數學傳播　47卷2期, pp. 38-64

二次域類數與二元二次型理論介紹

余家富 · 洪梵雲

前言

二元二次型是代數數論中研究得最透徹的題材之一。給一個整數 m 和一個係數皆爲整數的二元二次型 $f(x,y)=ax^2+bxy+cy^2$, 我們很自然會問方程式 $f(x,y)=m$ 有沒有整數解? 這些解的數量有多少? 如何得到這些解? 因爲二次型 $f(x,y)$ 可以在某個二次域 K (有理數 $\mathbb{Q}$ 的二次擴張) 中分解成兩個一次式的乘積, 上面的幾個問題自然就會和二次域的理論產生聯繫。粗略地說, 我們可以在二次型之間定義某種等價關係, 而這種關係定義出的等價類可以對應到二次域 K 中的模 (module)。因此上述的問題, 都可以轉換成關於模的問題, 而且容易計算。

在本文第一節中, 我們介紹數域中關於模的一些結果。在第二節我們討論有理係數的二元二次型, 並清楚說明了二次域中的模與二元二次型的關聯。在第三節, 我們將會討論質數在二次域中的分解, 並且用二次型的理論介紹了古典的高斯虧格理論 (Gauss genus theory)。

1. 數域中的模 (Modules in number fields)

我們首先介紹數域中的模 (modules) 概念以及相關結果。這裡僅討論在一個代數數域 K 裡的 $\mathbb{Z}$-模, 也就是 K 的加法結構中的一個交換子群。接下來我們只討論 K 中的有限生成 $\mathbb{Z}$-子模, 並簡稱爲模。把 K 的度數 (degree) 記爲 n。如果 M 是 K 中的一個模且包含 K 中線性獨立的 n 個元素, 我們則稱 M 是一個完全模 (*full module*)。例如 K 中的整數環 (the ring of integers) 即爲一個完全模。接下來的討論中, 我們考慮的模都是完全模。

1.1. 模的範數 (Norm of Modules)

定義. 令 M 爲一完全模。如果 K 中的一數 α 滿足 $\alpha M\subset M$, 則稱 α 是 M 的係數 (*coefficient*)。M 的所有係數構成一個 K 的子環 $\mathfrak{O}_M$, 稱作 M 的係數環 (*coefficient ring*)。

引理 1.1. 係數環 $\mathfrak{O}_M$ 是 K 中的完全模。

證明: 對任意 M 中的非零元素 γ, $\gamma\mathfrak{D}_M$ 是 M 這個模的子群, 所以 $\gamma\mathfrak{D}_M$ 也是一個模。類似地 $\mathfrak{D}_M = \gamma^{-1}(\gamma\mathfrak{D}_M)$ 也是一個模。我們接下來說明 $\mathfrak{D}_M$ 爲何是一個完全模。假設 $\mu_1, \ldots, \mu_n$ 是 M 的一組基底。對任一 K 中的非零元素 α, 存在有理數 $a_{ij} \in \mathbb{Q}$ 使得

$$\alpha\mu_i = \sum_{j=1}^{n} a_{ij}\mu_j, \quad 1 \le i, j \le n.$$

我們取一整數 c 使得 ca_{ij} 都是整數。如此一來, $c\alpha\mu_i$ 皆屬於 M , 所以 $c\alpha$ 落在係數環 $\mathfrak{D}_M$ 中。經過上述的過程, 對 K 的一組基底 $\alpha_1, \ldots, \alpha_n$ 我們都能找到整數 $c_1, \ldots, c_n$ 使得它們的乘積 $c_1\alpha_1, \ldots, c_n\alpha_n$ 屬於係數環 $\mathfrak{D}_M$。這些元素線性獨立, 所以 $\mathfrak{D}_M$ 是個完全模。 □

定義. 如果 M 是 K 中的完全模又是 K 的子環, 我們稱 M 是 K 的*序環* $(order)$。

引理 1.1 告訴我們 K 中任一完全模的係數環都是 K 的序環。相反地, 任一 K 的序環都是某個完全模的係數環: 因爲序環包含乘法單位元, 所以序環的係數環即是本身。

定義. 對 K 中的兩個模 M 和 M', 如果在 K 中存在 非零元素 α 使得 $M' = \alpha M$, 我們則稱 M 和 M' *相似* $(similar)$。

引理 1.2. 相似的完全模有相同的係數環。每個完全模 M 都會相似於一個模 M' 使得 $M' \subset \mathfrak{D}_M$。

我們將會討論 K 中的相似模形成的等價類, 並且我們會證明, 共享一個固定係數環 $\mathfrak{D}$ 的等價類只有有限多個。現在令 M 爲 K 中的完全模, 記係數環爲 $\mathfrak{D}$。我們分別取 $\mathfrak{D}$ 與 M 的基底 $\omega_1, \ldots, \omega_n$ 和 $\mu_1, \ldots, \mu_n$。定義一有理數矩陣 $A = (a_{ij})$ 使得

$$\mu_j = \sum_{i=1}^{n} a_{ij}\omega_i. \tag{1}$$

定義. 我們稱矩陣 A 的行列式的絕對值 $|\det(A)|$ 爲 M 的*範數* $(norm)$, 記爲 $N(M)$。

運用行列式的理論我們可以證明這個定義與 $\mathfrak{D}$ 和 M 的基底選擇無關。對 K 的一組基底 $\alpha_1, \ldots, \alpha_n$ 如果我們把判別式 (discriminant) 記做

$$D(\alpha_1, \ldots, \alpha_n) := \det(\mathrm{Tr}_{K\mathbb{Q}}(\alpha_i\alpha_j)).$$

則兩組判別式 $D = D(\mu_1, \ldots, \mu_n)$ and $D_0 = D(\omega_1, \ldots, \omega_n)$ 有以下的關係

$$D = D_0 N(M)^2. \tag{2}$$

如果一個模 M 包含於它本身的係數環, 則式 (1) 中的矩陣 (a_{ij}) 會是整數矩陣, 因此這時的範數 $N(M)$ 會是整數。下面是範數的一個具體意義。

定理 1.3. 如果一個完全模 M 包含於本身的係數環 $\mathfrak{D}$, 則範數 $N(M) = [\mathfrak{D} : M]$。

定理 1.3 可以從以下引理得到。對於任意一個 $\mathbb{Z}$-模 M, 如果對任何元素 $x \in M$ 和非零整數 $n, nx = 0$ 則 $x = 0$, 我們稱 M *沒有撓點* (*torsion-free*)。

引理 1.4. 若 M_0 是一個沒有撓點 、階數 (rank) 爲 n 的交換群, 而 M 是一個階數爲 n 的子群。則 M 在 M_0 中的指數 (index) $[M_0 : M]$ 總是有限。更進一步, 對任何 M_0 和 M 的各一組基底, $[M_0 : M]$ 等於式 (1) 中 基底變換矩陣 A 之行列式再取絕對值 $|\det(A)|$。

定理 1.5. 相似的兩個模 M 和 αM 其範數有以下的關係

$$N(\alpha M) = |N(\alpha)| \cdot N(M).$$

特別的, 如果一個模相似於序環 $\mathfrak{D}$, 則 $N(\alpha\mathfrak{D}) = |N(\alpha)|$。

證明: 若 $\mu_1, \ldots, \mu_n$ 是 M 的一組基底, 則 $\alpha\mu_1, \ldots, \alpha\mu_n$ 也是 αM 的一組基底。如果我們把基底變換 $\mu_i \mapsto \alpha\mu_i$ 的矩陣記做 C, 我們知道 α 的範數 $N(\alpha)$ 是 $|\det(C)|$。現在我們固定一組 $\mathfrak{D}$ 的基底, 並且把這組基底變換到 μ_i, $\alpha\mu_i$ 的矩陣記成 A 和 A', 則 $A' = AC$。因此

$$N(\alpha M) = |\det A'| = |\det A| \, |\det C| = N(M) \, |N(\alpha)| \, .$$

定理的後半成立, 因爲 $N(\mathfrak{D}) = 1$. □

1.2. 有限的類數

引理 1.6. 如果 M_1 是 K 中的一個完全模而且 M_2 是 M_1 的一個完全子模, 則只有有限多的完全模 M 使得 $M_2 \subset M \subset M_1$。

推論 1.7. 如果 M_0 是 K 中的一個完全模, 則對任何正整數 r, K 中只有有限多個包含 M_0 的完全模 M 使得 $[M : M_0] = r$。

證明: 這樣的完全模 M 滿足 $rM \subset M_0$, 所以我們可以對 $\frac{1}{r}M_0 \supset M \supset M_0$ 使用引理 1.6。□

定理 1.8. 令 K 爲一個度數爲 $n = s + 2t$ 的數域, 其中 s 和 $2t$ 分別是 K 的實嵌入 (real embedding) 和複嵌入 (complex embedding) 的個數。令 M 是 K 中的一個完全模, 其範數爲 D。則 M 中存在非零的元素 $\alpha \in M$ 使得

$$|N(\alpha)| \leq \left(\frac{2}{\pi}\right)^t \sqrt{|D|}. \tag{3}$$

證明的主要想法是運用數論中一個古典及有效的方法, 稱爲 數的幾何 (*geometry of numbers*), 由 Minkowski 在十九世紀末提出。詳細的證明請見 [1] 位於 127 頁 2.6.7 節的引理 3。

定理 1.9. 如果 $\mathfrak{D}$ 是 K 中的一個序環, 則 K 中只有有限多個相似模的等價類, 使得 $\mathfrak{D}$ 是它們的係數環。

證明: 取一個係數環爲 $\mathfrak{D}$ 的模 M。令 D 和 D_0 分別是模 M 和序環 $\mathfrak{D}$ 的判別式。我們取一數 $\alpha \in M$ 滿足式 (3)。由式 (2) 我們將式 (3) 寫成

$$|N(\alpha)| \leq \left(\frac{2}{\pi}\right)^t N(M)\sqrt{|D_0|}.$$

因爲 $\alpha\mathfrak{D} \subset M$, 我們有 $\mathfrak{D} \subset \frac{1}{\alpha}M$。由引理 1.4 和模的範數的定義我們得到

$$\left[\frac{1}{\alpha}M : \mathfrak{D}\right] = N\left(\frac{1}{\alpha}M\right)^{-1} = \frac{|N(\alpha)|}{N(M)} \leq \left(\frac{2}{\pi}\right)^t \sqrt{|D_0|}.$$

這證明了每一個係數環爲 $\mathfrak{D}$ 的相似模上的等價類, 都有一個模 M 使得

$$M' \supset \mathfrak{D}, \quad [M' : \mathfrak{D}] \leq \left(\frac{2}{\pi}\right)^t \sqrt{|D_0|}. \tag{4}$$

根據推論 1.7, 只有有限多個模 M' 滿足式 (4)。因此, 等價類的個數只有有限多個。 □

1.3. 極大序環 (maximal order)

首先我們複習代數中的高斯引理。

引理 1.10. 假設 $f(x) \in \mathbb{Z}[x]$ 首項係數爲 1 的多項式。則 $f(x)$ 在 $\mathbb{Z}[x]$ 中是不可約多項式, 若且唯若 $f(x)$ 在 $\mathbb{Q}[x]$ 中是不可約多項式。

接著由高斯引理, 我們可以得到

引理 1.11. 如果 $\alpha \in K$ 屬於某個序環 $\mathfrak{D}$, 則 α 的最小多項式的係數皆是整數。

證明: 我們知道 $\mathfrak{D} = \mathfrak{D}_M$ 是某個完全模 M 的序環。令 $\mu_1, \ldots, \mu_n$ 是 M 的一組基底, 則對於任何 $\alpha \in \mathfrak{D}$ 都存在整數 a_{ij} 使得

$$\alpha\mu_i = \sum_{j=1}^{n} a_{ij}\mu_j.$$

α 的特徵多項式即是矩陣 (a_{ij}) 的特徵多項式, 所以它的係數皆是整數。由高斯引理, α 的最小多項式也是整係數多項式。 □

由引理 1.11 我們知道, 序環中的每個元素都是代數整數, 屬於代數數域 K 的整數環 $\mathfrak{o}_K$。因此 $\mathfrak{o}_K$ 是 K 的極大序環, 也就是說, 每個序環都是 $\mathfrak{o}_K$ 的子環。

2. 數的二次型表示

在第二章中我們研究有理係數的二元二次型 $ax^2+bxy+cy^2$ 還有它們所表示的數。因爲這樣的二元二次型都會在某個二次域中分解成兩個一次項的乘積, 研究這些二次型所表示的數, 會和二次域中的完全模以及其係數環有所關聯。

定義.

(1) 令 $f(x,y)=ax^2+bxy+cy^2$ 爲一個有理係數的二元二次型。我們定義 $D_f:=b^2-4ac$ 爲 f 的判別式 $(discriminant)$。如果 f 是一個整係數的二次型且 $\gcd(a,b,c)=1$, 我們則稱 f 是本原 $(primitive)$ 二次型。

(2) 給定兩個整係數的二元二次型 $f(x,y)$ 和 $g(x,y)$。如果存在矩陣 $M\in \mathrm{GL}_2(\mathbb{Z})$ 使得 $f(x,y)=g((x,y)M)$, 我們則稱 f 和 g 是等價的 $(equivalent)$, 記爲 $f\sim g$。如果矩陣 M 在 $\mathrm{SL}_2(\mathbb{Z})$, 則我們稱$f$ 和 g 是狹義等價的 $(properly\ equivalent)$, 記爲 $f\sim_+ g$。

如果一個二元二次型和另一個本原的二元二次型等價, 則第一個二次型也是本原二次型。另外, 如果 $f(x,y)=g((x,y)M)$, 則 $D_f=(\det M)^2D_g$。由此我們可以得到, 等價的二次型有一樣的判別式。

2.1. 二次域中的序環

令 K 爲二次域 $\mathbb{Q}(\sqrt{d})$, 其中 d 爲不被 1 以外的平方數整除的數。我們令

$$\omega=\begin{cases}\dfrac{1+\sqrt{d}}{2}, & \text{如果 } d\equiv 1 \pmod 4;\\ \sqrt{d}, & \text{如果 } d\equiv 2,3 \pmod 4.\end{cases}$$

則整數環 $\mathfrak{o}_K=\mathbb{Z}[\omega]=\mathbb{Z}+\mathbb{Z}\omega$ 由 1 和 ω 生成。令 $\mathfrak{O}$ 爲 K 的一個序環, 則 $\mathfrak{O}\subset\mathfrak{o}_K$, 所以 $\mathfrak{O}$ 的每個元素都能被寫成

$$x+y\omega,\quad x,y\in\mathbb{Z}.$$

在所有元素中, 我們取 $a+f\omega$ 使得 f 是最小的正數, 則 $f\omega\in\mathfrak{O}$ 而且 $\mathfrak{O}=\{1,f\omega\}$。相反地, 對任何正數 f, 模 $\mathbb{Z}+\mathbb{Z}f\omega$ 都是一個序環。不同的正數 f 給出不同的序環, 所以我們得到

一個一一對應

$$\{K \text{ 的序環}\} \longleftrightarrow \mathbb{N}$$
$$\mathfrak{D}_f = \mathbb{Z} + \mathbb{Z}f\omega \longleftrightarrow f.$$

另外我們有 $f = [\mathfrak{o}_K : \mathfrak{D}_f]$。

現在我們計算序環 $\mathfrak{D}_f$ 的判別式 $\operatorname{disc}\mathfrak{D}_f$。根據定義 $\operatorname{disc}\mathfrak{D}_f = \det(\operatorname{Tr}(\alpha_i\alpha_j))$, 其中 $\alpha_1 = 1, \alpha_2 = f\omega$。如果 $d \equiv 1 \pmod 4$, 由 $\operatorname{Tr}(\sqrt{d}) = 0$ 我們得到

$$\operatorname{Tr}(\omega) = \operatorname{Tr}\left(\frac{1+\sqrt{d}}{2}\right) = 1,$$
$$\operatorname{Tr}(\omega^2) = \operatorname{Tr}\left(\frac{d+1}{4} + \frac{\sqrt{d}}{2}\right) = \frac{d+1}{2},$$
$$\operatorname{disc}\mathfrak{D}_f = \begin{vmatrix} \operatorname{Tr}(1) & \operatorname{Tr}(f\omega) \\ \operatorname{Tr}(f\omega) & \operatorname{Tr}(f^2\omega^2) \end{vmatrix} = \begin{vmatrix} 2 & f \\ f & f^2 \cdot \frac{d+1}{2} \end{vmatrix} = f^2 d.$$

如果 $d \equiv 2, 3 \pmod 4$, 則

$$\operatorname{disc}\mathfrak{D}_f = \begin{vmatrix} \operatorname{Tr}(1) & \operatorname{Tr}(f\omega) \\ \operatorname{Tr}(f\omega) & \operatorname{Tr}(f^2\omega^2) \end{vmatrix} = \begin{vmatrix} 2 & 0 \\ 0 & 2f^2 d \end{vmatrix} = 4f^2 d.$$

因此二次域中的每個序環都會被本身的判別式唯一決定。特別地, 整數環 $\mathfrak{o}_K$ 的判別式稱爲基本判別式 (*fundamental discriminant*), 記做 d_K 而且

$$d_K = \begin{cases} d, & \text{如果 } d \equiv 1 \pmod 4; \\ 4d, & \text{如果 } d \equiv 2, 3 \pmod 4. \end{cases}$$

整理一下, 我們證明了

命題 2.1. 令 d 爲一個不被 1 以外的平方數整除的數。任何 $K = \mathbb{Q}(\sqrt{d})$ 中的序環都可以寫成 $\mathfrak{D}_f = \{1, f\omega\}$, 其中 $f = [\mathfrak{o}_K : \mathfrak{D}]$ 而 $\mathfrak{D}_f$ 的判別式是 $f^2 d_K$。

2.2. 二次域中序環的單位元 (unit)

在二次域的序環 $\mathfrak{D}_f$ 中, 任何數都可以寫成 $x + yf\omega$, 其中 x, y 是整數。另外對任何序環 $\mathfrak{D}$, $\epsilon \in \mathfrak{D}$ 是單位元若且唯若 $N(\epsilon) = \pm 1$。因此, 如果我們想要找到 $\mathfrak{D}_f$ 的所有單位元, 我們可以試著解開方程式

$$N(x + yf\omega) = \pm 1, \tag{5}$$

這個方程式等價於

$$\begin{cases} x^2+fxy+f^2\dfrac{1-d}{4}y^2=\pm 1 & \text{如果 } d\equiv 1 \pmod 4; \\ x^2-df^2y^2=\pm 1 & \text{如果 } d\equiv 2,3 \pmod 4. \end{cases} \tag{6}$$

如果 K 是一個虛二次域, 則其中任何序環的單位元群 (*unit group*) 都只有有限多個元素, 並且由單位根 (*roots of unity*) 所構成。我們可以從解方程式的角度來看這件事。當 $d<0$ 時式 (6) 只有有限多個整數解。如果 $d=-1$ 且 $f=1$, 則式 (6) 有 4 組解

$$x=\pm 1, y=0;\ x=0, y=\pm 1,$$

而它們對應到的元素是 $\pm 1, \pm i$。當 $d=-3$ 且 $f=1$, 有 6 組解

$$x=\pm 1, y=0;\ x=0, y=\pm 1;\ x=1, y=-1;\ x=-1, y=1,$$

它們對應到 $\pm 1, (\pm 1\pm\sqrt{-3})/2$。對剩下的序環, 式 (6) 只有 2 組解 $x=\pm 1, y=0$, 對應到 ± 1。

對於實二次域 $\mathbb{Q}(\sqrt{d})$, 根據 Dirichlet 單位定理 (Dirichlet's unit theorem) 任何序環 $\mathfrak{O}_f$ 中的單位元都可以被寫成 $\pm\epsilon^n$, 其中 ϵ 是 $\mathfrak{O}_f$ 中大於 1 的最小單位元, 稱爲基本單位元 (*fundamental unit*)。

引理 2.2. 令 $\eta>1$ 是 $\mathfrak{O}_f$ 中的一個單位元, 並把它寫成 $\eta=x+yf\omega$ 的形式, 則 $x\geq 0$ 且 $y>0$ 都是正整數。若 $d\neq 5$ 或 $f\neq 1$, 則 $x>0$。

證明: 首先我們假設 $d\neq 5$ 或 $f\neq 1$。對任一數 $\alpha\in\mathbb{Q}(\sqrt{d})$, 將它的共軛記爲 α', 而 $\omega-\omega'>0$。因爲 $N(\eta)=\eta\eta'=\pm 1$, 所以 $\eta'=1/\eta$ 或 $-1/\eta$。在這兩種情況下 $\eta-\eta'>0$, 也就是說 $yf(\omega-\omega')>0$, 因此 $y>0$。另外, 因爲 $|\eta'|=|x+yf\omega'|<1$ 且 $f\omega'<-1$, 我們有 $x>0$。如果 $d=5$ 且 $f=1$, 則 $-1<f\omega'<0$ 而且我們有 $x\geq 0$。在這個情形下 $\omega=\frac{1+\sqrt{5}}{2}$ 是基本單位元, 所以 x 可能爲 0。 □

現在令 $\epsilon>1$ 爲序環 $\mathfrak{O}_f$ 的基本單位元。令 $x_n, y_n\in\mathbb{Z}$ 爲單位元 $\epsilon^n=x_n+y_nf\omega$ 中的係數 $(n\geq 1)$。我們可以證明當 $n>1$ 時 $x_n>x_1$ 且 $y_n>y_1$。爲了求出 ϵ, 我們必須找到式 (5) 的最小正整數解。事實上我們能先找出 x, y 的一個上界 C 再經由有限多個步驟找出 x, y 的值 (見 [1] 第 2 章 5.3 節)。

我們可以用連分數的一個基本結果來簡化這些步驟。假設實數 ξ 可以被表示爲

$$\xi=q_0+\cfrac{1}{q_1+\cfrac{1}{q_2+\cfrac{1}{q_3+\ddots}}}$$

其中 $q_0 \in \mathbb{Z}$ 且 $q_i \in \mathbb{N}$。考慮有限連分數

$$q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{\ddots + \cfrac{1}{q_{k-1} + \cfrac{1}{q_k}}}}}$$

我們將它記爲 $[q_0, \ldots, q_k]$。它可以寫成 P_k/Q_k, 其中 P_k, Q_k 是互質的兩個整數。我們稱分數 $\{P_k/Q_k\}$ 爲 ξ 的收斂元 (*convergents*)。下面是 [4] 的定理 5.1:

定理 2.3. 對任意正實數 $\xi > 0$ 和互質的正整數 x, y, 如果

$$\left|\frac{x}{y} - \xi\right| < \frac{1}{2y^2},$$

則 $\dfrac{x}{y}$ 是 ξ 的連分數展開中的一個收斂元。

若 $x + yf\omega$ 爲 $\mathfrak{D}_f$ 中的一個單位元, 由式 (5),

$$\left|\frac{x}{y} + f\omega'\right| = \frac{1}{y(x + yf\omega)}.$$

如果 $d \equiv 1 \pmod 4$, (除了$d = 5, f = 1$的情況以外) 我們有

$$\left|\frac{x}{y} - f\frac{\sqrt{d}-1}{2}\right| = \frac{1}{y^2(\frac{x}{y} + f\frac{\sqrt{d}+1}{2})} < \frac{1}{2y^2}$$

其中我們用到 $x/y > 0$ 和 $f(\sqrt{d}+1)/2 > 2$。如果 $d \equiv 2, 3 \pmod 4$, 則

$$\left|\frac{x}{y} - f\sqrt{d}\right| = \frac{1}{y(x + yf\sqrt{d})} \leq \frac{1}{y^2(\sqrt{d-1} + \sqrt{d})} < \frac{1}{2y^2}$$

其中我們用到 $x^2 = fdy^2 \pm 1 \geq dy^2 - 1 \geq y^2(d-1)$ 且 $d \geq 2$。由上述的定理, 最簡分數 x/y 是 $-f\omega'$ 的連分數展開中的某個收斂元。因此, 我們只需要測試 $-f\omega'$ 的收斂元中的分子和分母是否滿足方程式。我們用連分數計算收斂元 P_k/Q_k, 直到 $N(P_k + Q_k\omega f) = \pm 1$ 才停止。這時 $\epsilon = P_k + Q_k\omega f$ 即是基本單位元。對於 $d = 5, f = 1$ 的例外情況, 基本單位元是 $\omega = \frac{1+\sqrt{5}}{2}$。

例 2.4. 考慮二次域 $Q(\sqrt{6})$ 中的基本單位元 $\{1, 3\sqrt{6}\}$。我們先找出 $-3\omega' = 3\sqrt{6}$ 的連分數展開

$$\sqrt{54} = 7 + (\sqrt{54} - 7), \quad \frac{1}{\sqrt{54}-7} = 2 + \frac{\sqrt{54}-3}{5}, \quad \frac{5}{\sqrt{54}-3} = 1 + \frac{\sqrt{54}-6}{9},$$

$$\frac{9}{\sqrt{54}-6} = 6 + \frac{\sqrt{54}-6}{2}, \quad \frac{2}{\sqrt{54}-6} = 1 + \frac{\sqrt{54}-3}{9}, \quad \frac{9}{\sqrt{54}-3} = 2 + \frac{7\sqrt{54}-51}{15}.$$

再列出前面幾項收斂元。注意到當 $k \geq 1$ 我們有 $P_{k+1} = q_{k+1}P_k + P_{k-1}$ 還有 $Q_{k+1} = q_{k+1}Q_k + Q_{k-1}$。我們得到序環 $\{1, 3\sqrt{6}\}$ 的基本單位元 $485 + 66 \cdot 3\sqrt{6} = 485 + 198\sqrt{6}$。

k	-1	0	1	2	3	4	5
q_k	1	7	2	1	6	1	2
P_k	1	7	15	22	147	169	485
Q_k	0	1	2	3	20	23	66
$P_k^2 - 54Q_k^2$	-53	-5	9	-2	9	-5	1

2.3. 二次域的模

現在讓我們考慮二次域中的模。因爲任何模 $\{\alpha, \beta\}$ 都會相似到模 $\{1, \beta/\alpha\}$, 我們可以僅考慮形如 $\{1, \gamma\}$ 的模。注意到任何 $\mathbb{Q}(\sqrt{d})$ 中的無理數 γ 都是某個整係數多項式 $at^2 + bt + c$ 的根。我們可以假設 $\gcd(a, b, c) = 1$ 且 $a > 0$, 這些假設唯一決定了這個多項式, 我們將它記爲 $\phi_\gamma(t)$。如果 γ' 是 γ 的共軛, 則我們有 $\phi_\gamma(t) = \phi_{\gamma'}(t)$。相反地, 如果 $\phi_{\gamma_1}(t) = \phi_\gamma(t)$ 則 $\gamma_1 = \gamma$ 或 $\gamma_1 = \gamma'$。

引理 2.5. 如果無理數 $\gamma \in \mathbb{Q}(\sqrt{d}) \setminus \mathbb{Q}$ 對應到的多項式爲 $\phi_\gamma(t) = at^2 + bt + c$, 則模 $M = \{1, \gamma\}$ 的係數環 $\mathfrak{O}$ 爲序環 $\{1, a\gamma\}$, 其判別式爲 $D = b^2 - 4ac$。

證明: 考慮 $\mathbb{Q}(\sqrt{d})$ 中的一數 $\alpha = x + y\gamma$, 其中 x, y 是有理數。敘述 $\alpha M \subset M$ 等價於

$$\alpha 1 = x + y\gamma \in M \quad \text{且} \quad \alpha\gamma = -\frac{cy}{a} + \left(x - \frac{by}{a}\right)\gamma \in M.$$

因此 $\alpha \in \mathfrak{O}$ 若且唯若有理數 $x, y, cy/a, by/a$ 都是整數。因爲 $\gcd(a, b, c) = 1$, 第二個敘述等價於 $x, y \in \mathbb{Z}$ 且 $a \mid y$。因此 $\mathfrak{O} = \{1, a\gamma\}$。最後我們計算得

$$D = \begin{vmatrix} \mathrm{Tr}(1) & \mathrm{Tr}(a\gamma) \\ \mathrm{Tr}(a\gamma) & \mathrm{Tr}(a^2\gamma^2) \end{vmatrix} = \begin{vmatrix} 2 & -b \\ -b & b^2 - 2ac \end{vmatrix} = b^2 - 4ac. \qquad \square$$

推論 2.6. 沿用先前的符號, 模 $\{1, \gamma\}$ 的範數是 a^{-1}。

引理 2.7. 模 $\{1, \gamma\}$ 與模 $\{1, \gamma_1\}$ 相似, 若且唯若存在矩陣 $\left(\begin{smallmatrix} k & l \\ m & n \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z})$ 使得

$$\gamma_1 = \frac{k\gamma + l}{m\gamma + n}.$$

我們現在固定一個序環 $\mathfrak{O}$。在二次域 $\mathbb{Q}(\sqrt{d})$ 中, 考慮所有以 $\mathfrak{O}$ 爲係數環的模構成的集合。定理 1.9 告訴我們這樣的集合可以被分割成有限多個相似模的等價類。

現在我們定義模之間的乘法。如果模 $M=\{\alpha,\beta\}$ 且模 $M_1=\{\alpha_1,\beta_1\}$, 定義

$$MM_1=\{\alpha\alpha_1,\alpha\beta_1,\beta\alpha_1,\beta\beta_1\}.$$

我們可以將這個定義延伸到等價類上:$[M]\cdot[M_1]=[MM_1]$。

命題 2.8. 將模 M 的共軛模記做 M'。模 M 和 M' 有同樣的係數環 $\mathfrak{D}$。這時以下的關係成立

$$MM'=N(M)\mathfrak{D}. \tag{7}$$

證明: 首先我們假設 M 是 $\{1,\gamma\}$ 這種形式。令 γ 對應到的多項式爲 $\phi(t)=at^2+bt+c$, 則

$$\gamma'=-\gamma-\frac{b}{a},\quad \gamma\gamma'=-\frac{c}{a},$$

而且

$$\begin{aligned}MM'&=\left\{1,\gamma,-\gamma-\frac{b}{a},\frac{c}{a}\right\}=\left\{1,\gamma,-\frac{b}{a},\frac{c}{a}\right\}=\frac{1}{a}\{a,b,c,a\gamma\}\\&=\frac{1}{a}\{1,a\gamma\},\quad \text{因爲 } \gcd(a,b,c)=1.\end{aligned}$$

根據引理 2.5, 我們有 $MM'=\frac{1}{a}\mathfrak{D}=N(M)\mathfrak{D}$。

如果 M 是一般的模, 我們可以把它寫成 $M=\alpha M_1$, $M_1=\{1,\gamma\}$, 則

$$MM'=\alpha\alpha' M_1M_1'=N(\alpha)N(M_1)\mathfrak{D}=|N(\alpha)|\,N(M_1)\mathfrak{D}=N(M)\mathfrak{D}. \qquad \square$$

現在令 M 和 M_1 是兩個屬於序環 $\mathfrak{D}$ 的模。我們令 MM_1 的係數環爲 $\overline{\mathfrak{D}}$, 則由式 (7)

$$MM_1(MM_1)'=N(MM_1)\overline{\mathfrak{D}}.$$

另一方面, 模之間的乘法有交換律和結合律, 所以

$$MM_1(MM_1)'=MM'M_1M_1'=N(M)\mathfrak{D}N(M_1)\mathfrak{D}=N(M)N(M_1)\mathfrak{D}.$$

注意到兩個不同的序環並不相似 (因爲它們是本身的係數環), 所以 $\mathfrak{D}=\overline{\mathfrak{D}}$。因此我們證明了

$$N(MM_1)=N(M)N(M_1). \tag{8}$$

最後, 對任何係數環爲 $\mathfrak{D}$ 的模 M 我們有

$$M\mathfrak{D}=M,\quad M\left[\frac{1}{N(M)}M'\right]=\mathfrak{D}. \tag{9}$$

在一個二次域 K 中, 把係數環 $\mathfrak{D}$ 給定的模所形成的等價類記爲 $\mathrm{Cl}(\mathfrak{D})$。根據式 (9), $\mathrm{Cl}(\mathfrak{D})$ 在等價類之間的乘法運算下形成一個交換群, 稱作 $\mathfrak{D}$ 的理想類群 (*ideal class group*)。由定理 1.9 $\mathrm{Cl}(\mathfrak{D})$ 是一個有限交換群。

2.4. 模與二次型之間的對應

在二次域 $K=\mathbb{Q}(\sqrt{d})$ 中, 我們可以將模 M 的一組基底 α,β 對應到一個有理係數的二元二次型 $N(\alpha x+\beta y)$。因爲 M 的不同基底對應到等價的二次型, 我們有以下的映射

$$M \longmapsto \text{二次型的一個等價類.}$$

如果把模 M 換成 γM, 對應到的二次型會乘上 $N(\gamma)$, 因此我們得到映射

$$\{\text{模的相似類}\} \longrightarrow \{\text{二次型的等價類, 相差一個常數也視爲等價}\}.$$

在二次域中, 我們可以定義模之間的另一種相似。

定義. 在二次域 K 中給定兩個模 M 和 M_1。如果存在某數 $\alpha\in K$, $N(\alpha)>0$ 使得 $M_1=\alpha M$, 則稱兩個模 M 和 M_1 嚴格相似 (*strictly similar*)。

若 K 爲虛二次域, 則對任何非零的 $\gamma\in K$ 我們有 $N(\gamma)>0$, 所以若模 M_1,M_2 相似則它們嚴格相似。在實二次域,「相似」和「嚴格相似」的差別由基本單位元 ϵ 所決定。若 $N(\epsilon)=-1$, 則這兩個概念等價。但當 $N(\epsilon)=1$, 則每個相似等價類, 皆可以拆成兩個嚴格相似等價類。

現在我們描述模的等價類與二次型的等價類之間的對應關係。我們先引入一個定義。

定義. 對二次域 $\mathbb{Q}(\sqrt{d})$ 中的模 M, 如果它的一組基底 α,β 其行列式

$$\Delta:=\begin{vmatrix}\alpha & \beta\\ \alpha' & \beta'\end{vmatrix}$$

滿足

$$\begin{cases}\Delta>0, & \text{當 } d>0;\\ \dfrac{1}{i}\Delta>0, & \text{當 } d<0.\end{cases}\tag{10}$$

我們則說 α,β 是一組 $\mathbb{Q}(\sqrt{d})$ 的正定向 (*positively oriented*) 基底。注意到基底 $\{1,\sqrt{d}\}$ 並非正定向, $\{\sqrt{d},1\}$ 才是。

對 M 的一組正定向基底 α,β, 我們將它對應到下面的二次型

$$f(x,y)=Ax^2+Bxy+Cy^2:=\frac{N(\alpha x+\beta y)}{N(M)}=\frac{(\alpha x+\beta y)(\alpha' x+\beta' y)}{N(M)}.$$

假設 $\gamma = -\beta/\alpha$ 對應到的整係數多項式爲 $\phi_\gamma(t) = at^2 + bt + c$, 我們則有

$$N(\alpha x + \beta y) = \frac{N(\alpha)}{a}(ax^2 + bxy + cy^2). \tag{11}$$

另一方面, 模 $M = \alpha\{1, \gamma\}$ 的範數爲 $\frac{|N(\alpha)|}{a}$, 因此我們得到 $(A, B, C) = \pm(a, b, c)$。所以所對應的二次型 f 是本原二次型, 而且根據引理2.5 f 的判別式 $B^2 - 4AC$ 和 M 的係數環的判別式 $b^2 - 4ac$ 相等。

我們有以下將正定向基底對應到一個本原二次型的的映射

$$\{\alpha, \beta\} \longmapsto f(x, y) = \frac{N(\alpha x + \beta y)}{N(M)}. \tag{12}$$

如果一個二次型 $Q(z)$ 帶入任何非零的 $z \in \mathbb{R}^2$ 皆大於 0, 我們稱 f 爲正定二次型。如果 $\mathbb{Q}(\sqrt{d})$ 是虛二次域, f 則是一個正定二次型。這一小節的主要結果, 是下面模的等價類與二次型的等價類之間的對應關係。

定理 2.9. 在二次域 $\mathbb{Q}(\sqrt{d})$ 中, 我們用 $\mathfrak{M}$ 表示一個集合, 這個集合收集了 $\mathbb{Q}(\sqrt{d})$ 中的模在「嚴格相似」這個關係下形成的等價類。如果 $d > 0$, 我們考慮在 $\mathbb{Q}(\sqrt{d})$ 中可以分解成一次項的本原二元二次型, 並把它們的狹義等價類形成的集合記做 $\mathfrak{F}$。如果 $d < 0$, 我們則在上面的定義多加上正定二元二次型的條件。則 (12) 中的映射

$$\begin{aligned} \mathfrak{M} &\longrightarrow \mathfrak{F} \\ \{\alpha, \beta\} &\longmapsto f(x, y) \end{aligned}$$

是一個雙射。另外, 如果模 $\{\alpha, \beta\}$ 的係數環的判別式爲 D, 則對應到的二次型上的等價類其判別式也是 D。

證明: 首先我們證明這個映射是良好定義的 (well-defined)。如果模 $\{\alpha, \beta\}$ 和 $\{\alpha_1, \beta_1\}$ 嚴格相似, 則在 $\mathbb{Q}(\sqrt{d})$ 存在一個非零的數 η 使得 $N(\eta) > 0$ 而且模 $\{\eta\alpha, \eta\beta\}$ 與模 $\{\alpha_1, \beta_1\}$ 相等。這時存在一個可逆的整數矩陣 $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z})$ 使得

$$\begin{pmatrix} \alpha_1 \\ \beta_1 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \eta\alpha \\ \eta\beta \end{pmatrix}.$$

考慮這個關係式的共軛版本後, 兩邊再取判別式, 可以推得 $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$。另外,

$$(\alpha_1 x + \beta_1 y)(\alpha_1' x + \beta_1' y) = N(\eta)\,((\alpha a + \beta b)x + (\alpha c + \beta d)y)\,((\alpha' a + \beta' b)x + (\alpha' c + \beta' d)y)$$

這個關係式證明了

$$f_1(x, y) = f\left((x, y)\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right).$$

我們說明這個映射是一個單射。首先, 我們證明任何模 M 都會嚴格相似於一組正定向基底 $1, \gamma$ 形成的模 $\{1, \gamma\}$: 我們在 $K^\times$ 中取一數 δ 使得 $N(\delta) > 0$, 乘上某個正有理數後我們可以假設 $\delta \in M$ 且 δ 是本原的。這時在 M 中則存在某個 δ_1 使得 δ, δ_1 是 M 的一組正定向基底 (如果 δ, δ_1 是負定向則改變 δ_1 的正負號即可)。

現在我們假設兩組基底 $\{\alpha, \beta\} = \alpha\{1, \gamma\}$ 和 $\{\alpha_1, \beta_1\} = \alpha_1\{1, \gamma_1\}$ 對應到等價的二元二次型。如果 $N(\alpha) > 0$ 且 $N(\alpha_1) > 0$, 則存在某個可逆整數矩陣 $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ 使得

$$f_{(1,\gamma)}(x, y) = f_{(1,\gamma_1)}((x, y)g).$$

注意到 $-\gamma$ 是以下多項式的根

$$f_{(1,\gamma)}(x, 1) = f_{1,\gamma_1}((ax + c, bx + d)) = f_{(1,\gamma_1)}\left(\frac{ax + c}{bx + d}, 1\right)(bx + d)^2,$$

而 $-\gamma_1$ 是多項式 $f_{(1,\gamma_1)}(x, 1)$ 的根, 則 $g^t\gamma = \gamma_1$ 或 γ_1'。因爲兩組基底 $\{1, \gamma\}$ 和 $\{1, \gamma_1\}$ 皆爲正定向, 所以兩個模 $\{1, \gamma\}$ 和 $\{1, \gamma_1\}$ 相等。

最後我們證明這個映射是一個滿射。考慮 $\mathfrak{F}$ 中的一個二次型

$$g(x, y) = Ax^2 + Bxy + Cy^2 = A(x + y\gamma)(x + y\gamma'),$$

其中 $-\gamma$ 和 $-\gamma'$ 是 $g(x, 1)$ 的兩根, 而且 $\{1, -\gamma\}$ 是正定向基底。定義模 $M = \{1, -\gamma\}$ 和二次型

$$\phi_\gamma(x, y) = ax^2 + bxy + cy^2 = a(x + \gamma y)(x + \gamma' y) = f_{(1,\gamma')}(x, y).$$

如果 $A > 0$, 則 $A = a$ 且 $g = f_{(1,\gamma')}$。如果 $A < 0$, 我們可以取一數 α 使得 $N(\alpha) < 0$ 且 $\{\alpha, \alpha\gamma'\}$ 是一組正定向基底, 則我們有

$$f_{(\alpha,\alpha\gamma')}(x, y) = \frac{N(\alpha)(x + \gamma y)(x + \gamma' y)}{|N(\alpha)|\, N(1, \gamma)} = g. \qquad \square$$

我們在 $\mathfrak{M}$ 上定義了乘法。透過 $\mathfrak{M} \to \mathfrak{F}$ 這組一一對應, 我們則有 $\mathfrak{F}$ 上的乘法, 稱作二次型的等價類之間的合成 (*composition*)。注意在乘法結構下, $\mathfrak{M}$ 並不構成一個交換群。若 $\mathfrak{D}$ 是一個序環, 且令

$$\mathrm{Cl}^+(\mathfrak{D}) = \{\, \text{狹義等價類 } [M]_+ \in \mathfrak{M} \mid \mathfrak{D} \text{ 是模 } M \text{ 的係數環} \,\},$$

則 $\mathrm{Cl}^+(\mathfrak{D})$ 是一個交換群, 稱爲 $\mathfrak{D}$ 的狹義理想類群 (*ideal class group in the narrow sense*)。並且我們有 $\mathfrak{M} = \bigcup_{\mathfrak{D}} \mathrm{Cl}^+(\mathfrak{D})$。

2.5. 數的二次型表示與模的相似性

假設 $f(x,y)$ 是一個本原二次型, 判別式爲 D, 因此可以在 $\mathbb{Q}(\sqrt{D})$ 中分解成一次項的乘積。如果 $D<0$ 我們則進一步假設 f 正定。對任一正整數 m, 我們想找到方程式

$$f(x,y)=m \tag{13}$$

的每組整數解。由定理 2.9 我們可以找到一個模 M 以及一組正定向基底 α,β 使得

$$f(x,y)=\frac{N(\alpha x+\beta y)}{N(M)}. \tag{14}$$

若 $(x,y)\in\mathbb{Z}^2$ 是 $f(x,y)=m$ 的一組解, 我們得到 M 中的一數 $\xi=\alpha x+\beta y$ 滿足 $N(\xi)=mN(M)$。這個映射 $(x,y)\mapsto\alpha x+\beta y$ 給出了以下的一一對應

$$\begin{gathered}\big\{(x,y)\in\mathbb{Z}^2 : f(x,y)=m\big\}\longleftrightarrow\{\xi\in M : N(\xi)=mN(M)\}\\ (x,y)\longleftrightarrow\xi=\alpha x+\beta y.\end{gathered}$$

定義. 對模 M 中的任何兩數 μ_1,μ_2, 如果它們的商 μ_1/μ_2 是係數環 $\mathfrak{D}_M$ 中的可逆元, 我們則說它們是相伴的 $(associated)$。若 $(x_1,y_1),(x_2,y_2)$ 爲 $f(x,y)=m$ 的兩組解, 使得對應到的 $\xi_1,\xi_2\in M$ 相伴, 則我們則稱這兩組解相伴。這時候存在某個單位元 ϵ 使得 $\xi_2=\xi_1\epsilon$ 且 $N(\epsilon)=1$。

相伴性的定義不依賴 f 在式 (14) 的寫法。由定理 2.9, 每個 $\mathfrak{M}$ 中的等價類 C 都會對應到某個二次型的等價類。如果取其中的一個二次型 f, f 和 C 則有以下的關係。

定理 2.10. 考慮係數環爲 $\mathfrak{D}$ 的模之間的嚴格相似性。假設 C 是這個關係下的一個等價類, 且 C 對應到二次型 $f(x,y)$ 所代表的等價類。我們有以下的一一對應。

$$\Big\{\text{方程式 } f(x,y)=m \text{ 的相伴解 }\Big\}\longleftrightarrow\Big\{\text{模 } A\mid A\in C^{-1}, A\subset\mathfrak{D}, \text{且 } N(A)=m\Big\}.$$

如果 (x,y) 是對應到 A 的解且 $\xi=\alpha x+\beta y$, 則 $A=\xi M^{-1}$且$N(\xi)>0$, 其中M是屬於C的一個模。

證明: 令 M 爲等價類 C 中的一模, α,β 爲一組正定向基底且滿足式 (14)。首先解釋從左到右的對應。若 (x,y) 是滿足 $f(x,y)=m$ 的整數解, 則 $\xi=\alpha x+\beta y\in M$ 滿足 $N(\xi)=mN(M)>0$。考慮另一個模 $A=\xi M^{-1}$。我們有 $AM=\xi M^{-1}M=\xi\mathfrak{D}\subset M$, 所以 $A\subset\mathfrak{D}$, $N(A)=N(\xi)N(M^{-1})=m$, 且 $A\in C^{-1}$。

相反地, 假設等價類 C^{-1} 中有一模 A 其範數爲 m 且 $A\subset\mathfrak{D}$。因爲 M^{-1} 和 A 同屬於等價類 C^{-1}, 因此存在某個範數爲正的數 ξ 使得 $A=\xi M^{-1}$。我們有 $\xi\in MA\subset M$ 且

$N(\xi) = mN(M)$。如果 C^{-1} 中有另一模 A^{-1} 其範數爲 m 且 $A_1 \subset \mathfrak{D}$, 而且存在某數 ξ_1 使得 $A_1 = \xi_1 M^{-1}$ 且 $N(\xi_1) > 0$, 則 $A_1 = \xi_1\xi^{-1}A$。因此 $A = A_1$ 若且唯若 ξ, ξ_1 兩數相伴。□

對任意正整數 m 我們可以具體描述以下集合

$$M[A, m] := \{\text{係數環爲 } \mathfrak{D} \text{ 的模 } A \mid A \subset \mathfrak{D}, N(A) = m\}. \tag{15}$$

在集合中取一模 A, 令 k 爲 A 中的最小正整數。因爲 A 是 $\mathfrak{D}$-模且 $k \in \mathfrak{D}$, 我們可以把 A 寫成 $A = \{k, k\gamma\} = k\{1, \gamma\}$。滿足條件的不同 γ 只會相差正負號和加減某個整數, 所以我們可以要求 γ 符合

$$\begin{cases} \mathrm{Im}(\gamma) > 0, & \text{如果 } d < 0; \\ \mathrm{Irr}(\gamma) > 0, & \text{如果 } d > 0. \end{cases} \tag{16}$$

在第二種情況中我們要求 γ 的有理數部分屬於 $(-\frac{1}{2}, \frac{1}{2}]$ 而 $\mathrm{Irr}(\gamma)$ 指的是 γ 減去有理數部分。我們使用引理 2.5 的符號寫出

$$\gamma = \frac{-b + \sqrt{D}}{2a}. \tag{17}$$

根據我們對有理數部分的假設, 我們有

$$-a \le b < a. \tag{18}$$

因爲 $\mathfrak{D} = \{1, a\gamma\}$ 且 $A \subset \mathfrak{D}$, k 被 a 整除, 這時我們令整數 $s = k/a$。由引理 2.5 的推論我們得到

$$m = N(A) = \frac{k^2}{a} = as^2, \tag{19}$$

所以 A 可以寫成 $A = a\{1, \gamma\}$。

注意這樣的表示法是唯一的: 如果 $as\{1, \gamma\} = a_1 s_1\{1, \gamma_1\}$, 則 $as = a_1 s_1$, 因此 $\{1, \gamma\} = \{1, \gamma_1\}$。由引理 2.5 的推論我們得到 $a = a_1$, 因此 $s = s_1$。最後, 從 (16) 和 (18) 我們得到 $\gamma = \gamma_1$。

相反的, 給定 m 我們取滿足 (19) 的正整數 a 和 s。如果 b, c 符合

$$b^2 - 4ac = D, \quad \gcd(a, b, c) = 1, \quad -a \le b < a, \tag{20}$$

我們用 (17) 定義 γ, 則模 $A = as\{1, \gamma\}$ 被包含在自己的係數環 $\mathfrak{D} = \{1, a\gamma\}$ 中, 而且 $N(A) = a^2 s^2 \frac{1}{a} = m$。

因此, 如果要得到模 A 我們需要滿足 (19) 和 (20) 的四個整數 $s > 0$, $a > 0$, b, c。我們把上面的討論整理成以下定理。

定理 2.11. 令 m 爲正整數。以下的敘述等價:

(i) m 可以被某個判別式 D 的本原二次型表示。

(ii) 存在一個範數爲 m 的模 A, A 的係數環 $\mathfrak{O}$ 包含 A 而且判別式爲 D。

(iii) 存在整數 $s>0$, $a>0$, b, c 滿足以下條件

$$m=as^2,\quad b^2-4ac=D,\quad \gcd(a,b,c)=1,\quad -a\le b<a.$$

注意定理 2.11 是 (15) 中集合 $M[A,m]$ 非空的等價敘述。在定理 2.11 中, 如果 D 是基本判別式, 我們可以進一步簡化 (iii) 的敘述。

定理 2.12. 令 D 是某個二次域的判別式。對某個正整數 m, 把它寫成乘積 $m=as^2$, 其中 a 是不含平方數的部分。則 m 可以被某個判別式爲 D 的本原二次型表示, 若且唯若同餘關係式 $x^2\equiv D \pmod{4a}$ 有解。

證明: 如果 m 可以被某個二次型表示, 則根據定理 2.11 我們可以取整數 s_1,a_1,b_1,c_1 使得 $m=a_1s_1^2$ 且 $b_1^2-4a_1c_1=D$。這時 a 整除 a_1, 因此 $b_1^2\equiv D \pmod{4a}$.

相反地, 假設 b 是 $x^2\equiv D \pmod{4a}$ 的解, 則 $(b-2a)$ 也是解, 所以我們可以假設 $-a\le b<a$。存在某個整數 c 使得 $b^2-4ac=D$。我們宣稱 $\gcd(a,b,c)=1$。如果最大公因數 $\gcd(a,b,c)$ 不是 1, 由 D 的條件我們知道一定是 2。令 $a=2a'$, $b=2b'$, $c=2c'$。則我們推得 $(b')^2-4a'c'\equiv 0,1 \pmod 4$ 且 $D/4\equiv 2,3 \pmod 4$, 但這兩個敘述矛盾。根據定理 2.11 正整數 m 可以被某個判別式 D 的本原二次型表示。 □

例 2.13. 令 $m=p$ 爲質數, 二次體 $K=\mathbb{Q}(\sqrt{-1})$, 則基本判別式 $D=-4$。因爲 K 類數爲 1, 每一個判別式 D 的本原二次型皆和 x^2+y^2 (嚴格) 相似。定理 2.12 告訴我們

$$\begin{aligned} p=x^2+y^2 \text{ 有解 } &\Leftrightarrow x^2\equiv -4 \pmod{4p} \text{ 有解} \\ &\Leftrightarrow x^2\equiv -1 \pmod{p} \text{ 有解 } \Leftrightarrow p\equiv 1 \pmod 4 \text{ 或 } p=2. \end{aligned}$$

2.6. 虛二次域中的相似模

在這一小節中我們假設 $K=\mathbb{Q}(\sqrt{d})$, $d<0$ 是一個虛二次域。在這個情況下, 我們有更簡單的方法可以計算相似模的等價類個數。如果把 K 中的一數 α 想成在複數平面上的一個點, 則一個 K 中的模正好是 $\mathbb{C}=\mathbb{R}^2$ 上的網格 (*lattice*), 而相似的模即是相似的網格。

每個網格都有一組約化基底 (*reduced basis*) $\{\alpha,\beta\}$, 其中 α 是網格中最短的非零向量, β 是網格中和 α 不共線的最短向量。事實上 α,β 會形成網格的一組基底, 而且

$$\beta \text{ 投影至 } \alpha \text{ 的長度 } \le \frac{1}{2}|\alpha|.$$

現在讓我們考慮 M 中所有長度最短的非零向量, 假設有 w 個。如果 α 是這種向量, 則 $-\alpha$ 也是, 所以 w 一定是偶數。除此之外, 兩個最短向量 α, β 之間的夾角不能小於 $\pi/3$, 不然的話 $\alpha - \beta$ 就是一個更短的非零向量。因此 w 只可能是 $2, 4, 6$。

我們可以用以下的方法構造網格 M 的一組約化基底。如果 $w = 2$ 我們取 α 是其中一個最短的向量。M 中可能有 2 或 4 個不和 α 共線的最短向量, 我們在其中取 β 爲和 α (有向) 夾角最小的向量。如果 $w = 4$ 或 $w = 6$, 我們則令 α, β 爲一對夾角最小的最短向量。如果將旋轉後的約化基底視爲一樣, 則網格的約化基底是唯一的。

由先前的討論可以推論, 我們知道平面中的兩個網格 M 和 M_1 相似, 若且唯若它們的約化基底相似 (M 可以透過一次旋轉和一次伸縮變成 M_1)。

現在我們描述 K 中相似模形成的等價類。令 M 爲 K 中的模, 其約化基底爲 $\{\alpha, \beta\}$。考慮 M 的相似模 $\frac{1}{\alpha}M = \{1, \gamma = \frac{\beta}{\alpha}\}$。根據約化基底的性質 γ 滿足

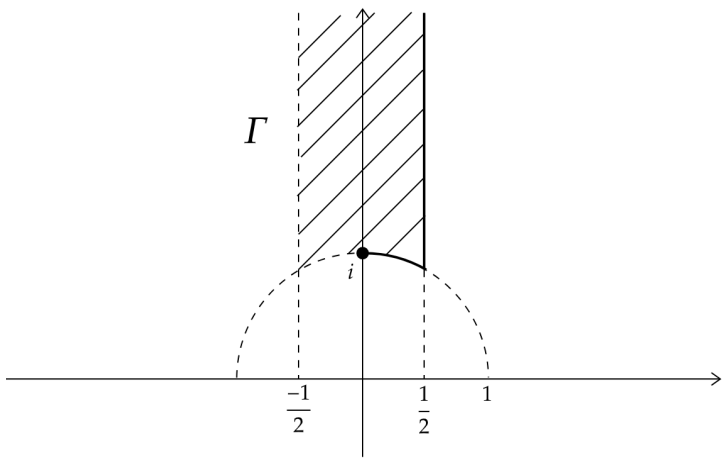
$$\mathrm{Im}\gamma > 0, \tag{21}$$

$$-\frac{1}{2} < \mathrm{Re}\gamma \leq \frac{1}{2}, \tag{22}$$

$$\begin{cases} |\gamma| > 1, & \text{如果 } -\frac{1}{2} < \mathrm{Re}\gamma < 0; \\ |\gamma| \geq 1, & \text{如果 } 0 \leq \mathrm{Re}\gamma \leq \frac{1}{2}. \end{cases} \tag{23}$$

定義. 如果 K 中的一數 γ 滿足 (21)、(22) 和 (23), 則稱 γ 爲約化 (*reduced*) 數, 這時我們也說模 $\{1, \gamma\}$ 是約化模 (*reduced module*)。

從幾何角度來看, 如果 γ 屬於下圖的區域 Γ, 則 γ 是約化數。



定理 2.14. K 中每個模的相似等價類都存在唯一的一個約化模。

證明: 我們知道每個等價類都有一個約化模, 所以只需證明不同的約化模不會相似。首先我們說明如果 $\gamma = x + yi$ 是一個約化數, 則 $1, \gamma$ 是模 $\{1, \gamma\}$ 的一組約化基底。我們宣稱 γ 是模中不在實數軸上的最短向量。也就是說, 對任何整數 k 和非零整數 l

$$|k + l\gamma| \geq |\gamma| .$$

因爲 $|x| \leq \frac{1}{2}$,

$$|k \pm \gamma|^2 = (k \pm x)^2 + y^2 \geq x^2 + y^2 = |\gamma|^2 .$$

如果 $|l| \geq 2$, 則

$$|k + l\gamma|^2 \geq l^2 y^2 > 2y^2 > x^2 + y^2 = |\gamma|^2 .$$

現在令 γ 和 γ_1 是兩個約化數。如果模 $\{1, \gamma\}$ 和模 $\{1, \gamma_1\}$ 相似, 則它們作爲基底也相似, 而這等價於 $\gamma = \gamma_1$。 □

給定兩個 K 中的模 M_1, M_2, 我們透過它們的約化模來判斷它們是否相似。如果兩個約化模相同, 則 M_1 和 M_2 相似; 相反地, 如果兩個約化模不同, 則 M_1 和 M_2 不相似。

現在固定一個判別式 $D < 0$ 的序環 $\mathfrak{O}$, 我們考慮以 $\mathfrak{O}$ 爲係數環的相似模形成的等價類。假設 $\{1, \gamma\}$ 是其中的約化模, 所以 $\gamma \in \Gamma$。使用引理 2.5 中的符號,

$$\gamma = \frac{-b + i\sqrt{|D|}}{2a}.$$

由條件 (22) 和 (23) 我們推得

$$-a \leq b < a, \text{ 且 } \begin{cases} c \geq a & \text{當 } b \leq 0; \\ c > a & \text{當 } b > 0. \end{cases} \tag{24}$$

因此要找到所有約化模, 我們只需找出所有滿足 (24) 和

$$D = b^2 - 4ac, \quad \gcd(a, b, c) = 1, \tag{25}$$

的整數序對 $(a, b, c), a > 0$。因爲係數環爲 $\mathfrak{O}$ 的等價類是有限的 (定理 1.9), 所以這種序對只有有限多個。我們也可以用另一種方法檢查: 給定 D,

$$|D| = 4ac - b^2 \geq 4a^2 - a^2 = 3a^2 \Rightarrow |b| \leq a < \sqrt{\frac{|D|}{3}},$$

所以可能的 (a, b) 只有有限多個, 因此 c 也是。

例 2.15. 假設 $K=\mathbb{Q}(\sqrt{-47})$。考慮係數環爲整數環 $\mathfrak{o}_K$ 的模, 我們想計算這些模上等價類的個數。由於 $D=-47$, 我們有不等式 $|b|\le a<\sqrt{\frac{47}{3}}$。因爲 D 是奇數, b 也必須是奇數, 所以 $b=\pm1,\pm3$。當 $b=\pm3$ 時, 我們得出 $4ac=b^2-D=56$, $ac=14$, 且 $|b|=3\le a<c$, 但這三個條件不可能同時成立。如果 $b=\pm1$, 我們由 $4ac=b^2-D=48$ 得出

$$(a,c)=(1,12),(2,6),\text{或}\,(3,4).$$

我們排除 $a=b=1$ 的情況, 所以 $\mathfrak{o}_K$ 有 5 個相似模的等價類。每個等價類都有一個約化模 $\{1,\gamma\}$, 其中 γ 的值爲

$$\frac{1+\sqrt{47}i}{2},\quad \frac{\pm1+\sqrt{47}i}{4},\quad \frac{\pm1+\sqrt{47}i}{6}.$$

例 2.16. 我們想找出模 $M=\{13,1+5i\}$ 中所有範數爲 650 的數。這個模的係數環爲 $\mathfrak{D}=\{1,5i\}$, 其判別式是 $D=-100$。模 M 的範數爲 13, 所以我們應該先找出滿足以下條件的模 A: 係數環爲 $\mathfrak{D}$, 範數爲 $m=50$, 且 $A\subset\mathfrak{D}$。用定理 2.10 的 (iii) 我們找出以下幾種可能的 a,b,c:

(1) $s=5,a=2,b=-2,c=13$;

(2) $s=1,a=50,b=10,c=1$;

(3) $s=1,a=50,b=-10,c=1$;

(4) $s=1,a=50,b=-50,c=13$.

在每種情況我們找出一個模 $A=as\{1,\gamma\},\gamma=\frac{-b+\sqrt{D}}{2a}$ 並找出相似的約化模。

(1) $10\left\{1,\frac{1+5i}{2}\right\}$;

(2) $50\left\{1,\frac{-1+i}{10}\right\}=(-5+5i)\{1,5i\}$;

(3) $50\left\{1,\frac{1+i}{10}\right\}=(5+5i)\{1,5i\}$;

(4) $50\left\{1,\frac{5+i}{10}\right\}=10i\{1,\frac{1+5i}{2}\}$.

另外, 相似到 M^{-1} 的約化模爲

$$M^{-1}=\left\{1,\frac{1-5i}{13}\right\}=\frac{1-5i}{13}\left\{1,\frac{1+5i}{2}\right\}.$$

只有 (1) 和 (4) 相似到 M^{-1}。在這兩個情況下滿足 $A=\xi M^{-1}$ 的數 ξ 分別是 $5+25i,-25+5i$。因爲 ±1 是 $\mathfrak{D}$ 中唯一的可逆元, M 有四個範數爲 650 的數:$\pm(5+25i),\pm(-25+5i)$。我們也證明了方程式 $13x^2+2xy+2y^2=50$ 有四組整數解 $(x,y)=(0,5),(0,-5),(2,-1),(-2,1)$。

3. 二次域

3.1. 質數的分解

在這一小節中, 我們使用符號 D 代表二次域 $\mathbb{Q}(\sqrt{d})$ 的基本判別式, 而 $\mathfrak{o}_K$ 代表 K 的整數環。代數數論告訴我們 $\mathfrak{o}_K$ 中的任一非零理想都可以唯一地寫成質理想的乘積。另外, 若 I 爲 $\mathfrak{o}_K$ 中的一個非零理想, I 則是一個完全模且 I 包含於本身的係數環 $\mathfrak{o}_K$。這時 I 的範數 $N(I)$ 爲 $\#(A/I)$。最後, 對一個奇質數 p 我們有 Legendre 符號

$$\left(\frac{D}{p}\right) = \begin{cases} 1, & \text{如果 } x^2 \equiv D \pmod{p} \text{ 有解}; \\ 0, & \text{如果 } x^2 \equiv D \pmod{p} \text{ 無解}. \end{cases}$$

我們知道質數 p 在二次域 $\mathbb{Q}(\sqrt{d})$ 分解成質理想的情況爲

定理 3.1. 在判別式爲 D 的二次域中, $p\mathfrak{o}_K$ 分解成

$$p\mathfrak{o}_K = \mathfrak{p}^2, \text{ 其中 } N(\mathfrak{p}) = p,$$

若且唯若 p 整除 D。如果 p 是不整除 D 的奇數, 則

$$p\mathfrak{o}_K = \begin{cases} \mathfrak{p}\mathfrak{p}', \text{其中 } \mathfrak{p} \neq \mathfrak{p}', N(\mathfrak{p}) = N(\mathfrak{p}') = p, & \text{如果 } \left(\frac{D}{p}\right) = 1; \\ \mathfrak{p}, \quad \text{其中 } N(\mathfrak{p}) = p^2, & \text{如果 } \left(\frac{D}{p}\right) = -1. \end{cases}$$

如果 2 不整除 D (因此 $D \equiv 1 \pmod 4$), 則

$$2\mathfrak{o}_K = \begin{cases} \mathfrak{p}\mathfrak{p}', \text{其中 } \mathfrak{p} \neq \mathfrak{p}', N(\mathfrak{p}) = N(\mathfrak{p}') = 2, & \text{如果 } D \equiv 1 \pmod 8; \\ \mathfrak{p}, \quad \text{其中 } N(\mathfrak{p}) = 4, & \text{如果 } D \equiv 5 \pmod 8. \end{cases}$$

我們可以改寫這個定理, 使得質理想的分解僅和 p 除以某些數的餘數有關。首先對正奇數 b 以及整數 c 我們可以定義*Jacobi* 符號 (*Jacobi symbol*) $\left(\frac{c}{b}\right)$。Jacobi 符號滿足以下的互反律

$$\left(\frac{c}{b}\right) = (-1)^{\frac{b-1}{2}\cdot\frac{c-1}{2}} \left(\frac{b}{|c|}\right),$$

並且當 b 是一個質數 p 時 Jacobi 符號 $\left(\frac{c}{p}\right)$ 就是 Legendre 符號。Jacobi 符號的好處是 b 可以是任意正奇數。

令 p 爲一奇質數。如果 $d = D \equiv 1 \pmod 4$,

$$\left(\frac{D}{p}\right) = \left(\frac{d}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{d-1}{2}} \left(\frac{p}{|d|}\right) = \left(\frac{p}{|d|}\right).$$

如果 $d \equiv 3 \pmod 4$,

$$\left(\frac{D}{p}\right) = \left(\frac{d}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{d-1}{2}} \left(\frac{p}{|d|}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{p}{|d|}\right).$$

如果 $d = 2d'$ 且 $2 \nmid d'$,

$$\left(\frac{D}{p}\right) = \left(\frac{d}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{d'}{p}\right) = (-1)^{\frac{p^2-1}{8}+\frac{p-1}{2}\frac{d'-1}{2}} \left(\frac{p}{|d'|}\right).$$

由互反律我們看到 p 除以 $|D|$ 的餘數, 決定了質數 p 的分解情況。如果 $d \equiv 1 \pmod 4$ 則 $\left(\frac{D}{p}\right)$ 僅和 p 除以 $|D|$ 的餘數有關。如果 $d \equiv 3 \pmod 4$, $D = 4d$, 則 p 除以 $|d|$ 的餘數決定了 $\left(\frac{p}{|d|}\right)$, 而且 p 除以 4 的餘數決定了 $(-1)^{\frac{p-1}{2}}$, 因此 $\left(\frac{D}{p}\right)$ 取決於 p 除以 $4|d| = |D|$ 的餘數。如果 $d = 2d'$, $D = 4d = 8d'$, 則 p 除以 $|d'|$ 的餘數決定了 $\left(\frac{p}{|d'|}\right)$, p 除以 4 的餘數決定了 $(-1)^{\frac{p-1}{2}}$, 而且 p 除以 8 的餘數決定了 $(-1)^{\frac{p^2-1}{8}}$, 因此 $\left(\frac{D}{p}\right)$ 取決於 p 除以 $8|d'| = |D|$ 的餘數。

我們定義一個新的函數來簡化這些結果。對於和 D 互質的整數 x, 定義

$$\chi(x) = \begin{cases} \left(\frac{x}{|d|}\right), & \text{如果 } d \equiv 1 \pmod 4; \\ (-1)^{\frac{x-1}{2}} \left(\frac{x}{|d|}\right), & \text{如果 } d \equiv 3 \pmod 4; \\ (-1)^{\frac{x^2-1}{8}+\frac{x-1}{2}\cdot\frac{d'-1}{2}} \left(\frac{x}{|d'|}\right), & \text{如果 } d = 2d'. \end{cases}$$

注意到當 $d \equiv 2, 3 \pmod 4$ 判別式 $D = 4d$ 且 x 是奇數, 所以 $(-1)^{\frac{x-1}{2}}$ 和 $(-1)^{\frac{x^2-1}{8}}$ 都是定義良好的。在前一段的論述中, 我們可以把質數 p 替換成 x, 所以 $\chi(x)$ 只依賴於 x 除以 $|D|$ 的餘數。另外, 對於和 $|D|$ 互質的兩數 x, x' 我們有 $\chi(xx') = \chi(x)\chi(x')$, 因此 χ 是一個定義在 $(\mathbb{Z}/|D|\mathbb{Z})^*$ 上, 秩爲 2 的特徵標 ($character$)。最後, 對於和 D 有共同質因數的整數 x 我們定義 $\chi(x) = 0$。

定義. 我們把 χ 稱作 $\mathbb{Q}(\sqrt{d})$ 的特徵標。

定理 3.2. 如果 χ 是二次域 $\mathbb{Q}(\sqrt{d})$ 的特徵標, 則質數 p 在 $\mathbb{Q}(\sqrt{d})$ 中的質理想分解爲

$$p\mathfrak{o}_K = \begin{cases} \mathfrak{p}\mathfrak{p}', \text{其中 } \mathfrak{p} \neq \mathfrak{p}' \text{ 且 } N(\mathfrak{p}) = N(\mathfrak{p}') = p, & \text{如果 } \chi(p) = 1; \\ \mathfrak{p}, \quad \text{其中 } N(\mathfrak{p}) = p^2, & \text{如果 } \chi(p) = -1; \\ \mathfrak{p}^2, \text{ 其中 } N(\mathfrak{p}) = p, & \text{如果 } \chi(p) = 0. \end{cases}$$

3.2. 數的二元二次型表示

在這一小節中, 我們將會把上一小節的結果應用在數的二元二次型表示中, 再用*Hilbert* 符號 (*Hilbert symbol*) 敘述得到的結果。

對 p 進數 $\mathbb{Q}_p$ 的非零兩數 α,β (p 可以是 ∞, 這時 $\mathbb{Q}_p=\mathbb{R}$), Hilbert 符號

$$\left(\frac{\alpha,\beta}{p}\right)=\begin{cases}1, & \text{如果等式 } \alpha x^2+\beta y^2-z^2=0 \text{ 在 } \mathbb{Q}_p^* \text{ 中有解;}\\ -1, & \text{如果等式 } \alpha x^2+\beta y^2-z^2=0 \text{ 在 } \mathbb{Q}_p^* \text{ 中無解.}\end{cases}$$

Hilbert 符號滿足以下性質

$$\begin{aligned}\left(\frac{\alpha,\beta}{p}\right)&=\left(\frac{\beta,\alpha}{p}\right);\\ \left(\frac{\alpha,\beta_1\beta_2}{p}\right)&=\left(\frac{\alpha,\beta_1}{p}\right)\left(\frac{\alpha,\beta_2}{p}\right);\\ \left(\frac{\alpha_1\alpha_2,\beta}{p}\right)&=\left(\frac{\alpha_1,\beta}{p}\right)\left(\frac{\alpha_2,\beta}{p}\right).\end{aligned}\tag{26}$$

除此之外, 假設 p 是質數, 對 $\mathbb{Q}_p$ 中的可逆元 ϵ,η 我們可以用以下公式算出 $\left(\frac{p,\epsilon}{p}\right)$ 和 $\left(\frac{\epsilon,\eta}{p}\right)$ 的值

$$\begin{aligned}&\left(\frac{p,\epsilon}{p}\right)=\left(\frac{\epsilon}{p}\right),\quad \left(\frac{\epsilon,\eta}{p}\right)=1 \quad \text{如果 } p\neq 2;\\ &\left(\frac{2,\epsilon}{2}\right)=(-1)^{\frac{\epsilon^2-1}{8}},\quad \left(\frac{\epsilon,\eta}{2}\right)=(-1)^{\frac{\epsilon-1}{2}\frac{\eta-1}{2}} \quad \text{如果 } p=2.\end{aligned}\tag{27}$$

如果 $p=\infty$, 則對兩個非零實數 a,b

$$\left(\frac{a,b}{\infty}\right)=\begin{cases}1, & \text{如果 } a>0 \text{ 或 } b>0;\\ -1, & \text{如果 } a<0 \text{ 且 } b<0.\end{cases}$$

定理 3.3. 一個正整數 a 可以被某個判別式 D 的二元二次型表示, 若且唯若任何滿足 $\chi(p)=-1$ 的質數 p 在 a 的質因數分解中出現偶數次。這個條件又等價於, 對任何不整除 D 的質數 p 我們有 $\left(\frac{a,D}{p}\right)=1$。

證明: 由定理 2.11, a 被某個判別式 D 的二元二次型表示, 若且唯若 $\mathbb{Q}(\sqrt{d})$ 中存在一個範數爲 a 的理想。定理 3.2 則描述了哪些整數 a 會是某個理想的範數: 對一個質理想 $\mathfrak{p}$, 當 $\chi(p)=0,1$ 則 $N(\mathfrak{p})=p$, 當 $\chi(p)=-1$ 則 $N(\mathfrak{p})=p^2$。因此 a 是某個理想 $\mathfrak{a}=\prod_{\mathfrak{p}}\mathfrak{p}^{a(\mathfrak{p})}$ 的範數, 若且唯若特徵標的值 $\chi(p)=-1$ 的質因數 p 皆出現偶數次。

考慮每個不整除 D 的質數 p。令 $a=p^kb$, 其中 $p\nmid b$。利用 Hilbert 符號的性質我們得到

$$\left(\frac{a,D}{p}\right)=\begin{cases}\left(\frac{b,D}{p}\right)\left(\frac{D}{p}\right)^k=\left(\frac{D}{p}\right)^k=\chi(p)^k, & \text{如果 } p\neq 2, p\nmid D;\\ (-1)^{\frac{b-1}{2}\cdot\frac{D-1}{2}+k\cdot\frac{D^2-1}{8}}=(-1)^{\frac{k(D^2-1)}{8}}=\chi(2)^k, & \text{如果 } p=2, 2\nmid D.\end{cases}$$

因此定理的第二部分成立。 □

例 3.4. 令 $D = -4$, 我們知道判別式 $D = -4$ 的二元二次型皆等價於 $x^2 + y^2$。如果 $a = \prod p_i^{k_i}$ 是 a 的質因數分解, 則根據定理 3.3 我們得到, a 可以被 $x^2 + y^2$ 表示, 若且唯若對所有 $p_i \equiv 3 \pmod 4$ 的質數 p_i 其次數 k_i 皆是偶數, 若且唯若對所有奇質數 p 我們有 $\left(\frac{a,-4}{p}\right) = 1$。

整數 a 可以被判別式 D 的二次型表示, 若且唯若 ab^2 可以被同樣的二次型表示。因此我們可以只考慮不被 (1 以外的) 平方數整除的整數 a。如果 $p \neq 2$, $p \nmid D$, 且 $p \nmid a$, 則 Hilbert 符號 $\left(\frac{a,D}{p}\right) = 1$。由定理 3.3 我們只需檢查 a 是否滿足有限多個條件, 而這些條件只和 a 的質因數除以 $|D|$ 的餘數有關。

上述的定理描述了整數 a 是否能被某些 (狹義) 等價類中的二次型表示。但我們也可以描述整數 a 是否能被給定的一個等價類中的二次型表示。事實上, 我們可以把收集二次型上的等價類的集合, 分割成兩兩不相交的族, 而每一個可以表示 a 的二次型都屬於同一族。

定義. 給定兩個判別式爲 D 的本原二元二次型。如果它們有理等價 (相差一個有理數可逆矩陣), 則說它們屬於同一個虧格 (*genus*)。

(整數) 等價的二次型一定有理等價, 因此同一等價類中的二次型會屬於同一個虧格, 而每個虧格都是某些等價類的聯集。因此判別式 D 的二次型, 其形成的虧格數量有限。

令 $f = ax^2+bxy+cy^2$ 是一個非奇異的有理二次型。我們可以把行列式 $d(f) = ac-b^2/4$ 寫成

$$d(f) = d_0(f)c^2,$$

其中 $d_0(f)$ 是不被平方數整除的整數。整數 $d_0(f)$ 是二次型的有理等價類上的一個不變量。假設非零有理數 α 可以被 f 表示, 當 p 是質數或 $p = \infty$ 我們定義

$$e_p(f) = \left(\frac{\alpha, -d(f)}{p}\right) = \left(\frac{\alpha, D_f}{p}\right),$$

其中 $D_f = b^2 - 4ac = -4d(f)$ 是 f 的判別式。我們可以證明這個定義不依賴於 α 的選擇。另外, $e_p(f)$ 也是二次型有理等價類上的一個不變量, 稱爲 *Hasse* 不變量 (*Hasse invariant*)。進一步我們有下面的結果, 這是二次型理論中著名的局部整體法則 (*local-global principle*)。

定理 3.5 (Hasse-Minkowski)**.** 兩個二元二次型 f 和 g 有理等價, 若且唯若對任何 p (包含 ∞)

$$d_0(f) = d_0(g) \quad \text{且} \quad e_p(f) = e_p(g).$$

證明請參考 [1] 第 2.1 章 Theorem 3 (第 71 頁)。

因此對一個虧格 G , 我們可以定義

$$e_p(G) = e_p(f) = \left(\frac{a, D}{p}\right),$$

其中 f 是 G 的一個二次型, 而這個定義不依賴於 f 的選取。

引理 3.6. 對判別式爲 D 的任一個虧格 G 我們有

$$e_p(G) = 1, \text{ 如果 } p \nmid D \text{ 或 } p = \infty. \tag{28}$$

證明: 根據定理 3.3 的第二部分, 對任何質數 $p \nmid D$, 我們有 $e_p(f) = \left(\frac{a,D}{p}\right) = 1$。除此之外, 因爲在 $D < 0$ 時我們只考慮正定的二次型, 所以 $e_\infty(f) = 1$。 □

根據定理 3.5 以及引理 3.6, 每個虧格 G 都可以被 $\{e_p(G) \mid p \text{ 是 } D \text{ 的質因數}\}$ 唯一決定。

定理 3.7. 令 a 是一個正整數, 且 G 是一個判別式爲 D 的虧格。a 可以被 G 的某個二次型 (整數) 表示, 若且唯若對所有質數 p

$$\left(\frac{a, D}{p}\right) = e_p(G).$$

證明: 必要性很容易證明, 因此我們只證明充分性。對於某個正整數 a, 如果給定任何質數 p 條件 $\left(\frac{a,D}{p}\right) = e_p(G)$ 都成立, 則根據條件 (28), 對於不整除 D 的 p 我們有 $\left(\frac{a,D}{p}\right) = 1$。由定理 3.3 正整數 a 可以被某個判別式 D 的二次型 f 表示, 而且對任何 p 我們都有 $e_p(f) = \left(\frac{a,D}{p}\right) = e_p(G)$。因此 f 屬於 G, 敘述成立。 □

我們現在來思考如何計算判別式 D 的虧格個數。令 $p_1, \ldots, p_t$ 是 D 的所有質因數。由定理 (28) 每個虧格都被 $e_i = e_{p_i}(G)$, $i = 1, \ldots, t$ 所唯一決定。現在令 $f \in G$ 且 $a \neq 0$ 是被 f 表示的數, 則

$$e_1 \cdots e_t = \prod_p e_p(G) = \prod_p \left(\frac{a, D}{p}\right) = 1.$$

相反地, 我們有以下結果。

定理 3.8. 如果整數 $e_i, i = 1, \ldots, t$ 的值爲 ± 1 且滿足關係式

$$e_1 \cdots e_t = 1 \tag{29}$$

則存在唯一的一個虧格 G 使得

$$e_{p_i}(G) = e_i.$$

證明: 令 k_i 爲 p_i 整除 D 的次數。對所有 $i=1,\dots,t$ 我們取一整數 a_i 使得 $p_i \nmid a_i$, $\left(\frac{a_i,D}{p_i}\right)=e_i$。接下來我們透過以下的同餘方程組求 a

$$a \equiv a_i \pmod{p_i^{k_i}} \quad (1 \le i \le t).$$

如果 p_i 是一個奇質數, 令 $D_i = D/p_i^{k_i}$ 並且由 Hilbert 符號的性質 (26) 我們有

$$\left(\frac{a,D}{p_i}\right) = \left(\frac{a,p_i}{p_i}\right)^{k_i}\left(\frac{a,D_i}{p_i}\right)$$

因爲 a 和 D_i 都是 $\mathbb{Q}_{p_i}$ 中的可逆元, 由性質 (27) 我們得到

$$\left(\frac{a,p_i}{p_i}\right)^{k_i}\left(\frac{a,D_i}{p_i}\right) = \left(\frac{a}{p_i}\right)^{k_i} = \left(\frac{a_i}{p_i}\right)^{k_i}$$

由相同的過程我們有 $\left(\frac{a_i,D}{p_i}\right)=\left(\frac{a_i}{p_i}\right)^{k_i}$, 所以 $\left(\frac{a,D}{p_i}\right)=\left(\frac{a_i,D}{p_i}\right)$。

對於 $p_i=2$ 的情況, 我們令 $k=k_i$, $a'=a_i$。這時 D 一定是下面兩種情況

$$\begin{cases} D=8D', \quad D' \equiv 1 \pmod 2, \quad k=3; \\ D=4D', \quad D' \equiv 3 \pmod 4, \quad k=2. \end{cases}$$

由 Hilbert 符號的性質 (26) 和 (27) 我們有

$$\left(\frac{a,D}{2}\right) = \left(\frac{a,2}{2}\right)^{k}\left(\frac{a,D'}{2}\right) = \begin{cases} \left(\frac{a,D'}{2}\right) = (-1)^{\frac{a-1}{2}}, & \text{如果 } k=2; \\ \left(\frac{a,2}{2}\right)\left(\frac{a,D'}{2}\right) = (-1)^{\frac{a^2-1}{8}}(-1)^{\frac{a-1}{2}\frac{D'-1}{2}}, & \text{如果 } k=3. \end{cases}$$

同樣地,

$$\left(\frac{a',D}{2}\right) = \begin{cases} (-1)^{\frac{a'-1}{2}}, & \text{如果 } k=2; \\ (-1)^{\frac{a'^2-1}{8}}(-1)^{\frac{a'-1}{2}\frac{D'-1}{2}}, & \text{如果 } k=3. \end{cases}$$

當 $a \equiv a' \pmod 4$ 我們有 $(-1)^{\frac{a-1}{2}} = (-1)^{\frac{a'-1}{2}}$。當 $a \equiv a' \pmod 8$ 我們有 $(-1)^{\frac{a^2-1}{8}} = (-1)^{\frac{a'^2-1}{8}}$。因此 $\left(\frac{a,D}{2}\right)=\left(\frac{a',D}{2}\right)$。所以對任意 p_i 我們都有

$$\left(\frac{a,D}{p_i}\right) = \left(\frac{a_i,D}{p_i}\right) = e_i.$$

最後我們只需找到整數 a 使得對不整除 D 的質數 p, $\left(\frac{a,D}{p}\right)=1$。這些整數 a 組成模 $|D|$ 的一個同餘類。在這裡我們使用 Dirichlet 定理。

定理 3.9. 假設 a,d 是互質的兩個正整數。則等差數列 $a, a+d, a+2d, \dots$ 中有無限多個質數。

從這些 a 所組成的同餘類我們可以取一奇質數 q, 則我們有

$$\left(\frac{q,D}{p_i}\right)=\left(\frac{a,D}{p_i}\right)=e_i;$$
$$\left(\frac{q,D}{p}\right)=1, \qquad \text{如果 } p\nmid D,\ p\neq 2,\ \text{且 } p\neq q;$$
$$\left(\frac{q,D}{2}\right)=(-1)^{\frac{q-1}{2}\frac{D-1}{2}}=1, \qquad \text{如果 } p=2\nmid D \text{ 且 } p\neq q.$$

由 Hilbert 符號的乘積公式 $\prod_p\left(\frac{q,D}{p}\right)=1$ 我們得到 $\left(\frac{q,D}{q}\right)=1$。

我們知道存在整數 a 滿足

$$\left(\frac{a,D}{p_i}\right)=e_i,\quad (1\le i\le t);$$
$$\left(\frac{a,D}{p}\right)=1,\quad \text{如果 } p\nmid D.$$

根據定理 3.3, a 可以被某個判別式 D 的二次型 f 表示。令 f 屬於虧格 G, 則

$$e_{p_i}(G)=\left(\frac{a,D}{p_i}\right)=e_i\quad (1\le i\le t). \qquad \square$$

因爲總共有 2^{t-1} 種可能的 $e_i=\pm 1$ 滿足 (29), 所以判別式 D 的虧格個數是 2^{t-1}。

考慮判別式爲 D 的本原二元二次型 (如果 $D<0$ 我們則要求必須是正定二次型), 並且將它們的狹義等價類形成的集合記做 $\mathfrak{F}_D$。在合成運算下, $\mathfrak{F}_D$ 形成一個有限交換群。定理 3.8 告訴我們, 對 D 的每個質因數 p 我們有特徵標 $e_p:\mathfrak{F}_D\to\{\pm 1\}$, 而且對任兩個虧格 G 和 G', 所有特徵標 e_p 在 G 和 G' 的取值相等 $e_p(G)=e_p(G')$, 若且唯若 $G=G'$。

由定理 2.9 中模與二次型之間的一一對應關係, 我們得到 t 個特徵標 $\chi_i^+:\mathrm{Cl}^+(K)\to\{\pm 1\}$, 它們滿足 $\prod_i\chi_i^+=1$。在之前的文章 ‹高斯虧格理論› 我們使用這些特徵標來定義虧格: 兩個狹義理想類 $[\mathfrak{a}]$ 和 $[\mathfrak{b}]$ 屬於相同的虧格, 若且唯若對任何 i 我們有 $\chi_i^+([\mathfrak{a}])=\chi_i^+([\mathfrak{b}])$。因此這兩種虧格的定義等價, 而且定理 3.8 僅是前文 ‹高斯虧格理論› 中定理 3.6 的另一種敘述方式。不過在之前的定理, 我們還知道每個虧格有 $\left|\mathrm{Cl}^+(K)^2\right|$ 個等價類。

結語

有理係數的二元二次型和二次域中的理想類分別有不同的推廣。我們可以考慮係數在任何代數數域或大域體 (global fields) 中的多元二次型。這些二次型在廣泛研究下產生了豐富的理論, 比如說在這個情況下我們仍有局部 - 整體法則, 關於數的二次型表示也有令人滿意的結果。有興趣的讀者可以參考 O'Meara 的著作 [5]。除此之外, 我們還可以用另一種方式推廣二次擴張 $K/\mathbb{Q}$ 中的高斯虧格理論。對任何 Abel 擴張 (abelian extension) K/k, 我們可以定義所

謂的「虧格體 (genus field)」, 它推廣了古典的高斯虧格理論。有興趣的讀者可以參考石田信 (Makoto Ishida) 的著作 [2]。一般來說, 在多元二次型和體擴張 K/k 的狹義理想類群之間, 並沒有如同定理 2.9 的一一對應關係。不過, 如果考慮的是係數在數域 k 中的二元二次型還有二次擴張 K/k 的話, 那麼我們可以透過比較複雜的方式得到這個優美的一一對應。關於這個主題, 我們推薦讀者參考 Towber 的文章 [6] 還有 Kneser 的文章 [3]。

註: 本文取材於 [1]。第一、二、三節分別是根據 2.6、2.7、3.8 節改寫而成。

參考文獻

1. Z. I. Borevich and I. R. Shafarevich, *Number Theory*, Academic press, 1986.
2. Makoto Ishida, *The Genus Fields of Algebraic Number Fields*, volume 555. Springer, 2006.
3. Martin Kneser, Composition of binary quadratic forms, *Journal of Number Theory*, 15(3) (1982), 406-413.
4. Carl Olds, *Continued Fractions*, Mathematical Association of America, 1963.
5. O. T. O'Meara, *Introduction to Quadratic Forms*, volume 117. Springer, 2013.
6. Jacob Towber, Composition of oriented binary quadratic form-classes over commutative rings, *Advances in Mathematics*, 36(1) (1980), 1-107.
7. 余家富、洪梵雲。高斯虧格理論。數學傳播季刊, 46(1), 40-63, 2022。

—本文作者余家富爲中央研究院數學研究所研究員, 洪梵雲投稿時爲中央研究院數學所一年期研習員—