq s)$ が $(f'(A_i), C_i) = 1$ をみたすとする。このとき $\theta - A_i \bmod K^{\times\ell} \in H_\ell(K)$ なることが容易に示される。さらに、ある条件のもとで $\theta - A_1, \dots, \theta - A_s$ は $K^\times/K^{\times\ell}$ で独立となる。したがって、 $\dim H_\ell(K) \geq s$ 。

$$\therefore \rho_k(K) \geq s - rk - 1 \quad \text{or} \quad s - rk.$$

つまり、大まかに言って、不定方程式 (2) の解がたくさんあれば、 $\rho_k(K)$ の下からの良い評価が得られるわけである。最も簡単な例をあげよう。

例 1 (実 2 次体)

ℓ を奇素数とし $f(X) = X^2 - (p^{2\ell} + q^{2\ell})$ なる形の 2 次多項式を考える。ここで、 p, q は相異なる奇素数である。 $K = \mathbb{Q}(\theta)$, $\theta^2 = (p^{2\ell} + q^{2\ell})$ とおく。

$$f(p^\ell) = -q^{2\ell}, \quad f'(p^\ell) = 2p^\ell \not\equiv 0 \pmod{q},$$

より $\theta - p^\ell \pmod{K^{x\ell}} \in H_\ell(K)$, 同様に $\theta - q^\ell \pmod{K^{x\ell}} \in H_\ell(K)$ となる。ここで

$$(3) \quad p \equiv q \equiv 1 \pmod{\ell}, \quad \left(\frac{2}{p}\right)_\ell \neq 1, \quad \left(\frac{2}{q}\right)_\ell \neq 1$$

なる条件のもとで、 $\theta - p^\ell$, $\theta - q^\ell$ が $K^x/K^{x\ell}$ で独立となることが次のようにして示される。まず $\mathfrak{p} = (p, \theta + q^\ell)$ は K の 1 次の素idealとなり $\sigma_K/\mathfrak{p} \simeq \mathbb{Z}/p\mathbb{Z}$ が成り立つ。いま、ある $a, b \in \mathbb{Z}/\ell\mathbb{Z}$ に対して $(\theta - p^\ell)^a (\theta - q^\ell)^b \in K^{x\ell}$ とする。

$$(\theta - p^\ell)^a (\theta - q^\ell)^b \equiv (-q^\ell)^a (-2q^\ell)^b = (\pm q^{a+b})^\ell 2^b \pmod{\mathfrak{p}}$$

であるが、(3) より 2 は $\pmod{\mathfrak{p}}$ で ℓ べき剰余でないから $b = 0$ 、同様にして $a = 0$ を得る。よって独立性がいえた。したがって $\dim H_\ell(K) \geq 2$ 。いまの場合 $w_K = 2$, $r_K = 1$ だから $\rho_k(K) \geq 1$ 。すなわち K の類数は ℓ で割れる。さらに (3) をみたす p, q を走らせることにより、このような実 2 次体が無数に存在することが示される。 (例 1 終)

上の議論を少し修正して l が素数でないときにも同様の結果を得ることができ、すなわち “実 2 次体で類数が与えられた自然数で割り切れるものが無数に存在する。” この結果は 1970 年代初めに、Yamamoto[16], Weinberger[14] によって証明されている。また上の方法を、精密化、一般化することにより、高次の代数体についていくつかの結果を示すことができる (Nakano[8], [9], [11])。この場合にも $Y^n = \pm f(X)$ なる形の不定方程式が重要な役割を果たしている。

§ 3.

以下、特に $l = 2$ の場合について考える。この場合を特別視するのはいくつかの理由がある。ひとつは、 $C_2(K)$ を考えることは、類体論により、 K 上の指数 2 の不分岐 Kummer 拡大を考えることと同値であること、もうひとつは、不定方程式 $Y^2 = f(X)$ の扱い易さである。特に $\deg f(X) = 3$ のときは楕円曲線が考察の対象となる。これについては後で詳しく述べる。

さて、§ 1 で述べたことから $[K:Q]$ が偶数の場合は除いてもよい。以下、 $[K:Q]$ は奇数とする。まず $H_2(K)$ の部分群

$$H_2^+(K) = \{ a \in H_2(K) ; a \equiv \text{square (mod 4), and } a \text{ is totally positive. } \}$$

を考える。これが well-defined であることはすぐにわかる。類体論と Kummer 拡大の分岐理論より $\rho_2(K) = \dim H_2^+(K)$ が成り立つ。 $H_2^+(K)$ の定義は $H_2(K)$ に比べて条件がきついが、 $\rho_2(K)$ の評価に際して K の単数群の影響を受けない

分、扱い易いといえる。実際、奇素数に対してよりも良い評価が得られることがある (Nakano[9], [10])。ひとつの例をあげよう。

例 2 (奇数次純代数体)

奇数 $n (>1)$ に対して、 n 次純代数体の ideal 類群の 2-rank について考える。

まず、

$$D(X, Y, Z) = \frac{X^2+Y^2+Z^2}{4} - \frac{XY+YZ+ZX}{2}$$

なる対称式の 3 通りの表現

$$D(X, Y, Z) = \left(\frac{-X+Y+Z}{2}\right)^2 - YZ = \left(\frac{X-Y+Z}{2}\right)^2 - ZX = \left(\frac{X+Y-Z}{2}\right)^2 - XY$$

に着目して

$$A_1 = yz, \quad C_1 = \frac{-x^n+y^n+z^n}{2},$$

$$A_2 = zx, \quad C_2 = \frac{x^n-y^n+z^n}{2},$$

$$A_3 = xy, \quad C_3 = \frac{x^n+y^n-z^n}{2}.$$

とおくと

$$D(x^n, y^n, z^n) = C_1^2 - A_1^n = C_2^2 - A_2^n = C_3^2 - A_3^n$$

が成り立つ。すなわち $f(X) = X^n + D(x^n, y^n, z^n)$ とおくと $(X, Y) = (A_i, C_i)$

は $Y^2 = f(X)$ の解となる。 $K = \mathbb{Q}(\theta)$, $\theta^n = D(x^n, y^n, z^n)$ とする。例 1 の方法

を少し修正することにより、うまく $x, y, z \in \mathbb{Z}$ を選べば $\theta^d + A_i^d \bmod K^{\times 2} \in H_2^+(K)$ ($i=1, 2, 3, d|n, d < n$)、かつ $\{\theta^d + A_i^d\}_{i=1,2,3}$ は $K^\times/K^{\times 2}$ で独立となる。すなわち $\rho_2(K) \geq 3\Delta_n$ を得る。ここで Δ_n は n より小さい n の約数の個数である。 (例 2 終)

上の例で、特に $n = 3$ の場合には、Craig[1] が

$$(4) \quad Y^2 = X^3 + D$$

なる形の不定方程式で解をたくさん持つものを与えている。彼はそれを 2 次体の ideal 類群の 3-rank に応用した (X, Y の役目を入れ換える!) が、上のような方法によって純 3 次体に応用すると “ $\rho_2(K) \geq 6$ なる純 3 次体 K が無数に存在する。” ことが証明できる (Nakano[12], $\Delta_3 = 1$ だから、上の評価より良くなっていることに注意)。一方、Kihara[5], [6] は (4) で定義される楕円曲線 E の $\mathbb{Q}$ 上の Mordell-Weil rank について考察している。 $K = \mathbb{Q}(\theta)$, $\theta^3 = D$ とするとき

$$\begin{array}{ccc} E(\mathbb{Q})/2E(\mathbb{Q}) & \longrightarrow & K^\times/K^{\times 2} \\ \downarrow & & \downarrow \\ (x, y) & \longrightarrow & \theta + x \bmod K^{\times 2} \end{array}$$

なる単射準同型があり、これにより $\text{rank } E(\mathbb{Q})$ と $\dim H_2^+(K)$ i.e. $\rho_2(K)$ が関係するのである。この例からもわかるように、一般に、不定方程式 $Y^m = f(X)$ を代数曲線とみて幾何学的に扱うのは有効であると思われる。実際、Mestre [7] はそのような方法を用いて、ideal 類群に関するいくつかの結果を得ている。

§ 4.

上で述べたように (4) で定義される楕円曲線は 2 次体の ideal 類群とも密接に関係し興味深い (Honda[3]) が、ここではそれにはふれず、別の形の楕円曲線と 3 次体の ideal 類群の 2-rank との関連を Washington の仕事を通じて見ることにする (詳細は [13] を参照)。

$f(X) \in \mathbb{Z}[X]$ を monic な 3 次既約多項式とし、 E を $Y^2 = f(X)$ で定義される $\mathbb{Q}$ 上の楕円曲線とする。 $f(X)$ のひとつの根 θ を固定し $K = \mathbb{Q}(\theta)$ とおくと

$$\begin{array}{ccc} \lambda : E(\mathbb{Q}) & \longrightarrow & K^\times / K^{\times 2} \\ \downarrow & & \downarrow \\ (x, y) & \longrightarrow & x - \theta \pmod{K^{\times 2}} \end{array}$$

なる準同型が定義できて、 $\text{Ker } \lambda = 2E(\mathbb{Q})$ となる。すなわち、単射準同型

$$\lambda : E(\mathbb{Q})/2E(\mathbb{Q}) \longrightarrow K^\times / K^{\times 2}$$

を得る。 E の 2-descent に対する Selmer 群、Shafarevich-Tate 群を、それぞれ S, III と書けば、

$$(5) \quad 1 \longrightarrow E(\mathbb{Q})/2E(\mathbb{Q}) \longrightarrow S \longrightarrow \text{III} \longrightarrow 1$$

なる完全系列が得られる。ここで、自然に $S \subset K^\times / K^{\times 2}$ とみなすことができ、準同型 $E(\mathbb{Q})/2E(\mathbb{Q}) \rightarrow S$ は上で定義した λ によって実現される。

さて、特に $m \in \mathbb{Z}$ に対し

$$f(X) = X^3 + mX^2 - (m+3)X + 1$$

なる形の多項式を考える。 $f(X)$ は任意の m に対して既約であり、その判別式は $(m^2+3m+9)^2$ 、したがって K は $\mathbb{Q}$ 上 3 次の巡回体となる。いま、 K から $\mathbb{Q}$ への norm 写像を N とし

$$H = \{ a \in H_2(K) ; Na > 0 \}, \quad U = U_2(K) \cap H$$

とおくと、これらは well-defined であり、(1) と同様の完全系列を得る；

$$(6) \quad 1 \longrightarrow U \longrightarrow H \longrightarrow C \longrightarrow 1.$$

ただし C は $C_2(K)$ の略である（以下同様）。ここで、次の仮定をおく。

仮定 $m^2 + 3m + 9$ は square-free である。

このとき $S \subset H$ であり (6) の $H \rightarrow C$ を S に制限することにより、完全系列

$$(7) \quad 1 \longrightarrow \langle -\theta \rangle K^{*2}/K^{*2} \longrightarrow S \longrightarrow C \longrightarrow 1$$

の成り立つことが証明される。（ここが Washington の証明の本質的な部分である。）ここで

$$E_0(Q) = \{ P \in E(Q) ; \lambda(P) \text{ is totally positive} \}$$

とおく。これは $E(Q)$ の部分群である。

定理 1 (Washington) 仮定のもとで

$$(i) \quad 1 \longrightarrow E_0(Q)/2E(Q) \longrightarrow C \longrightarrow \text{III} \longrightarrow 1 \text{ (exact),}$$

$$(ii) \quad 1 + \rho_2(K) \geq \text{rank } E(Q).$$

(略証) (i) は $(0, 1) \in E(Q)$, $\lambda((0, 1)) = -\theta$ に注意して、2つの完全系列 (7), (5) を並べ、

$$\begin{array}{ccccccc}
1 & \rightarrow & \langle (0,1) \rangle + 2E(Q)/2E(Q) & \rightarrow & S & \longrightarrow & C \longrightarrow 1 \\
& & \downarrow & & \parallel & & \downarrow \\
1 & \longrightarrow & E(Q)/2E(Q) & \longrightarrow & S & \longrightarrow & III \longrightarrow 1
\end{array}$$

この図式に Snake lemma を適用して、

$$\text{Ker}(C \rightarrow III) \cong \text{Coker}(\langle (0,1) \rangle + 2E(Q)/2E(Q) \rightarrow E(Q)/2E(Q)) \cong E_0(Q)/2E(Q)$$

なる同型から得られる。最後の同型は

$$\langle (0,1) \rangle + E_0(Q) = E(Q), \quad 2E(Q) \subset E_0(Q)$$

から導かれ、これにより (ii) も示される。

(略証終)

§ 5.

さて、 $f(X)$ のかわりに $g(X) = -f(-X) = X^3 - mX^2 - (m+3)X - 1$ を使うとどうなるであろうか。 E' を $Y^2 = g(X)$ によって定義される $\mathbb{Q}$ 上の楕円曲線とすると、

$$\begin{array}{ccc}
\lambda' : E'(Q)/2E'(Q) & \longrightarrow & K^\times / K^{\times 2} \\
\downarrow & & \downarrow \\
(x, y) & \longrightarrow & x + \theta \pmod{K^{\times 2}}
\end{array}$$

なる単射準同型が定義できる ($g(-\theta) = 0$ に注意)。 E' の 2-descent に対する Selmer 群、Shafarevich-Tate 群をそれぞれ S', III' で表わす。さらに

$$E'_0(Q) = \{ P \in E'(Q) ; \lambda'(P) \text{ is totally positive} \}$$

とおき、Washington のやったことをそのままこの場合に実行すれば、仮定のも
とで

$$(i)' \quad 1 \longrightarrow E'_0(Q)/2E'(Q) \longrightarrow C \longrightarrow III' \longrightarrow 1 \text{ (exact),}$$

$$(ii)' \quad 1 + \rho_2(K) \geq \text{rank } E'(Q).$$

が得られる。したがって

$$\text{系} \quad \text{仮定のもとで} \quad 1 + \rho_2(K) \geq \max \{ \text{rank } E(Q), \text{rank } E'(Q) \}.$$

最後に E, E' を同時に用いることにより Washington の結果の精密化を行なう。
 $k = Q(i), i^2 = -1$, とおくと、 $E \ni (x, y) \rightarrow (-x, iy) \in E'$ により E, E' は k 上同型となる。そこで、この同型によって $E'(Q), E'_0(Q)$ に対応する $E(k)$ の部分群をそれぞれ E_1, E_2 と書く；

$$\begin{array}{ccc} E(k) & \cong & E'(k) \\ \cup & & \cup \\ E_1 & \cong & E'(Q) \\ \cup & & \cup \\ E_2 & \cong & E'_0(Q) \end{array}$$

このとき $E(Q) \cap E_1 = \{0\}$ 、従って $E(Q) + E_1$ は直和となる。

$$\tilde{\chi} : E(Q) + E_1 \cong E(Q) \oplus E'(Q) \rightarrow S S' \subset K^\times / K^{\times 2}$$

とすると $\text{Ker } \tilde{\chi} = 2E(k)$ が示される。(特に $2E(k) \subset E(Q) + E_1$ となる。)

そこで

$$(8) \quad 1 \longrightarrow E(Q) + E_1 / 2E(k) \longrightarrow S S' \longrightarrow III \longrightarrow 1$$

なる完全系列により Shafarevich-Tate 群の類似物 III を定義する。さらに $P = (x, y) \in E(k)$ に対してその複素共役を $\bar{P} = (\bar{x}, \bar{y}) \in E(k)$ で表わし、 $E(k)$ から $E(Q)$ への norm 写像 N を $NP = P + \bar{P}$ ($P \in E(k)$) で定義する。 $E'(k)$ か

ら $E'(Q)$ への norm 写像 N' も同様に定義する. このとき

定理 2 仮定のもとで

$$(I) \quad 1 \longrightarrow E_0(Q) + E_2/2E(k) \longrightarrow C \longrightarrow III \longrightarrow 1 \text{ (exact),}$$

$$(II) \quad 1 + \rho_2(K) \geq \text{rank } E'(Q) + \dim E_0(Q)/NE(k) \\ = \text{rank } E(Q) + \dim E'_0(Q)/N'E'(k).$$

(略証) (7) の役目を果たす完全系列として

$$1 \rightarrow \langle -\theta, -1+\theta \rangle K^{\times 2}/K^{\times 2} \rightarrow S S' \longrightarrow C \longrightarrow 1$$

をとることができる. これを、 $\tilde{\chi}((0,1)) = -\theta$, $\tilde{\chi}((-1,i)) = -1+\theta$ に注意して

(8) と共に並べ、

$$\begin{array}{ccccccc} 1 & \rightarrow & \langle (0,1), (-1,i) \rangle + 2E(k)/2E(k) & \rightarrow & S S' & \longrightarrow & C \longrightarrow 1 \\ & & \downarrow & & \parallel & & \downarrow \\ 1 & \longrightarrow & E(Q) + E_1/2E(k) & \longrightarrow & S S' & \longrightarrow & III \longrightarrow 1 \end{array}$$

Snake lemma を適用して (I) が導かれる. また、(II) は

$$\begin{array}{ccccccc} 1 & \longrightarrow & E_2/2E_1 & \longrightarrow & E_0(Q) + E_2/2E(k) & \longrightarrow & E_0(Q)/NE(k) \longrightarrow 1 \\ & & \downarrow & & & & \\ & & E'_0(Q)/2E'(Q) & & & & \end{array}$$

なる完全系列より示すことができる.

(略証終)

Washington の定理または系と比べると $\rho_2(K)$ の評価は $\dim E_0(Q)/NE(k)$ または $\dim E'_0(Q)/N'E'(k)$ の分だけ良くなっている.

最後に、 E' が E の twist のひとつになっていることを付け加えておこう。
すなわち E の他の twist について考えることも可能であり、実際、ある程度
同様の議論ができるようである。これについては別の機会にゆずることにする。

References

- [1] M. Craig, A construction for irregular discriminants, Osaka J. Math. 14(1977), 365-402.
- [2] G. Gras, Sur les ℓ -classes d'idéaux dans les extensions cycliques relatives de degré premier ℓ , Ann. Inst. Fourier 23, no. 3(1973), 1-48.
- [3] T. Honda, Isogenies, rational points and section points of group varieties, Japan. J. Math. 30(1960), 84-101.
- [4] M. Ishida, The genus fields of algebraic number fields, Lecture Notes in Math. 555, Springer-Verlag, 1976.
- [5] S. Kihara, On the rank of the elliptic curve $y^2=x^3+k$, Proc J. Acad. 63A(1987), 76-78.
- [6] S. Kihara, On elliptic curves of the form $y^2=x^3+k$ with rank at least 6 over $\mathbb{Q}$ (preprint).
- [7] J. F. Mestre, Groupes de classes d'idéaux non cycliques de corps de nombres, Séminaire Théorie des Nombres, Paris 1981-82,

Progress in Math. 38, Birkhäuser, 1983.

- [8] S. Nakano, Class numbers of pure cubic fields, Proc. Japan Acad. 59A(1983), 263-265.
- [9] S. Nakano, On ideal class groups of algebraic number fields, J. Reine Angew. Math. 358(1985), 61-75.
- [10] S. Nakano, On the construction of pure number fields of odd degrees with large 2-class groups, Proc. Japan Acad. 62A(1986), 61-64.
- [11] S. Nakano, Ideal class groups of cubic cyclic fields, Acta Arith. 46(1986), 297-300.
- [12] S. Nakano, Construction of pure cubic fields with large 2-class groups, to appear in Osaka J. Math.
- [13] L. C. Washington, Class numbers of the simplest cubic fields, Math. Comp. 48(1987), 371-384.
- [14] P. J. Weinberger, Real quadratic fields with class numbers divisible by n , J. Number Theory 5(1973), 237-241.
- [15] O. Yahagi, Construction of number fields with prescribed ℓ -class groups, Tokyo J. Math. 1(1978), 275-283.
- [16] Y. Yamamoto, On unramified Galois extensions of quadratic number fields, Osaka J. Math. 7(1970), 57-76.