Narrow Class Group

Daniel Camilo Rodriguez Ruiz

18 de junio de 2024

Resumen

En la charla del seminario de Teoría de Cuerpos de Clase Explícita se estudia el Narrow class group. Se presentan algunas definiciones y propiedades básicas, se identifica al Narrow class group como un grupo de clases generalizado y usando el teorema de existencia se define el Narrow class field. También se muestran dos ejemplos en donde se exhiben estos conceptos.

Gran parte de esta charla está basada en [5].

Índice

1. Definición y Propiedades **1**

1.1. Definiciones 2

1.2. Finitud del Narrow class group 2

1.3. Relación entre el Narrow class group y el grupo de unidades 4

2. Ejemplo **5**

2.1. Grupo de clases de $K = \mathbb{Q}(\sqrt{3})$ 5

2.2. Narrow class group de $K = \mathbb{Q}(\sqrt{3})$ 6

3. Generalización del cuerpo de clases de Hilbert **6**

3.1. El Narrow class group visto como un grupo de clases generalizado 6

3.2. Narrow class field 7

3.3. Ejemplos de Narrow class field 7

4. Apéndice **10**

4.1. Sobre el discriminante 10

4.2. Enteros algebraicos de un cuerpo bicuadrático 11

1. Definición y Propiedades

En este capítulo se presenta la definición del Narrow class group de un cuerpo de números haciendo énfasis en los cuerpos cuadráticos, además, se presentan algunas propiedades importantes de este grupo.

1.1. Definiciones

Definición 1. Sea K un cuerpo de números tal que $[K : \mathbb{Q}] = n$. Sean $\sigma_1, \ldots, \sigma_s : K \longrightarrow \mathbb{R}$ y $\sigma_{s+1}, \overline{\sigma_{s+1}}, \ldots, \sigma_{s+t}, \overline{\sigma_{s+t}} : K \longrightarrow \mathbb{C}$ los homomorfismos reales y complejos que fijan a $\mathbb{Q}$.

Se dice que $\alpha \in K^*$ es totalmente positivo si $\sigma_i(\alpha) > 0$ para todo $i = 1, \ldots, s$. Si no hay homomorfismos reales, se tiene que todo $\alpha \in K^*$ es totalmente positivo.

Definición 2. Sea K un cuerpo de números. Un ideal fraccionario principal J se dice totalmente positivo su generador es un elemento totalmente positivo, es decir, $J = \alpha\mathcal{O}_K$ donde $\alpha \in K^*$ es totalmente positivo.

Se denota como P_K^+ el conjunto de todos los ideales principales totalmente positivos.

Note que P_K^+ es un subgrupo de los ideales fraccionarios I_K, y de esta forma se introduce el Narrow class group del cuerpo K.

Definición 3. Sea K un cuerpo de números, se define el Narrow class group de K como

$$Cl(K) := I_K / P_K^+.$$

Nota 1.

1. En $Cl^+(K)$ se tiene que $[I] = [J]$ si y solo si $IJ^{-1} = \alpha\mathcal{O}_K$ donde $\alpha \in K^*$ es totalmente positivo.
2. Si $K = \mathbb{Q}(\sqrt{D})$ es un cuerpo cuadrático real, la anterior equivalencia se traduce en que la norma del elemento es positiva, esto es, $[I] = [J]$ si y solo si $IJ^{-1} = \alpha\mathcal{O}_K$ donde $\alpha \in K^*$ y $N(\alpha) > 0$.

Ahora, se va a descartar de nuestro interés el caso de un cuerpo cuadrático imaginario K puesto que el Narrow class group coincide con el grupo de clases usual $Cl(K)$.

Definición 4. Sea K un cuerpo de números, se define K_+ como el conjunto de todos los elementos totalmente positivos de K.

Además, si $U(\mathcal{O}_K)$ es el grupo de unidades de $\mathcal{O}_K$, se define $U(\mathcal{O}_K)_+ := U(\mathcal{O}_K) \cap K_+$ el conjunto de unidades de $\mathcal{O}_K$ que son totalmente positivas.

Nota 2.

1. K_+ es un subgrupo de K^* y $U(\mathcal{O}_K)_+$ es un subgrupo de $U(\mathcal{O}_K)$.
2. Si el cuerpo K solo tiene homomorfismos complejos, entonces $K^* = K_+$.

Proposición 1. Si $K = \mathbb{Q}(\sqrt{D})$ es un cuerpo cuadrático imaginario, entonces $Cl^+(K) = Cl(K)$.

Demostración. Consecuencia directa de la nota 2. □

1.2. Finitud del Narrow class group

En esta sección se muestra que el Narrow class group es finito usando la finitud del grupo de clases usual.

Si K es un cuerpo de números, entonces se tiene el siguiente homomorfismo sobreyectivo

$$\begin{array}{ccc} Cl^+(K) & \xrightarrow{\pi_K} & Cl(K) \\ [I] & \longmapsto & \pi_K([I]) := [I] \end{array}$$

y por lo tanto se tiene que

$$Cl^+(K)/ker(\pi_K) \cong Cl(K). \tag{1}$$

Ahora, considere el siguiente diagrama conmutativo de sucesiones exactas

$$\begin{array}{ccccccccc} 1 & \longrightarrow & P_K^+ & \longrightarrow & I_K & \longrightarrow & Cl^+(K) & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \iota} & & \downarrow{\scriptstyle id} & & \downarrow{\scriptstyle \pi_K} & & \\ 1 & \longrightarrow & P_K & \longrightarrow & I_K & \longrightarrow & Cl(K) & \longrightarrow & 1 \end{array}$$

y por el lema de la serpiente existe una sucesión exacta

$$ker(\iota) \longrightarrow ker(id) \longrightarrow ker(\pi_K) \longrightarrow coker(\iota) \longrightarrow coker(id) \longrightarrow coker(\pi_K)$$

pero id es un isomorfismo, esto implica que $ker(id)$ y $coker(id)$ son grupos triviales, de modo que la sucesión

$$1 \longrightarrow ker(\pi_K) \longrightarrow coker(\iota) \longrightarrow 1$$

es exacta, esto implica que $ker(\pi_K) \cong coker(\iota)$. Así, se concluye que

$$ker(\pi_K) \cong P_K/P_K^+, \tag{2}$$

y por lo tanto

$$Cl(K) \cong Cl^+(K)/\left(P_K/P_K^+\right),$$

y puesto que el grupo de clases $Cl(K)$ es finito, se obtiene que $Cl^+(K)/\left(P_K/P_K^+\right)$ es finito.

Definición 5. Dado $x \in \mathbb{R}$ no nulo, se define el signo de x como $sgn(x) := \frac{x}{|x|} = \pm 1$.

Proposición 2. Sean K un cuerpo de números y $\sigma_1, \ldots, \sigma_s : K \longrightarrow \mathbb{R}$ los homomorfismos reales que fijan a $\mathbb{Q}$. El homomorfismo

$$\begin{array}{rcl} K^* & \xrightarrow{\theta} & \{-1,1\}^s \\ \alpha & \longmapsto & \theta(\alpha) := (sgn(\sigma_1(\alpha)), \ldots, sgn(\sigma_s(\alpha))) \end{array}$$

es sobreyectivo y $ker(\theta) = K_+$.

Demostración. Ver ([5], pág. 67, (2.14)). □

Note que $-1 \in U(\mathcal{O}_K)$ pero $-1 \notin U(\mathcal{O}_K)_+$, de modo que $U(\mathcal{O}_K) \subsetneq U(\mathcal{O}_K)_+$, y esto implica que el cociente $U(\mathcal{O}_K)/U(\mathcal{O}_K)_+$ es no trivial.

Corolario 1. Si K es un cuerpo de números, entonces $K^*/K_+ \cong \{-1,1\}^s$, donde s es el número de homomorfismos de K en $\mathbb{R}$ que fijan a $\mathbb{Q}$.

Por otro lado, a partir del siguiente diagrama conmutativo con filas exactas y columnas inyectivas

$$\begin{array}{ccccccccc} 1 & \longrightarrow & U(\mathcal{O}_K)_+ & \longrightarrow & K_+ & \longrightarrow & P_K^+ & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & U(\mathcal{O}_K) & \longrightarrow & K^* & \longrightarrow & P_K & \longrightarrow & 1 \end{array}$$

se induce la sucesión exacta

$$1 \longrightarrow U(\mathcal{O}_K)/U(\mathcal{O}_K)_+ \longrightarrow K^*/K_+ \longrightarrow P_K/P_K^+ \longrightarrow 1,$$

y por (2) y el corolario 1 se obtiene la sucesión exacta

$$1 \longrightarrow U(\mathcal{O}_K)/U(\mathcal{O}_K)_+ \longrightarrow \{-1,1\}^s \longrightarrow ker(\pi_K) \longrightarrow 1.$$

La exactitud de esta sucesión implica que

$$\{-1,1\}^s / \left(U(\mathcal{O}_K)/U(\mathcal{O}_K)_+\right) \cong ker(\pi_K). \tag{3}$$

Puesto que $\{-1,1\}^s$ es finito, entonces $U(\mathcal{O}_K)/U(\mathcal{O}_K)_+$ es finito y por lo tanto $ker(\pi_K)$ es finito.

De este modo se concluye que $Cl^+(K)$ es un grupo finito.

Ahora, si K es un cuerpo cuadrático real se tiene que $s = 2$, de (3) se obtiene que

$$|ker(\pi_K)| = \frac{4}{|U(\mathcal{O}_K)/U(\mathcal{O}_K)_+|}.$$

Puesto que el cociente $U(\mathcal{O}_K)/U(\mathcal{O}_K)_+$ es no trivial, entonces $|ker(\pi_K)|$ es igual a 1 ó 2.

1.3. Relación entre el Narrow class group y el grupo de unidades

En esta sección el grupo de unidades adquiere gran importancia, pues hay ejemplos de cuerpos cuadráticos que contienen unidades de norma -1 y hay otros que solo contienen unidades de norma 1. La condición anterior caracteriza el tamaño del $ker(\pi_K)$.

Teorema 1. Si K es un cuerpo cuadrático real, entonces $ker(\pi_K)$ tiene orden 1 ó 2 según si la norma de la unidad fundamental de $\mathcal{O}_K$ es -1 ó 1.

Demostración. Si $|ker(\pi_K)| = 1$, entonces $|U(\mathcal{O}_K)/U(\mathcal{O}_K)_+| = 4$, de modo que el homomorfismo $U(\mathcal{O}_K)/U(\mathcal{O}_K)_+ \longrightarrow \{-1,1\}^2$ resulta un isomorfismo, así, para cada $(\delta_1, \delta_2) \in \{-1,1\}$ existe $\eta \in U(\mathcal{O}_K)$ tal que $sgn(\sigma_1(\eta)) = \delta_1$ y $sgn(\sigma_2(\eta)) = \delta_2$, en particular $sgn(\sigma_1(\eta)) = 1$ y $sgn(\sigma_2(\eta)) = -1$. Esto implica que $N(\eta) = \sigma_1(\eta)\sigma_2(\eta) = -1$, y por lo tanto $\mathcal{O}_K$ contiene unidades de norma -1, de modo que la unidad fundamental de $\mathcal{O}_K$ tiene norma -1.

Recíprocamente, si η es la unidad fundamental de $\mathcal{O}_K$ tal que $N(\eta) = -1$, entonces $\sigma_1(\eta)\sigma_2(\eta) = -1$, de manera que $sgn(\sigma_1(\eta)) \neq sgn(\sigma_2(\eta))$. De modo que $1, -1, \eta, -\eta$ son unidades distintas de $\mathcal{O}_K$ con imágenes distintas en $\{-1,1\}^2$, y por lo tanto serán distintas en el cociente $U(\mathcal{O}_K)/U(\mathcal{O}_K)_+$, de modo que $|U(\mathcal{O}_K)/U(\mathcal{O}_K)_+| = 4$, esto implica que $|ker(\pi_K)| = 1$. □

Corolario 2. Si K es un cuerpo cuadrático real, entonces $Cl(K) \cong Cl^+(K)$ si y solo si $\mathcal{O}_K$ contiene una unidad de norma -1.

Demostración. Supóngase que $Cl(K) \cong Cl^+(K)$, usando (1) se obtiene que $ker(\pi_K)$ es el grupo trivial, de modo que $|ker(\pi_K)| = 1$, y por lo tanto la norma de la unidad fundamental de $\mathcal{O}_K$ es -1.

Recíprocamente, si $\mathcal{O}_K$ contiene una unidad de norma -1, entonces la unidad fundamental de $\mathcal{O}_K$ tiene norma -1, y así $|ker(\pi_K)| = 1$. Usando (1) se obtiene que $|Cl(K)| = |Cl^+(K)|$, y por lo tanto $Cl(K) \cong Cl^+(K)$. □

2. Ejemplo

En este capítulo se presenta un ejemplo de un cuerpo cuadrático real al que se le calcula el grupo de clases y el Narrow class group.

2.1. Grupo de clases de $K = \mathbb{Q}(\sqrt{3})$

Para realizar el cálculo del grupo de clases se hará uso del siguiente lema.

Lema 1. Sea K un cuerpo de números, y sean $\sigma_1, \ldots, \sigma_n : K \longrightarrow \mathbb{C}$ los homomorfismos que fijan a $\mathbb{Q}$. Entonces cada clase en $Cl(K)$ contiene un ideal J de $\mathcal{O}_K$ tal que $\| J \| \leq \lambda$, donde λ está dado por

$$\lambda := \prod_{i=1}^{n} \left(\sum_{j=1}^{n} |\sigma_i(\alpha_j)| \right) \tag{4}$$

donde $\{\alpha_1, \ldots, \alpha_n\}$ es una $\mathbb{Z}-$base de $\mathcal{O}_K$.

Demostración. Ver ([9], pág 131, Corolario 1). □

Este lema proporciona una cota superior para la norma de los ideales, es importante aclarar que dicha cota no es muy fina, pero este ejemplo se trabaja haciendo uso de ella.

Para $K = \mathbb{Q}(\sqrt{3})$ se tiene que $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\sqrt{3}$. Así, se tiene que $\left\{1, \sqrt{3}\right\}$ es una $\mathbb{Z}-$base de $\mathbb{O}_K$, y $\sigma_1, \sigma_2 : K \longrightarrow \mathbb{R}$ son los homomorfismos identidad y conjugación respectivamente.

De modo que, en este caso se tiene que

$$\lambda = \Big(|\sigma_1(1)| + |\sigma_1(\sqrt{3})|\Big)\Big(|\sigma_2(1)| + |\sigma_2(\sqrt{3})|\Big) = (1+\sqrt{3})^2 = 4 + 2\sqrt{3},$$

luego, $7 < \lambda < 8$. El lema anterior implica que cada clase $[I] \in Cl(K)$ contiene un ideal J de $\mathcal{O}_K$ con $\| J \| \leq 7$.

A ver los posibles ideales J de $\mathcal{O}_K$ con esta condición. Para ver esto se debe tener que los posibles divisores primos de J están entre los ideales primos de $\mathcal{O}_K$ que contienen a $2, 3, 5$ y 7, entonces se deben estudiar los ideales $2\mathcal{O}_K, 3\mathcal{O}_K, 5\mathcal{O}_K$ y $7\mathcal{O}_K$.

(a) $2\mathcal{O}_K = \mathfrak{p}^2$, donde $\mathfrak{p} = (1+\sqrt{3})\mathcal{O}_K$:

$$\begin{aligned}(2\mathcal{O}_K + (1+\sqrt{3})\mathcal{O}_K)(2\mathcal{O}_K + (1+\sqrt{3})\mathcal{O}_K) &= 2\mathcal{O}_K(2\mathcal{O}_K + (1+\sqrt{3})\mathcal{O}_K + (2+\sqrt{3})\mathcal{O}_K) \\ &= 2\mathcal{O}_K.\end{aligned}$$

Note que $\mathfrak{p} = 2\mathcal{O}_K + (1+\sqrt{3})\mathcal{O}_K$, esto implica la igualdad. Además,

$$\| \mathfrak{p} \|^2 = \| \mathfrak{p}^2 \| = \| 2\mathcal{O}_K \| = |N(2)| = 4,$$

y entonces $\| \mathfrak{p} \| = 2$, de modo que $\mathfrak{p}$ es primo.

(b) $3\mathcal{O}_K = \mathfrak{p}^2$, donde $\mathfrak{p} = \sqrt{3}\mathcal{O}_K$:

$$\begin{aligned}(3\mathcal{O}_K + \sqrt{3}\mathcal{O}_K)(3\mathcal{O}_K + \sqrt{3}\mathcal{O}_K) &= 3\mathcal{O}_K(3\mathcal{O}_K + \sqrt{3}\mathcal{O}_K + \mathcal{O}_K) \\ &= 3\mathcal{O}_K.\end{aligned}$$

Note que $\mathfrak{p} = 3\mathcal{O}_K + \sqrt{3}\mathcal{O}_K$, esto implica la igualdad. Además,

$$\| \mathfrak{p} \|^2 = \| \mathfrak{p}^2 \| = \| 3\mathcal{O}_K \| = |N(3)| = 9,$$

y entonces $\| \mathfrak{p} \| = 3$, de modo que $\mathfrak{p}$ es primo.

(c) $5\mathcal{O}_K$ es un ideal primo de $\mathcal{O}_K$ pues 3 no es un residuo cuadrático $(mod\, 5)$.

(d) $7\mathcal{O}_K$ es un ideal primo de $\mathcal{O}_K$ pues 3 no es un residuo cuadrático $(mod\, 7)$.

Lo anterior implica que los únicos ideales J de $\mathcal{O}_K$ con $\| J \| \leq 7$ son $\mathcal{O}_K, 2\mathcal{O}_K, (1+\sqrt{3})\mathcal{O}_K, \sqrt{3}\mathcal{O}_K$, los cuales son todos principales. De manera que cada clase $[I] \in Cl(K)$ contiene un ideal principal, y por lo tanto $[I]$ es la clase del neutro en $Cl(K)$, de modo que $Cl(K)$ es trivial.

2.2. Narrow class group de $K = \mathbb{Q}(\sqrt{3})$

La unidad fundamental de $\mathcal{O}_K$ es $\eta = 2 + \sqrt{3}$, y además $N(\eta) = 1$. En efecto, primero note que $\eta = 2 + \sqrt{3}$ es una unidad de $\mathcal{O}_K$, pues

$$(2 + \sqrt{3})(2 - \sqrt{3}) = 1,$$

ahora se debe probar que 2 es minimal, es decir, cualquier otra unidad $\theta = c + d\sqrt{3}$ de $\mathcal{O}_K$ con $\theta > 1$ debe cumplir que $2 < c$.

Así, si $b \neq 0$, se tiene

$$|N(1 + b\sqrt{3})| = |3b^2 - 1| \geq 2,$$

por lo tanto, $\eta = 2 + \sqrt{3}$ es la unidad fundamental de $\mathcal{O}_K$.

Nota 3. La unidad fundamental también se puede calcular usando fracciones continuas, pero aquí no se va a realizar ese cálculo.

El teorema 1 implica que $|ker(\pi_K)| = 2$, y de (1) se obtiene que $|Cl^+(K)| = 2$. Por lo tanto

$$Cl^+(K) \cong \mathbb{Z}/2\mathbb{Z}.$$

3. Generalización del cuerpo de clases de Hilbert

En este capítulo se presenta una generalización del cuerpo de clases de Hilbert de un cuerpo de números, esta se obtiene del teorema de existencia aplicado a cierto módulo.

3.1. El Narrow class group visto como un grupo de clases generalizado

Sea K un cuerpo de números, y sean $\sigma_1, \ldots, \sigma_s : K \longrightarrow \mathbb{R}$ los s homomorfismos reales que fijan a $\mathbb{Q}$. Considere el módulo $\mathfrak{m} := \mathfrak{m}_0\mathfrak{m}_\infty$ donde $\mathfrak{m}_0 := 1$ y $\mathfrak{m}_\infty := \prod_{i=1}^{s} \sigma_i$.

Puesto que no hay primos finitos en $\mathfrak{m}$, entonces $I_K(\mathfrak{m}) = I_K$. Además, por el mismo argumento se tiene que $P_{K,1}(\mathfrak{m}) = P_K^+$.

Luego, tomando $H := P_K^+$ se obtiene que $P_{K,1}(\mathfrak{m}) \subseteq H \subseteq I_K(\mathfrak{m})$, es decir $P_K^+ \subseteq P_K^+ \subseteq I_K$, y por lo tanto P_K^+ es un subgrupo de congruencia para $\mathfrak{m}$, de lo que se concluye que $Cl^+(K) = I_K/P_K^+$ es un grupo de clases de ideales generalizado.

3.2. Narrow class field

Al aplicar el teorema de existencia con el módulo $\mathfrak{m} = 1$ se obtiene la existencia del cuerpo de clases de Hilbert, de modo que si se aplica el teorema de existencia a módulos no triviales se obtiene una generalización del cuerpo de clases de Hilbert llamado *ray class field*. En particular, cuando se aplica con cierto módulo especial se obtiene el Narrow class field.

Sea K un cuerpo de números, y sean $\sigma_1, \ldots, \sigma_s : K \longrightarrow \mathbb{R}$ los s homomorfismos que fijan a $\mathbb{Q}$.

Considere el módulo $\mathfrak{m} := \mathfrak{m}_0\mathfrak{m}_\infty$ donde $\mathfrak{m}_0 := 1$ y $\mathfrak{m}_\infty := \prod_{i=1}^{s} \sigma_i$. Si $H := P_{K,1}(\mathfrak{m}) = P_K^+$ el subgrupo de congruencia para $\mathfrak{m}$, el teorema de existencia implica que existe una única extensión abeliana $K_\mathfrak{m}$ de K tal que todos los primos de K que ramifican en $K_\mathfrak{m}$ dividen a $\mathfrak{m}$. Además, si

$$\Phi_{K_\mathfrak{m}/K,\mathfrak{m}} : I_K(\mathfrak{m}) \longrightarrow Gal(K_\mathfrak{m}/K)$$

es el homomorfismo de Artin, entonces $H = ker\left(\Phi_{K_\mathfrak{m}/K,\mathfrak{m}}\right)$, y por teorema de Artin se obtiene que

$$I_K/P_K^+ \cong Gal(K_\mathfrak{m}/K),$$

es decir,

$$Cl^+(K) \cong Gal(K_\mathfrak{m}/K).$$

El cuerpo $K_\mathfrak{m}$ es llamado el Narrow class field.

3.3. Ejemplos de Narrow class field

En esta sección se presentan dos ejemplos en donde se evidencia la diferencia entre el cuerpo de clases de Hilbert y el Narrow class field.

Ejemplo 1. Sea $K = \mathbb{Q}(\sqrt{3})$, en el capítulo anterior se calculó que $Cl(K)$ es trivial. Por otro lado, aplicando el teorema de existencia con el módulo $\mathfrak{m} = 1$ se obtiene la existencia del cuerpo de clases de Hilbert L de K. El teorema de Artin implica que

$$I_K/P_K \cong Gal(L/K),$$

es decir,

$$Cl(K) \cong Gal(L/K.)$$

De modo que $Gal(L/K)$ es el grupo trivial y por tanto $[L : K] = 1$, esto es, $L = K$. Así, el cuerpo de clases de Hilbert de $K = \mathbb{Q}(\sqrt{3})$ es $L = K$.

Por otro lado, también se calculó que $Cl^+(K) \cong \mathbb{Z}/2\mathbb{Z}$.

Si $K_\mathfrak{m}$ es el Narrow class field de K, entonces $\mathbb{Z}/2\mathbb{Z} \cong Gal(K_\mathfrak{m}/K)$, y por lo tanto $[K_\mathfrak{m} : K] = 2$.

Se afirma que $K_\mathfrak{m} = \mathbb{Q}(\sqrt{3}, \sqrt{-1})$. Para ver esto, si se denota $N := \mathbb{Q}(\sqrt{3}, \sqrt{-1})$, entonces N debe ser una extensión cuadrática de K, de Galois abeliana y tal que todos los primos de K que ramifican en N dividen a $\mathfrak{m}$.

Se tiene que $p(x) = x^2 + 1 \in K[x]$ es el polinomio mínimo de $\sqrt{-1}$ sobre K, esto implica que $[N : K] = 2$. Además, se tiene que N es una extensión normal y separable de K, entonces N es una extensión de Galois abeliana de K.

Puesto que $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$ con $\mathfrak{m}_0 = 1$ y $\mathfrak{m}_\infty = \sigma_1\sigma_2$, donde σ_1, σ_2 son los homomorfismos de K en $\mathbb{R}$ que fijan a $\mathbb{Q}$, entonces σ_1 y σ_2 se extienden exactamente a dos homomorfismos de N en $\mathbb{C}$ respectivamente, así, σ_1 y σ_2 ramifican en N.

Falta ver que ningún primo finito de K ramifica en N. Para ver esto se emplea el corolario 3 y el teorema 2.

Ya que $\{1, \sqrt{3}\}$ es una $\mathbb{Z}-$base de $\mathcal{O}_K$, y $\sigma_1(a + b\sqrt{3}) = a + b\sqrt{3}$ y $\sigma_2(a + b\sqrt{3}) = a - b\sqrt{3}$, donde $a, b \in \mathbb{Q}$, entonces

$$\begin{aligned} d_{K/\mathbb{Q}} &= \begin{vmatrix} \sigma_1(1) & \sigma_1(\sqrt{3}) \\ \sigma_2(1) & \sigma_2(\sqrt{3}) \end{vmatrix}^2 \\ &= \begin{vmatrix} 1 & \sqrt{3} \\ 1 & -\sqrt{3} \end{vmatrix}^2 \\ &= 12. \end{aligned}$$

Además, $\left\{1, \sqrt{3}, \frac{\sqrt{3}+i}{2}, \frac{1+\sqrt{3}i}{2}\right\}$ es una $\mathbb{Z}-$base de $\mathcal{O}_N$, y

$$\sigma_1(a + bi) = a + bi, \sigma_2(a + bi) = a - bi, \sigma_3(a + bi) = \overline{a} + \overline{b}i, \sigma_4(a + bi) = \overline{a} - \overline{b}i,$$

donde $a, b \in K$ y para cada $a = p + \sqrt{3}q \in K$ se denota $\overline{a} = p - \sqrt{3}q$, entonces

$$\begin{aligned} d_{N/\mathbb{Q}} &= \begin{vmatrix} \sigma_1(1) & \sigma_1(\sqrt{3}) & \sigma_1\left(\frac{\sqrt{3}+i}{2}\right) & \sigma_1\left(\frac{1+\sqrt{3}i}{2}\right) \\ \sigma_2(1) & \sigma_2(\sqrt{3}) & \sigma_2\left(\frac{\sqrt{3}+i}{2}\right) & \sigma_2\left(\frac{1+\sqrt{3}i}{2}\right) \\ \sigma_3(1) & \sigma_3(\sqrt{3}) & \sigma_3\left(\frac{\sqrt{3}+i}{2}\right) & \sigma_3\left(\frac{1+\sqrt{3}i}{2}\right) \\ \sigma_4(1) & \sigma_4(\sqrt{3}) & \sigma_4\left(\frac{\sqrt{3}+i}{2}\right) & \sigma_4\left(\frac{1+\sqrt{3}i}{2}\right) \end{vmatrix}^2 \\ &= \begin{vmatrix} 1 & \sqrt{3} & \frac{\sqrt{3}+i}{2} & \frac{1+\sqrt{3}i}{2} \\ 1 & \sqrt{3} & \frac{\sqrt{3}-i}{2} & \frac{1-\sqrt{3}i}{2} \\ 1 & -\sqrt{3} & \frac{-\sqrt{3}+i}{2} & \frac{1-\sqrt{3}i}{2} \\ 1 & -\sqrt{3} & \frac{-\sqrt{3}-i}{2} & \frac{1+\sqrt{3}i}{2} \end{vmatrix}^2 \\ &= 12^2. \end{aligned}$$

Luego, el corolario 3 implica que

$$12^2 = 12^2 N_{K/\mathbb{Q}}(d_{N/K}),$$

por lo tanto $N_{K/\mathbb{Q}}(d_{N/K}) = 1$, esto implica que $d_{N/K}$ es una unidad de $\mathcal{O}_K$, y por lo tanto $d_{N/K}\mathcal{O}_K = \mathcal{O}_K$. Esto implica que N es una extensión no ramificada de K, y por la unicidad del teorema de existencia se concluye que $N = K_{\mathfrak{m}}$.

Ejemplo 2. Sea $\mathcal{O}$ un orden en un cuerpo cuadrático K con discriminante $D = 21$, entonces $\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K$ donde $f := [\mathcal{O}_K : \mathcal{O}]$ es el conductor.

Puesto que el discriminante satisface que $D = f^2 d_K$ donde d_K es el discriminante de K, entonces $21 = f^2 d_K$, de manera que $f^2 = 1$ y $d_K = 21$.

Luego, como $K = Frac(\mathcal{O}) = Frac(\mathcal{O}_K)$, se obtiene que $K = \mathbb{Q}(\sqrt{21})$.

Para calcular el grupo de clases de K se hará uso del siguiente lema.

Lema 2. Sea K un cuerpo de números tal que $n = [K : \mathbb{Q}]$, y supóngase que K tiene r homomorfismos reales y $2s$ homomorfismos complejos que fijan a $\mathbb{Q}$. Entonces cada clase en $Cl(K)$ contiene un ideal J de $\mathcal{O}_K$ tal que $\| J \| \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{|d_K|}$.

Demostración. Ver ([9], pág 136, Corolario 2). □

La cota anterior es llamada *constante de Minkowski.*

Para $K = \mathbb{Q}(\sqrt{21})$ se tiene que $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\frac{1+\sqrt{21}}{2}$. El lema anterior implica que la cota de Minkowski en este caso es $\frac{1}{2}\sqrt{21} = 2{,}29$, de donde cada clase $[I] \in Cl(K)$ contiene un ideal J de $\mathcal{O}_K$ con $\| J \| \leq 2$. Así, los divisores de J deben estar entre los ideales primos de $\mathcal{O}_K$ que contienen a 2, entonces se debe estudiar el ideal $2\mathcal{O}_K$.

Puesto que $21 \equiv 5 \, (mod\, 8)$, entonces $2\mathcal{O}_K$ es un ideal primo de $\mathcal{O}_K$. Esto implica que el único ideal J de $\mathcal{O}_K$ con $\| J \| \leq 2$ es $\mathcal{O}_K$. Así, cada clase $[I] \in Cl(K)$ contiene un ideal principal, por lo tanto $Cl(K)$ es trivial.

Aplicando el teorema de existencia con el módulo $\mathfrak{m} = 1$ se obtiene la existencia de L que es el cuerpo de clases de Hilbert de K, y por teorema de Artin se cumple que

$$I_K/P_K \cong Gal(L/K),$$

es decir, $Cl(K) \cong Gal(L/K)$. Esto implica que $Gal(L/K)$ es el grupo trivial, y por tanto $L = K$. Así, el cuerpo de clases de Hilbert de K es $L = K$.

Por otro lado, la unidad fundamental de $\mathcal{O}_K$ es $\eta = \frac{5+\sqrt{21}}{2}$, y además $N(\eta) = 1$. En efecto, primero note que η es una unidad de $\mathcal{O}_K$, pues

$$\left(\frac{5+\sqrt{21}}{2}\right)\left(\frac{5-\sqrt{21}}{2}\right) = 1,$$

y además, η es la unidad más pequeña que es mayor que 1. Luego, el teorema 1 implica que $|ker(\pi_K)| = 2$, y de (1) se obtiene que $|Cl^+(K)| = 2$. Por lo tanto

$$Cl^+(K) \cong \mathbb{Z}/2\mathbb{Z}.$$

Por otro lado, para $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$, donde $\mathfrak{m}_0 = 1$ y $\mathfrak{m}_\infty = \sigma_1\sigma_2$, con $\sigma_1(a + b\sqrt{21}) = a + b\sqrt{21}$ y $\sigma_2(a + b\sqrt{21}) = a - b\sqrt{21}$ para todo $a, b \in \mathbb{Q}$, se tiene la existencia del Narrow class field $K_\mathfrak{m}$ de K, y así $Cl^+(K) \cong Gal(K_\mathfrak{m}/K)$, es decir, $\mathbb{Z}/2\mathbb{Z} \cong Gal(K_\mathfrak{m}/K)$, de donde $[K_\mathfrak{m} : K] = 2$.

Sea afirma que $K_\mathfrak{m} = \mathbb{Q}(\sqrt{-3}, \sqrt{-7})$. En efecto, denote $N := \mathbb{Q}(\sqrt{-3}, \sqrt{-7})$. Luego, $N = \mathbb{Q}(\sqrt{-3} + \sqrt{-7})$ y $p(x) = x^4 + 20x^2 + 16 \in \mathbb{Z}[x]$ es el polinomio mínimo de $\sqrt{-3} + \sqrt{-7}$ sobre $\mathbb{Q}$, esto implica que $[\mathbb{Q}(\sqrt{-3} + \sqrt{-7}) : \mathbb{Q}] = 4$. Puesto que

$$[\mathbb{Q}(\sqrt{-3} + \sqrt{-7}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{-3} + \sqrt{-7}) : \mathbb{Q}(\sqrt{21})][\mathbb{Q}(\sqrt{21}) : \mathbb{Q}],$$

y por tanto, $[\mathbb{Q}(\sqrt{-3} + \sqrt{-7}) : \mathbb{Q}(\sqrt{21})] = 2$, es decir, $[N : K] = 2$. Esto implica que N es una extensión de Galois abeliana de K.

Por otro lado, puesto que N es un cuerpo imaginario y los dos homomorfismos σ_1, σ_2 de K son homomorfismos reales, entonces cada uno se extiende a dos homomorfismos de N a $\mathbb{C}$, esto implica que σ_1 y σ_2 ramifican en N.

Falta ver que ningún primo finito de K ramifica en N. Para ver esto se emplea el corolario 3 y el teorema 2.

Ya que $\left\{1, \frac{1+\sqrt{21}}{2}\right\}$ es una $\mathbb{Z}-$base de $\mathcal{O}_K$, y $\sigma_1(a+b\sqrt{21}) = a+b\sqrt{21}$ y $\sigma_2(a+b\sqrt{21}) = a-b\sqrt{21}$, donde $a, b \in \mathbb{Q}$, entonces

$$\begin{aligned} d_{K/\mathbb{Q}} &= \begin{vmatrix} \sigma_1(1) & \sigma_1\left(\frac{1+\sqrt{21}}{2}\right) \\ \sigma_2(1) & \sigma_2\left(\frac{1+\sqrt{21}}{2}\right) \end{vmatrix}^2 \\ &= \begin{vmatrix} 1 & \frac{1+\sqrt{21}}{2} \\ 1 & \frac{1-\sqrt{21}}{2} \end{vmatrix}^2 \\ &= 21. \end{aligned}$$

Además, $\left\{1, \frac{1+\sqrt{-3}}{2}, \frac{1+\sqrt{-7}}{2}, \frac{1+\sqrt{-3}+\sqrt{-7}+\sqrt{-3}\sqrt{-7}}{4}\right\}$ es una $\mathbb{Z}-$base de $\mathcal{O}_N$, y

$\sigma_1(a+b\sqrt{-7}) = a+b\sqrt{-7}, \sigma_2(a+b\sqrt{-7}) = a-b\sqrt{-7}, \sigma_3(a+b\sqrt{-7}) = \overline{a}+\overline{b}\sqrt{-7}, \sigma_4(a+b\sqrt{-7}) = \overline{a}-\overline{b}\sqrt{-7}$,

donde $a, b \in \mathbb{Q}(\sqrt{-3})$ y para cada $a = p+\sqrt{-3}q \in \mathbb{Q}(\sqrt{-3})$ se denota $\overline{a} = p-\sqrt{-3}q$, entonces

$$\begin{aligned} d_{N/\mathbb{Q}} &= \begin{vmatrix} \sigma_1(1) & \sigma_1\left(\frac{1+\sqrt{-3}}{2}\right) & \sigma_1\left(\frac{1+\sqrt{-7}}{2}\right) & \sigma_1\left(\frac{1+\sqrt{-3}+\sqrt{-7}+\sqrt{-3}\sqrt{-7}}{4}\right) \\ \sigma_2(1) & \sigma_2\left(\frac{1+\sqrt{-3}}{2}\right) & \sigma_2\left(\frac{1+\sqrt{-7}}{2}\right) & \sigma_2\left(\frac{1+\sqrt{-3}+\sqrt{-7}+\sqrt{-3}\sqrt{-7}}{4}\right) \\ \sigma_3(1) & \sigma_3\left(\frac{1+\sqrt{-3}}{2}\right) & \sigma_3\left(\frac{1+\sqrt{-7}}{2}\right) & \sigma_3\left(\frac{1+\sqrt{-3}+\sqrt{-7}+\sqrt{-3}\sqrt{-7}}{4}\right) \\ \sigma_4(1) & \sigma_4\left(\frac{1+\sqrt{-3}}{2}\right) & \sigma_4\left(\frac{1+\sqrt{-7}}{2}\right) & \sigma_4\left(\frac{1+\sqrt{-3}+\sqrt{-7}+\sqrt{-3}\sqrt{-7}}{4}\right) \end{vmatrix}^2 \\ &= \begin{vmatrix} 1 & \frac{1+\sqrt{-3}}{2} & \frac{1+\sqrt{-7}}{2} & \frac{1+\sqrt{-3}+\sqrt{-7}+\sqrt{-3}\sqrt{-7}}{4} \\ 1 & \frac{1+\sqrt{-3}}{2} & \frac{1-\sqrt{-7}}{2} & \frac{1+\sqrt{-3}-\sqrt{-7}-\sqrt{-3}\sqrt{-7}}{4} \\ 1 & \frac{1-\sqrt{-3}}{2} & \frac{1+\sqrt{-7}}{2} & \frac{1-\sqrt{-3}+\sqrt{-7}-\sqrt{-3}\sqrt{-7}}{4} \\ 1 & \frac{1-\sqrt{-3}}{2} & \frac{1-\sqrt{-7}}{2} & \frac{1-\sqrt{-3}-\sqrt{-7}+\sqrt{-3}\sqrt{-7}}{4} \end{vmatrix}^2 \\ &= 21^2. \end{aligned}$$

Luego, el corolario 3 implica que

$$21^2 = 21^2 N_{K/\mathbb{Q}}(d_{N/K}),$$

por lo tanto $N_{K/\mathbb{Q}}(d_{N/K}) = 1$, esto implica que $d_{N/K}$ es una unidad de $\mathcal{O}_K$, y por lo tanto $d_{N/K}\mathcal{O}_K = \mathcal{O}_K$. Esto implica que N es una extensión no ramificada de K, y por la unicidad del teorema de existencia se concluye que $N = K_{\mathfrak{m}}$.

4. Apéndice

4.1. Sobre el discriminante

Se presentan algunos resultados sobre el discriminante de un cuerpo de números.

Proposición 3. Sean K, L cuerpos de números tales que $K \subseteq L$. Si $d_{L/K}$ denota al discriminante de L con respecto a K, y $\mathfrak{D}_{L/K}$ denota al diferente de L con respecto a K. Entonces se tiene que

$$d_{L/K} = N_{L/K}(\mathfrak{D}_{L/K}).$$

Demostración. Ver ([11], pág 201, Teorema 2.9). □

Corolario 3. ([11], pág. 202, Corolario 2.10) Sean K, L, M cuerpos de números tales que $K \subseteq L \subseteq M$. Si $d_{M/K}$ denota al discriminante de M con respecto a K y $d_{L/K}$ denota al discriminante de L con respecto a K. Entonces

$$d_{M/K} = d_{L/K}^{[M:L]} N_{L/K}(d_{M/L}).$$

Demostración. Puesto que $\mathfrak{D}_{M/K} = \mathfrak{D}_{M/L}\mathfrak{D}_{L/K}$ y $N_{M/K} = N_{L/K} \circ N_{M/L}$, entonces

$$\begin{aligned} d_{M/K} &= N_{M/K}(\mathfrak{D}_{M/K}) \qquad \text{(por proposición 3)}, \\ &= N_{M/K}(\mathfrak{D}_{M/L}\mathfrak{D}_{L/K}) \\ &= N_{M/K}(\mathfrak{D}_{M/L})N_{M/K}(\mathfrak{D}_{L/K}) \\ &= N_{L/K}(N_{M/L}(\mathfrak{D}_{M/L}))N_{L/K}(N_{M/L}(\mathfrak{D}_{L/K})) \\ &= N_{L/K}(d_{M/L})N_{L/K}(\mathfrak{D}_{L/K}^{[M:L]}) \\ &= N_{L/K}(d_{M/L})d_{L/K}^{[M:L]}. \end{aligned}$$

□

Corolario 4. ([11], pág. 202, Corolario 2.12) Sea L/K una extensión de cuerpos de números. Entonces, un ideal primo $\mathfrak{p}$ de K es ramificado en L si y solo si $\mathfrak{p}$ divide al discriminante $d_{L/K}$.

En particular, puesto que ningún ideal primo divide al anillo, se tiene que L es una extensión no ramificada de K si $d_{L/K}\mathcal{O}_K = \mathcal{O}_K$.

4.2. Enteros algebraicos de un cuerpo bicuadrático

Se presenta el teorema que exhibe una $\mathbb{Z}-$base de un cuerpo bicuadrático.

Teorema 2. Dado un cuerpo bicuadrático de la forma $K := \mathbb{Q}(\sqrt{m}, \sqrt{n})$ donde $m, n \in \mathbb{Z}$ distintos y libres de cuadrados, y sea $l = mcd(n, m)$, de modo que $m = lm_1$ y $n = ln_1$ para algunos $m_1, n_1 \in \mathbb{Z}$. Entonces.

(1). Si $(m, n) \equiv (1, 1), (m_1, n_1) \equiv (1, 1)\,(mod\,4)$, entonces $\left\{1, \frac{1+\sqrt{m}}{2}, \frac{1+\sqrt{n}}{2}, \frac{1+\sqrt{m}+\sqrt{n}+\sqrt{m_1 n_1}}{4}\right\}$ es una $\mathbb{Z}-$base para $\mathcal{O}_K$.

(2). Si $(m, n) \equiv (1, 1), (m_1, n_1) \equiv (3, 3)\,(mod\,4)$, entonces $\left\{1, \frac{1+\sqrt{m}}{2}, \frac{1+\sqrt{n}}{2}, \frac{1-\sqrt{m}+\sqrt{n}+\sqrt{m_1 n_1}}{4}\right\}$ es una $\mathbb{Z}-$base para $\mathcal{O}_K$.

(3). Si $(m, n) \equiv (1, 2)\,(mod\,4)$, entonces $\left\{1, \frac{1+\sqrt{m}}{2}, \sqrt{n}, \frac{\sqrt{n}+\sqrt{m_1 n_1}}{2}\right\}$ es una $\mathbb{Z}-$base para $\mathcal{O}_K$.

(4). Si $(m, n) \equiv (2, 3)\,(mod\,4)$, entonces $\left\{1, \sqrt{m}, \sqrt{n}, \frac{\sqrt{m}\sqrt{m_1 n_1}}{2}\right\}$ es una $\mathbb{Z}-$base para $\mathcal{O}_K$.

(5). Si $(m, n) \equiv (3, 3)\,(mod\,4)$, entonces $\left\{1, \sqrt{m}, \frac{\sqrt{m}+\sqrt{n}}{2}, \frac{1+\sqrt{m_1 n_1}}{2}\right\}$ es una $\mathbb{Z}-$base para $\mathcal{O}_K$.

Demostración. Ver ([12], pág 524, Teorema 2). □

Referencias

[1] S. Alaca and K. S. Williams, *Introductory algebraic number theory*, Cambridge University Press, Cambridge, 2004.

[2] N. Childress, *Class field theory*, Universitext, Springer, New York, 2009.

[3] D. A. Cox, *Primes of the form $x^2 + ny^2$*, A Wiley-Interscience Publication, John Wiley & Sons, Inc., New York, 1989.

[4] J. Esmonde and M. Ram Murty, *Problems in algebraic number theory*, Graduate Texts in Mathematics, 190, Springer-Verlag, New York, 1999.

[5] A. Fröhlich and M. J. Taylor, *Algebraic number theory*, Cambridge Studies in Advanced Mathematics, 27, Cambridge University Press, Cambridge, 1993.

[6] K. Ireland and M. Rosen, *A classical introduction to modern number theory*, second edition, Graduate Texts in Mathematics, 84, Springer-Verlag, New York, 1990.

[7] G. J. Janusz, *Algebraic number fields*, second edition, Graduate Studies in Mathematics, 7, American Mathematical Society, Providence, RI, 1996.

[8] S. Lang, *Algebraic number theory*, second edition, Graduate Texts in Mathematics, 110, Springer-Verlag, New York, 1994.

[9] D. A. Marcus, *Number fields*, Springer-Verlag, Berlin, Heidelberg, New York, 1977.

[10] J. S. Milne, *Algebraic Number Theory*, v3.08, https://www.jmilne.org/math/CourseNotes/ANT.pdf, 2020.

[11] J. Neukirch, *Algebraic number theory*, Springer-Verlag, Berlin Heidelberg, 1999.

[12] K. Williams, *Integers of biquadratic fields*, Canad. Math. Bull. 13 (1970).