Reto 6

Carlos Quesada

1. Solución

El grupo de clase de $\mathbb{Q}(\sqrt{-74})$ es:

$$\mathcal{H}_{\mathbb{Q}(\sqrt{-74})} = \{[\mathcal{O}_K], [\mathfrak{p}_2], [\mathfrak{p}_3], [\mathfrak{q}_3], [\mathfrak{p}_5], [\mathfrak{q}_5], [\mathfrak{p}_2\mathfrak{p}_3], [\mathfrak{p}_2\mathfrak{q}_3], [\mathfrak{p}_2\mathfrak{p}_5], [\mathfrak{p}_2\mathfrak{q}_5]\},$$

isomorfo a C_{10} y cada una de las clases de los siguientes ideales generan el grupo:

$$\mathfrak{p}_5$$

$$\mathfrak{q}_5$$

$$\mathfrak{p}_2\mathfrak{p}_3$$

$$\mathfrak{p}_2\mathfrak{q}_3$$

2. Demostración

Para demostrarlo hay que seguir los pasos habituales. En primer lugar calculamos la cota de Minkowski. Para ello necesitamos saber n, t y $\Delta_{\mathbb{Q}(\sqrt{-74})}$ donde:

$$n = [\mathbb{Q}(\sqrt{-74}) : \mathbb{Q}] = 2$$

$$t = \text{la mitad de las raíces complejas} = 1$$

$$\Delta_{\mathbb{Q}(\sqrt{-74})} \overset{74\not\equiv 1(mod 4)}{\Longrightarrow} = 4 \cdot (-74) = -296$$

Con lo cual:

$$\mathcal{M}_{\mathbb{Q}(\sqrt{-74})} = (\frac{4}{\pi})^1 \frac{2}{2^2} \sqrt{|-296|} \simeq 10,95$$

Por lo tanto $\forall I \subset \mathcal{O}_K$ ideal, I es equivalente a otro ideal J de norma menor que $\mathcal{M}_{\mathbb{Q}(\sqrt{-74})}$. Como los ideales con norma un número no primo se pueden factorizar en otros con norma prima, necesitamos calcular los ideales con norma un número menor que 11 y primo, para caracterizar todas las clase de los posibles ideales de $\mathcal{O}_K$. Antes de nada calculemos $\mathcal{O}_K$. Como $74 \not\equiv 1(mod\, 4) \Rightarrow \mathcal{O}_K = \mathbb{Z}[\sqrt{-74}]$. Por tanto, $f_\theta = x^2 + 74$, algo que también necesitaremos más adelante.

Norma 1

$N_K(I) = 1 \Longleftrightarrow I = \mathcal{O}_K \Rightarrow [I] = [< \alpha >]$. Así pues tenemos un primer ideal $I = \mathcal{O}_K$

Norma 2

$N_K(I) = 2 \Rightarrow 2 \in I \Rightarrow < 2 > \subset I \Rightarrow I | < 2 >$

Factorizamos $< 2 >$:

$f_\theta = x^2 (mod\ 2) \Rightarrow < 2 > = < 2, \sqrt{-74} >^2$

Con lo cual tenemos nuestro segundo ideal $\mathfrak{p}_2 = < 2, \sqrt{-74} >$

Norma 3

$N_K(I) = 3 \Rightarrow 3 \in I \Rightarrow < 3 > \subset I \Rightarrow I | < 3 >$

Factorizamos $< 3 >$:

$f_\theta = x^2 - 1 (mod\ 3) = (x+1)(x-1) \Rightarrow < 3 > = < 3, \sqrt{-74} + 1 > < 3, \sqrt{-74} - 1 >$

Obtenemos otros dos ideales:

$\mathfrak{p}_3 = < 3, \sqrt{-74} + 1 >, \mathfrak{q}_3 = < 3, \sqrt{-74} - 1 >$

Norma 5

$N_K(I) = 5 \Rightarrow 5 \in I \Rightarrow < 5 > \subset I \Rightarrow I | < 5 >$

Factorizamos $< 5 >$:

$f_\theta = x^2 - 1 (mod\ 5) = (x+1)(x-1) \Rightarrow < 5 > = < 5, \sqrt{-74} + 1 > < 5, \sqrt{-74} - 1 >$

Obtenemos otros dos ideales:

$\mathfrak{p}_5 = < 5, \sqrt{-74} + 1 >, \mathfrak{q}_5 = < 5, \sqrt{-74} - 1 >$

Norma 7

$N_K(I) = 7 \Rightarrow 7 \in I \Rightarrow < 7 > \subset I \Rightarrow I | < 7 >$

Factorizamos $< 7 >$:

$f_\theta = x^2 + 4 (mod\ 7)$ que no factoriza módulo 7, con lo que no pueden existir ideales con norma=7.

Norma 4

$N_K(I) = 4 \Rightarrow$ Factorizamos el ideal $< 4 >$:

$< 4 > = \mathfrak{p}_2^4$. Como cada ideal es de norma 2, la única posibilidad para ideal de norma cuatro es $\mathfrak{p}_2^2$, pero esto es igual a $< 2 > \sim \mathcal{O}_K$ que ya lo teníamos, y por tanto no aporta nada nuevo.

Norma 8

$N_K(I) = 8 \Rightarrow$ Factorizamos el ideal $< 8 >$:

$< 8 >= \mathfrak{p}_2^6$. Como cada ideal es de norma 2, la única posibilidad para ideal de norma ocho es $\mathfrak{p}_2^3$, pero esto es igual a $< 2 > \mathfrak{p}_2 \sim \mathfrak{p}_2$ que ya lo teníamos, y por tanto no aporta nada nuevo.

Norma 9

$N_K(I) = 9 \Rightarrow$ Factorizamos el ideal $< 9 >$:

$< 9 >= \mathfrak{p}_3^2\mathfrak{q}_3^2$. Eso quiere decir que se factoriza en combinaciones de $\mathfrak{p}_3$ y $\mathfrak{q}_3$. Si fuera $\mathfrak{p}_3\mathfrak{q}_3$ tenemos el ideal $< 3 > \sim < \alpha >$ que por tanto no es nuevo. Pero no sabemos que ocurre con $\mathfrak{p}_3^2$ y $\mathfrak{q}_3^2$.

Norma 6

$N_K(I) = 6 \Rightarrow$ Factorizamos el ideal $< 6 >$.

Se tiene que $< 6 >= \mathfrak{p}_2^2\mathfrak{p}_3\mathfrak{q}_3$. Así pues, los posibles ideales de norma 6, son las combinaciones de entre los anteriores que se descomponen como ideal de norma 2 y 3, es decir puede ser: $\mathfrak{p}_2\mathfrak{p}_3$ ó $\mathfrak{p}_2\mathfrak{q}_3$.

Norma 10

$N_K(I) = 10 \Rightarrow$ Factorizamos el ideal $< 10 >$.

Así pues, se descompone como ideal de norma 2 y 5, es decir puede ser: $\mathfrak{p}_2\mathfrak{p}_5$ ó $\mathfrak{p}_2\mathfrak{q}_5$.

Hemos comprobado todas las normas y solo hemos obtenido 12 ideales que son $\mathcal{O}_K$, $\mathfrak{p}_2$, $\mathfrak{p}_3$, $\mathfrak{q}_3$, $\mathfrak{p}_5$, $\mathfrak{q}_5$, $\mathfrak{p}_3^2$, $\mathfrak{q}_3^2$, $\mathfrak{p}_2\mathfrak{p}_3$, $\mathfrak{p}_2\mathfrak{q}_3$, $\mathfrak{p}_2\mathfrak{p}_5$ y $\mathfrak{p}_2\mathfrak{q}_5$.

Comprobemos cuales de ellos están relacionados. Primero veamos si $\mathcal{O}_K \not\sim \mathfrak{p}$, para $\mathfrak{p}$ uno de los ideales anteriores. Basta con tomar normas. Si $\mathfrak{p} \sim \mathcal{O}_K$, entonces $\mathfrak{p} =< \alpha >$, para algún $\alpha \in \mathcal{O}_K$. Por lo tanto, $N_K(\mathfrak{p}) = |N_K(\alpha)| = a^2 + 74b^2$. Vemos que esto no se puede cumplir para la norma de ninguno de los ideales anteriores, salvo para $\mathfrak{p}_3^2$ y $\mathfrak{q}_3^2$ cuya norma es $9 = 3^2 + 74 \cdot 0$. Pero se puede ver rápidamente que éstos tampoco están relacionados con $\mathcal{O}_K$, porque si lo estuvieran:

$$\mathfrak{p}_3^2 =< \alpha > \Rightarrow < 3 > \mathfrak{p}_3 =< \alpha > \mathfrak{q}_3 \Rightarrow \mathfrak{p}_3 \sim \mathfrak{q}_3$$

Que es falso, como demostraremos en unas líneas. Para $\mathfrak{q}_3^2$ el procedimiento es idéntico. Ahora miremos los que tienen normas iguales entre ellos. Ninguno de ellos son iguales. Es muy fácil verlo en todos los casos, multiplicando sencillamente por uno de ellos a cada lado. En el caso de comprobar $\mathfrak{p}_3 \sim \mathfrak{q}_3$ multiplicamos en ambos lados por $\mathfrak{p}_3$ y obtenemos $\mathfrak{p}_3^2 \sim < 3 > \Rightarrow \mathfrak{p}_3^2 =< \alpha >$. Pero sabemos que $\mathfrak{p}_3^2$ tiene norma nueve con lo que $\alpha = 3$ que es imposible, ya que tendríamos que $\mathfrak{p}_3^2 =< 3 >= \mathfrak{p}_3\mathfrak{q}_3 \Rightarrow \mathfrak{p}_3 = \mathfrak{q}_3$ que es falso.

Los otros casos con normas iguales se deducen de forma exactamente igual. Faltan por comprobar los casos en los que tienen normas distintas. Pero para ello procedemos inicialmente de forma similar. Multiplicamos por lo necesario para que en un lado quede un principal, y de ahí vemos si podría existir por normas:

$$\begin{aligned}
\mathfrak{p}_2 \sim \mathfrak{p}_3 &\quad \Rightarrow \mathfrak{p}_2\mathfrak{q}_3 =< \alpha > \quad \Rightarrow 6 = a^2 + 74b^2 \text{ imposible} \\
\mathfrak{p}_2 \sim \mathfrak{q}_3 &\quad \Rightarrow \mathfrak{p}_2\mathfrak{p}_3 =< \alpha > \quad \Rightarrow 6 = a^2 + 74b^2 \text{ imposible} \\
\mathfrak{p}_2 \sim \mathfrak{p}_5 &\quad \Rightarrow \mathfrak{p}_2\mathfrak{q}_5 =< \alpha > \quad \Rightarrow 10 = a^2 + 74b^2 \text{ imposible} \\
\mathfrak{p}_2 \sim \mathfrak{q}_5 &\quad \Rightarrow \mathfrak{p}_2\mathfrak{p}_5 =< \alpha > \quad \Rightarrow 10 = a^2 + 74b^2 \text{ imposible}
\end{aligned}$$

Mientras tengamos una norma producto factores que son coprimos entre ellos y no son cuadrados no obtendremos algo que sea un cuadrado por lo que necesitamos una norma mayor que 74 para que el $74b^2$ tenga influencia. Para todas las otras combinaciones siempre obtendremos que no están relacionados, mirando sus normas de forma análoga a lo anterior. El único caso en el que se sobrepasa el 74 es cuando comparamos norma 9 con 10. Ahí obtenemos que:

$$\mathfrak{p}_2\mathfrak{p}_5 \sim \mathfrak{p}_3^2 \quad \Rightarrow \mathfrak{p}_2\mathfrak{q}_5\mathfrak{q}_3^2 =< \alpha > \quad \Rightarrow 90 = a^2 + 74b^2 \Rightarrow a = \pm 4, b = \pm 1$$

Con las otras posibilidades de normas 9 y 10 ocurre lo mismo, con lo cual tenemos que comprobar si por ejemplo $\mathfrak{p}_3^2 \sim \mathfrak{p}_2\mathfrak{q}_5$ ó $\mathfrak{p}_2\mathfrak{p}_5$.

Por lo obtenido anteriormente, si $\mathfrak{p}_2\mathfrak{p}_5 \sim \mathfrak{p}_3^2 \Rightarrow \mathfrak{q}_3^2\mathfrak{p}_2\mathfrak{p}_5 =< \pm 4 \pm \sqrt{-74} >$. Que es cierto para $< 4 + \sqrt{-74} >$. El otro caso es análogo y se obtiene que $\mathfrak{p}_2\mathfrak{q}_5 \sim \mathfrak{q}_3^2$. Así pues hemos demostrado que existen 10 y sólo 10 ideales que no están relacionados, con lo que el orden del grupo es 10, y por tanto el grupo ha de ser C_{10} (es abeliano).

Veamos ahora cuales son los generadores. Escribiendo C_{10} como:

$$\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\} \text{ con la suma}$$

tenemos que el 1, 3, 7 y 9 son elementos de orden 10 es decir generadores. Buscamos por tanto 4 de nuestros ideales que necesiten ser elevados a 10 para que den un ideal principal, es decir que no exista ninguna potencia menor que 10 a la cual, si lo elevamos obtenemos un ideal principal. Estos ideales se pueden hallar fácilemtne con SAGE y son:

$$\mathfrak{p}_5, \mathfrak{q}_5, \mathfrak{p}_2\mathfrak{p}_3, \mathfrak{p}_2\mathfrak{q}_3$$