代数的整数論 類体論

@alg_d

2013 年 2 月 9 日

0　初めに

この PDF は某国某所で某氏によって開催されたとあるセミナーで発表する内容をまとめたものです．当然，こんな量喋りきれるはずは無いので当日は適当に必要な部分だけ喋りますが，PDF の用量に制限は無いので書けるだけ書いています．今回の話は類体論がどういうものかを理解してもらうのが目的です．類体論をやるには当然代数的整数論の基本的な知識が必要ですが，頑張ってその辺をごまかしています．(無理なところは諦めてその辺の知識を仮定しています．) 目的が目的なので類体論の証明などは殆どやりません．というかそういうのを勉強したい方は本を読んで下さい．ドゥードゥー

1　導入　～有理数体の類体論へ～

定理 (Fermat の二平方和定理)**.** $p \neq 2$ を素数とするとき

$$\text{ある } x, y \in \mathbb{Z} \text{ が存在して } p = x^2 + y^2 \iff p \equiv 1 \pmod 4$$

証明. ($\Longrightarrow$) $p = x^2 + y^2$ と書けたとする．p は奇数だから，x を偶数 y を奇数としてよい．$x = 2x'$, $y = 2y' + 1$ と書けば

$$p = x^2 + y^2 = (2x')^2 + (2y' + 1)^2 = 4x'^2 + 4y'^2 + 4y' + 1 \equiv 1 \pmod 4$$

($\Longleftarrow$) $p \equiv 1 \pmod 4$ とする．$t^2 \equiv -1 \pmod p$ となる $t \in \mathbb{Z}$ が存在する．

∴) Wilson の定理により $(p-1)! \equiv -1 \pmod p$ である．よって $p = 4k + 1$ と書け

ば $\bmod p$ で

$$\begin{aligned}-1 &\equiv (p-1)! \\ &= \big(1\cdot 2\cdots(2k)\big)\big((2k+1)(2k+2)\cdots(p-2)(p-1)\big) \\ &= \big(1\cdot 2\cdots(2k)\big)\big((p-2k)(p-(2k-1))\cdots(p-2)(p-1)\big) \\ &\equiv (2k)!(-1)^{2k}(2k)! = ((2k)!)^2\end{aligned}$$

正整数 e を $(e-1)^2 < p < e^2$ となるように取る．

$A := \{0, 1, \cdots, e-1\}^2$ と置くと，$|A| = e^2 > p$ だから Dirichlet の抽斗論法 (鳩の巣原理) により異なる二元 $(a,b),(c,d) \in A$ が存在して $a - bt \equiv c - dt \pmod p$ となる．故に $(a-c) - (b-d)t \equiv 0 \pmod p$ となり，$(a-c)^2 + (b-d)^2 = \big((a-c) - (b-d)t\big)\big((a-c) + (b-d)t\big) \equiv 0 \pmod p$ である．故に $(a-c)^2 + (b-d)^2 > 0$ は p の倍数であるが，一方 $0 \le a, b, c, d \le e-1$ より $(a-c)^2, (b-d)^2 \le (e-1)^2$ となる．従って $(a-c)^2 + (b-d)^2 \le 2(e-1)^2 < 2p$ が分かるので $p = (a-c)^2 + (b-d)^2$ でなければならない． □

この定理はこのように初等的に証明でき，Dirichlet の抽斗論法がこの様なところに現れるのが面白いが，実はこの証明は今考えている環 $\mathbb{Z}$ を $\mathbb{Z}[i] := \{x + yi \mid x, y \in \mathbb{Z}\}$ に拡大して考えればより自然にできる．何故かというと $\mathbb{Z}[i]$ では $x^2 + y^2 = (x+yi)(x-yi)$ と書けるので，この定理は「素数 p は環 $\mathbb{Z}[i]$ でいつ分解するか?」という問題になるからである．

それを説明するため，まず $\mathbb{Z}[i]$ での《素因数分解》について述べる．自然数の素因数分解の一意性とは次のようであった．

定理. 任意の正整数 n は $n = p_1^{e_1} \cdots p_g^{e_g}$ (p_i は相異なる素数，$e_i > 0$) と (順番を除いて) 一意に書ける．

これを $\mathbb{Z}[i]$ に拡張するのであるが，その前に $\mathbb{Z}[i]$ は環であるが $\mathbb{N}$ は環でない．そこで自然数の素因数分解の一意性を環 $\mathbb{Z}$ の言葉に直しておく．

定理. 任意の整数 $n \neq 0$ は $n = w p_1^{e_1} \cdots p_g^{e_g}$ ($w = \pm 1$, p_i は相異なる素数，$e_i > 0$) と (順番を除いて) 一意に書ける．

この定理を $\mathbb{Z}[i]$ に一般化すると以下のようになる．

定義. $P \in \mathbb{Z}[i]$ が $\mathbb{Z}[i]$-素数 $\iff$ P は条件「P が xy を割り切る $\Longrightarrow$ P は x または y を

割り切る」を満たし，かつ，$\operatorname{Re} P > 0,\ \operatorname{Im} P \geq 0$
(これはここだけの用語である．)

定理. 任意の $\alpha(\neq 0) \in \mathbb{Z}[i]$ は $\alpha = wP_1^{e_1} \cdots P_g^{e_g}$ ($w \in \{\pm 1, \pm i\}$, P_j は相異なる $\mathbb{Z}[i]$-素数，$e_i > 0$) と (順番を除いて) 一意に書ける．

複素共役写像 $x + yi \longmapsto x - yi$ を ρ で表す．整域 $\mathbb{Z}[i]$ の分数体は $\mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}$ であり，体準同型 $\mathbb{Q}(i) \longrightarrow \mathbb{C}$ は id と ρ の二つしかない．

˙.˙) $\varphi\colon \mathbb{Q}(i) \longrightarrow \mathbb{C}$ を体準同型とする．(即ち $\varphi(x+y) = \varphi(x) + \varphi(y)$, $\varphi(xy) = \varphi(x)\varphi(y)$, $\varphi(1) = 1$ である．) $\varphi(0) = \varphi(0+0) = \varphi(0) + \varphi(0)$ より $\varphi(0) = 0$．正整数 n に対し

$$\varphi(n) = \varphi(1 + \cdots + 1) = \varphi(1) + \cdots + \varphi(1) = 1 + \cdots + 1 = n.$$

よって

$$0 = \varphi(0) = \varphi(n - n) = \varphi(n) + \varphi(-n) = n + \varphi(-n)$$

だから $\varphi(-n) = -n$ となる．従って任意の $n \in \mathbb{Z}$ について $\varphi(n) = n$ である．故に $\frac{n}{m} \in \mathbb{Q}$ に対して $n = \varphi(n) = \varphi(m\frac{n}{m}) = \varphi(m)\varphi(\frac{n}{m}) = m\varphi(\frac{n}{m})$ だから $\varphi(\frac{n}{m}) = \frac{n}{m}$ である．以上により，$\varphi\colon \mathbb{Q}(i) \longrightarrow \mathbb{C}$ が体準同型ならば常に「任意の $\alpha \in \mathbb{Q}$ に対して $\varphi(\alpha) = \alpha$」であることが分かる．

$\mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}$ であるから，$\varphi\colon \mathbb{Q}(i) \longrightarrow \mathbb{C}$ は $\varphi(i)$ の値によって定まる．ところが $i^2 + 1 = 0$ だから $0 = \varphi(0) = \varphi(i^2 + 1) = \varphi(i)^2 + 1$ により $\varphi(i) = \pm i$ の二通りしかない．明らかに $\varphi(i) = i$ のとき $\varphi = \mathrm{id}$，$\varphi(i) = -i$ のとき $\varphi = \rho$ である．

$N(\alpha) := \mathrm{id}(\alpha)\rho(\alpha)$ と書く．$\alpha = x + yi \in \mathbb{Z}[i]$ とすれば $N(\alpha) = (x + yi)(x - yi) = x^2 + y^2 \in \mathbb{Z}$ であり，$N(\alpha) = 1 \Longleftrightarrow x^2 + y^2 = 1 \Longleftrightarrow \alpha = \pm 1, \pm i$ となる．± 1, $\pm i$ は $\mathbb{Z}[i]$-素数でないから，$\mathbb{Z}[i]$-素数 P に対して $N(P) > 1$ である．また定義から明らかに $N(\alpha\beta) = N(\alpha)N(\beta)$ が成り立つ．

素数 $p \in \mathbb{Z} \subset \mathbb{Z}[i]$ の素因数分解が $p = wP_1^{e_1} \cdots P_g^{e_g}$ であるとする．このとき

$$p^2 = N(p) = N(wP_1^{e_1} \cdots P_g^{e_g}) = N(w)N(P_1)^{e_1} \cdots N(P_g)^{e_g}.$$

$w = \pm 1$ または $w = \pm i$ だから $N(w) = 1$ で，$N(P_j) > 1$ は有理整数だから $N(P_j) =$

p^{f_j}, $f_j > 0$ と書ける．このとき $p^2 = p^{e_1 f_1 + \cdots + e_g f_g}$ であり $2 = \sum_{j=1}^{g} e_j f_j$ が分かる．故に

$$\begin{cases} g = 1,\ e_1 = 1,\ f_1 = 2 \\ g = 1,\ e_1 = 2,\ f_1 = 1 \\ g = 2,\ e_1 = e_2 = f_1 = f_2 = 1 \end{cases}$$

のうちのどちらかである．即ち，素数 p の $\mathbb{Z}[i]$ での分解の仕方は三通りしかない．

Fermat の二平方和定理の別証明． $p \equiv 1 \pmod 4 \Longrightarrow p = x^2 + y^2$ を示す．$p \equiv 1 \pmod 4$ だから，先ほど示したように $t^2 \equiv -1 \pmod p$ なる $t \in \mathbb{Z}$ が取れる．即ち $t^2 + 1 = pm,\ m \in \mathbb{Z}$ と書ける．よって $pm = (t+i)(t-i)$ である．

上で書いたように p の分解の仕方は三通りしかないが，そのうち $g = 1,\ e_1 = 1,\ f_1 = 2$ の場合，即ち $p = wP_1$ だったと仮定する．明らかに $w = 1,\ p = P_1$ である．故に $\mathbb{Z}[i]$ での素因数分解の一意性から $t + i$ か $t - i$ は p で割り切れなければならない．しかし明らかに $\dfrac{t \pm i}{p} \notin \mathbb{Z}[i]$ であるから矛盾する．

故に $g = 1,\ e_1 = 2,\ f_1 = 1$ または $g = 2,\ e_j = f_j = 1$ である．そこで $p = wP_1P_2$ ($P_1 = P_2$ も許す) と書けば，上で書いたようにこの場合 $N(P_1) = p$ である．従って $P_1 = x + yi$ と置けば $p = N(x + yi) = x^2 + y^2$ である． □

$p \equiv 0, 2 \pmod 4$ となる素数は 2 しか存在しないが，$2 = -i(1+i)^2$ と書けて $1 + i$ は $\mathbb{Z}[i]$-素数である．以上をまとめると次の表のようになる．

$p \bmod 4$	e_i	f_i	g	分解の形	素数の例
0	−	−	−	−	−
1	1	1	2	$p = wP_1P_2,\ N(P_j) = p$	$5, 13, 17 \cdots$
2	2	1	1	$p = wP_1^2,\ N(P_1) = p$	2
3	1	2	1	$p = wP_1,\ N(P_1) = p^2$	$3, 7, 11 \cdots$

このように素数の分解の仕方が mod で決まってしまうことがあり，これが類体論 (Class Field Theory) の例である．類体論の「類」とは mod n による剰余類のことであり，類別から定まる体を類体というのである．(実は，素数の分解が上の表のようになる体は $\mathbb{Q}(i)$ しかないことが知られている．)

$K/\mathbb{Q}$ を n 次拡大とする．即ち $K \supset \mathbb{Q}$ は $\mathbb{Q}$ 上の線型空間として n 次元となるような体である．このとき $\mathbb{Q}(i)$ の時と同様に，体準同型 $K \longrightarrow \mathbb{C}$ は丁度 n 個存在することが分かる．それらを $\sigma_1, \cdots, \sigma_n$ として，$\alpha \in K$ に対して $N_{K/\mathbb{Q}}(\alpha) := \sigma_1(\alpha) \cdots \sigma_n(\alpha)$ と定める．$N_{K/\mathbb{Q}}$ を K の (絶対) ノルムと呼ぶ．$N_{K/\mathbb{Q}}(\alpha) \in \mathbb{Q}$ であることが分かる．

K の整数環を $\mathcal{O}_K$ とし，$\mathcal{O}_K$ で素因数分解ができるとする．このとき素数 $p \in \mathbb{Z} \subset \mathcal{O}_K$ が $p = wP_1^{e_1} \cdots P_g^{e_g}$ と素因数分解したとする．$\mathbb{Q}(i)$ の時と同様に，$N(w) = 1, N(P_j) =$

p^{f_j} と書ける事が分かり

$$p^n = N(p) = N(wP_1^{e_1}\cdots P_g^{e_g}) = p = N(P_1)^{e_1}\cdots N(P_g)^{e_g} = p^{e_1f_1+\cdots+e_gf_g}$$

から $n = \sum_{j=1}^{g} e_j f_j$ である．特に $g \leq n$ が分かる．

※ 一般に $\mathcal{O}_K$ で素因数分解ができるとは限らないが,「素イデアル分解」ならば一般の $\mathcal{O}_K$ でできる．今述べたことは素イデアル分解でも同様に成り立つ.

定義. 素数 $p \in \mathbb{Z} \subset \mathcal{O}_K$ が $p = wP_1^{e_1}\cdots P_g^{e_g}$ と素因数分解したとする．

(1) ある j について $e_j > 1$ となるとき，p は $K/\mathbb{Q}$ で分岐するという．
(2) $g = 1,\ e_1 = n,\ f_1 = 1$ となるとき，p は $K/\mathbb{Q}$ で完全分岐するという．
(3) $e_1 = \cdots = e_g = 1$ となるとき，p は $K/\mathbb{Q}$ で不分岐であるという．
(4) $g = n,\ e_j = 1,\ f_j = 1$ となるとき，p は $K/\mathbb{Q}$ で完全分解するという．

$\zeta_n := e^{\frac{2\pi i}{n}}$ と置き，$K := \mathbb{Q}(\zeta_n)$ を考える．このとき $\mathcal{O}_K = \mathbb{Z}[\zeta_n]$ である．$\zeta_4 = i$ であるから，これは $\mathbb{Z}[i]$ の一般化と考えられる．例として，$n = 7$ としてみると，$\mathbb{Q}(\zeta_7)/\mathbb{Q}$ では素数 p の分解は次のように mod 7 で判定できる．

$p \bmod 7$	e_i	f_i	g	分解の形	素数の例
0	6	1	1	$p = wP_1^6,\ N(P_j) = p$	7
1	1	1	6	$p = wP_1P_2\cdots P_6,\ N(P_j) = p$	$29, 43, \cdots$
2	1	3	2	$p = wP_1P_2,\ N(P_j) = p^3$	$2, 23, \cdots$
3	1	6	1	$p = wP_1,\ N(P_j) = p^6$	$3, 17, \cdots$
4	1	3	2	$p = wP_1P_2,\ N(P_j) = p^3$	$11, 67, \cdots$
5	1	6	1	$p = wP_1,\ N(P_j) = p^6$	$5, 19, \cdots$
6	1	2	3	$p = wP_1P_2P_3,\ N(P_j) = p^2$	$13, 41, \cdots$

mod 7 で 0 になる素数は勿論 7 しかないが，$\mathbb{Q}(\zeta_n)/\mathbb{Q}$ で分岐する素数はこの 7 唯一つなのである．ところでこの唯一つの《例外》7 を除いた $\{\overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}\} = (\mathbb{Z}/7\mathbb{Z})^\times$ は乗法で群になっている．各元 $\overline{a} \in (\mathbb{Z}/7\mathbb{Z})^\times$ の位数 (即ち初めて $a^k \equiv 1 \pmod 7$ となる $k > 0$) を考えると，次の表のように「$\overline{a}$ の位数」=「$\overline{a}$ での f_i」となっていることが分

かる.

$p \bmod 7$	f_i	g	$\bmod 7$ での位数
1	1	6	1
2	3	2	3
3	6	1	6
4	3	2	3
5	6	1	6
6	2	3	2

実は一般に，次のことが成り立つ.

定理. n を正整数とするとき

(1) $p \mid n \Longleftrightarrow p$ は $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ で分岐する.
(2) $p \equiv 1 \pmod{n} \Longleftrightarrow p$ は $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ で完全分解する.
(3) もっと一般に，p の $(\mathbb{Z}/n\mathbb{Z})^\times$ での位数を f, $\varphi(n) = fg$ とすれば p は $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ で g 個に分解する.

※ 先も書いたとおり，一般には素イデアル分解を考える必要がある.

実は「$p \equiv 1 \pmod{n} \Longleftrightarrow p$ は $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ で完全分解する」となるような拡大体 $K/\mathbb{Q}$ は $\mathbb{Q}(\zeta_n)$ しかない．このように，素数の類別から体が一意に定まることがある．この意味で $\mathbb{Q}(\zeta_n)$ を $\mathbb{Q}$ の類体 (class field) と呼ぶ.

何故このような事が言えるのかというと Galois 群 $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ が関係している．素数の分解の仕方というのは代数的な話であるが，Galois 群 $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ というのは体 $\mathbb{Q}(\zeta_n)$ の自己同型群，つまり $\mathbb{Q}(\zeta_n)$ の代数的な情報が詰まった群である．ところでこの Galois 群には自然な同型 $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$ が知られている．(これが Artin の相互律の一例である．) この同型を介して $a \mod n$ から代数的な情報である分解の仕方が分かるのである.

さて，もっと一般に任意の $H \subset (\mathbb{Z}/7\mathbb{Z})^\times$ を取るとき，$\overline{p} \in H$ となる素数 p が全て完全分解するような体 $K/\mathbb{Q}$ は存在するだろうか?

例えば $H = \{\overline{1}, \overline{2}\}$ の場合を考えてみる．$p \equiv 1 \pmod{7}$ となる素数が完全分解するのはそのような素数 p の位数が $((\mathbb{Z}/7\mathbb{Z})^\times$ で)1 だからであった．そこで，$p \equiv 1, 2 \pmod{7}$ となる素数の位数が 1 になればよいのではないだろうか．その為には $(\mathbb{Z}/7\mathbb{Z})^\times$ の剰余群を考えればよい.

そこで $H \subset (\mathbb{Z}/7\mathbb{Z})^\times$ を $\overline{1}$ と $\overline{2}$ を含む最小の部分群とすると $H = \{\overline{1}, \overline{2}, \overline{4}\}$ である.

このとき $(\mathbb{Z}/7\mathbb{Z})^\times/H$ を考えれば，勿論この群では $p \equiv 1, 2, 3 \pmod 7$ となる素数 p の位数が 1 になる．Galois 理論により部分群 $(\mathbb{Z}/7\mathbb{Z})^\times \supset H \supset \{\overline{1}\}$ に対応する部分体 $\mathbb{Q}(\zeta_7) \supset K \supset \mathbb{Q}$ が存在する．Galois 理論により $\mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/7\mathbb{Z})^\times/H$ であり

$$\begin{aligned} K &= \{\alpha \in \mathbb{Q}(\zeta_7) \mid \text{任意の}\sigma \in H \text{に対し}\sigma(\alpha) = \alpha\} \\ &= \{\alpha \in \mathbb{Q}(\zeta_7) \mid \sigma_2(\alpha) = \alpha\}. \end{aligned}$$

ここで $\sigma_2 \in \mathrm{Gal}(\mathbb{Q}(\zeta_7)/\mathbb{Q})$ は $\sigma_2(\zeta_7) = \zeta_7^2$ で定まる同型である．$\zeta = \zeta_7$ と書くと $(\zeta-1)(1+\zeta+\zeta^2+\zeta^3+\zeta^4+\zeta^5+\zeta^6) = \zeta^7-1 = 0$ となる．故に $1+\zeta+\zeta^2+\zeta^3+\zeta^4+\zeta^5+\zeta^6 = 0$ である．$\alpha = a_0 + a_1\zeta + a_2\zeta^2 + a_3\zeta^3 + a_4\zeta^4 + a_5\zeta^5$ $(a_i \in \mathbb{Q})$ と書けば，

$$\begin{aligned} \sigma_2(\alpha) &= a_0 + a_1\zeta^2 + a_2\zeta^4 + a_3\zeta^6 + a_4\zeta + a_5\zeta^3 \\ &= (a_0 - a_3) + (a_4 - a_3)\zeta + (a_1 - a_3)\zeta^2 + (a_5 - a_3)\zeta^3 + (a_2 - a_3)\zeta^4 - a_3\zeta^5. \end{aligned}$$

故に

$$\alpha \in K \iff \sigma_2(\alpha) = \alpha \iff \begin{cases} a_0 = a_0 - a_3 \\ a_1 = a_4 - a_3 \\ a_2 = a_1 - a_3 \\ a_3 = a_5 - a_3 \\ a_4 = a_2 - a_3 \\ a_5 = -a_3 \end{cases} \iff \begin{cases} a_1 = a_2 = a_4 \\ a_3 = a_5 = 0 \end{cases}$$

が分かる．よって $K = \{a_0 + a_1(\zeta + \zeta^2 + \zeta^4) \mid a_0, a_1 \in \mathbb{Q}\}$ である．ところで $\alpha := 1 + 2(\zeta + \zeta^2 + \zeta^4)$ とすれば $K = \mathbb{Q}(\alpha)$ で

$$\begin{aligned} \alpha^2 &= (1 + 2\zeta + 2\zeta^2 + 2\zeta^4)^2 \\ &= 1 + 4\zeta^2 + 4\zeta^4 + 4\zeta + 4\zeta + 4\zeta^2 + 4\zeta^4 + 8\zeta^3 + 8\zeta^5 + 8\zeta^6 \\ &= 1 + 8\zeta + 8\zeta^2 + 8\zeta^3 + 8\zeta^4 + 8\zeta^5 + 8\zeta^6 \\ &= -7. \end{aligned}$$

故に $\alpha = \sqrt{-7}$ であり $K = \mathbb{Q}(\sqrt{-7})$ である．$\mathbb{Q}(\sqrt{-7})/\mathbb{Q}$ では次のように素数が分解することが知られている．

$p \bmod 7$	f_i	g	$\bmod H$ での位数
1	1	2	1
2	1	2	1
3	2	1	2
4	1	2	1
5	2	1	2
6	2	1	2

よって，確かに「$p \equiv 1, 2, 4 \pmod 7 \Longleftrightarrow p$ は $K/\mathbb{Q}$ で完全分解する」となっている．

一般に，n を正整数として $H \subset (\mathbb{Z}/n\mathbb{Z})^\times$ を部分群とすると，代数体 $K_H/\mathbb{Q}$ で，素数 p に対し「$\overline{p} \in H \Longleftrightarrow p$ は $K_H/\mathbb{Q}$ で完全分解する」となるものが存在する．この K_H を H についての $\mathbb{Q}$ の類体という．しかもこのとき $\mathrm{Gal}(K_H/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times/H$ となる．

定理. $H_0 \subset H_1 \Longleftrightarrow K_{H_0} \supset K_{H_1}$

特に，H についての $\mathbb{Q}$ の類体は一意に決まることが分かる．

さて，$\mathrm{Gal}(K_H/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times/H$ であるから $\mathbb{Q}$ の類体は $\mathbb{Q}$ の有限次アーベル拡大である．ところが実は逆，即ち $\mathbb{Q}$ の有限次アーベル拡大は類体であることが分かる．

定理 (Kronecker-Weber の定理)**.** 任意の有限次アーベル拡大 $K/\mathbb{Q}$ に対して，ある正整数 n が存在して $K \subset \mathbb{Q}(\zeta_n)$

定理. 任意の有限次アーベル拡大 $K/\mathbb{Q}$ に対して，ある正整数 n と部分群 $H \subset (\mathbb{Z}/n\mathbb{Z})^\times$ が存在して $K = K_H$

2 代数体の類体論

$K/\mathbb{Q}$ を代数体, $\mathfrak{m}$ を K のイデアルとする．以下, K は総虚であるとする．(即ち, 埋め込み $K \longrightarrow \mathbb{R}$ は存在しないとする．これは以下の議論を簡単にするための仮定である．)

$$\begin{aligned} I_K(\mathfrak{m}) &:= \{\mathfrak{a} \subset K \mid \mathfrak{a} \text{ は分数イデアル}, (\mathfrak{a}, \mathfrak{m}) = 1\} \\ P_K(\mathfrak{m}) &:= \{(\alpha) \mid \alpha \in K^\times,\ \alpha \equiv 1 \pmod{\mathfrak{m}}\} \\ Cl_K(\mathfrak{m}) &:= I_K(\mathfrak{m})/P_K(\mathfrak{m}) \end{aligned}$$

と置く．

定理. $H \subset Cl_K(\mathfrak{m})$ を部分群とするとき，このときある拡大体 $K(\mathfrak{m}, H)/K$ が存在して，$\mathfrak{m}$ を割らない任意の素イデアル $\mathfrak{p}$ に対して

$$\overline{\mathfrak{p}} \in H \Longleftrightarrow \mathfrak{p} \text{ は } K(\mathfrak{m}, H)/K \text{ で完全分解する}$$

が成り立つ．更に, $f > 0$ を $\overline{\mathfrak{p}}^f \in H$ となる最小の自然数, $[K(\mathfrak{m}, H) : K] = fg$ とすれば $\mathfrak{p}$ は $K(\mathfrak{m}, H)/K$ で g 個の素イデアルに分解する．また $\mathrm{Gal}(K(\mathfrak{m}, H)/K) \cong Cl_K(\mathfrak{m})/H$.

定理. L/K をアーベル拡大とするとき，ある K のイデアル $\mathfrak{m}$ と部分群 $H \subset Cl_K(\mathfrak{m})$ が存在して $L = K(\mathfrak{m}, H)$ となる．さらに $H = \{\overline{N_{L/K}(\mathfrak{a})} \mid \mathfrak{a} \text{ は } L \text{ のイデアル}, (\mathfrak{a}, \mathfrak{m}) = 1\}$

と書ける.

$K(\mathfrak{m}) := K(\mathfrak{m}, 1)$ と書くことにする．特に $\mathfrak{m} = \mathcal{O}_K$ とするとき，$K(\mathcal{O}_K)/K$ は不分岐なアーベル拡大であり，しかもそのうちで最大なものである．これを Hilbert 類体，もしくは絶対類体という.

定理 (Artin の相互律)**.** L/K をアーベル拡大とし，類体論によって L に対応する $\mathfrak{m}$ と $H \subset Cl_K(\mathfrak{m})$ を取る．$\mathfrak{m}$ と素な K の素イデアル $\mathfrak{p}$ に対して $\mathfrak{p}$ の Frobenius 写像と呼ばれる $\left(\dfrac{L/K}{\mathfrak{p}}\right) \in \mathrm{Gal}(L/K)$ が定まる．このとき，類体論の同型 $Cl_K(\mathfrak{m})/H \cong \mathrm{Gal}(L/K)$ は $\overline{\mathfrak{p}} \longmapsto \left(\dfrac{L/K}{\mathfrak{p}}\right)$ で与えられる.

3 応用例

命題. 素数 $p \neq 2, 5$ に対して

$$\text{ある } x, y \in \mathbb{Z} \text{ が存在して } p = x^2 + 5y^2 \Longleftrightarrow p \equiv 1, 9 \pmod{20}$$

Fermat の二平方和定理の場合と同様に，$K := \mathbb{Q}(\sqrt{-5})$ で考えればよいということは分かるだろう．$K \subset \mathbb{Q}(\zeta_n)$ となる最小の n は $n = 20$ であり，K に対応する $\mathrm{Gal}(\mathbb{Q}(\zeta_{20})/\mathbb{Q}) \cong (\mathbb{Z}/20\mathbb{Z})^\times$ の部分群は $\{\overline{1}, \overline{3}, \overline{7}, \overline{9}\}$ である．故に

$$K/\mathbb{Q} \text{ で } p \text{ が完全分解する} \Longleftrightarrow p \equiv 1, 3, 7, 9 \pmod{20}$$

あれ? $1, 9 \pmod{20}$ じゃなくて $1, 3, 7, 9 \pmod{20}$ が出てきたぞ…?? これは何故かというと，$\mathbb{Q}(\sqrt{-5})$ では《素因数分解》ができないからである．つまり，$p \equiv 1, 3, 7, 9 \pmod{20}$ のとき p は $K/\mathbb{Q}$ で完全分解するが，それは元としての分解ではなくてイデアルの分解 $(p) = \mathfrak{p}_1\mathfrak{p}_2$ なのである．ここでもし $\mathfrak{p}_1, \mathfrak{p}_2$ が単項イデアルならば，即ち $\mathfrak{p}_1 = (x_1 + y_1\sqrt{-5})$, $\mathfrak{p}_2 = (x_2 + y_2\sqrt{-5})$ と書けたならば $(p) = (x_1 + x_2\sqrt{-5})(x_2 + y_2\sqrt{-5})$ となり数として $p = w(x_1 + x_2\sqrt{-5})(x_2 + y_2\sqrt{-5})$ と分解できることが分かるから，Fermat の二平方和定理の時と同様の議論ができる.

L/K を Hilbert 類体とすれば

$$\mathfrak{p} \text{ が単項イデアルである} \Longleftrightarrow \mathfrak{p} \text{ が } L/K \text{ で完全分解する}$$

である．$L = K(i) = \mathbb{Q}(\sqrt{-5}, i)$ であることが知られており, $L/\mathbb{Q}$ はアーベル拡大である．$L \subset \mathbb{Q}(\zeta_n)$ となる最小の n も $n = 20$ であり，L に対応する $\mathrm{Gal}(\mathbb{Q}(\zeta_{20})/\mathbb{Q}) \cong (\mathbb{Z}/20\mathbb{Z})^\times$

の部分群は $\{\overline{1}, \overline{9}\}$ である．故に

$$
\begin{aligned}
&p = x^2 + 5y^2 \text{と書ける} \\
\iff &p = (x + \sqrt{-5}y)(x - \sqrt{-5}y) \\
\iff &K/\mathbb{Q} \text{で} p = \mathfrak{p}_1\mathfrak{p}_2 \text{と完全分解かつ} \mathfrak{p}_1 \text{と} \mathfrak{p}_2 \text{が単項イデアル} \\
\iff &K/\mathbb{Q} \text{で} p = \mathfrak{p}_1\mathfrak{p}_2 \text{と完全分解かつ} L/K \text{で} \mathfrak{p}_1 \text{と} \mathfrak{p}_2 \text{が完全分解} \\
\iff &p \text{は} L/\mathbb{Q} \text{で完全分解} \\
\iff &p \equiv 1, 9 \pmod{20}
\end{aligned}
$$

命題. mod 20 で 3 か 7 になる二つの素数 p, q に対して，ある $x, y \in \mathbb{Z}$ が存在して $pq = x^2 + 5y^2$.

証明. $p \equiv 3, 7 \pmod{20}$ だから $K := \mathbb{Q}(\sqrt{-5})$ とすると $K/\mathbb{Q}$ で $p = \mathfrak{p}_1\mathfrak{p}_2$ と完全分解し，$\mathfrak{p}_1, \mathfrak{p}_2$ は非単項イデアルである．$q = \mathfrak{q}_1\mathfrak{q}_2$ も同様．このとき $pq = \mathfrak{p}_1\mathfrak{q}_1\mathfrak{p}_2\mathfrak{q}_2$ であるが K の類数は 2 であるから $\mathfrak{p}_1\mathfrak{q}_1, \mathfrak{p}_2\mathfrak{q}_2$ は単項イデアルである．$\mathfrak{p}_1\mathfrak{q}_1 = (x + y\sqrt{-5})$ と書けば $\mathfrak{p}_2\mathfrak{q}_2 = (x - y\sqrt{-5})$ であり $pq = x^2 + 5y^2$ となる． □

命題. 素数 $p \neq 2$ に対して

$$\text{ある } x, y \in \mathbb{Z} \text{ が存在して } p = x^2 - 8y^2 \iff p \equiv 1 \pmod{8}$$

証明. ($\Longrightarrow$) $p = x^2 - 8y^2$ と書けたとすると p が奇数だから x も奇数．$x = 2z + 1$ と書けば mod 8 で $p \equiv (2z+1)^2 = 4z^2 + 4z + 1 = 4z(z+1) + 1 \equiv 1$.

($\Longleftarrow$) $K := \mathbb{Q}(\sqrt{2})$ で考えると $x^2 - 8y^2 = x^2 - 2(2y)^2 = (x + 2y\sqrt{2})(x - 2y\sqrt{2})$ であるから $\mathfrak{m} := (2)$ とすれば

$$p = x^2 - 8y^2 \text{と書ける} \iff p = (a + b\sqrt{2})(a - b\sqrt{2}),\ a + b\sqrt{2} \equiv 1 \pmod{\mathfrak{m}} \text{ と書ける}$$

である．$K \subset \mathbb{Q}(\zeta_n)$ となる最小の n は $n = 8$ であり，類体論により

$$K/\mathbb{Q} \text{ で } p \text{ が完全分解する} \iff p \equiv 1, 7 \pmod{8}$$

$$K(\mathfrak{m})/K \text{ で } a + b\sqrt{2} \text{が完全分解する} \iff a + b\sqrt{2} \equiv 1 \pmod{\mathfrak{m}}$$

であるから

$$p = x^2 - 8y^2 \text{と書ける} \iff K(\mathfrak{m})/\mathbb{Q} \text{ で } p \text{ が完全分解する}$$

$p = x^2 - 8y^2$と書ける
$\iff p = (x + 2y\sqrt{2})(x - 2y\sqrt{2})$
$\iff K/\mathbb{Q}$ で $p = w(a + b\sqrt{2})(a - b\sqrt{2})$ と完全分解かつ $a + b\sqrt{2} \equiv 1 \mod \mathfrak{m}$ かつ $a \pm b\sqrt{2} > 0$
$\iff K/\mathbb{Q}$ で $p = w(a + b\sqrt{2})(a - b\sqrt{2})$ と完全分解かつ $K(\mathfrak{m})/K$ で $a + b\sqrt{2}$が完全分解
$\iff p$ は $K(\mathfrak{m})/\mathbb{Q}$ で完全分解
$\iff p \equiv 1 \pmod 8$

□

4 現在の類体論

さて，今まで類体論をざっと眺めてきたが，類体論をちゃんと勉強しようと例えば『数論 I』などを読んでみるとここで書いてきたようなこととは全然違うことが書いてありビックリすると思われる (というか筆者の実体験)。今回紹介したのは高木貞治先生が作った時の類体論であり，現在では証明も含めて色々と整理されている．ここではそれを軽く紹介する．

既に書いたように「類体 = アーベル拡大体」，即ち類体論とはアーベル拡大の理論である．ところでアーベル拡大体たちの合成体はアーベル拡大になるから，特に体 k の全てのアーベル拡大の合成体はまたアーベル拡大である．これを最大アーベル拡大といい k^{ab}/k と書く．この拡大の Galois 群 $\mathrm{Gal}(k^{\mathrm{ab}}/k)$ を知ることが重要である．何故ならば任意のアーベル拡大 K/k は k^{ab}/k の中間体であり，よって Galois 理論によって $\mathrm{Gal}(k^{\mathrm{ab}}/k)$ の部分群と対応しているからである．

※ k^{ab}/k は大抵は無限次拡大になるから，その Galois 理論はよく知られている有限次 Galois 理論より難しくなる．何故かというと無限次 Galois 拡大では中間体の数より部分群の数の方が多いからである．そこで，無限次 Galois 理論では中間体と閉部分群の対応を考える．(Galois 群には標準的に位相を入れることができる．これを Krull 位相という．)

この Galois 群 $\mathrm{Gal}(k^{\mathrm{ab}}/k)$ は難しく分かりにくいものなのであるが，類体論が言うにはこれを分かりやすい群で《近似》することができるのである．

代数体の場合に入る前に，まずより簡単な場合から説明する．

まず有限体 $\mathbb{F}_q$ (q は素数 p の冪乗) の場合を考える．$\mathbb{F}$ には各 $n > 0$ に対して n 次拡大体 $\mathbb{F}_{q^n}$ が唯一つ存在し，$\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \cong \mathbb{Z}/n\mathbb{Z}$ である．故に $\mathbb{F}_q^{\mathrm{ab}}$ は $\mathbb{F}_q$ の代数閉包 $\mathbb{F}_q^{\mathrm{alg}}$

である．$V := \{x \in \mathbb{F}_q^{\mathrm{ab}} \mid \text{ある正整数 } n \text{ が存在して } x^n = 1\}$ と置くとき $\mathbb{F}_q^{\mathrm{ab}} = \mathbb{F}_q(V)$ であることが知られている．

さて，Galois 理論によれば二つの集合

$$\{\mathbb{F} \mid \mathbb{F}_q \subset \mathbb{F} \subset \mathbb{F}_q^{\mathrm{ab}} \text{は中間体 }\}$$
$$\{H \mid H \subset \mathrm{Gal}(\mathbb{F}_q^{\mathrm{ab}}/\mathbb{F}) \text{ は閉部分群 }\}$$

の間に一対一対応があり，さらに $\mathbb{F}$ と H が対応しているとき $\mathrm{Gal}(\mathbb{F}/\mathbb{F}_q) \cong \mathrm{Gal}(\mathbb{F}_q^{\mathrm{ab}}/\mathbb{F})/H$ である．特に $[\mathbb{F} : \mathbb{F}_q] = [\mathrm{Gal}(\mathbb{F}_q^{\mathrm{ab}}/\mathbb{F}) : H]$ であるから二つの集合

$$A := \{\mathbb{F} \mid \mathbb{F}_q \subset \mathbb{F} \subset \mathbb{F}_q^{\mathrm{ab}},\ [\mathbb{F} : \mathbb{F}_q] < \infty\}$$
$$B := \{H \mid H \subset \mathrm{Gal}(\mathbb{F}_q^{\mathrm{ab}}/\mathbb{F}) \text{ は閉部分群, } [\mathrm{Gal}(\mathbb{F}_q^{\mathrm{ab}}/\mathbb{F}) : H] < \infty\}$$

の間に一対一対応がある．既に書いたとおり $A = \{\mathbb{F}_{q^n} \mid 0 < n \in \mathbb{Z}\}$ である．

ところで，加法群 $\mathbb{Z}$ を考えるとこれの指数有限部分群の全体は $C := \{n\mathbb{Z} \mid n > 0\}$ である．よって A と C の間にも一対一対応 $\mathbb{F}_{q^n} \longmapsto n\mathbb{Z}$ がある．実はこの対応はただの対応ではない．$\varphi\colon \mathbb{F}_q^{\mathrm{ab}} \longrightarrow \mathbb{F}_q^{\mathrm{ab}}$ を $\varphi(x) := x^q$ で定めれば $\varphi \in \mathrm{Gal}(\mathbb{F}_q^{\mathrm{ab}}/\mathbb{F}_q)$ である．そこで群の単射準同型 $\rho\colon \mathbb{Z} \longrightarrow \mathrm{Gal}(\mathbb{F}_q^{\mathrm{ab}}/\mathbb{F}_q)$ を $\rho(m) := \varphi^m$ で定める．$n > 0$ に対し，制限による自然な写像 $r\colon \mathrm{Gal}(\mathbb{F}_q^{\mathrm{ab}}/\mathbb{F}) \longrightarrow \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F})$ が存在する．このとき合成 $r \circ \rho\colon \mathbb{Z} \longrightarrow \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F})$ は全射で $\ker(r \circ \rho) = n\mathbb{Z}$ となる．故に ρ から $\mathbb{Z}/n\mathbb{Z} \cong \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F})$ が得られる．

以上により，次が分かる．二つの集合

$$\{\mathbb{F}/\mathbb{F}_q \mid \text{有限次拡大体 }\}$$
$$\{H \subset \mathbb{Z} \mid \text{指数有限部分群 }\}$$

の間に一対一対応があり，$\mathbb{F}$ と H が対応しているとき ρ から自然に同型 $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}) \cong \mathbb{Z}/n\mathbb{Z}$ が得られる．つまり，準同型 $\rho\colon \mathbb{Z} \longrightarrow \mathrm{Gal}(\mathbb{F}_q^{\mathrm{ab}}/\mathbb{F}_q)$ により $\mathrm{Gal}(\mathbb{F}_q^{\mathrm{ab}}/\mathbb{F}_q)$ が分かりやすい群 $\mathbb{Z}$ で《近似》され，$\mathbb{Z}$ が Galois 群のような役割を果たしているのである．

次に有限次拡大体 $K/\mathbb{Q}_p$ の場合を考える．この場合も有限体の時のように，ある準同型 $\rho\colon K^\times \longrightarrow \mathrm{Gal}(K^{\mathrm{ab}}/K)$ が存在し，$\mathrm{Gal}(K^{\mathrm{ab}}/K)$ が乗法群 $K^\times$ で《近似》される．

有限次アーベル拡大 L/K に対して $r\colon \mathrm{Gal}(K^{\mathrm{ab}}/K) \longrightarrow \mathrm{Gal}(L/K)$ を制限写像とすると，$r \circ \rho$ は全射で $H := \ker(r \circ \rho) \subset K^\times$ は指数有限な開部分群である．よって $K^\times/H \cong \mathrm{Gal}(L/K)$ であり，この対応 $L \longmapsto H$ により二つの集合

$$\{L/K \mid \text{有限次アーベル拡大 }\}$$
$$\{H \subset K^\times \mid \text{指数有限開部分群 }\}$$

の間の一対一対応が得られる．またこの対応において $H = N_{L/K}(L^\times)$ である．

代数体 K の時も同様に $\mathrm{Gal}(K^{\mathrm{ab}}/K)$ が《近似》されるのであるが，少々複雑である．

K の素点 v による完備化を K_v で表す．有限素点 v に対しては K_v の整数環を $\mathcal{O}_v$ で表す．環 $\mathbb{A}_K := \left\{(a_v)_v \in \prod_v K_v \mid \text{殆ど全ての有限素点 } v \text{ について } a_v \in \mathcal{O}_v \in\right\}$ をアデール環 (adele ring) といい，これの乗法群 $\mathbb{A}_K^\times$ をイデール群 (idele group) という．

※ イデールという名前は ideal element 略して id. el. による．またアデールは additive idele からきている．

対角埋込 $K \ni x \longmapsto (\cdots, x, x, \cdots) \in \mathbb{A}_K^\times$ により K を部分群 $K \subset \mathbb{A}_K^\times$ とみなし，剰余群 $C_K := \mathbb{A}_K^\times/K$ をイデール類群という．このときある準同型 $\rho\colon C_K \longrightarrow \mathrm{Gal}(K^{\mathrm{ab}}/K)$ が存在し，$\mathrm{Gal}(K^{\mathrm{ab}}/K)$ が乗法群 $K^\times$ で《近似》される．

有限次アーベル拡大 L/K に対して $r\colon \mathrm{Gal}(K^{\mathrm{ab}}/K) \longrightarrow \mathrm{Gal}(L/K)$ を制限写像とすると，$r \circ \rho$ は全射で $H := \ker(r \circ \rho) \subset K^\times$ は指数有限な開部分群である．よって $K^\times/H \cong \mathrm{Gal}(L/K)$ であり，この対応 $L \longmapsto H$ により二つの集合

$$\{L/K \mid \text{有限次アーベル拡大 }\}$$
$$\{H \subset C_K \mid \text{指数有限開部分群 }\}$$

の間の一対一対応が得られる．またこの対応において $H = N_{L/K}(C_L)$ である．

5 Kronecker の青春の夢

既に紹介したように次の定理が成立する．

定理 (Kronecker-Weber の定理)**.** 任意の有限次アーベル拡大 $K/\mathbb{Q}$ に対して，ある正整数 n が存在して $K \subset \mathbb{Q}(\zeta_n)$ となる．

この定理は，$\mathbb{Q}$ の類体はこのように具体的に書ける，という意味の定理であった．一般の代数体 K(もっと言えば代数体と限らない任意の体) について，類体 $K(\mathfrak{m})$ を具体的に書くことは出来るだろうか? これを「類体の構成問題」といい，Hilbert の第 12 問題となっている未解決問題である．

ところで，$\mathbb{Q}$ の場合は類体が $\zeta_n = e^{\frac{2\pi i}{n}}$，即ち「円周の n 等分点」で与えられている．一般の体の時も類体は何らかの「n 等分点」で与えられないだろうか? これが，虚二次体の場合は楕円曲線の n 等分点で与えられるであろう，というのが Kronecker の青春の夢である．

※ 1880 年，Kronecker が Dedekind への手紙の中で「um meinen liebsten Jugendtraum」(私の一番のお気に入りの青春の夢) と書いたらしい.

定義. 重根を持たない多項式 $x^3 + ax + b$ $(a, b \in \mathbb{C})$ を使って定義される曲線 $E := \{(x, y) \in \mathbb{C} \mid y^2 = x^3 + ax + b\}$ を $\mathbb{C}$ 上の楕円曲線という.

$j(E) := 1728\dfrac{a^3}{a^3 - 27b^2}$ を j 不変量という.

定理. 楕円曲線 E_1, E_2 が同型である $\Longleftrightarrow j(E_1) = j(E_2)$

$\omega_1, \omega_2 \in \mathbb{C}$ は $\mathbb{R}$ 上一次独立であるとする．$\Lambda := \{x\omega_1 + y\omega_2 \mid x, y \in \mathbb{C}\}$ を格子という.

$\mathbb{C}$ 上の有理型関数 f が「任意の $\omega \in \Lambda$ に対して $f(z + \omega) = f(z)$」を満たすとき，f を格子 Λ の楕円関数という．Weierstraßの $\wp$ 関数

$$\wp(z) := \frac{1}{z^2} + \sum_{\omega \in \Lambda \setminus 0} \left(\frac{1}{(z + \omega)^2} - \frac{1}{\omega^2} \right)$$

は楕円関数であり，その微分 $\wp'$ も楕円関数である.

$$g_2 := 60 \sum_{\omega \in \Lambda \setminus 0} \frac{1}{\omega^4},\ g_3 := 140 \sum_{\omega \in \Lambda \setminus 0} \frac{1}{\omega^6}$$

と置く.

定理. $\wp, \wp'$ は微分方程式 $\wp'^2 = 4\wp^3 - g_2\wp - g_3$ を満たし，Λ の楕円関数全体が成す体は $\mathbb{C}(\wp, \wp') =$「$\mathbb{C}$ と $\wp$ と $\wp'$ で生成される体」である.

楕円曲線 $E := \{(x, y) \in \mathbb{C} \mid y^2 = 4x^3 - g_2x - g_3\}$ を考えると定理より $z \in \mathbb{C}$ に対して $(\wp(z), \wp'(z)) \in E \cup \{(\infty, \infty)\}$ であるが，実は $\mathbb{C}/\mathfrak{a} \ni z + \mathfrak{a} \longmapsto (\wp(z), \wp'(z)) \in E \cup \{O\}$ $(O := (\infty, \infty))$ は全単射である．これにより $E \cup \{O\}$ に群構造を入れることが出来る．この群構造は，よく知られている楕円曲線の幾何学的な群構造の入れ方と一致する．$E \cup \{O\}$ の単位元は O である．以下簡単のため，$E \cup \{O\}$ を E と書く.

定理. 群 E の自己準同型環 $\mathrm{End}(E)$ は虚二次体の整環か $\mathbb{Z}$ に同型である.

$\mathrm{End}(E) \ncong \mathbb{Z}$ のとき，E は虚数乗法を持つという.

K を虚二次体，$\mathcal{O}_K \subset K$ を整数環とする (整数環は整環である．)．$\mathrm{End}(E) \cong \mathcal{O}_K$ となるような楕円曲線 E が存在する．E は群であるから E の n 等分点全体がなす集合 $E[n] := \{(x, y) \in E \mid n(x, y) = O\}$ が定まるが，もっと一般に $\mathfrak{m} \subset \mathcal{O}_K$ をイデアルと

するとき $\mathfrak{m}$ 等分点全体がなす集合 $E[\mathfrak{m}]$ を定義することが出来る．($\mathfrak{m} = (n)$ のとき，$E[\mathfrak{m}] = E[n]$ である．)

定義. E を $\mathrm{End}(E) \cong \mathcal{O}_K$ となるようなの楕円曲線とするとき，E は $y^2 = x^3 + ax + b,\ a, b \in K(j(E))$ と書ける．このとき

$$h(x,y) := \begin{cases} x & (AB \neq 0 \text{ のとき}) \\ x^2 & (B = 0 \text{ のとき}) \\ x^3 & (A = 0 \text{ のとき}) \end{cases}$$

を Weber 関数という．

定理. K を虚二次体，$\mathcal{O}_K$ を K の整数環，E を $\mathrm{End}(E) \cong \mathcal{O}_K$ となるような楕円曲線とする．$\mathfrak{m}$ を K のイデアルとすれば $K(\mathfrak{m}) = K(j(E), h(E[\mathfrak{m}]))$ である．特に K の Hilbert 類体は $K(j(E))$ で与えられる．

例. $K = \mathbb{Q}(i)$ の場合．楕円曲線 $E\colon y^2 = x^3 + x$ を考えると $\mathrm{End}(E) = \mathbb{Z}[i]$ である．Weber 関数は $h(x,y) = x^2$，j 不変量は $j(E) = 1728$ となる．$(x_1, y_1), (x_2, y_2) \in E$ に対して

$$\lambda := \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & (x_1 \neq x_2) \\ \dfrac{3x_1^2 + 1}{2y_1 + x_1} & (x_1 = x_2) \end{cases},\ \nu := \begin{cases} \dfrac{y_1 x_2 - y_2 x_1}{x_2 - x_1} & (x_1 \neq x_2) \\ \dfrac{-x_1^3 + x_1}{2y_1 + x_1} & (x_1 = x_2) \end{cases}$$

と置けば

$$(x_1, y_1) + (x_2, y_2) = \begin{cases} O & (x_1 = x_2 \text{かつ } y_1 + y_2 = 0 \text{ のとき}) \\ (\lambda^2 - x_1 - x_2, -\lambda(\lambda^2 - x_1 - x_2) - \nu) & (\text{それ以外}) \end{cases}$$

と書ける．

$2(x,y) = O$ とすると $y + y = 0$ だから $y = 0$．よって $x^3 + x = 0$ より $x = 1, \pm i$ である．従って $E[2] = \{O, (0,0), (\pm i, 0)\}$ が分かる．故に $K((2)) = K$ である．

次に $E[3]$ を考える．$(x,y) \notin E[2]$ とすれば $2(x,y) = \left(\dfrac{x^4 - 2x^2 + 1}{4y^2}, \dfrac{x^6 + 5x^4 - 5x^2 - 1}{8y^3} \right)$ であるから $3(x,y) = O$ となるためには $2(x,y) + (x,y) = O$，即ち $\dfrac{x^4 - 2x^2 + 1}{4y^2} = x$ でなければならない．故に $x^4 - 2x^2 + 1 = 4x^4 + 4x^2$，従って $3x^4 + 6x^2 - 1 = 0$ でなければならない．この四次方程式の解は $\alpha := \sqrt{\dfrac{2\sqrt{3} - 3}{3}}$ として $\alpha, -\alpha, \dfrac{1}{\sqrt{3}\alpha}, -\dfrac{1}{\sqrt{3}\alpha}$ で与え

られる．$\beta := \sqrt{\dfrac{2\alpha}{\sqrt{3}}} = \sqrt[4]{\dfrac{8\sqrt{3}-12}{9}}$ と置けば

$$E[3] = \left\{ O,\ (\alpha, \pm\beta),\ (-\alpha, \pm i\beta),\ \left(\frac{1}{\sqrt{3}\alpha}, \frac{\pm 2}{\sqrt[4]{27}\beta}\right),\ \left(-\frac{1}{\sqrt{3}\alpha}, \frac{\pm 2i}{\sqrt[4]{27}\beta}\right) \right\}$$

となる．また $K((3)) = K(h(E[3])) = K(\sqrt{3})$ である．

最後に $E[4]$ を考える．$(x, y) \notin E[2]$ とすると $4(x, y) = O$ となるには $2(x, y)$ の y 座標が 0 でなければならない．よって $x^6 + 5x^4 - 5x^2 - 1 = 0$ である．$\gamma := (\sqrt{2} - 1)i$ と置けばこの六次方程式の解は $\pm 1, \pm\gamma, \pm\dfrac{1}{\gamma}$ である．よって $K((4)) = K(h(E[4])) = K(\gamma^2) = K(\sqrt{2})$ である． □

有限体上の一変数代数関数体の場合には Drinfeld 加群の等分点によって，局所体の場合には形式群の等分点によって類体が構成できることが知られている．

6 Riemann 面における類似

歴史的にはまず Riemann 面における分岐の理論というのがあり，Hilbert が Riemann 面の不分岐拡大のアナロジーとして考えたのが Hilbert 類体，それを高木貞治が分岐有りの場合に一般化してできたものが類体論である．ここではその Riemann 面の場合というのを軽く紹介する．

K を $\mathbb{C}$ 上の一変数代数関数体 (即ち $\mathbb{C}(x)$ の有限次拡大体) とする．K はあるコンパクト Riemann 面 X 上の有理型関数体となる．形式的な有限和 $\sum_{P \in X} n(P)P$ $(n(P) \in \mathbb{Z})$ を因子といい，因子全体がなす群 $I_K = \bigoplus_{P \in X} \mathbb{Z}P$ を因子群という．(記号は上でやった整数論のものに合わせており，恐らく標準的な記号ではない．) 因子 $D = \sum n(P)P$ に対して $\deg(D) := \sum n(P)$ を D の次数という．次数 0 の因子全体 $I_K^0(X) := \{D \in I_K \mid \deg(D) = 0\}$ は I_K の部分群をなす．$f \in K$ を X 上の有理型関数とみて

$$\mathrm{ord}_P(f) := \begin{cases} k & (P \text{ が } f \text{ の位数 } k \text{ の零点のとき}) \\ -k & (P \text{ が } f \text{ の位数 } k \text{ の極のとき}) \\ 0 & (\text{それ以外}) \end{cases}$$

と定めれば，$(f) := \sum_{P \in X} \mathrm{ord}_P(f)P$ は因子である．これを f が定める主因子という．主因子全体 $P_K(X) := \{(f) \mid f \in K\}$ は I_K の部分群をなす．また $P_K \subset I_K^0 \subset I_K$ である．$Cl_K := I_K/P_K$ を因子類群という．$Cl_K^0 := I_K^0/P_K$ と置く．

L/K を有限次拡大とすると，この拡大においても分岐を定義することができる．L も $\mathbb{C}$ 上の一変数代数関数体となるから L はあるコンパクト Riemann 面 Y 上の有理型関数体となり，包含写像 $K \longrightarrow L$ から写像 $Y \longrightarrow X$ が得られる．L/K の分岐は Riemann 面 $Y \longrightarrow X$ の意味での分岐と一致する．また「L/K が不分岐 $\Longleftrightarrow$ $Y \longrightarrow X$ が被覆」が成り立つ．

定理. L/K を不分岐有限次アーベル拡大とするとき，ある有限部分群 $H \subset Cl_K^0$ が存在して $\mathrm{Gal}(L/K) \cong H$ である．この対応により K の不分岐有限次アーベル拡大と CL_K^0 の有限部分群とが一対一対応する．

参考文献

[1] 高木 貞治, 『代数的整数論 一般論及類体論』, 岩波書店, 1971 年
今回の内容は基本的にこの本による．(そうでもないかもしれない．)

[2] 加藤 和也，黒川 信重，斎藤 毅,『数論 I—Fermat の夢と類体論』，岩波書店，2005 年
応用例はこの本を参考にした．今回この PDF を書いて，この例を全く理解していなかったことが分かった．

[3] J. H. Silverman,『楕円曲線論概説 上』，シュプリンガーフェアラーク東京，2003 年
虚数乗法論による虚二次体の類体の構成ついて書いてある．

[4] 岩澤 健吉,『代数函数論』,
代数関数体の本，かと思いきや Riemann 面の本，かと思いきや整数論の本である．
(本の後ろの方の内容がモロ類体論である．)