El 2-subgrupo de Sylow del grupo de clases de ideales de un orden cuadrático real.

Gonzalo Tornaría

RESUMEN

Presentamos un algoritmo que permite calcular efectivamente una base del 2-subgrupo de Sylow del grupo de clases de ideales de un orden cuadrático real.

1 Introducción

En [5], Shanks propone el siguiente problema: dado un cuerpo cuadrático imaginario K de discriminante $\Delta < 0$, donde se conoce completamente la factorización de Δ, calcular el 2-subgrupo de Sylow de su grupo de clases de ideales. Para estudiar este problema, es posible trabajar con clases de formas cuadráticas binarias enteras en vez de clases de ideales, dado que los grupos correspondientes son isomorfos.

El famoso Teorema de Duplicación de Gauss [2] afirma que una forma cuadrática tiene raíz cuadrada si y sólo si está en el género principal. La demostración dada por Gauss es constructiva, utiliza formas cuadráticas ternarias, y la eficiente reducción de tales formas. Basándose en estas ideas Shanks describe un algoritmo para la extracción de raíces cuadradas de formas cuadráticas, y con él resuelve el problema planteado de forma eficiente para el caso en que el grupo es cíclico o de la forma $\mathsf{C}(2) \times \mathsf{C}(2^n)$. En el caso general propone utilizar el algoritmo de raíz cuadrada para construir explícitamente todas las formas del 2-subgrupo de Sylow, pero observa que esto es ineficiente, y deja planteada la cuestión de resolver el problema con el mínimo número posible de operaciones de raíz cuadrada.

Lagarias [3] describe un algoritmo para construir una base de un p-grupo abeliano finito en el que podemos extraer raíces p-ésimas. Aplicando este algoritmo al 2-subgrupo de Sylow del grupo de clases de formas cuadráticas binarias enteras de discriminante $\Delta < 0$, se resuelve el problema general de manera eficiente.

Es posible aplicar el algoritmo cuando $\Delta > 0$, obteniéndose una base del 2-subgrupo de Sylow del grupo de clases de formas cuadráticas de discriminante Δ. Esto está estrechamente vinculado con el grupo de clases de un orden cuadrático real, pero en este caso no siempre hay un isomorfismo. Cuando la norma de la unidad fundamental es positiva, el grupo de clases del orden

cuadrático será un cociente del grupo de clases de formas cuadráticas por un subgrupo de orden 2.

Morton [4] describe también el algoritmo de la base, y lo aplica directamente al 2-subgrupo del grupo de clases de ideales de un orden cuadrático cualquiera, pero tomando las clases de ideales en el sentido restringido, y por lo tanto trabajando efectivamente con el grupo de clases de formas cuadráticas.

Además, el método utilizado para calcular raíces cuadradas de clases de ideales depende de resolver ciertas ecuaciones ternarias, para lo que no se conocen algoritmos eficientes.

En este trabajo presentaremos un algoritmo para construir una base del cociente de un p-grupo abeliano finito por un subgrupo de orden p dado por un generador, y mostraremos como aplicar este algoritmo al 2-subgrupo de Sylow del grupo de clases de formas cuadráticas binarias enteras de discriminante $\Delta > 0$, con lo que se determina el 2-subgrupo de Sylow del grupo de clases de un orden cuadrático real cualquiera, de manera eficiente.

2 El algoritmo de la base

Sea $\mathfrak{H}$ un p-grupo abeliano finito con elemento identidad 1, cuya operación de grupo denotaremos multiplicativamente.

Definición 2.1 Decimos que un conjunto $\{b_1, b_2, \ldots, b_g\}$ de elementos de $\mathfrak{H}$, de órdenes $\{p^{s_1}, p^{s_2}, \ldots, p^{s_g}\}$ respectivamente, es una *base* de $\mathfrak{H}$ si todo elemento $h \in \mathfrak{H}$ puede ser expresado de forma única como

$$h = \prod_{j=1}^{g} (b_j)^{\lambda_j}, \qquad 0 \le \lambda_j < p^{s_j}.$$

Si además se cumple que $s_1 \le s_2 \le \cdots \le s_g$, decimos que $\{b_1, b_2, \ldots, b_g\}$ es una *base ordenada*.

En lo que sigue utilizaremos la siguiente notación:

$$\mathfrak{H}^p = \{h^p \mid h \in \mathfrak{H}\},$$
$$\mathfrak{H}_l = \left\{h \in \mathfrak{H} \mid h^{p^l} = 1\right\},$$

y denotaremos $\mathfrak{X}$ al grupo de carácteres de $\mathfrak{H}$ de orden p, es decir, los homomorfismos $\chi : \mathfrak{H} \to \mathbb{F}_p$. Al menor l para el cual $\mathfrak{H}_l = \mathfrak{H}$ lo llamaremos el *exponente* de $\mathfrak{H}$.

El algoritmo de la base permite calcular una base ordenada de un p grupo abeliano finito $\mathfrak{H}$ cuando conocemos:

- Una base $\{\chi_1, \chi_2, \ldots, \chi_g\}$ del grupo $\mathfrak{X}$ de carácteres de $\mathfrak{H}$ de orden p, y un algoritmo para evaluar $\chi_j(h)$, cualquiera sea j, y cualquiera sea $h \in \mathfrak{H}$.

- Un conjunto $\{t_1, t_2, \ldots, t_n\}$, generador del subgrupo $\mathfrak{H}_1$ de elementos de orden p en $\mathfrak{H}$.

- Un algoritmo que dado $h \in \mathfrak{H}^p$, encuentre un elemento $k \in \mathfrak{H}$ tal que $k^p = h$. Es decir, que calcule raíces p-ésimas en $\mathfrak{H}$.

Este algoritmo será útil cuando $\mathfrak{H}$ no es dado explícitamente, como es el caso cuando se trata del 2-subgrupo de Sylow de un grupo de clases de formas cuadráticas. Destacamos que el algoritmo no efectúa ninguna comparación entre los elementos del grupo. Esto es de suma importancia pues permite trabajar con clases de equivalencia para las que no tenemos representantes canónicos, como es el caso de las clases de formas cuadráticas indefinidas.

Observemos que el grupo $\mathfrak{H}/\mathfrak{H}^p$ puede ser considerado como un espacio vectorial sobre el cuerpo finito $\mathbb{F}_p$, ya que todos sus elementos tienen orden p. Definimos entonces los invariantes

$$r_l = \dim \pi(\mathfrak{H}_l),$$

donde $\pi : \mathfrak{H} \to \mathfrak{H}/\mathfrak{H}^p$ es la proyección canónica.

El siguiente teorema nos da un criterio para reconocer una base ordenada de $\mathfrak{H}$:

Teorema 2.2 (Lagarias [3, Theorem 3.3]) *Sea $\mathfrak{H}$ un p-grupo abeliano y sea $\pi : \mathfrak{H} \to \mathfrak{H}/\mathfrak{H}^p$ la proyección canónica. Entonces $\{b_1, b_2, \ldots, b_g\}$ es una base ordenada de $\mathfrak{H}$ si y sólo si, para todo l,*

1. *$\{b_1, b_2, \ldots, b_{r_l}\} \subseteq \mathfrak{H}_l$,*
2. *$\{\pi(b_1), \pi(b_2), \ldots, \pi(b_{r_l})\}$ es una base de $\pi(\mathfrak{H}_l)$.* □

La clave para poder aplicar este teorema es que la base dada para el grupo $\mathfrak{X}$ induce una base dual para $\mathfrak{H}/\mathfrak{H}^p$. En coordenadas con respecto a esta base, la proyección canónica $\pi : \mathfrak{H} \to \mathfrak{H}/\mathfrak{H}^p$ se puede calcular fácilmente como

$$\pi(h) = (\chi_1(h), \chi_2(h), \ldots, \chi_g(h)) .$$

Comenzando con $b_j = t_j$ para $j = 1, 2, \ldots, n$, bastará con aplicar el método de eliminación de Gauss a $\{\pi(b_1), \pi(b_2), \ldots, \pi(b_n)\}$ para obtener una base de

$\pi(\mathfrak{H}_1)$, y $n - r_1$ vectores nulos, que corresponderán a elementos en $\mathfrak{H}^p$. Calculando las raíces p-ésimas de estos últimos elementos, obtendremos un conjunto generador de $\mathfrak{H}_2$, que cumplirá el criterio del teorema 2.2 con $l = 1$. Repitiendo este procedimiento tantas veces como el exponente de $\mathfrak{H}$, obtendremos una base ordenada.

DEFINICIÓN 2.3 Decimos que una matriz $g \times n$,

$$\mathbf{M} = (m_{i,j}),$$

es *escalonada por columnas* si existe $r \leq n$, al que llamamos *rango* de $\mathbf{M}$, tal que

1. Para $1 \leq j \leq r$, $m_{j,j} \neq 0$, y $m_{i,j} = 0$ si $i < j$.
2. Las últimas $n - r$ columnas de $\mathbf{M}$ son iguales a 0.

El siguiente algoritmo tiene la propiedad de no modificar las primeras columnas de $\mathbf{M}$ si ya están escalonadas:

ALGORITMO 2.4 (ESCALONAR POR COLUMNAS)
Dada una matriz $g \times n$ sobre un cuerpo,

$$\mathbf{M} = (m_{i,j}),$$

este algoritmo devuelve una matriz $\mathbf{T}$ escalonada por columnas tal que $\mathbf{T} = \mathbf{PMR}$ con $\mathbf{P}$ una matriz $g \times g$ de permutación y $\mathbf{R}$ una matriz $n \times n$ de determinante 1.

1. Hacer $k \leftarrow 1$.
2. Si $m_{k,k} = 0$, buscar un índice (i, j) con $k \leq i \leq g$, $k \leq j \leq n$, tal que $m_{i,j} \neq 0$, e intercambiar las filas k e i y las columnas k y j.
   Si un tal índice no existe, devolver $\mathbf{M}$, de rango $k - 1$.
3. Para $j > k$, sumar $-\frac{m_{k,j}}{m_{k,k}}$ veces la columna k a la columna j.
4. Hacer $k \leftarrow k + 1$ y volver al paso 2.

Ahora podemos describir el algoritmo de la base, que coincide esencialmente con el dado por Lagarias en [3, pp. 494–495].

ALGORITMO 2.5 (BASE DE UN p-GRUPO ABELIANO FINITO)
Sea $\mathfrak{H}$ un p-grupo abeliano finito. Dados una base de $\mathfrak{X}$, un conjunto generador de $\mathfrak{H}_1$, y un algoritmo para calcular raíces p-ésimas en $\mathfrak{H}^p$, este algoritmo devuelve una base ordenada de $\mathfrak{H}$.

1. Para $j = 1, 2, \ldots, n$, hacer $b_j \leftarrow t_j$, $s_j \leftarrow 1$, donde $\{t_1, t_2, \ldots, t_n\}$ es el conjunto generador de $\mathfrak{H}_1$.
   Calcular la matriz $g \times n$ dada por

$$\mathbf{M} = (\chi_i(b_j)), \tag{2.1}$$

   donde $\{\chi_1, \chi_2, \ldots, \chi_g\}$ es la base de $\mathfrak{X}$.

2. Usando el algoritmo 2.4 sobre el cuerpo $\mathbb{F}_p$, calcular a partir de $\mathbf{M}$ una matriz $\mathbf{T}$ escalonada por columnas, de rango r.
   Al hacerlo, cada vez que se intercambian las filas k e i se intercambian también χ_k con χ_i, cada vez que se intercambian las columnas k y j se intercambian b_k con b_j, y al sumar d veces la columna k a la columna j se multiplica b_j por $(b_k)^d$.

3. Si $r = g$, devolver $\{b_1, b_2, \ldots, b_g\}$, de órdenes $\{p^{s_1}, p^{s_2}, \ldots, p^{s_g}\}$ respectivamente.

4. Para $j = r+1, \ldots, n$, remplazar b_j por una de sus raíces p-ésimas y hacer $s_j \leftarrow s_j + 1$.
   Recalcular $\mathbf{M}$ como en (2.1), observando que las primeras r columnas coinciden con las de $\mathbf{T}$, y volver al paso 2.

Teorema 2.6 (Lagarias [3, Theorem 3.4]) *En el algoritmo 2.5:*

1. *Después de la l-ésima pasada por el paso 2, $\{b_1, b_2, \ldots, b_n\}$ genera $\mathfrak{H}_l$, y $\{\pi(b_1), \pi(b_2), \ldots, \pi(b_r)\}$ es una base de $\pi(\mathfrak{H}_l)$.*
   El orden de b_j es p^{s_j} para $j = 1, 2, \ldots, r$, y estos elementos quedan fijos hasta el final del algoritmo. Además $s_{r+1} = s_{r+2} = \cdots = s_n = l$.
   En particular $b_j \in \mathfrak{H}_{s_j}$ para todo j.

2. *El algoritmo termina después de pasar s veces por el paso 2, donde s es el exponente de $\mathfrak{H}$.*

3. *Al terminar, $\{b_1, b_2, \ldots, b_g\}$ es una base ordenada de $\mathfrak{H}$.* □

3 El cociente por un subgrupo de orden p.

Si $\{b_1, b_2, \ldots, b_g\}$ es una base ordenada del p-grupo abeliano $\mathfrak{H}$, y $\mathfrak{N} \subseteq \mathfrak{H}$ es un subgrupo, no es cierto en general que $\{b_1\mathfrak{N}, b_2\mathfrak{N}, \ldots, b_g\mathfrak{N}\}$ sea una base ordenada de $\mathfrak{H}/\mathfrak{N}$.

Mostraremos aquí como modificar el algoritmo 2.5 cuando $\mathfrak{N}$ es un grupo de orden p generado por

$$t = \prod_{j=1}^{n} (t_j)^{\lambda_j},$$

para que la proyección sobre $\mathfrak{N}$ de la base obtenida sea una base ordenada de $\mathfrak{H}/\mathfrak{N}$. Observemos que no hay pérdida de generalidad en suponer conocida una expresión de t en términos del conjunto generador $\{t_1, t_2, \ldots, t_n\}$, pues en caso contrario bastará con agregar el propio t al conjunto generador.

A estos efectos, tendremos una matriz $n \times n$ con coeficientes en $\mathbb{F}_p$, que llevará la cuenta de las combinaciones efectuadas con los b_j en el paso 2. Como resultado adicional se obtendrá, al finalizar el algoritmo, un sistema completo de $n - g$ relaciones independientes en el conjunto generador de $\mathfrak{H}_1$.

Por el teorema 2.6, durante el algoritmo siempre tenemos que $b_j \in \mathfrak{H}_{s_j}$, por lo que

$$(b_j)^{p^{s_j-1}} \in \mathfrak{H}_1.$$

Los coeficientes de la matriz

$$\mathbf{U} = (u_{i,j}),$$

verificarán

$$b_j^{p^{s_j-1}} = \prod_{i=1}^{n} (t_i)^{u_{i,j}}. \tag{3.1}$$

La matriz $\mathbf{U}$ tendrá rango n, y podremos, al finalizar el algoritmo, encontrar coeficientes $\alpha_i \in \mathbb{F}_p$ tales que

$$\mathbf{U} \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix} = \begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \vdots \\ \lambda_n \end{pmatrix},$$

o lo que es lo mismo, que

$$\prod_{j=1}^{n} (b_j)^{\alpha_j p^{s_j-1}} = \prod_{j=1}^{n} (t_j)^{\lambda_j} = t \in \mathfrak{N}.$$

Sea i el menor índice para el que $\alpha_i \neq 0$. Si $i > g$, esto significa que $t = 1$, y por lo tanto el subgrupo $\mathfrak{N}$ es trivial. En otro caso podemos asumir que $s_{i-1} < s_i$, permutando algunos b_j si fuera necesario, sin que la base deje de estar ordenada.

Remplazamos entonces b_i por

$$b_i' = \prod_{j=i}^{g} (b_j)^{\alpha_j p^{s_j - s_i}},$$

que cumple $(b_i')^{s_i - 1} \in \mathfrak{N}$.

LEMA 3.1 *El conjunto* $\{b_1, b_2, \ldots, b_g\}$ *así obtenido es una base ordenada de* $\mathfrak{H}$*, y* $\{b_1\mathfrak{N}, b_2\mathfrak{N}, \ldots, b_g\mathfrak{N}\}$ *es una base ordenada de* $\mathfrak{H}/\mathfrak{N}$*.*

El orden de b_j *es* p^{s_j}*, mientras que el orden de* $b_j\mathfrak{N}$ *es* p^{s_j} *cuando* $j \neq i$*, y el orden de* $b_i\mathfrak{N}$ *es* $p^{s_i - 1}$*.*

Demostración. Observemos que

$$\pi(b_i') = \prod_{j=i}^{r_{s_i}} \pi(b_j)^{\alpha_j},$$

y como $\alpha_i \neq 0$, la condición 2 del teorema 2.2 no se ve alterada al sustituir b_i por b_i'.

Además, es claro que $\{b_1\mathfrak{N}, b_2\mathfrak{N}, \ldots, b_g\mathfrak{N}\}$ así obtenido es un conjunto generador de $\mathfrak{H}/\mathfrak{N}$. Como ahora $(b_i)^{s_i - 1} = t$, el orden de $b_i\mathfrak{N}$ es $p^{s_i - 1}$, y por coincidir el orden de $\mathfrak{H}/\mathfrak{N}$ con el producto de los órdenes de los $b_j\mathfrak{N}$, se concluye que éstos forman una base de $\mathfrak{H}/\mathfrak{N}$. Como asumimos que $s_{i-1} < s_i$, se sigue que se trata de una base ordenada. □

Para calcular la matriz $\mathbf{U}$, comenzamos en el paso 1 con $\mathbf{U} = \mathbf{Id}_n$, y en el paso 2 recalculamos las columnas de $\mathbf{U}$ de la siguiente manera:

- Toda vez que se intercambia b_k con b_j, se intercambian las columnas k y j de $\mathbf{U}$.
- Toda vez que se multiplica b_j por $(b_k)^d$, si $s_j = s_k$ se suma d veces la columna k a la columna j de $\mathbf{U}$.

LEMA 3.2 *En todo momento del algoritmo 2.5, la matriz* $\mathbf{U}$ *así calculada verifica las ecuaciones* (3.1)*, y tiene rango* n*.*

Demostración. Es claro que las ecuaciones (3.1) valen después del paso 1. Cuando en el paso 2 se intercambia b_k con b_j y se intercambian las columnas k y j de $\mathbf{U}$, siguen valiendo. Por otra parte, si $b_j' = b_j(b_k)^d$, tenemos que

$$(b_j')^{p^{s_j - 1}} = (b_j)^{p^{s_j - 1}} (b_k)^{dp^{s_j - 1}} = \prod_{i=1}^{n} (t_i)^{u_{i,j} + \delta d u_{i,k}},$$

donde $\delta = \delta(s_j, s_k)$ vale 1 si $s_j = s_k$ y 0 si $s_j \neq s_k$. Observando que, en cualquier caso $s_j \geq s_k$, es que se sigue que

$$(b_k)^{dp^{s_j-1}} = (b_k)^{\delta dp^{s_k-1}},$$

pues si $s_j > s_k$ entonces el exponente dp^{s_j-1} anula a b_k. Finalmente, al cambiar b_j por una raíz p-ésima e incrementar s_j en el paso 4, el valor de $(b_j)^{p^{s_j-1}}$ no cambia.

La segunda afirmación vale trivialmente al comienzo del algoritmo, y ninguno de los pasos 2 o 4 altera este hecho. □

ALGORITMO 3.3 (BASE DE UN p-GRUPO ABELIANO FINITO, CON COCIENTE) Sea $\mathfrak{H}$ un p-grupo abeliano finito. Dados una base de $\mathfrak{X}$, un conjunto generador de $\mathfrak{H}_1$, un algoritmo para calcular raíces p-ésimas en $\mathfrak{H}^p$, y dado $t = (t_1)^{\lambda_1}(t_2)^{\lambda_2}\cdots(t_n)^{\lambda_n}$, este algoritmo calcula una base ordenada de $\mathfrak{H}$, que al proyectar es base ordenada del cociente $\mathfrak{H}/\langle t\rangle$, devuelve los órdenes respectivos, y determina si $t = 1$ o no.

1. Para $j = 1, 2, \ldots, n$, hacer $b_j \leftarrow t_j$ y $s_j \leftarrow 1$, donde $\{t_1, t_2, \cdots, t_n\}$ es el conjunto generador de $\mathfrak{H}_1$.
   Calcular la matriz $g \times n$ dada por

   $$\mathbf{M} = (\chi_i(b_j)), \tag{3.2}$$

   donde $\{\chi_1, \chi_2, \ldots, \chi_g\}$ es la base de $\mathfrak{X}$.
   Hacer $\mathbf{U} \leftarrow \mathbf{Id}_n$ (coeficientes en $\mathbb{F}_p$).

2. Usando el algoritmo 2.4 sobre el cuerpo $\mathbb{F}_p$, calcular a partir de $\mathbf{M}$ una matriz $\mathbf{T}$ escalonada por columnas, de rango r.
   Al hacerlo, cada vez que se intercambian las filas k e i se intercambian también χ_k con χ_i, cada vez que se intercambian las columnas k y j se intercambian b_k con b_j y las columnas k y j de $\mathbf{U}$, y al sumar d veces la columna k a la columna j se multiplica b_j por $(b_k)^d$, y si $s_j = s_k$ se suma d veces la columna k a la columna j de la matriz $\mathbf{U}$.

3. Si $r = g$, ir al paso 5.

4. Para $j = r+1, \ldots, n$, remplazar b_j por una de sus raíces p-ésimas, y hacer $s_j \leftarrow s_j + 1$.
   Recalcular $\mathbf{M}$ como en (3.2), observando que las primeras r columnas coinciden con las de $\mathbf{T}$, y volver al paso 2.

5. Resolver el sistema lineal

$$\mathbf{U}\begin{pmatrix}\alpha_1\\ \alpha_2\\ \vdots\\ \alpha_n\end{pmatrix}=\begin{pmatrix}\lambda_1\\ \lambda_2\\ \vdots\\ \lambda_n\end{pmatrix}.$$

6. Sea i el menor índice tal que $\alpha_i \neq 0$ Si $i > g$, devolver $\{b_1, b_2, \ldots, b_g\}$, de órdenes $\{p^{s_1}, p^{s_2}, \ldots, p^{s_g}\}$ respectivamente, afirmando que $t = 1$.

7. En otro caso, sea k el menor índice tal que $s_k = s_i$, y hacer

$$(b_k, b_i) \leftarrow \left(\prod_{j=i}^{g} b_j^{\alpha_j p^{s_j - s_i}}, b_k\right).$$

   Devolver $\{b_1, b_2, \ldots, b_g\}$, de órdenes $\{p^{s_1}, p^{s_2}, \ldots, p^{s_g}\}$ respectivamente, y afirmar que $t \neq 1$, y que $\{b_1\langle t\rangle, b_2\langle t\rangle, \ldots, b_g\langle t\rangle\}$ es base ordenada de $\mathfrak{H}/\langle t\rangle$, con órdenes $\{p^{s_1}, p^{s_2}, \ldots, p^{s_k-1}, \ldots, p^{s_g}\}$.

LEMA 3.4 *Al terminar el algoritmo, las últimas $n - g$ columnas de la matriz* $\mathbf{U}$ *serán los coeficientes de un sistema completo de relaciones independientes en el conjunto* $\{t_1, t_2, \ldots, t_n\}$.

Demostración. Al finalizar tendremos que $\pi(b_{g+1}) = \cdots = \pi(b_n) = 0$, y $s_{g+1} = \cdots = s_n = s$, donde s es el exponente de $\mathfrak{H}$, por lo que

$$(b_j)^{p^{s_j-1}} = 1,$$

para $j = g+1, \ldots, n$. Por las ecuaciones (3.1), las últimas $n - g$ columnas de la matriz $\mathbf{U}$ nos dan entonces $n - g$ relaciones en el conjunto $\{t_1, t_2, \ldots, t_n\}$, que serán independientes por el lema 3.2. Como $\mathfrak{H}_1$ tiene dimensión g, estas relaciones generan todas las posibles. □

4 El 2-subgrupo de Sylow para un orden cuadrático real

El algoritmo 2.5 puede aplicarse directamente al 2-subgrupo de Sylow del grupo $\mathcal{F}(\Delta)$ de clases de formas cuadráticas binarias enteras de discriminante Δ. En efecto, la teoría de géneros de Gauss [2] nos permite dar explícitamente una base del grupo de carácteres cuadráticos de $\mathcal{F}(\Delta)$ y un conjunto generador del subgrupo de clases de orden 2 [3, pp. 499-500], y un algoritmo para extracción de raíces cuadradas [5]. Las referencias citadas consideran solamente el

caso de formas cuadráticas binarias enteras en el sentido clásico; para el caso general ver [6].

Podemos relacionar el grupo de clases de ideales $\mathbf{C}(\mathcal{O})$ de un orden cuadrático $\mathcal{O}$ de discriminante Δ con el grupo $\mathcal{F}(\Delta)$:

TEOREMA 4.1 *Sea $\mathcal{O}$ el orden cuadrático de discriminante Δ.*

1. *Si $f = [a, b, c]$ es una forma cuadrática primitiva de discriminante Δ, entonces*
$$\mathcal{I}(f) = \left\langle a, \frac{-b + \sqrt{\Delta}}{2} \right\rangle_{\mathbb{Z}}$$
es un ideal propio de $\mathcal{O}$.

2. *La aplicación $f \mapsto \mathcal{I}(f)$ induce un epimorfismo*
$$\mathcal{I} : \mathcal{F}(\Delta) \longrightarrow \mathbf{C}(\mathcal{O}).$$
Cuando $\Delta < 0$, se trata de un isomorfismo, mientras que si $\Delta > 0$, su núcleo tiene orden 1 o 2, generado por
$$f_{-1} = \begin{cases} \left[-1, -1, \frac{\Delta-1}{4}\right] & \text{si } \Delta \equiv 1 \pmod 4, \\ \left[-1, 0, \frac{\Delta}{4}\right] & \text{si } \Delta \equiv 0 \pmod 4. \end{cases}$$

Demostración. Ver Cox [1, Theorem 7.7] □

Se sigue del teorema que el cálculo del 2-subgrupo de Sylow para un orden cuadrático imaginario de discriminante Δ es equivalente al cálculo del 2-subgrupo de Sylow para $\mathcal{F}(\Delta)$, pero en el caso de un orden cuadrático real no siempre es así.

En este caso, el algoritmo 3.3 nos permitirá decidir si $\mathcal{F}(\Delta)$ y $\mathbf{C}(\mathcal{O})$ son isomorfos, y en caso que no lo sean calcular el 2-subgrupo de Sylow de este último como el cociente del 2-subgrupo de Sylow de $\mathcal{F}(\Delta)$ por $\langle f_{-1} \rangle$.

EJEMPLO 4.2 Sea $\mathrm{K} = \mathbb{Q}\left(\sqrt{\Delta}\right)$ el cuerpo cuadrático real de discriminante $\Delta = 3110728 = 8 \cdot 17 \cdot 89 \cdot 257$. Determinaremos una base ordenada del 2-subgrupo de Sylow del grupo $\mathbf{C}_{\mathrm{K}}$ de clases de ideales de su orden maximal.

Para esto, trabajaremos con el grupo $\mathcal{F}(\Delta)$ de clases de formas cuadráticas binarias enteras de discriminante Δ. En primer lugar, una base del grupo de carácteres cuadráticos de $\mathcal{F}(\Delta)$ está dada por $\{\chi_{17}, \chi_{89}, \chi_{257}\}$, donde, identificando el grupo aditivo de $\mathbb{F}_2$ con el grupo multiplicativo $\{\pm\}$,
$$\chi_p(f) = \begin{cases} + & \text{si } f \text{ representa residuos cuadráticos módulo } p, \\ - & \text{si } f \text{ representa no residuos cuadráticos módulo } p. \end{cases}$$

					χ_{17}	χ_{89}	χ_{257}
t_1	=	f_{-1}	=	$[-1, 0, 777682]$	+	+	+
t_2	=	f_{17}	=	$[17, 0, -45746]$	+	+	+
t_3	=	f_{89}	=	$[89, 0, -8738]$	+	+	+
t_4	=	f_{257}	=	$[257, 0, -3026]$	+	+	+
t_5	=	$\sqrt{t_1}$	=	$[449, 1518, -449]$	−	+	−
t_6	=	$\sqrt{t_2}$	=	$[446, 1356, -713]$	+	+	+
t_7	=	$\sqrt{t_3}$	=	$[198, 1492, -1117]$	−	+	+
t_8	=	$\sqrt{t_4}$	=	$[97, 1710, -481]$	−	+	−
t_9	=	$t_7 t_5$	=	$[106, 1560, -1597]$	+	+	−
t_{10}	=	$t_8 t_5$	=	$[-121, 1522, 1641]$	+	+	+
t_{11}	=	$\sqrt{t_6}$	=	$[66, 1712, -681]$	+	−	−
t_{12}	=	$\sqrt{t_{10}}$	=	$[93, 1744, -186]$	+	+	−
t_{13}	=	$t_{11} t_9$	=	$[-442, 1020, 1171]$	+	−	+
t_{14}	=	$t_{12} t_9$	=	$[222, 1472, -1063]$	+	+	+

Tabla 4.1: Formas cuadráticas para el ejemplo 4.2.

Un conjunto generador para el subgrupo de clases de orden 2 está dado por $\{t_1, t_2, t_3, t_4\}$ como en la tabla 4.1.

Al inicio del algoritmo, calculamos **M**:

M	t_1	t_2	t_3	t_4
χ_{17}	+	+	+	+
χ_{89}	+	+	+	+
χ_{257}	+	+	+	+
s	1	1	1	1

U	t_1	t_2	t_3	t_4
t_1	1	0	0	0
t_2	0	1	0	0
t_3	0	0	1	0
t_4	0	0	0	1

La matriz **M** ya está escalonada por columnas, con rango $r_1 = 0$. Calculamos entonces las raíces cuadradas de t_1, t_2, t_3, y t_4 (ver tabla 4.1), y recalculamos **M**:

M	t_5	t_6	t_7	t_8
χ_{17}	−	+	−	−
χ_{89}	+	+	+	+
χ_{257}	−	+	+	−
s	2	2	2	2

U	t_5^2	t_6^2	t_7^2	t_8^2
t_1	1	0	0	0
t_2	0	1	0	0
t_3	0	0	1	0
t_4	0	0	0	1

Debemos ahora escalonar **M**. Para esto basta con "sumar" (multiplicar) la primera columna a la tercera y a la cuarta, e intercambiar las filas segunda

y tercera y las columnas segunda y tercera. Las matrices $\mathbf{M}$ y $\mathbf{U}$ resultan:

$\mathbf{M}$	t_5	t_9	t_6	t_{10}
χ_{17}	$-$	$+$	$+$	$+$
χ_{257}	$-$	$-$	$+$	$+$
χ_{89}	$+$	$+$	$+$	$+$
s	2	2	2	2

$\mathbf{U}$	t_5^2	t_9^2	t_6^2	t_{10}^2
t_1	1	1	0	1
t_2	0	0	1	0
t_3	0	1	0	0
t_4	0	0	0	1

La matriz $\mathbf{M}$ tiene rango $r_2 = 2$. Calculamos ahora las raíces cuadradas de t_6 y t_{10}, y recalculamos $\mathbf{M}$:

$\mathbf{M}$	t_5	t_9	t_{11}	t_{12}
χ_{17}	$-$	$+$	$+$	$+$
χ_{257}	$-$	$-$	$-$	$-$
χ_{89}	$+$	$+$	$-$	$+$
s	2	2	3	3

$\mathbf{U}$	t_5^2	t_9^2	t_{11}^4	t_{12}^4
t_1	1	1	0	1
t_2	0	0	1	0
t_3	0	1	0	0
t_4	0	0	0	1

La matriz $\mathbf{M}$ se escalona multiplicando la segunda columna a la tercera y a la cuarta. La matriz $\mathbf{U}$ no se ve afectada puesto que $s_2 \neq s_3$ y $s_2 \neq s_4$.

$\mathbf{M}$	t_5	t_9	t_{13}	t_{14}
χ_{17}	$-$	$+$	$+$	$+$
χ_{257}	$-$	$-$	$+$	$+$
χ_{89}	$+$	$+$	$-$	$+$
s	2	2	3	3

$\mathbf{U}$	t_5^2	t_9^2	t_{13}^4	t_{14}^4
t_1	1	1	0	1
t_2	0	0	1	0
t_3	0	1	0	0
t_4	0	0	0	1

Ahora $\mathbf{M}$ tiene rango $r_3 = 3$, y concluimos que el 2-subgrupo de Sylow de $\mathcal{F}(\Delta)$ es

$$\mathsf{C}(4) \times \mathsf{C}(4) \times \mathsf{C}(8),$$

con generadores t_5, t_9, y t_{13}.

Por otra parte, la última columna de $\mathbf{U}$ nos da la relación $t_1 t_4 = t_{14}^4$; como t_{14} es un cuadrado, t_{14}^4 es equivalente a la forma principal, y concluimos que $t_1 = t_4$ es la (única) relación del conjunto $\{t_1, t_2, t_3, t_4\}$. En particular, $t_1 = [-1, 0, 777682]$ no es equivalente a la forma principal $[1, 0, -777682]$. Deducimos por lo tanto que la ecuación de Pell $X^2 - 777682Y^2 = -1$ no tiene solución o, lo que es lo mismo, la norma de la unidad fundamental de K es positiva.

Por el teorema 4.1, debemos hacer el cociente por el subgrupo generado por $t = t_1$. Para esto resolvemos el sistema

$$\mathbf{U} \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \\ \alpha_4 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix},$$

cuya solución es claramente $(\alpha_1, \alpha_2, \alpha_3, \alpha_4) = (1, 0, 0, 0)$. Concluimos por lo tanto que el 2-subgrupo de Sylow de $\mathbf{C}_{\mathrm{K}}$ es

$$\mathsf{C}(2) \times \mathsf{C}(4) \times \mathsf{C}(8),$$

con generadores

$$\left\langle 449, \frac{-1518 + \sqrt{\Delta}}{2} \right\rangle_{\mathbb{Z}},$$
$$\left\langle 106, \frac{-1560 + \sqrt{\Delta}}{2} \right\rangle_{\mathbb{Z}},$$
$$\left\langle -442, \frac{-1020 + \sqrt{\Delta}}{2} \right\rangle_{\mathbb{Z}},$$

de órdenes 2, 4, y 8, respectivamente.

Referencias

[1] D. A. Cox, *Primes of the form $x^2 + ny^2$: Fermat, class field theory and complex multiplication*. John Wiley & Sons Inc., New York, 1989.

[2] C. F. Gauss, *Disquisitiones arithmeticæ*. Leipzig, 1801.

[3] J. C. Lagarias, *On the Computational complexity of determining the solvability or unsolvability of the equation $X^2 - DY^2 = -1$*. Trans. Amer. Math. Soc. **260** (1980), no. 2, 485–508.

[4] P. Morton, *On Rédei's theory of the Pell equation*. J. Reine Angew. Math. **307/308** (1979), 373–398.

[5] D. Shanks, *Gauss's ternary form reduction and the 2-Sylow subgroup*. Math. Comp. **25** (1971), 837–853.

[6] G. Tornaría, *El 2-subgrupo de Sylow del grupo de clases de formas cuadráticas binarias enteras*. Trabajo Monográfico para la Licenciatura en Matemática, Centro de Matemática, Montevideo, 1999.