數學傳播　46卷1期, pp. 40-63

高斯虧格理論

余家富・洪梵雲

摘要: 本文介紹二次體較完備的理論, 包含理想類群的計算, 上同調群的計算, 並帶入古典的高斯虧格理論 (Gauss Genus Theory)。

前言

數域 (number field) — 有理數的有限擴張 — 是代數數論中最基本的研究對象。有些只牽涉到有理數的數論問題, 在更大的數域中考慮, 反而能得到更多資訊。例如求方程式

$$x^n + y^n = z^n$$

的所有整數解 (x, y, z)。費馬大定理告訴我們若 $n \geq 3$ 則此方程式沒有平凡解, 也就是說, 如果 (x, y, z) 爲一組解, 則 $xyz = 0$。費馬大定理在數論發展中扮演極爲重要的角色, 最終這個問題在上世紀末由普林斯頓大學的魏爾斯 (Wiles) 成功解決。

現在我們介紹證明裡的一個重要方法。我們可以考慮 n 是一個大於 3 的質數 p 的情況。假設 x, y, z 是一組解, 我們可以假設它們沒有公因數。接著我們觀察到如果 p 整除 x, y, z 其中兩數, 則第三數也會被 p 整除, 因此情況可以分成兩種: (1) p 不整除 x, y, z 中的任何一數, 或是 (2) p 恰好整除其中一數。

接下來我們將試著證明 (1) 的情況會導致矛盾。如果我們令 $\omega = e^{2\pi i/p}$ 並分解 $x^p + y^p = z^p$, 則

$$(x + y)(x + y\omega)(x + y\omega^2) \cdots (x + y\omega^{p-1}) = z^p.$$

這相當於是數域 $\mathbb{Q}[\omega]$ 中的乘法問題。更進一步, 我們可以將上面的等式看成其整數環 $\mathbb{Z}[\omega]$ 中的理想。

代數數論中有以下幾個重要的性質: 若 K 是一個數域, R 是其所對應的整數環 (number ring), 也就是所有在 K 裡滿足一個首項係數爲 1 的整係數多項式 $f(\alpha) = 0, f(x) \in \mathbb{Z}[x]$ 的元素 α, 則 R 中的理想都能被唯一分解成質理想 (prime ideal) 的乘積。另外在我們能定義理想間的等價關係: 對 R 中的理想 A, B, 如果存在 $\alpha, \beta \in R$ 使得 $\alpha A = \beta B$, 則定義

$A \sim B$。事實上, 這樣定義出來的理想類 (上述關係定義出的等價類) 只會是有限多個, 而理想類的個數稱作 K 的 類數 (*class number*), 通常記做 h。理想之間的乘法引導出了理想類之間的乘法 $[A][B] = [AB]$。在這個運算下, 理想類組成了一個有限交換群, 稱作 理想類群 (*ideal class group*)。而理想類群的單位元正是包含了所有主理想 (principal ideal) 的理想類, 記爲 C_0。最後, 當 $K = \mathbb{Q}[e^{2\pi i/p}]$, 其中 p 是一個奇質數時, 如果 p 不整除 $R = \mathbb{Z}[e^{2\pi i/p}]$ 的類數 h, 則稱 p 是一個 正則質數 (*regular prime*)。

讓我們回到剛才的討論中。經由一些論述, 我們可以得到整除 $(x + y\omega)$ 的質理想, 一定不會整除其他的理想

$$(x + y), (x + y\omega^2), \ldots, (x + y\omega^{p-1}).$$

因此, $(x + y\omega)$ 一定是某個理想 I 的 p 次方。將 I 的理想類記做 C, 則 $C^p = C_0$。這時如果 p 是正則質數, 那麼理想類群不會有階數爲 p 的元素, 因此 $C = C_0$, 也就是說 I 本身就是一個主理想 (α)。我們有

$$(x + y\omega) = I^p = (\alpha)^p = (\alpha^p),$$

所以存在單位元 $u \in R$ 使得 $x + y\omega = u\alpha^p$。由此可以得到 $x \equiv y \pmod{p}$。類似地如果我們將原本的 $x^p + y^p = z^p$ 改寫成 $x^p + (-z)^p = (-y)^p$, 則可得到 $x \equiv -z \pmod{p}$。這時

$$2x^p \equiv x^p + y^p = z^p \equiv -x^p \pmod{p}.$$

所以 $p \mid 3x^p$, p 整除 x, 得到矛盾。

事實上, 數學家 Kummer 證明了對於任意正則質數 p, 費馬大定理成立。

由此, 我們可以看見類數以及理想類群在代數數論中的重要性, 而二次體更是其中最基本的例子。很多在二次體上觀察到的現象都可以推廣到一般的數域。在本篇文章中我們將探討如何計算二次體的理想類群, 以及在其中觀察到的現象。

1. 二次體的理想類群 (Ideal class group)

在第一節中, 我們將計算二次體的理想類群。首先, 我們會先引入本原理想 (primitive ideal, 定義 1.4) 的概念, 方便後續的計算, 並描述理想類群的生成元。接著, 我們會討論如何得到生成元之間的關係, 以決定理想類群的結構。最後則是幾個實際計算的例子。

1.1. 基本定義與性質

設 $k = \mathbb{Q}(\sqrt{m})$ 爲一個二次體, 其中 m 是一個整數, 不被大於 1 的平方數整除 (square-free)。我們將 k 中的整數環 (ring of integers) 記爲 $\mathfrak{o}_k$。我們知道$\mathfrak{o}_k$作爲一個$\mathbb{Z}$-模 ($\mathbb{Z}$-

module) 有一組自然基底 (canonical basis) $\{1, \omega\}$。其中

$$\omega = \begin{cases} \sqrt{m}, & m \equiv 2, 3 \pmod 4; \\ \frac{1+\sqrt{m}}{2}, & m \equiv 1 \pmod 4, \end{cases}$$

而且 k 的判別式 (discriminant) Δ_k 爲

$$\Delta_k = \begin{cases} 4m, & m \equiv 2, 3 \pmod 4; \\ m, & m \equiv 1 \pmod 4. \end{cases}$$

令 $\mathfrak{m}$ 爲 $\mathfrak{o}_k$ 的一個自由 $\mathbb{Z}$-子模 (free $\mathbb{Z}$-submodule), 而且基底爲 $\{u, v\}$ (也就是說, $\mathfrak{m} = \mathbb{Z}u + \mathbb{Z}v$, 我們將這種情況記做 $\mathfrak{m} = [u, v]$)。我們知道存在一個整數矩陣 $A \in M_2(\mathbb{Z})$ 使得 $[u, v] = [1, \omega]A$, 而 $[\mathfrak{o}_k : \mathfrak{m}] = |\det A|$。由基本的整除性質我們知道 $[\mathfrak{o}_k : \mathfrak{m}] \in \mathfrak{m}$, 所以 $\mathfrak{m} \cap \mathbb{Z}$ 非零, 並且有一個整除 $[\mathfrak{o}_k : \mathfrak{m}]$ 的正整數 a 使得 $\mathfrak{m} \cap \mathbb{Z} = \mathbb{Z}a$。類似地, 因爲 $[\mathfrak{o}_k : \mathfrak{m}]\omega \in \mathfrak{m}$, $\mathfrak{m}$ 中存在以下形式的元素:

$$b + c\omega, \quad b, c \in \mathbb{Z} \text{ 且 } c \geq 1.$$

取 $b + c\omega$ 使得其中的 c 是這些元素中的 c 最小的。我們能證明

命題 1.1. $\mathfrak{m} = [a, b + c\omega]$.

因此, 給定 $\mathfrak{m}$ 我們可以唯一決定正整數 a, c, 以及整數 b 模 a 的餘數。

定義 1.2. 我們稱 $\mathfrak{m} = [a, b + c\omega]$ 爲 m 的自然基底表示 (*canonical basis expression*)。

以下列出一些自然基底表示的性質。

命題 1.3.

(a) 對於正整數 a, c 和整數 b, 令 $\mathfrak{m} = [a, b + c\omega]$。那麼 $\mathfrak{m}$ 是一個秩 (rank) 爲 2 的自由模, 且 $\{a, b + c\omega\}$ 是它的一組自然基底。

(b) 如果 $[a, b + c\omega]$ 是 $\mathfrak{o}_k$ 中的一個理想, 那麼 $c \mid a$ 且 $c \mid b$。

(c) $[a, b + c\omega]$ 是一個理想若且唯若 $a \mid N(b + \omega)$, 其中 $N = N_{k/\mathbb{Q}}$ 是從 k 到 $\mathbb{Q}$ 的範數映射 (norm map)。

(d) 對一個理想 $\mathfrak{a} = [\alpha, \beta]$, 我們有 $\mathfrak{a} = (\alpha, \beta)$。

(e) 對一個 $\mathfrak{o}_k$ 中的理想 $\mathfrak{a}$, 令它的共軛爲 $\mathfrak{a}'$ (意即 $\mathfrak{a}' = \sigma(\mathfrak{a})$, 其中 σ 是 $\mathrm{Gal}(k/\mathbb{Q})$ 中唯一非單位元的元素)。則我們有 $\mathfrak{a}\mathfrak{a}' = (\mathrm{N}\mathfrak{a})$, 其中 $\mathrm{N}\mathfrak{a} = |\mathfrak{o}_k/\mathfrak{a}|$ 是 $\mathfrak{a}$ 的範數(norm)。

定義 1.4. 假設 $\mathfrak{a}$ 是 $\mathfrak{o}_k$ 中的一個理想。若 $d = 1$ 是唯一滿足 $d \mid \mathfrak{a}$ 的正整數, 我們稱 $\mathfrak{a}$ 爲本原理想 (*primitive ideal*)。每個理想都等價於唯一一個本原理想。

命題 1.5. (a) 子模 $[a, b+c\omega]$ 是一個本原理想, 若且唯若 $c=1$ 且 $a \mid N(b+\omega)$。

(b) 令 $\mathfrak{a}=[a, b+\omega]$ 爲一個本原理想。如果 $a=a_1a_2$ 爲兩正整數 a_1, a_2 的乘積, 則 $\mathfrak{a}_i = [a_i, b+\omega], i=1,2$ 都是本原理想, 而且 $\mathfrak{a}=\mathfrak{a}_1\mathfrak{a}_2$.

我們在這邊列出幾個二次體的性質。

- 對每個二次體 k, 我們在質數上定義 Kronecker 符號 (*Kronecker symbol*) 爲

$$\chi_k(p)=\begin{cases} 0, & p=\mathfrak{p}^2 \,(p \text{ 在 } k \text{ 中分歧 (ramifies)});\\ 1, & p=\mathfrak{p}\mathfrak{p}', \mathfrak{p}\neq\mathfrak{p}' \,(p \text{ 在 } k \text{ 中完全分裂 (splits completely)});\\ -1, & p=\mathfrak{p}, \,(p \text{ 在 } k \text{ 中仍是質理想}). \end{cases}$$

這些值也可以透過以下的算式求得:

$$\chi_k(p)=\begin{cases} 0, & p \mid \Delta_k;\\ \left(\frac{\Delta_k}{p}\right), & p\nmid\Delta_k \text{ 且 } p\neq 2;\\ (-1)^{\frac{\Delta_k^2-1}{8}}, & p\nmid\Delta_k \text{ 且 } p=2 \,(\text{這只會發生在 } m\equiv 1 \pmod 4). \end{cases}$$

因爲 $\mathfrak{o}_k=\mathbb{Z}[\omega]$, 我們可以透過在模 p 中分解 ω 的最小多項式 $f_\omega(X)$, 來得知 p 在 k 中的質理想分解。我們將 p 在 k 分解出的質理想記爲 $\mathfrak{p}_p$ 和 $\mathfrak{p}'_p$。

我們可以將以上的定義用乘法擴展到子群

$$I_{\mathbb{Q}}(\Delta_k)=\left\{a\in\mathbb{Q}^\times : a>0, \gcd(a,\Delta_k)=1\right\},$$

其對應域爲 $\{\pm 1\}$。延伸後的映射稱爲*Kronecker* 特徵標 (*Kronecker character*), 一樣記爲 χ_k。

- k 所對應的 *Minkowski* 常數 M_k 爲

$$M_k=\begin{cases} \frac{1}{2}\sqrt{\Delta_k}, & \Delta_k>0;\\ \frac{2}{\pi}\sqrt{-\Delta_k}, & \Delta_k<0. \end{cases}$$

Minkowski 常數有一個重要性質: 理想類群 H_k 的每個理想類都包含一個 $\mathfrak{o}_k$ 中的理想 $\mathfrak{a}$, 使得 $\mathrm{N}\mathfrak{a}\leq M_k$.

命題 1.6. 對一個二次體 k, 記 $S_k=\{p : p\leq M_k \text{ 且 } \chi_k(p)\neq -1\}$。則 k 的理想類群 H_k 可以由以下質理想的理想類生成: $\mathfrak{p}_p$, $p\in S_k$。

證明: 從每個理想類中, 我們取一個理想 $\mathfrak{a}$ 使得 $\mathrm{N}\mathfrak{a}\leq M_k$。$\mathfrak{a}$ 的任一質理想因子 (以下簡稱質因子) $\mathfrak{p}$ 滿足 $\mathrm{N}\mathfrak{p}\leq M_k$, 因此 H_k 可由滿足 $\mathrm{N}\mathfrak{p}\leq M_k$ 的質理想 $\mathfrak{p}$ 的理想類生成。對這樣的

質理想 $\mathfrak{p}$, 我們令 p 爲其對應下 (lying under) 的質數, 意即 $p\mathbb{Z} = \mathfrak{p} \cap \mathbb{Z}$。如果 $\chi_k(p) = -1$, 則 $\mathfrak{p} = p$ 而且 $\mathfrak{p}$ 的理想類是 H_k 中的單位元。如果 $\chi_k(p) \neq -1$, 則 $\mathrm{N}\mathfrak{p} = p = \mathfrak{p}_p\mathfrak{p}'_p$。在 H_k 中, $\mathfrak{p}_p$ 的理想類與 $\mathfrak{p}'_p$ 的理想類互爲反元素。因此要生成 H_k 的話, 只要取 $\mathfrak{p}_p$ 的理想類就足夠了。 □

1.2. 計算與例子

在接下來的內容中, 我們定義多項式

$$P(X) = N_{k/\mathbb{Q}}(X + \omega) = \begin{cases} X^2 - m, & m \equiv 2, 3 \pmod 4; \\ X^2 + X + \dfrac{1-m}{4}, & m \equiv 1 \pmod 4. \end{cases}$$

注意到 $P(X)$ 也是 $-\omega$ 的最小多項式。因爲 H_k 由滿足 $p \in S_k$ 的質理想 $\mathfrak{p}_p$ 的等價類生成, 我們可以透過了解這些生成元滿足的關係式來確定 H_k 的結構。

令 b 是一個非負整數, 使得 $P(b) = N(b + \omega)$ 的質因數皆是 S_k 的元素:

$$|P(b)| = |N(b + \omega)| = p_1^{e_1} \cdots p_n^{e_n}, p_i \in S_k.$$

本原主理想 $(b + \omega)$ 有以下的自然基底表示

$$(b + \omega) = [|N(b + \omega)|, b + \omega],$$

而由 $|N(b + \omega)|$ 的質因數分解我們看到

$$1 \sim (b + \omega) = [p_1, b + \omega]^{e_1} \cdots [p_n, b + \omega]^{e_n}.$$

因爲右式的每個因子都是形爲 $[p, b + \omega]$、範數爲 p 的質理想, 我們有

$$[p, b + \omega] = \mathfrak{p}_p \text{ 或 } \mathfrak{p}'_p. \text{ 這等價於 } [p, b + \omega] \sim \mathfrak{p}_p \text{ 或 } \mathfrak{p}_p^{-1}.$$

由前述 $(b + \omega)$ 的分解, 我們得到關係式

$$\mathfrak{p}_{p_1}^{\pm e_1} \cdots \mathfrak{p}_{p_n}^{\pm e_n} \sim 1. \tag{$*$}$$

對每個 b 進行這樣的過程後, 我們得到如 $(*)$ 的關係式, 讓我們最終能決定 H_k 的結構。在以下的例子中, 記 C_n 爲階數是 n 的循環群。

例 1.7. 考慮 $m = 58$ 的情況。此時 $\omega = \sqrt{58}$ 且 $\Delta_k = 232$。Minkowski 常數爲 $M_k = \frac{1}{2}\sqrt{\Delta_k} = \sqrt{58}$, 因此我們只需考慮質數 $2, 3, 5, 7$。它們代入 Kronecker 符號的值爲

p	2	3	5	7
$\chi_k(p)$	0	1	-1	1

因此集合 $S_k = \{2, 3, 7\}$。對於質數 $p \in S_k$, 我們在模 p 下分解 ω 的最小多項式 $f_\omega(X) = X^2 - 58$。

- $p = 2$. $X^2 - 58 \equiv X^2$, 所以

$$2 = \mathfrak{p}_2, \text{ 其中 } \mathfrak{p}_2 = (2, \omega) = [2, \omega].$$

- $p = 3$. $X^2 - 58 \equiv (X + 1)(X + 2)$, 所以

$$3 = \mathfrak{p}_3\mathfrak{p}_3', \text{ 其中 } \mathfrak{p}_3 = (3, \omega + 1) = [3, \omega + 1], \mathfrak{p}_3' = [3, \omega + 2].$$

- $p = 7$. $X^2 - 58 \equiv (X + 3)(X + 4)$, 所以

$$7 = \mathfrak{p}_7\mathfrak{p}_7', \text{ 其中 } \mathfrak{p}_7 = [7, \omega + 3], \mathfrak{p}_7' = [7, \omega + 4].$$

現在我們計算 $P(b) = b^2 - 58$ 在 $b \geq 0$ 的值。如果它們的質因數皆在 S_k 中, 則列出。

2	$-54 = -1 \cdot 2 \cdot 3^3$
3	$-49 = -1 \cdot 7^2$
4	$-42 = -1 \cdot 2 \cdot 3 \cdot 7$
7	$-9 = -1 \cdot 3^2$
8	$6 = 2 \cdot 3$.

- 由 2 的質理想分解, 我們有 $1 \sim \mathfrak{p}_2^2$。
- $b = 8.1 \sim [6, 8 + \omega] = [2, 8 + \omega][3, 8 + \omega] = \mathfrak{p}_2\mathfrak{p}_3'$, 因此 $\mathfrak{p}_3 \sim \mathfrak{p}_2$。
- $b = 4.1 \sim [42, 4 + \omega] = [2, 4 + \omega][3, 4 + \omega][7, 4 + \omega] = \mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_7'$, 因此 $\mathfrak{p}_7 \sim 1$。

理想類群由 $\mathfrak{p}_2$ 的等價類生成。最後, 因爲 $(2, \omega)$ 並非主理想, 可以確定理想類群同構到 C_2。

例 1.8. 考慮 $m = -58$ 的情況。$\omega = \sqrt{-58}$ 且 $\Delta_k = -232$。Minkowski 常數 $M_k = \frac{4\sqrt{58}}{\pi}$, 因此只需考慮質數 $2, 3, 5, 7$。它們代入 Kronecker 符號的值爲

p	2	3	5	7
$\chi_k(p)$	0	-1	-1	-1

因此 $S_k = \{2\}$。質數 2 在 k 中的質理想分解爲 $2 = [2, \omega]^2$. 因爲 $(2, \omega)$ 並非一個主理想, 可以確定理想類群同構到 C_2。

例 1.9. 考慮 $m = 105$ 的情況。這時 $\omega = \frac{1+\sqrt{105}}{2}$ 且 $\Delta_k = 105$。Minkowski 常數爲 $M_k = \frac{1}{2}\sqrt{\Delta_k} = \frac{\sqrt{105}}{2}$, 所以只需考慮質數 $2, 3, 5$。它們代入 Kronecker 符號的值爲

p	2	3	5
$\chi_k(p)$	1	0	0

因此 $S_k = \{2, 3, 5\}$。對 S_k 中的質數 p, 我們透過分解 ω 的最小多項式 $f_\omega(X) = X^2 - X - 26$ 來決定質理想 $\mathfrak{p}_p, \mathfrak{p}'_p$。

- $p = 2$. $X^2 - X - 26 \equiv X(X+1) \pmod 2$, 因此

$$2 = \mathfrak{p}_2\mathfrak{p}'_2, \text{ 其中 } \mathfrak{p}_2 = (2, \omega) = [2, \omega],\ \mathfrak{p}'_2 = (2, \omega+1) = [2, \omega+1].$$

- $p = 3$. $X^2 - X - 26 \equiv (X+1)^2 \pmod 3$, 因此

$$3 = \mathfrak{p}_3^2, \text{ 其中 } \mathfrak{p}_3 = (3, \omega+1) = [3, \omega+1].$$

- $p = 5$. $X^2 - X - 26 \equiv (X+2)^2 \pmod 5$, 因此

$$5 = \mathfrak{p}_5^2, \text{ 其中 } \mathfrak{p}_5 = (5, \omega+2) = [5, \omega+2].$$

現在我們計算一些 $P(b) = b^2 + b - 26 (b \geq 0)$ 的值, 如果它們的質因數全在 S_k 則將之列出。接下來我們找出 $\mathfrak{p}_p$ 的等價類之間的關係。

b	$P(b)$
1	$-24 = -2^3 \cdot 3$
2	$-20 = -2^2 \cdot 5$
4	$-6 = -2 \cdot 3$
5	$4 = 2^2$
6	$16 = 2^4$
7	$30 = 2 \cdot 3 \cdot 5$
9	$64 = 2^6$

- $b = 5$. 這時 $1 \sim (b+\omega) = [|P(b)|, b+\omega] = [4, 5+\omega] = [4, 1+\omega] = [2, 1+\omega]^2 = \mathfrak{p}_2'^2$, 因此

$$\mathfrak{p}_2^2 \sim 1.$$

- $b = 2$. 這時 $1 \sim [20, 2+\omega] = [2, \omega]^2[5, 2+\omega] = \mathfrak{p}_2^2\mathfrak{p}_5$, 因此

$$\mathfrak{p}_5 \sim 1.$$

- $b = 4$. 這時 $1 \sim [6, 4+\omega] = [2, \omega][3, 1+\omega] = \mathfrak{p}_2\mathfrak{p}_3$, 因此

$$\mathfrak{p}_3 \sim \mathfrak{p}'_2.$$

由以上的計算結果, 可以確定理想類群由 $\mathfrak{p}_2$ 的理想類生成, 而 $\mathfrak{p}_2$ 的理想類的階數 (order) 爲 1 或 2。注意到 $\mathfrak{p}_2 = (2, \omega)$ 並非一個主理想, 所以它的階數爲 2。因此, 我們確定理想類群同構到 C_2。

例 1.10. 考慮 $m = -105$ 的情況。這時 $\omega = \sqrt{-105}$ 且 $\Delta_k = -420 = -2^2 \cdot 3 \cdot 5 \cdot 7$。Minkowski 常數爲 $M_k = \frac{2}{\pi}\sqrt{-\Delta_k} = \frac{4\sqrt{105}}{\pi}$, 所以我們只需考慮質數 $2, 3, 5, 7, 11, 13$。它們代入 Kronecker 符號的值是

p	2	3	5	7	11	13
$\chi_k(p)$	0	0	0	0	1	1

因此 $S_k = \{2, 3, 5, 7, 11, 13\}$。現在我們在模 p 底下分解多項式 $f_\omega(X) = X^2 + 105$, 其中 $p \in S_k$。

- $p = 2$. $X^2 + 105 \equiv (X + 1)^2$, 所以

$$2 = \mathfrak{p}_2^2, \text{ 其中 } \mathfrak{p}_2 = (2, \omega + 1) = [2, 1 + \omega].$$

- $p = 3$. $X^2 + 105 \equiv X^2$, 所以

$$3 = \mathfrak{p}_3^2, \text{ 其中 } \mathfrak{p}_3 = (3, \omega) = [3, \omega].$$

- $p = 5$. $X^2 + 105 \equiv X^2$, 所以

$$5 = \mathfrak{p}_5^2, \text{ 其中 } \mathfrak{p}_5 = (5, \omega) = [5, \omega].$$

- $p = 7$. $X^2 + 105 \equiv X^2$, 所以

$$7 = \mathfrak{p}_7^2, \text{ 其中 } \mathfrak{p}_7 = (7, \omega) = [7, \omega].$$

- $p = 11$. $X^2 + 105 \equiv (X + 4)(X + 7)$, 所以

$$11 = \mathfrak{p}_{11}\mathfrak{p}'_{11}, \text{ 其中 } \mathfrak{p}_{11} = (11, \omega + 4) = [11, 4 + \omega], \mathfrak{p}'_{11} = (11, \omega + 7) = [11, 7 + \omega].$$

- $p = 13$. $X^2 + 105 \equiv (X + 5)(X + 8)$, 所以

$$13 = \mathfrak{p}_{13}\mathfrak{p}'_{13}, \text{ 其中 } \mathfrak{p}_{13} = (13, \omega + 5) = [11, 5 + \omega], \mathfrak{p}'_{13} = (13, \omega + 8) = [11, 8 + \omega].$$

我們計算一些 $P(b) = b^2 + 105, b \geq 0$ 的值。如果質因數都在 S_k 中, 則將 $P(b)$ 列出。

b	$P(b)$
0	$105 = 3 \cdot 5 \cdot 7$
4	$121 = 11^2$
5	$130 = 2 \cdot 5 \cdot 13$
7	$154 = 2 \cdot 7 \cdot 11$
8	$169 = 13^2$

由上述的分解, 我們得知 $\mathfrak{p}_p, p = 2, 3, 5, 7$ 的等價類在理想類群的階數爲 1 或 2。

- $b = 4$. $1 \sim [121, \omega + 4] = [11, \omega + 4]^2 = \mathfrak{p}_{11}^2$, 所以 $\mathfrak{p}_{11}$ 的等價類爲 1 或 2 階。
- $b = 8$. $1 \sim [169, \omega + 8] = [13, \omega + 8]^2 = {\mathfrak{p}'_{13}}^2$, 所以 $\mathfrak{p}_{13}$ 的等價類爲 1 或 2 階。
- $b = 5$. $1 \sim [130, \omega + 5] = [2, \omega + 5][5, \omega + 5][13, \omega + 5] = \mathfrak{p}_2\mathfrak{p}_5\mathfrak{p}_{13}$, 所以 $\mathfrak{p}_5 \sim \mathfrak{p}_2\mathfrak{p}_{13}$。
- $b = 7$. $1 \sim [154, \omega + 7] = [2, \omega + 7][7, \omega + 7][11, \omega + 7] = \mathfrak{p}_2\mathfrak{p}_7\mathfrak{p}'_{11}$, 所以 $\mathfrak{p}_7 \sim \mathfrak{p}_2\mathfrak{p}_{11}$。
- $b = 0$. $1 \sim [105, \omega] = [3, \omega][5, \omega][7, \omega] = \mathfrak{p}_3\mathfrak{p}_5\mathfrak{p}_7$, 所以 $\mathfrak{p}_3 \sim \mathfrak{p}_2\mathfrak{p}_{13}$。

由以上資訊, 我們得知理想類群由三個元素生成:$\mathfrak{p}_2$、$\mathfrak{p}_{11}$、$\mathfrak{p}_{13}$ 的等價類。注意到這些理想並非主理想, 所以它們的階數都是 2。現在我們檢查它們之間是否有其它關係。

- $\mathfrak{p}_2\mathfrak{p}_{11} = (2, \omega + 1)(11, \omega + 4) = (22, \omega + 15)$。這個理想不是主理想。
- $\mathfrak{p}_2\mathfrak{p}_{13} = (2, \omega + 1)(13, \omega + 5) = (26, \omega + 15)$。這個理想不是主理想。
- $\mathfrak{p}_{11}\mathfrak{p}_{13} = (2, \omega + 1)(13, \omega + 5) = (26, \omega + 5)$。這個理想不是主理想。
- $\mathfrak{p}_2\mathfrak{p}_{11}\mathfrak{p}_{13} = (2, \omega + 1)(11, \omega + 4)(13, \omega + 5) = (286, \omega + 213)$。這個理想不是主理想。

因此, k 的理想類群同構於 $C_2 \times C_2 \times C_2$。

我們在往後的兩個例子中省略計算過程, 只敘述主要結果。讀者可以用數學軟體系統, 例如 **Sage**, 來檢查例子中理想類之間的關係, 甚至可以用一行指令得知理想類群的結構 [1]。

例 1.11. 考慮 $m = 2021$ 的情況。這時 $\omega = \frac{1+\sqrt{2021}}{2}$ 且 $\Delta_k = 2021 = 43 \cdot 47$。集合 $S_k = \{5, 17, 19\}$。我們列出 S_k 中的質數 p 在 k 中的質理想分解:

$$\begin{aligned} 5 &= \mathfrak{p}_5\mathfrak{p}'_5, \text{ 其中 } \mathfrak{p}_5 = [5, \omega - 1],\ \mathfrak{p}'_5 = [5, \omega] \\ 17 &= \mathfrak{p}_{17}\mathfrak{p}'_{17}, \text{ 其中 } \mathfrak{p}_{17} = [17, \omega + 3],\ \mathfrak{p}'_{17} = [17, \omega + 13] \\ 19 &= \mathfrak{p}_{19}\mathfrak{p}'_{19}, \text{ 其中 } \mathfrak{p}_{19} = [19, \omega + 5],\ \mathfrak{p}'_{19} = [19, \omega + 13]. \end{aligned}$$

$\mathfrak{p}_{17}\mathfrak{p}'_5$ 和 $\mathfrak{p}_{19}\mathfrak{p}_5$ 在理想類群中都等價於 1, 所以可以推得理想類群由 $\mathfrak{p}_5$ 的理想類生成。$\mathfrak{p}_5, \mathfrak{p}_5^2$ 都不是主理想, 但 $\mathfrak{p}_5^3$ 是主理想。因此理想類群同構到 C_3。

[1] 請參閱 https://doc.sagemath.org/html/en/reference/number_fields/sage/rings/number_field/class_group.html

例 1.12. 考慮 $m = -2021$ 的情況。這時 $\omega = \sqrt{-2021}$, 而且

$$S_k = \{2, 3, 5, 7, 11, 17, 23, 29, 31, 43, 47, 53\}.$$

我們列出 S_k 中的質數 p 在 k 中的質理想分解:

$$\begin{aligned}
2 &= \mathfrak{p}_2^2, \text{ 其中 } \mathfrak{p}_2 = [2, \omega + 1],\\
3 &= \mathfrak{p}_3\mathfrak{p}_3', \text{ 其中 } \mathfrak{p}_3 = [3, \omega + 1],\ \mathfrak{p}_3' = [3, \omega + 1],\\
5 &= \mathfrak{p}_5\mathfrak{p}_5', \text{ 其中 } \mathfrak{p}_5 = [5, \omega + 2],\ \mathfrak{p}_5' = [5, \omega + 3],\\
7 &= \mathfrak{p}_7\mathfrak{p}_7', \text{ 其中 } \mathfrak{p}_7 = [7, \omega + 3],\ \mathfrak{p}_7' = [7, \omega + 4],\\
11 &= \mathfrak{p}_{11}\mathfrak{p}_{11}', \text{ 其中 } \mathfrak{p}_{11} = [11, \omega + 5],\ \mathfrak{p}_{11}' = [11, \omega + 6],\\
17 &= \mathfrak{p}_{17}\mathfrak{p}_{17}', \text{ 其中 } \mathfrak{p}_{17} = [17, \omega + 6],\ \mathfrak{p}_{17}' = [17, \omega + 11],\\
23 &= \mathfrak{p}_{23}\mathfrak{p}_{23}', \text{ 其中 } \mathfrak{p}_{23} = [23, \omega + 7],\ \mathfrak{p}_{23}' = [23, \omega + 16],\\
29 &= \mathfrak{p}_{29}\mathfrak{p}_{29}', \text{ 其中 } \mathfrak{p}_{29} = [29, \omega + 3],\ \mathfrak{p}_{29}' = [29, \omega + 26],\\
31 &= \mathfrak{p}_{31}\mathfrak{p}_{31}', \text{ 其中 } \mathfrak{p}_{31} = [31, \omega + 5],\ \mathfrak{p}_{31}' = [31, \omega + 26],\\
43 &= {\mathfrak{p}_{43}}^2, \text{ 其中 } \mathfrak{p}_{43} = [43, \omega],\\
47 &= {\mathfrak{p}_{47}}^2, \text{ 其中 } \mathfrak{p}_{47} = [47, \omega],\\
53 &= \mathfrak{p}_{53}\mathfrak{p}_{53}', \text{ 其中 } \mathfrak{p}_{53} = [53, \omega + 24],\ \mathfrak{p}_{53}' = [53, \omega + 29].
\end{aligned}$$

以下的理想乘積都是主理想, 也就是說, 它們在理想類群中都等價於 1。

$$\mathfrak{p}_2{\mathfrak{p}_5'}^{17}\mathfrak{p}_{43},\ \mathfrak{p}_3{\mathfrak{p}_5'}^{9}\mathfrak{p}_{43},\ \mathfrak{p}_7{\mathfrak{p}_5'}^{5}\mathfrak{p}_{43},\ \mathfrak{p}_{11}{\mathfrak{p}_5'}^{14}\mathfrak{p}_{43},\ \mathfrak{p}_{17}{\mathfrak{p}_5}^{6},\ \mathfrak{p}_{23}{\mathfrak{p}_5}^{2}\mathfrak{p}_{43},\ \mathfrak{p}_{29}{\mathfrak{p}_5'}^{13},\ \mathfrak{p}_{31}{\mathfrak{p}_5'}^{13}\mathfrak{p}_{43},\ \mathfrak{p}_{47}\mathfrak{p}_{43}.$$

我們發現理想類群由兩個元素生成:$\mathfrak{p}_{43}$ 和 $\mathfrak{p}_5$ 的理想類。43 在 k 中的質理想分解告訴我們, $\mathfrak{p}_{43}$ 的理想類的階數爲 2。至於 $\mathfrak{p}_5$, 它的 34 次方是一個主理想, 但它的 2 次方和 17 次方並不是。因此, k 的理想類群同構於 $C_2 \times C_{34}$。

2. 二次體上的上同調 (Cohomology)

在第二節中, 我們將二次體的 Galois 群作用在狹義理想類群上, 觀察上同調群發生的現象。

2.1. 循環體上的上同調

在這一小節中, 我們複習一些群作用在模上的結果。

定義 2.1. 如果一個群 G 在 $\mathbb{Z}$-模 A 上的群作用, 滿足

$$\text{對任何 } a,b\in A \text{ 和 } \sigma\in G,\quad \sigma(a+b)=\sigma a+\sigma b$$

則稱 A 爲一個 G-模 $(G\text{-}module)$。

定義 2.2. 如果在兩個 G-模之間的同態 $f:A\to B$ 滿足

$$\text{對任何 } a\in A \text{ 和 } \tau\in G,\quad f(\tau a)=\tau f(a)$$

則稱 f 爲一個 G-同態 $(G\text{-}homomorphism)$。

在這一小節, 我們假設 $G=\langle\sigma\rangle$ 是一個階數爲 n 的循環群。定義

$$\Delta=1-\sigma, N=1+\sigma+\cdots+\sigma^{n-1}.$$

也就是說, 對於 $a\in A$

$$\Delta(a)=a-\sigma(a), N(a)=a+\sigma(a)+\cdots+\sigma^{n-1}(a).$$

注意到 Δ 和 N 是 A 的自同態。它們滿足 $\Delta N=N\Delta=0$, 所以我們可以考慮以下序列

$$A\xrightarrow{N}A\xrightarrow{\Delta}A \quad \text{和} \quad A\xrightarrow{\Delta}A\xrightarrow{N}A.$$

定義 2.3. 以下的兩個群

$$H^0(A)=\frac{\ker\Delta}{\operatorname{Im}N} \quad \text{和} \quad H^1(A)=\frac{\ker N}{\operatorname{Im}\Delta}$$

被稱爲 A 的 上同調群 $(cohomology\ groups)$。有時我們記 $A^G=\ker\Delta$ 和 ${}_NA=\ker N$。

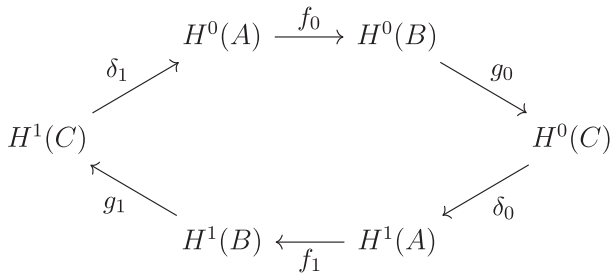
命題 2.4. 假設 A, B 爲兩個 G-模且 $f:A\to B$ 是一個 G-同態。則 f 導出上同調群間的同態

$$H^0(A)\xrightarrow{f_0}H^0(B) \text{ 和 } H^1(A)\xrightarrow{f_1}H^1(B).$$

定理 2.5. 對任何 G-模的正合序列 (exact sequence)

$$1\to A\xrightarrow{f}B\xrightarrow{g}C\to 1, \quad \text{也就是 } f \text{ 是單射, } g \text{ 是滿射, 且 } \ker g=\operatorname{Im}f.$$

存在同態 δ_0 和 δ_1 使得下圖的每個序列皆爲正合序列



定義 2.6. 設 G 爲一有限循環群且 A 爲一 G-模。當 $H^0(A)$ 和 $H^1(A)$ 都是有限群時, 我們稱有理數

$$Q(A) = \frac{|H^1(A)|}{|H^0(A)|}$$

爲 A 的 *Herbrand* 商 (*Herbrand quotient*)。

命題 2.7. 設 $1 \to A \to B \to C \to 1$ 爲 G-模之間的正合序列。若 $Q(A), Q(B), Q(C)$ 中的任兩個數有定義, 那第三數也有定義, 而且

$$Q(A)Q(B) = Q(C).$$

推論 **2.8.** 假設 B 是一個 G-模, A 是 B 的 G-子模, 且 $C = B/A$ 有限。若 $Q(A)$, $Q(B)$ 其中一數有定義, 則它們皆有定義, 而且 $Q(A) = Q(B)$。

2.2. 二次體上的上同調

使用先前的術語, 如果我們進一步假設 $A = 0$ 且 B 有限的話, 那麼 $C = B$ 且 $Q(A) = Q(B) = 1$, 因此 $|H^0(B)| = |H^1(B)|$。將上面的討論整理如下:

命題 2.9. 設 A 爲一有限 G-模。我們有 $|H^0(A)| = |H^1(A)|$。

設 $k/\mathbb{Q}$ 爲二次體, 其 Galois 群爲 $G = \mathrm{Gal}(k/\mathbb{Q}) = \langle\sigma\rangle$。我們將 k 中的分式理想 (fractional ideal) 所構成的群記爲 I_k, 稱爲 k 的分式理想群, 並將 I_k 的一個子群 — 由 k 中的分式主理想 (principal fractional ideal) $(\alpha), \alpha \in k^\times$ 所構成的群, 記爲 P_k。

定義 2.10.

(1) 定義

$$P_k^+ = \big\{(\alpha) \in P_k : N_{k/\mathbb{Q}}(\alpha) > 0\big\}$$

它是 P_k 的子群。

(2) 若 k 是實二次體, 則 k 的單位群 (unit group) $\mathfrak{o}_k^\times$ 可表示成 $\{\pm\epsilon^n, n \in \mathbb{Z}\}$。其中 $\epsilon > 1$ 的唯一單位元稱作 基本單位元 (*fundamental unit*)。

命題 2.11. 當 k 是一個實二次體, 我們令 ϵ 爲 k 的基本單位元。則

$$[P_k : P_k^+] = \begin{cases} 1, & \Delta_k < 0 \text{ 或 } (\Delta_k > 0 \text{ 且 } N\epsilon = -1); \\ 2, & \Delta_k > 0 \text{ 且 } N\epsilon = 1. \end{cases}$$

定義 2.12. 我們將商群

$$H_k^+ = I_k/P_k^+$$

稱作 狹義理想類群 (*ideal class group in the narrow sense*)。它的階數 h_k^+ 則稱爲 狹義類數 (*class number in the narrow sense*)。

上述的命題可以被重新改寫爲

命題 2.13.

$$h_k^+ = \begin{cases} h_k, & \Delta_k < 0 \text{ 或 } (\Delta_k > 0 \text{ 且 } N\epsilon = -1); \\ 2h_k, & \Delta_k > 0 \text{ 且 } N\epsilon = 1. \end{cases}$$

我們將 P_k^+ 在分式理想群上導出的等價關係記做 $\mathfrak{a} \underset{\sim}{+} \mathfrak{b}$。

注意到如果 $\mathfrak{a} \underset{\sim}{+} \mathfrak{b}$, 則存在 α 使得 $\mathfrak{b} = (\alpha)\mathfrak{a}$ 且 $N(\alpha) > 0$, 所以 $\mathfrak{b}^\sigma = (\alpha^\sigma)\mathfrak{a}^\sigma$, 其中 $N(\alpha^\sigma) = N(\alpha) > 0$; 也就是說, $\mathfrak{a}^\sigma \underset{\sim}{+} \mathfrak{b}^\sigma$。因此, 我們能定義群 G 在 H_k^+ 上的作用。

接下來我們將探討兩個上同調群

$$H^0(H_k^+) = (H_k^+)^G/NH_k^+ \quad \text{和} \quad H^1(H_k^+) = {}_NH_k^+/(H_k^+)^{1-\sigma}.$$

備註 2.14. 對 $\mathfrak{o}_k$ 中的理想 $\mathfrak{a}$, 我們介紹了兩種範數的概念:

$$\mathrm{N}_k(\mathfrak{a}) = [\mathfrak{o}_k : \mathfrak{a}] \text{ 和 } N\mathfrak{a} = \mathfrak{a}\mathfrak{a}^\sigma = \mathfrak{a}^{1+\sigma}.$$

它們之間的關係爲 $N\mathfrak{a} = (\mathrm{N}_k\mathfrak{a})$。

命題 2.15. 對一個二次體 $k/\mathbb{Q}$, 我們有

$$H^0(H_k^+) = {}_2H_k^+ = \left\{ g \in H_k^+ \mid g^2 = 1 \right\} \quad \text{和} \quad H^1(H_k^+) = {}^{H_k^+}\!/_{(H_k^+)^2}.$$

因此 $H^0(H_k^+) \simeq H^1(H_k^+)$.

證明: 設 $[\mathfrak{a}] \in H_k^+$ 是一個狹義理想類。因爲 $N\mathfrak{a} = (\mathrm{N}_k\mathfrak{a}) \underset{\sim}{+} 1$, 我們有 $N[\mathfrak{a}] = 1$。換句話說, $NH_k^+ = \{1\}$, 因此 $H^0(H_k^+) = (H_k^+)^G$。接著,

$$[\mathfrak{a}] \in (H_k^+)^G \Leftrightarrow [\mathfrak{a}]^\sigma = [\mathfrak{a}] \Leftrightarrow \mathfrak{a}^\sigma \underset{\sim}{+} \mathfrak{a} \Leftrightarrow \mathfrak{a}^{-1} \underset{\sim}{+} \mathfrak{a} \Leftrightarrow \mathfrak{a}^2 \underset{\sim}{+} 1$$

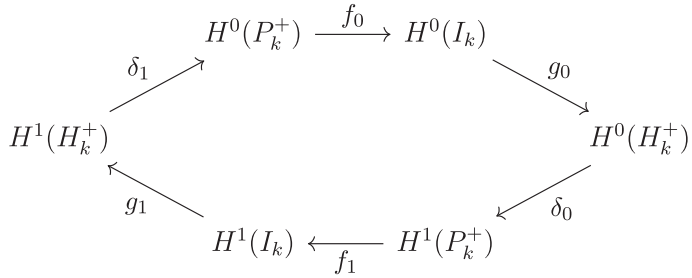
所以 $H^0(H_k^+) = {}_2H_k^+$。

根據一開始的論述, 我們有 ${}_NH_k^+ = H_k^+$。現在我們假設 $\mathfrak{a}\mathfrak{a}^\sigma \underset{\sim}{+} 1$, 則 $\mathfrak{a}^{-\sigma} \underset{\sim}{+} \mathfrak{a}$; 等價地, $\mathfrak{a}^{1-\sigma} \underset{\sim}{+} \mathfrak{a}^2$, 因而 $(H_k^+)^{1-\sigma} = (H_k^+)^2$。這就證明了 $H^1(H_k^+) = H_k^+/(H_k^+)^2$。 □

我們有以下 G-模的正合序列 $(G = \langle\sigma\rangle)$

$$1 \longrightarrow P_k^+ \xrightarrow{f} I_k \xrightarrow{g} H_k^+ \longrightarrow 1.$$

由定理 2.5, 我們得到正合的六邊形



事實上我們可以證明 $H^1(I_k) = 1$。並且以下命題成立

命題 2.16. $H^1(P_k^+) = 1.$

證明: 對任何 $(\alpha) \in {}_N P_k^+$, 我們有 $N(\alpha) = (N\alpha) = (1)$ 且 $N\alpha > 0$, 所以 $N\alpha = 1$。我們不妨假設 $\alpha > 0$。因爲 $N\alpha = \alpha\alpha^\sigma = 1$,

$$\alpha + 1 = \alpha + \alpha\alpha^\sigma = \alpha(1 + \alpha^\sigma).$$

現在令 $\beta = \alpha + 1 \neq 0$。$\beta = \alpha\beta^\sigma$, 所以

$$\beta\alpha^{-1} = \beta^\sigma, \text{ 且 } N\beta = \beta\beta^\sigma = \beta^2\alpha^{-1} > 0.$$

最後, $\alpha = \beta^{1-\sigma}$, 所以 $(\alpha) = (\beta)^{1-\sigma} \in (P_k^+)^{1-\sigma}$。 □

備註 2.17. 如果我們考慮的是 H_k 而不是 H_k^+, 那麼我們無法證明 $H^1(P_k) = 1$, 因爲從 $(\alpha) \in {}_N P_k$ 無法推得 $N\alpha = 1$。

命題 2.18. 我們有下列正合序列

$$1 \longrightarrow (P_k^+)^G \longrightarrow I_k^G \longrightarrow (H_k^+)^G \longrightarrow 1.$$

證明: 因爲 $H^1(P_k^+) = 1$, 在六邊形中的同態

$$I_k^G \big/ NI_k = H^0(I_k) \xrightarrow{g_0} H^0(H_k^+) = (H_k^+)^G$$

是一個蓋射。因此 $I_k^G \to (H_k^+)^G$ 也是一個蓋射, 所以給定的序列是一個正合序列。 □

命題 2.19. 設 k 爲一個二次體, $l_1, \dots, l_t$ 爲判別式 Δ_k 的所有不同質因數, $\mathfrak{l}_1, \dots, \mathfrak{l}_t$ 爲 k 中的質理想, 分別對應於 $l_1, \dots, l_t$ 之上 (lying above):$l_i = \mathfrak{l}_i^2$ 且 $\mathfrak{l}_i^\sigma = \mathfrak{l}_i$。若 $2 \mid \Delta_k$ 我們令 $l_1 = 2$。則群 $I_k^G/(P_k^+)^G$ 由以下 2^t 個理想的理想類構成:

$$\mathfrak{l}_1^{\epsilon_1} \cdots \mathfrak{l}_t^{\epsilon_t}, \quad \epsilon_i = 0, 1.$$

證明: 將 $I_\mathbb{Q}$ 自然地嵌入 I_k 後, 我們有 $I_\mathbb{Q} \subset (P_k^+)^G$。假設 $\mathfrak{p}$ 是 $\mathfrak{a} \in I_k^G$ 的一個質因子 (也就是整除 $\mathfrak{a}$ 的質理想)。如果對於某個質數 p 我們有 $\mathfrak{p} = (p)$, 那麼 $\mathfrak{p}$ 的理想類是群 $I_k^G/(P_k^+)^G$ 中的單位元。如果 $\mathfrak{p}\mathfrak{p}^\sigma = (p)$,

$$\text{對任何 } \alpha, \beta \in \mathbb{N},\ \mathfrak{p}^\alpha(\mathfrak{p}^\sigma)^\beta \mid \mathfrak{a} \Longrightarrow (\mathfrak{p}^\sigma)^\alpha \mathfrak{p}^\beta \mid \mathfrak{a}^\sigma = \mathfrak{a}.$$

取一組最大的 α, β, 則 $\alpha = \beta$。因此

$$\mathfrak{p}^\alpha(\mathfrak{p}^\sigma)^\beta = (\mathfrak{p}\mathfrak{p}^\sigma)^\alpha = (p)^\alpha \in I_\mathbb{Q},$$

而且 $\mathfrak{p}$ 的理想類也是群 $I_k^G/(P_k^+)^G$ 中的單位元。因此唯一貢獻 $I_k^G/(P_k^+)^G$ 非平凡部分的質因子只有 $\mathfrak{l}_1^{\epsilon_1} \cdots \mathfrak{l}_t^{\epsilon_t}$ 的理想類。 □

命題 2.20. 我們有 $|I_k^G/(P_k^+)^G| \le 2^{t-1}$.

證明: 我們只須證明存在一組 $(\epsilon_1, \dots, \epsilon_t) \neq (0, \dots, 0)$ 使得

$$\mathfrak{l}_1^{\epsilon_1} \cdots \mathfrak{l}_t^{\epsilon_t} \underset{\sim}{+} 1.$$

分兩種情況:

情況 1: $(\Delta_k < 0)$ 或 $(\Delta_k > 0$ 且 $N\epsilon = -1)$。

(a) $m \equiv 1 \pmod 4$. 這時 $\Delta_k = m = \pm l_1 \cdots l_t$, 所以 $(\sqrt{m}) = \mathfrak{l}_1 \cdots \mathfrak{l}_t$。必要時乘上 ϵ, 我們得到 $\mathfrak{l}_1 \cdots \mathfrak{l}_t \underset{\sim}{+} 1$。

(b) $m \equiv 2 \pmod 4$. $\Delta_k = 4m = \pm 8 l_2 \cdots l_t$, 所以 $(\sqrt{m}) = \mathfrak{l}_1\mathfrak{l}_2 \cdots \mathfrak{l}_t \underset{\sim}{+} 1$。

(c) $m \equiv 3 \pmod 4$. $\Delta_k = 4m = \pm 4 l_2 \cdots l_t$, 所以 $(\sqrt{m}) = \mathfrak{l}_2 \cdots \mathfrak{l}_t \underset{\sim}{+} 1$.

情況 2: $\Delta_k > 0$ 且 $N\epsilon = 1$. 我們可以取 ϵ 使得 $\epsilon > 1$。令 $(1+\epsilon) = (a)\mathfrak{a}$, 其中 $a \in \mathbb{N}$ 且 $\mathfrak{a}$ 是本原理想。注意到 $\epsilon(1+\epsilon^\sigma) = 1+\epsilon$, 由此可以推得 $\mathfrak{a}^\sigma = \mathfrak{a}$, 因此 $\mathfrak{a} \in I_k^G$。由上一個命題的證明, 我們可以將 $\mathfrak{a}$ 寫爲 $\mathfrak{a} = \mathfrak{l}_1^{\epsilon_1} \cdots \mathfrak{l}_t^{\epsilon_t}$, 其中 $\epsilon_i = 0, 1$。如果 $(\epsilon_1, \dots, \epsilon_t) = (0, \dots, 0)$, 那麼 $\mathfrak{a} = (1)$, 也因此對某個單位元 $\eta \in \mathfrak{o}_k^\times$, $1 + \epsilon = a\eta$。我們有 $\epsilon + \epsilon^\sigma = \epsilon + \epsilon^{-1} > 0$, 所以 $N\eta > 0$, 故 $N\eta = 1$。因爲 $1 + \epsilon^\sigma = a\eta^\sigma = a\eta^{-1}$,

$$\epsilon = \frac{1+\epsilon}{1+\epsilon^\sigma} = \eta^2.$$

這和 ϵ 是基本單位元的假設矛盾。因爲 $N(1+\epsilon)>0$,

$$1 \underset{\sim}{+} (1+\epsilon) \underset{\sim}{+} \mathfrak{a} = \mathfrak{l}_1^{\epsilon_1} \cdots \mathfrak{l}_t^{\epsilon_t}. \qquad \square$$

定理 2.21. 兩個群 $H^0(H_k^+)$ 和 $H^1(H_k^+)$ 同構, 而且它們的階數爲 2^{t-1}, 其中 t 是 Δ_k 相異質因數的個數。

證明: 由命題 2.15, 我們知道群 $H^0(H_k^+)$ 和 $H^1(H_k^+)$ 同構, 並且

$$|H^0(H_k^+)| = |(H_k^+)^G| = \left| I_k^G \big/ (P_k^+)^G \right|.$$

我們只須證明命題 2.20 中的等號成立; 也就是說, 證明 $I_k^G/(P_k^+)^G$ 中的生成元在群中的關係式

$$\mathfrak{l}_1^{\epsilon_1} \cdots \mathfrak{l}_t^{\epsilon_t} \underset{\sim}{+} 1 \qquad (*)$$

只有之前的證明中的找到的那些而已。假設

$$\mathfrak{l}_1^{\epsilon_1} \cdots \mathfrak{l}_t^{\epsilon_t} = (\alpha), \quad N\alpha > 0.$$

$(\alpha)^\sigma = (\alpha)$, 所以對某個單位元 η 我們有 $\alpha^\sigma = \eta\alpha$。$N\eta = 1$。

分三種情況:

情況 1. 假設 $\Delta_k < 0$。我們排除 $k = \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3})$ 的顯然情形後 (這時 $h_k = h_k^+ = 1$), 便可以假設 $\eta = \pm 1$。如果 $\eta = 1$, 則 $\alpha^\sigma = \alpha$, 因此 $\alpha \in \mathbb{Z}$。理想 $\mathfrak{l}_1^{\epsilon_1} \cdots \mathfrak{l}_t^{\epsilon_t}$ 是本原理想, 所以 $\alpha = \pm 1$, 故 $\epsilon_1 = \cdots = \epsilon_t = 0$。如果 $\eta = -1$, 則 $\alpha^\sigma = -\alpha$。因爲 α 是純虛數, 所以可以被寫成 $\alpha = a\sqrt{m}$, 其中 $a \in \mathbb{Z}$。由於理想 $\mathfrak{l}_1^{\epsilon_1} \cdots \mathfrak{l}_t^{\epsilon_t}$ 是本原理想, $a = \pm 1$, 因而 $(*)$ 中的理想是 $\mathfrak{l}_1^{\epsilon_1} \cdots \mathfrak{l}_t^{\epsilon_t} = (\sqrt{m})$。這是命題 2.20 證明中的情況 1。

情況 2. 假設 $\Delta_k > 0$ 且 $N\epsilon = -1$。因爲 $N\eta = 1$, 所以存在整數 v 使得 $\eta = \epsilon^{2v}$。此時 $\alpha^\sigma = \epsilon^{2v}\alpha$。

$$(\epsilon^\sigma)^v \alpha^\sigma = (\epsilon^\sigma)^v \epsilon^{2v} \alpha = (N\epsilon)^v \epsilon^v \alpha = (-1)^v \epsilon^v \alpha.$$

如果 v 是偶數, 則 $(\epsilon^v\alpha)^\sigma = (\epsilon^v\alpha)$, 所以 $\epsilon^v\alpha$ 是整數。因爲 $\mathfrak{l}_1^{\epsilon_1} \cdots \mathfrak{l}_t^{\epsilon_t}$ 是本原理想, 我們有 $\epsilon_1 = \cdots = \epsilon_t = 0$。如果 v 是奇數, 則存在整數 $a \in \mathbb{Z}$ 使得 $\epsilon^v\alpha = a\sqrt{m}$。

$$\mathfrak{l}_1^{\epsilon_1} \cdots \mathfrak{l}_t^{\epsilon_t} = (\alpha) = (a\sqrt{m}) \Rightarrow a = \pm 1.$$

我們得到命題 2.20 證明中情況 1 的關係式。

情況 3. 假設 $\Delta_k > 0$ 且 $N\epsilon = 1$。此時 $\epsilon = \dfrac{1+\epsilon}{1+\epsilon^\sigma}$。存在整數 n 使得

$$\eta = \epsilon^{-n} = \frac{(1+\epsilon^\sigma)^n}{(1+\epsilon)^n}, \quad \alpha^\sigma = \eta\alpha = \frac{(1+\epsilon^\sigma)^n}{(1+\epsilon)^n}\alpha$$

所以

$$\frac{\alpha}{(1+\epsilon)^n} \in \mathbb{Q}, \quad \text{存在} a \in \mathbb{Q}^\times \text{使得} \alpha = a(1+\epsilon)^n.$$

因此我們有 $\mathfrak{l}_1^{\epsilon_1}\cdots\mathfrak{l}_t^{\epsilon_t} = (a)(1+\epsilon)^n$。如同命題 2.20 證明中的情況 2, $(1+\epsilon) = (b)\mathfrak{l}_1^{\eta_1}\cdots\mathfrak{l}_t^{\eta_t}$ 其中 $\eta_i = 0, 1$, $(\eta_1, \ldots, \eta_t) \neq (0, \ldots, 0)$, 且 $b \in \mathbb{N}$。因此, 存在互質的兩個正整數 A, B 使得

$$A\mathfrak{l}_1^{\epsilon_1}\cdots\mathfrak{l}_t^{\epsilon_t} = B\mathfrak{l}_1^{n\eta_1}\cdots\mathfrak{l}_t^{n\eta_t}.$$

如果 n 是偶數, 則右邊的理想可被一個整數生成, 因此 $(\epsilon_1, \ldots, \epsilon_t) = (0, \ldots, 0)$。如果 n 是奇數, 我們不妨假設 $n = 1$, 則 $A\mathfrak{l}_1^{\epsilon_1}\cdots\mathfrak{l}_t^{\epsilon_t} = B\mathfrak{l}_1^{\eta_1}\cdots\mathfrak{l}_t^{\eta_t}$。因爲 $\mathfrak{l}_1^{\epsilon_1}\cdots\mathfrak{l}_t^{\epsilon_t}$ 和 $\mathfrak{l}_1^{\eta_1}\cdots\mathfrak{l}_t^{\eta_t}$ 都是本原理想, 我們有 $A = B = 1$ 且 $(\epsilon_1, \ldots, \epsilon_t) = (\eta_1, \ldots, \eta_t)$。這是命題 2.20 證明中的情況 2。□

定理 2.22. 假設 k 是一個二次體。如果它的判別式 Δ_k 是質數, 則狹義類數 h_k^+ 是奇數。如果更進一步假設 $\Delta_k > 0$, 則 k 的基本單位元 ϵ 滿足 $N\epsilon = -1$。

證明: Δ_k 的相異質因數個數 (定理 2.21 中的 t) 等於 1, 所以 $|H^0(H_k^+)| = |{}_2H_k^+| = 1$。在 H_k^+ 中並沒有偶數階的元素, 因此 h_k^+ 是奇數。更進一步, 如果 $\Delta_k > 0$ 而且 $N\epsilon = 1$, 則由命題 2.13 我們得到 $h_k^+ = 2h_k$, 矛盾。□

備註 2.23. 對二次體 $k = \mathbb{Q}(\sqrt{m})$ 來說, $t = 1$ 若且唯若 k 是 $\mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{2})$, 或 $\mathbb{Q}(\sqrt{l^*})$, 其中 l 是一個奇質數而 $l^* = (-1)^{\frac{l-1}{2}}l$。

定理 2.24. 設 k 爲二次體。當 $\Delta_k > 0$, 令 ϵ 爲基本單位元。則我們可以列出以下結果

	$H^0(\mathfrak{o}_k^\times)$	$H^1(\mathfrak{o}_k^\times)$	$Q(\mathfrak{o}_k^\times)$
$\Delta_k < 0$	2	2	1
$\Delta_k > 0, N\epsilon = 1$	2	4	2
$\Delta_k < 0, N\epsilon = -1$	1	2	2

證明: 首先, $H^0(\mathfrak{o}_k^\times) = (\mathfrak{o}_k^\times)^G/N(\mathfrak{o}_k^\times) = \{\pm 1\}/N(\mathfrak{o}_k^\times)$。這完成了第一行的證明。對於表格其他部分, 我們分成以下情形討論。

- 假設 $\Delta_k < 0$ 且 $k \neq \mathbb{Q}(i)$ 或 $\mathbb{Q}(\sqrt{-3})$. 此時 $\mathfrak{o}_k^\times = \{\pm 1\}$. 因爲 ${}_N\mathfrak{o}_k^\times = \mathfrak{o}_k^\times = \{\pm 1\}$ 且 $(\mathfrak{o}_k^\times)^{1-\sigma} = \{1\}$, 所以 $H^1(\mathfrak{o}_k^\times)$ 的階數是 2。

- 假設 $k=\mathbb{Q}(i)$. 因爲 $\mathfrak{o}_k^\times=\{\pm1,\pm i\}={}_N\mathfrak{o}_k^\times$, $(\mathfrak{o}_k^\times)^{1-\sigma}=\{\pm1\}$, 所以 $H^1(\mathfrak{o}_k^\times)$ 的階數是 2。

- 假設 $k=\mathbb{Q}(\sqrt{-3})=\mathbb{Q}(\rho)$. 因爲 $\mathfrak{o}_k^\times=\{\pm1,\pm\rho,\pm\rho^2\}={}_N\mathfrak{o}_k^\times$ 且 $(\mathfrak{o}_k^\times)^{1-\sigma}=\{1,\rho^2,\rho\}$, 所以 $|H^1(\mathfrak{o}_k^\times)|=2$。

- 假設 $\Delta_k>0$ 且 $N\epsilon=1$. 此時 $\mathfrak{o}_k^\times=\{\pm1\}\times\langle\epsilon\rangle={}_N\mathfrak{o}_k^\times$ 且 $(\mathfrak{o}_k^\times)^{1-\sigma}=\{1\}\times\langle\epsilon\rangle^{1-\sigma}$. 因爲 $1=\epsilon\epsilon^\sigma$, 我們有 $\dfrac{\epsilon}{\epsilon^\sigma}=\epsilon^2$, 因此 $\langle\epsilon\rangle^{1-\sigma}=\langle\epsilon^2\rangle$。所以 $|H^1(\mathfrak{o}_k^\times)|=4$。

- 假設 $\Delta_k>0$ 且 $N\epsilon=-1$. 此時 $\mathfrak{o}_k^\times=\{\pm1\}\times\langle\epsilon\rangle$ 且 ${}_N\mathfrak{o}_k^\times=\{\pm1\}\times\langle\epsilon^2\rangle$, 因爲 $\dfrac{\epsilon}{\epsilon^\sigma}=-\epsilon^2$, 所以 $\langle\epsilon\rangle^{1-\sigma}=\langle-\epsilon^2\rangle$, 因此 $|H^1(\mathfrak{o}_k^\times)|=2$。 □

3. 高斯虧格理論

在第三節中, 對於一個二次體 k, 我們將定義 $(\mathbb{Z}/\Delta_k\mathbb{Z})^\times$ 上的數個特徵標 (character), 並且討論這些特徵標和二次體的上同調群間的關係。

3.1. 二次體上的 Kronecker 特徵標

假設 $k=\mathbb{Q}(\sqrt{m})$ 是二次體, 其中 m 是一個整數, 不被大於 1 的平方數整除。記 $S=\{p\text{是質數}:p\mid\Delta_k\}$。則對於 $p\notin S$, p 在 k 中沒有分歧 (unramified)。記

$$I_{\mathbb{Q}}(\Delta_k)=I_{\mathbb{Q}}(S)=\left\{a\in\mathbb{Q}^\times:a>0,\,\gcd(a,\Delta_k)=1\right\}.$$

我們知道 Artin 映射 $\alpha_{k/\mathbb{Q}}:I_{\mathbb{Q}(\Delta_k)}\to\mathrm{Gal}(k/\mathbb{Q})$ 由以下方式給定:

$$\alpha_{k/\mathbb{Q}}(p)=\left(\frac{k/\mathbb{Q}}{p}\right),$$

其中 $\left(\frac{k/\mathbb{Q}}{p}\right)$ 是 Artin 符號, σ 是 $\mathrm{Gal}(k/\mathbb{Q})$ 中的元素使得對任何 $x\in\mathfrak{o}_k$, $\sigma(x)\equiv x^p \bmod \mathfrak{p}_p$。我們有唯一的同構映射 $\varphi:\mathrm{Gal}(k/\mathbb{Q})\to\{\pm1\}$, 而且 *Kronecker* 特徵標 (*Kronecker character*) χ_k 被定義成 $\alpha_{k/\mathbb{Q}}$ 和 ψ 的合成

$$\begin{array}{ccc} & & \mathrm{Gal}(k/\mathbb{Q}) \\ & \overset{\alpha_{k/\mathbb{Q}}}{\nearrow} & \wr\big\downarrow\varphi \\ I_{\mathbb{Q}}(\Delta_k) & \xrightarrow{\chi_k} & \{\pm1\} \end{array}$$

我們接下來決定 $\chi_k(p)$ 的值。首先, 對 $p\nmid\Delta_k$, $\chi_k(p)=1$ 若且唯若 $\alpha_{k/\mathbb{Q}}(p)=1$ 若且

唯若 p 在 $k/\mathbb{Q}$ 中完全分歧 (split completely)。接著, 如果 $p \neq 2$, 則

$$\left(\frac{\Delta_k}{p}\right) = 1 \Longleftrightarrow p \text{ 在 } k \text{ 中完全分歧。}$$

如果 $p = 2$, 注意到這時 $m \equiv 1 \pmod 4$ 且 $\Delta_k = m$, 則

$$\Delta_k \equiv 1 \pmod 8 \Longleftrightarrow 2 \text{ 在 } k \text{ 中完全分歧。}$$

最終我們得到

$$\chi_k(p) = \begin{cases} \left(\frac{\Delta_k}{p}\right), & p \neq 2; \\ (-1)^{\frac{\Delta_k^2-1}{8}}, & p = 2. \end{cases}$$

Artin 映射 $\alpha_{k/\mathbb{Q}}$ 是個滿射。我們將探討它的核 $\ker \alpha_{k/\mathbb{Q}} = \ker \chi_k$。對 $a, a' \in I_{\mathbb{Q}}(\Delta_k)$ 我們記 $a = \dfrac{b}{c}, a' = \dfrac{b'}{c'}$, 其中 b, c, b', c' 是使得 $(\Delta_k, c) = (\Delta_k, c') = 1$ 的自然數。接著我們定義

$$a \equiv a' \pmod{\Delta_k} \quad \text{若 } bc' \equiv b'c \pmod{\Delta_k}.$$

記

$$S(\Delta_k) = \{a \in I_{\mathbb{Q}}(\Delta_k) : a \equiv 1 \pmod{\Delta_k}\}.$$

則 $S(\Delta_k)$ 是 $I_{\mathbb{Q}}(\Delta_k)$ 的一個子群。

現在令 I_k 爲 k 的分式理想群, 並記

$$I_k(\Delta_k) = \{\mathfrak{a} \in I_k : (\mathfrak{a}, \Delta_k) = 1\}.$$

範數映射 N_k 導出了一個同態 $I_k(\Delta_k) \longrightarrow I_{\mathbb{Q}}(\Delta_k)$。我們也將導出的映射記爲 N_k。

使用 Dirichlet 的等差數列定理 (Dirichlet's Theorem on arithmetic progressions), 我們可以證明

定理 3.1. 對任何二次體 k 我們有 $\ker \chi_k = S(\Delta_k)\mathrm{N}_k(I_k(\Delta_k))$。

3.2. 高斯虧格理論

如果 $\Delta_k \equiv 1 \pmod 4$, 則 $\Delta_k = m = \pm l_1 l_2 \cdots l_t$, 其中 l_i 是質數。對於和 Δ_k 互質的整數 n, 我們有

$$\chi_k(n) = \left(\frac{n}{l_1}\right) \cdots \left(\frac{n}{l_t}\right).$$

如果 $\Delta_k \equiv 0 \pmod 4$, 我們記

$$\Delta_k = 4m = 2^\beta \Delta_k', \quad \beta = \begin{cases} 3, & m \equiv 2 \pmod 4; \\ 2, & m \equiv 3 \pmod 4. \end{cases}$$

則對於和 Δ_k 互質的整數 n, 我們有

$$\chi_k(n) = (-1)^{\frac{n-1}{2}\frac{\Delta_k'-1}{2}+\left(\frac{n^2-1}{8}\right)\beta} \left(\frac{n}{l_2}\right) \cdots \left(\frac{n}{l_t}\right).$$

我們可以驗證

$$(-1)^{\frac{n-1}{2}\frac{\Delta_k'-1}{2}+\left(\frac{n^2-1}{8}\right)\beta} = \begin{cases} (-1)^{\frac{n-1}{2}}, & m \equiv 3 \pmod 4; \\ (-1)^{\frac{n^2-1}{8}}, & m \equiv 2 \pmod 8; \\ (-1)^{\frac{n^2-1}{8}+\frac{n-1}{2}}, & m \equiv 6 \pmod 8. \end{cases}$$

總結一下, 我們得到

定理 3.2. 設 $l_1, l_2, \ldots, l_t$ 爲 Δ_k 的相異質因數, 而且如果 $2 \mid \Delta_k$ 則令 $l_1 = 2$。對任何 $i = 1, \ldots, t$, 我們用以下方式定義群 $(\mathbb{Z}/\Delta_k\mathbb{Z})^\times$ 上的特徵標 χ_i:

(i) 如果 $2 \mid \Delta_k$, 則

$$\chi_1(n) = \begin{cases} (-1)^{\frac{n-1}{2}}, & m \equiv 3 \pmod 4; \\ (-1)^{\frac{n^2-1}{8}}, & m \equiv 2 \pmod 8; \\ (-1)^{\frac{n^2-1}{8}+\frac{n-1}{2}}, & m \equiv 6 \pmod 8, \end{cases}$$

$$\chi_i(n) = \left(\frac{n}{l_i}\right), \quad \text{對 } 2 \le i \le t.$$

(ii) 如果 $2 \nmid \Delta_k$, 則

$$\chi_i(n) = \left(\frac{n}{l_i}\right), \quad \text{對 } 1 \le i \le t.$$

則 Kronecker 特徵標 χ_k 可以被寫成

$$\chi_k(n) = \chi_1(n)\chi_2(n)\cdots\chi_t(n), \quad \text{對任何和 } \Delta \text{ 互質的整數 } n.$$

定理 3.3. 等式 $\chi_k(n) = 1$ 成立, 若且唯若存在一個理想 $\mathfrak{a} \subset \mathfrak{o}_k$ 使得 $(\mathfrak{a}, \Delta_k) = 1$ 且 $n \equiv \mathrm{N}\mathfrak{a} \pmod{\Delta_k}$。

證明: 定理 3.1 可以推得 ($\Leftarrow$) 方向。

($\Rightarrow$) 根據 Dirichlet 的等差數列定理, 存在奇質數 p 使得 $n \equiv p \pmod{\Delta_k}$。因爲 $\chi_k(p) = \chi_k(n) = 1$ 且 $p \nmid \Delta_k$, 我們有 $p = \mathrm{N}\mathfrak{p}$, 其中 $\mathfrak{p}$ 是 k 中對應 p 之上 (lying over p) 的質理想。因此 $n \equiv \mathrm{N}\mathfrak{p} \pmod{\Delta_k}$。 □

命題 3.4. 給定一個 $\mathfrak{o}_k$ 中的理想 $\mathfrak{m}$。則 H_k^+ 中的每個狹義理想類都有一個和 $\mathfrak{m}$ 互質的理想。

證明: 固定任何一個狹義理想類 $C \in H_k^+$, 並從 C^{-1} 取一個理想 $\mathfrak{a}$。令整除 $\mathfrak{m}$ 的不同質理想爲 $\mathfrak{p}_1, \ldots, \mathfrak{p}_l$。我們只須找到一個理想 $\mathfrak{b}$, 使得 $\mathfrak{ab} \underset{\sim}{+} 1$ 且 $(\mathfrak{b}, \mathfrak{p}_1 \cdots \mathfrak{p}_l) = 1$。對任何 $i = 1, \ldots, l$, 取 $\alpha_i \in \mathfrak{o}_k$ 使得

$$\alpha_i \in \mathfrak{a}\mathfrak{p}_1 \cdots \mathfrak{p}_{i-1}\mathfrak{p}_{i+1} \cdots \mathfrak{p}_l \text{ 且 } \alpha_i \notin \mathfrak{a}\mathfrak{p}_1 \cdots \mathfrak{p}_l,$$

並記 $\alpha = \alpha_1 + \cdots + \alpha_l$。則 $\alpha \in \mathfrak{a}$, 但對任何 $j = 1, \ldots, l$ 我們有 $\alpha \notin \mathfrak{a}\mathfrak{p}_j$。現在令 $a = \mathrm{N}\mathfrak{a}$ 和 $b = \mathrm{N}\mathfrak{m}$。將 β 記爲 $\beta = \alpha + abt$, 其中 t 是待定的正整數。那麼由 $a \in \mathfrak{a}$ 可推得 $\beta \in \mathfrak{a}$。但是, 對所有 $1 \le j \le l$, $\beta \notin \mathfrak{a}\mathfrak{p}_j$: 如果對某個 j 我們有 $\beta \in \mathfrak{a}\mathfrak{p}_j$, 則因爲 $abt \in \mathfrak{a}\mathfrak{p}_j$ 我們得到 $\alpha \in \mathfrak{a}\mathfrak{p}_j$, 矛盾。除此之外, $N(\alpha + abt) = N\alpha + \mathrm{Tr}_{k/\mathbb{Q}}(\alpha)abt + a^2b^2t^2$。我們取足夠大的 t 使得 $N\beta > 0$。最後, 因爲 $\beta \in \mathfrak{a}$, 我們能找到一個理想 $\mathfrak{b}$ 使得 $\mathfrak{ab} = (\beta)$。這個理想 $\mathfrak{b}$ 滿足

$$\mathfrak{ab} \underset{\sim}{+} 1 \quad \text{且} \quad (\mathfrak{b}, \mathfrak{p}_1 \cdots \mathfrak{p}_l) = 1. \qquad \square$$

命題 3.5. 考慮 $\mathfrak{o}_k$ 中滿足 $(\alpha, \Delta_k) = 1$ 的元素 α。對任何 $1 \le i \le t$ 我們有 $\chi_i(N\alpha) = 1$。

證明: 假設 $l = l_i \neq 2$。l 在 k 中分歧, 所以對於整除 l 的質理想 $\mathfrak{l}$, $[\mathfrak{o}_k/\mathfrak{l} : \mathbb{Z}/l\mathbb{Z}] = 1$。因此存在整數 a 使得 $(a, \Delta_k) = 1$ 且 $\alpha \equiv a \pmod{\mathfrak{l}}$。因爲 $\sigma(\mathfrak{l}) = \mathfrak{l}$, 我們有 $N\alpha = \alpha\sigma(\alpha) \equiv a^2 \pmod{l}$。因此 $\chi_i(N\alpha) = 1$。

當 $l = 2$, 我們有 $\Delta_k = 4m$, 其中 $m \equiv 2, 3 \pmod 4$。記 $\alpha = x + y\sqrt{m}$, 則 $N\alpha = x^2 - my^2$.

- 如果 $m \equiv 3 \pmod 4$, 則 $N\alpha \equiv x^2 + y^2 \equiv 1 \pmod 4$. $\chi_1(N\alpha) = (-1)^{\frac{N\alpha - 1}{2}} = 1$。
- 如果 $m \equiv 2 \pmod 4$, 則因爲 m 是偶數, 當 $N\alpha$ 是奇數時 x 必也是奇數。
  - 當 $m \equiv 2 \pmod 8$, 則 $N\alpha \equiv x^2 - 2y^2 \equiv 1, 7 \pmod 8$.
  $$\chi_1(N\alpha) = (-1)^{\frac{(N\alpha)^2 - 1}{8}} = 1.$$
  - 當 $m \equiv 6 \pmod 8$, 則 $N\alpha \equiv x^2 + 2y^2 \equiv 1, 3 \pmod 8$.
  $$\chi_1(N\alpha) = (-1)^{\frac{(N\alpha)^2 - 1}{8} + \frac{N\alpha - 1}{2}} = 1. \qquad \square$$

由命題 3.4, 任何 H_k^+ 中的狹義理想類都可以被寫成 $[\mathfrak{a}]$, 其中理想 $\mathfrak{a}$ 滿足 $(\mathfrak{a}, \Delta_k) = 1$。若 $[\mathfrak{a}] = [\mathfrak{b}]$, 則存在 $\alpha, \beta \in \mathfrak{o}_k$ 使得

$$(\beta)\mathfrak{a} = (\alpha)\mathfrak{b}, \quad (\alpha, \Delta_k) = (\beta, \Delta_k) = 1, \quad \text{還有 } N\alpha N\beta > 0.$$

我們說明爲何 $N\alpha N\beta > 0$: 這時 $\mathfrak{b} = (\gamma)\mathfrak{a}$ 對某個 γ 使得 $N\gamma > 0$, 取一個理想 $\mathfrak{c}$ 滿足 $\mathfrak{ac} = (\alpha)$ 和 $(\mathfrak{c}, \Delta_k) = 1$, 則

$$(\gamma) = \frac{\mathfrak{b}}{\mathfrak{a}} = \frac{\mathfrak{bc}}{\mathfrak{ac}} = \frac{\mathfrak{bc}}{(\alpha)}, \quad \mathfrak{bc} = (\alpha\gamma) \quad \text{且} \quad \beta = \alpha\gamma,$$

因此 $N\alpha N\beta = (N\alpha)^2 N\gamma > 0$。對 $(\beta)\mathfrak{a} = (\alpha)\mathfrak{b}$ 兩邊取範數, 我們有 $|N\beta|\mathrm{N}\mathfrak{a} = |N\alpha|\mathrm{N}\mathfrak{b}$。因爲 $N\alpha N\beta > 0$, 我們有 $N\beta\mathrm{N}\mathfrak{a} = N\alpha\mathrm{N}\mathfrak{b}$。由命題 3.5 我們知道 $\chi_i(N\alpha) = \chi_i(N\beta) = 1$, 所以 $\chi_i(\mathrm{N}\mathfrak{a}) = \chi_i(\mathrm{N}\mathfrak{b})$。我們因此可以對 $i = 1, \ldots, t$ 良好地定義以下映射

$$\begin{aligned} \chi_i^+ : H_k^+ &\longrightarrow \{\pm 1\}, \\ [\mathfrak{a}] &\longmapsto \chi_i(\mathrm{N}\mathfrak{a}). \end{aligned}$$

定理 3.6. 映射 $\chi_i^+ : H_k^+ \to \{\pm 1\}$ 是一個 H_k^+ 的特徵標。而且我們有

$$\prod_{i=1}^{t} \chi_i^+ = 1 \quad \text{(平凡特徵標)} \qquad \text{且} \qquad \bigcap_{i=1}^{t} \ker \chi_i^+ = (H_k^+)^2.$$

證明: 我們驗證 χ_i^+ 是個特徵標:

$$\chi_i^+([\mathfrak{a}][\mathfrak{b}]) = \chi_i^+([\mathfrak{ab}]) = \chi_i(\mathrm{N}(\mathfrak{ab})) = \chi_i(\mathrm{N}\mathfrak{a})\chi_i(\mathrm{N}\mathfrak{b}) = \chi_i^+([\mathfrak{a}])\chi_i^+([\mathfrak{b}]).$$

由定理 3.3,

$$\prod_{i=1}^{t} \chi_i^+([\mathfrak{a}]) = \prod_{i=1}^{t} \chi_i(\mathrm{N}\mathfrak{a}) = \chi_k(\mathrm{N}\mathfrak{a}) = 1.$$

因此 χ_i^+ 的乘積正是平凡特徵標。

對於定理的第二部分, 因爲 $\chi_i^2 = 1$, 顯然我們有

$$\bigcap_{i=1}^{t} \ker \chi_i^+ \supset (H_k^+)^2.$$

現在我們考慮同態

$$\begin{aligned} \psi : H_k^+ &\longrightarrow \{\pm 1\} \times \cdots \times \{\pm 1\}, \\ [\mathfrak{a}] &\longmapsto \left(\chi_1^+([\mathfrak{a}]), \ldots, \chi_t^+([\mathfrak{a}])\right). \end{aligned}$$

因爲 $\prod_i \chi_i^+ = 1$, ψ 並非滿射。不過, 我們將會證明 $\prod_i \chi_i^+ = 1$ 是特徵標 χ_i 之間唯一的關係式。假設 $\epsilon = (\epsilon_1, \dots, \epsilon_t) \in \{\pm 1\}^t$ 滿足關係式 $\epsilon_1 \cdots \epsilon_t = 1$。我們的目標是找到 $[\mathfrak{a}] \in H_k^+$ 使得 $\psi([\mathfrak{a}]) = \epsilon$。對每個 $i = 1, \dots, t$, 因爲 χ_i 不是模 Δ_k 上的平凡特徵標, 所以存在整數 n_i, $(n_i, \Delta_k) = 1$ 使得 $\chi_i(n_i) = \epsilon_i$。接下來我們分情況討論如下:

- 如果 $\Delta_k = l_1 l_2 \cdots l_t$ 且 $m \equiv 1 \pmod 4$, 我們取整數 n 使得

$$n \equiv n_i \pmod{l_i} \text{ 對任何 } 1 \le i \le t.$$

- 如果 $\Delta_k = 2^\beta l_2 l_3 \cdots l_t$ 且 $m \equiv 2, 3 \pmod 4$, 我們取 n 使得

$$n \equiv n_1 \pmod{2^\beta}, \qquad n \equiv n_i \pmod{l_i} \text{ 對 } 2 \le i \le t.$$

由 Dirichlet 的等差數列定理, 我們能找到奇質數 p 使得 $p \equiv n \pmod{\Delta_k}$。則

$$\chi_i(p) = \chi_i(n) = \chi_i(n_i) = \epsilon_i, \quad 1 \le i \le t.$$

因爲

$$\chi_k(p) = \prod_{i=1}^{t} \chi_i(p) = \epsilon_1 \cdots \epsilon_t = 1,$$

由定理 3.3 我們有 $p = \mathrm{N}\mathfrak{p}$, 因此

$$\chi_i^+([\mathfrak{p}]) = \chi_i(\mathrm{N}\mathfrak{p}) = \chi_i(p) = \epsilon_i \quad \text{且} \quad \psi([\mathfrak{p}]) = \epsilon.$$

我們證明了 $[H_k^+ : \ker \psi] = 2^{t-1}$。另一方面, 我們有

$$\ker \psi = \bigcap_{i=1}^{t} \ker \chi_i^+ \supset (H_k^+)^2 \quad \text{和} \quad [H_k^+ : (H_k^+)^2] = 2^{t-1}.$$

因此 $\ker \psi = (H_k^+)^2$. □

備註 3.7. 對於狹義等價類 $[\mathfrak{a}], [\mathfrak{b}]$, 其中 $\mathfrak{a}, \mathfrak{b} \subset \mathfrak{o}_k$ 且 $(\mathfrak{a}, \Delta_k) = (\mathfrak{b}, \Delta_k) = 1$, 我們在 H_k^+ 上定義等價關係:

$$[\mathfrak{a}] \approx [\mathfrak{b}] \quad \text{若且唯若} \quad \text{對任何 } i = 1, \dots, t, \text{ 我們有 } \chi_i^+([\mathfrak{a}]) = \chi_i^+([\mathfrak{b}]).$$

H_k^+ 中由這個關係定義出的一個等價類, 稱作一個狹義理想類的 虧格 $(genus)$。由定理 3.6, 上述條件等價於

$$\text{對任何 } i = 1, \dots, t \text{ 我們有 } \chi_i(\mathrm{N}\mathfrak{a}) = \chi_i(\mathrm{N}\mathfrak{b}),$$

也等價於

$$[\mathfrak{a}] \equiv [\mathfrak{b}] \mod (H_k^+)^2.$$

因此 $\approx$ 在 H_k^+ 中只是模 $(H_k^+)^2$ 而已; 也就是說, 一個虧格就是 $H_k^+/(H_k^+)^2$ 的一個陪集。另外

$$\text{一個虧格中狹義理想類的數量 } = |(H_k^+)^2| = [H_k^+ : {}_2H_k^+].$$

因此如果我們記 $h_k^* = |(H_k^+)^2|$ 則 $h_k^+ = 2^{t-1}h_k^*$。

例 3.8. 令 $m = -14$, $k = \mathbb{Q}(\sqrt{-14})$。則 $\omega = \sqrt{-14}$, $\Delta_k = -2^3 \cdot 7$, 以及 $M_k = \frac{2}{\pi}\sqrt{|\Delta_k|} \approx 4.76$。在這個例子中, $H_k = H_k^+$ 而且等價類群由 $\mathfrak{p}_2, \mathfrak{p}_3$ 的等價類生成。ω 的最小多項式是 $f_\omega(X) = X^2 + 14$。

- 當 $p = 2$, $f_\omega(X) \equiv X^2 \pmod 2$。因此 $2 = \mathfrak{p}_2^2$, 其中 $\mathfrak{p}_2 = (2, \omega) = [2, \omega]$。
- 當 $p = 3$, $f_\omega(X) \equiv X^2 - 1 \equiv (X+1)(X-1) \pmod 3$。因此 $3 = \mathfrak{p}_3\mathfrak{p}_3'$, 其中 $\mathfrak{p}_3 = (3, \omega+1) = [3, 1+\omega]$ 且 $\mathfrak{p}_3' = (3, -1+\omega) = [3, 2+\omega]$。

現在 $N(2+\omega) = 18 = 2 \cdot 3^2$, 所以

$$1 \sim (2+\omega) = [N(2+\omega), 2+\omega] = [2, 2+\omega][3, 2+\omega]^2 = \mathfrak{p}_2(\mathfrak{p}_3')^2 \sim \mathfrak{p}_2\mathfrak{p}_3^{-2},$$

故 $\mathfrak{p}_2 \sim \mathfrak{p}_3^2$。因此 H_k^+ 是由 $\mathfrak{p}_3$ 的等價類生成的循環群。

我們有 $\mathfrak{p}_2^2 = 2 \sim 1$ 但 $\mathfrak{p}_2 \nsim 1$: 如果 $\mathfrak{p}_2 = (x + y\omega)$ 則存在整數 $x, y \in \mathbb{Z}$ 使得 $2 = N(x+y\omega) = x^2 + 14y^2$, 但這是不可能的。因此 H_k^+ 是階數爲 4, 由 $\mathfrak{p}_3$ 的等價類生成的循環群。我們有

$$(H_k^+)^2 = \left\{[\mathfrak{o}_k], [\mathfrak{p}_3^2]\right\},\ t = 2,\ h_k^* = 2,$$

所以狹義理想類群有兩個虧格。

註: 本文取材於 [2]。第二節及第三節根據 4.6 及 4.7 章節直接整理撰寫。第一節介紹文中計算類群的方法, 並選一些例子依其方法重新計算。

參考文獻

1. Daniel Marcus, *Number Fields*, Universitext, Springer, 2018.
2. Takashi Ono, *An Introduction to Algebraic Number Theory*, The University Series in Mathematics. New York: Plenum Press, 1990.

—本文作者余家富爲中央研究院數學研究所研究員, 洪梵雲投稿時爲台灣大學數學系四年級學生—