Reto 6

Rafa Granero[1]

Lema 1 *El grupo de clase del cuerpo* $K = \mathbb{Q}(\sqrt{-74})$ *es isomorfo a* C_{10}.

Demostración:
Como $-74 \equiv 2 \ (4)$ tenemos que el anillo de enteros del cuerpo K es

$$\mathbb{Z}[\sqrt{-74}]$$

Calculamos la cota de Minkowski, sabiendo que

$$t = 1, \Delta_k = 4 * (-74), n = 2$$

$$M_k = 10{,}8375$$

Así que en el grupo de clase todo ideal es equivalente a uno de norma menor o igual que 10. Debemos factorizar los ideales generados por los primos hasta 10. El polinomio mínimo es

$$p(x) = x^2 + 74$$

Aplicamos el resultado visto en clase[2] y obtenemos

$$< 2 >=< 2, \sqrt{-74} >^2 = \mathfrak{p}_2^2$$

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

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

$$< 7 >=< 7, -70 >=< 7 >$$

Con estos ideales podemos factorizar todos los de norma menor que once. Por ejemplo, si un ideal tuviese norma 4 tendríamos

$$< 4 > \subset I \Rightarrow I | < 4 >= \mathfrak{p}_2^4$$

Vemos que no hay ideales de norma 7. Tampoco tengo que preocuparme por los ideales de norma 4 ni ocho, pues

$$< 4 >= \mathfrak{p}_2^4$$

de donde I con norma 4 es $< 2 >$, que es principal.

$$< 8 >= \mathfrak{p}_2^6$$

de donde el I con norma 8 es $\mathfrak{p}_2^3$ que equivale a $\mathfrak{p}_2$. Los ideales con norma 9 son $< 3 >= \mathfrak{p}_3\mathfrak{q}_3, \mathfrak{p}_3^2, \mathfrak{q}_3^2$. Los ideales de norma 10 son $\mathfrak{p}_2\mathfrak{p}_5$ y $\mathfrak{p}_2\mathfrak{q}_5$. Faltan los ideales de norma 6, que son

[1] Gracias, Yasmina, por dejarme el SAGE.

[2] En concreto dice así:

Lema 2 *Sea* K *es un cuerpo de números y* $O_K = \mathbb{Z}[\theta]$, *entonces si* $f_\theta(x) \in \mathbb{Z}[x]$ *es el polinomio mínimo de* θ, $p \in \mathbb{Z}$ *es un primo y* $\bar{f}_\theta(x) = \bar{f}_1^{r_1} ... \bar{f}_s^{r_s}$ *la descomposición en polinomios irreducibles de* $f_\theta(x)$ *en* $\mathbb{F}_p[x]$. *Obtenemos que la descomposición en ideales primos de* O_K *del ideal* $< p >$ *es*

$$< p >=< p, f_1(\theta) >^{r_1} ... < p, f_s(\theta) >^{r_s}$$

$\mathfrak{p}_2\mathfrak{p}_3$ y $\mathfrak{p}_2\mathfrak{q}_3$. Veamos nuestros candidatos a representantes de las clases de los elementos del grupo de clase

$$\{\mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{q}_3, \mathfrak{p}_5, \mathfrak{q}_5, \mathfrak{p}_2\mathfrak{p}_3, \mathfrak{p}_2\mathfrak{q}_3, \mathfrak{p}_2\mathfrak{p}_5, \mathfrak{p}_2\mathfrak{q}_5, \mathfrak{p}_3^2, \mathfrak{q}_3^2, O\}$$

Está claro que el orden del grupo es múltiplo de dos.

Para ver cuales son equivalentes al total buscamos elementos de norma 2,3,5,6,9 y 10. Un elemento es de la forma

$$a + b\sqrt{-74}$$

y su norma es

$$a^2 + b^2 * 74$$

Vemos que, de todos los casos anteriores sólo tiene solución el penúltimo, $N_k(\alpha) = 9$, que nos da $\alpha = \pm 3$. Por lo tanto ninguno es equivalente al elemento neutro. Veamos las relaciones entre ellos. Si $\mathfrak{p}_2$ y $\mathfrak{p}_3$ estuviesen relacionados se tendría que $\mathfrak{p}_2\mathfrak{q}_3$ estaría relacionado con el total. Pero esto no ocurre, pues no hay ningún elemento de norma 6. Igual para $\mathfrak{q}_3$. Razonamos de manera análoga para los casos $\mathfrak{p}_5, \mathfrak{q}_5, \mathfrak{q}_3$ y tenemos que $\mathfrak{p}_2$ no es equivalente a ninguno de los anteriores. Si $\mathfrak{p}_2$ fuese equivalente a $\mathfrak{p}_2\mathfrak{p}_3$ tendríamos que $\mathfrak{p}_3^2$ sería principal, pero no hay ningun elemento de norma 9 salvo el 3, por lo que este ideal debería ser $< 3 >$, pero $\mathfrak{p}_3^2 \neq < 3 >$. Se hace igual para $\mathfrak{p}_2\mathfrak{q}_3$, $\mathfrak{p}_2\mathfrak{p}_5$ y $\mathfrak{p}_2\mathfrak{q}_5$. Si $\mathfrak{p}_2$ es equivalente a $\mathfrak{p}_3^2$ entonces $\mathfrak{p}_2^2$ equivale a $\mathfrak{p}_3^4$ que equivale al total, luego es principal. Tiene norma $3^4 = 81$ luego debería existir un elemento de norma 81, este elemento es el 9, entonces el único ideal posible es $< 9 >=< 3 >^2 = \mathfrak{p}_3^2\mathfrak{q}_3^2$ luego debería tenerse que $\mathfrak{p}_3$ fuese equivalente a $\mathfrak{q}_3$. Si razonamos igual con $\mathfrak{q}_3^2$ llegamos a lo mismo. Si esta última equivalencia fuese cierta, entonces $\mathfrak{p}_3^2$ sería equivalente a O, *i.e.* sería principal, pero en ese caso sería el ideal $< 3 >$ y no es así.

Veamos las equivalencias de $\mathfrak{p}_3$. Si $\mathfrak{p}_3$ es equivalente a $\mathfrak{p}_5$ entonces $\mathfrak{p}_5\mathfrak{q}_3$ sería principal, pero no existe ningún elemento de norma 15, así que no son equivalentes. Razonamos igual con $\mathfrak{q}_5$ y llegamos a que tampoco son equivalentes. Si $\mathfrak{p}_3$ es equivalente a $\mathfrak{p}_2\mathfrak{q}_3$ entonces $\mathfrak{p}_2\mathfrak{q}_3^2$ es principal, pero no hay ningun elemento de norma 18. Si $\mathfrak{p}_3$ fuese equivalente a $\mathfrak{p}_2\mathfrak{p}_3$ entonces $\mathfrak{p}_2\mathfrak{p}_3\mathfrak{q}_3 = \mathfrak{p}_2 < 3 >$ sería equivalente al total, pero entonces $\mathfrak{p}_2$ sería principal y esto no es así. Si $\mathfrak{p}_3$ fuese equivalente a $\mathfrak{p}_2\mathfrak{p}_5$, o a $\mathfrak{p}_2\mathfrak{q}_5$, se tendría que $\mathfrak{p}_2\mathfrak{q}_3\mathfrak{p}_5$ sería principal, pero entonces hay un elemento de norma 30. No existe un elemento así. $\mathfrak{p}_3$ Sólo puede ser equivalente a su cuadrado si es principal, pero esto es falso. Sólo falta un caso, $\mathfrak{p}_3$ equivalente a $\mathfrak{q}_3^2$, si fuese cierto entonces $\mathfrak{q}_3^3$ sería principal. Cómo $\mathfrak{q}_3$ no lo es se ha de tener que el orden de este ideal es tres (en particular h_k debería ser multiplo de tres). Si este ideal es principal existe un elemento de norma $3^3 = 27$, pero no hay tal elemento.

El razonamiento para ver que $\mathfrak{q}_3$ no es equivalente a $\mathfrak{p}_5$ ni a $\mathfrak{q}_5$ es idéntico al anterior. Ocurre lo mismo en el caso de $\mathfrak{p}_2\mathfrak{q}_3$. Ver que $\mathfrak{q}_3$ no puede ser equivalente a $\mathfrak{p}_2\mathfrak{p}_3$ se reduce a ver que no hay elementos de norma 18. Si $\mathfrak{q}_3$ fuese equivalente a $\mathfrak{p}_2\mathfrak{p}_5$ o a $\mathfrak{p}_2\mathfrak{q}_5$ entonces $\mathfrak{p}_3\mathfrak{p}_2\mathfrak{p}_5$ o $\mathfrak{p}_3\mathfrak{p}_2\mathfrak{q}_5$ serían principales, pero no hay elementos de norma 30. Si $\mathfrak{q}_3$ fuese equivalente a $\mathfrak{p}_3^2$ entonces, como antes, $\mathfrak{p}_3^3$ sería principal y habría un elemento de norma 27, pero no es así. Como $\mathfrak{q}_3$ no es principal, hemos visto que no es equivalente a ninguno.

Vamos con $\mathfrak{p}_5$. Si fuese equivalente a $\mathfrak{q}_5$ entonces $\mathfrak{q}_5^2$ sería principal. Existirá un elemento de norma 25. Este elemento es 5 y por lo tanto se ha de tener $\mathfrak{q}_5^2 =< 5 >$. Sin embargo

$$\mathfrak{q}_5^2 =< 25, 5(\sqrt{-74} - 1), -73 - 2\sqrt{-74} >$$

y el último generador vemos que no está en el ideal $< 5 >$. Si fuese equivalente a $\mathfrak{p}_2\mathfrak{p}_3$ entonces $\mathfrak{q}_5\mathfrak{p}_2\mathfrak{p}_3$ sería principal, pero no existe ningún elemento de norma 30. Este mismo

argumento sirve para $\mathfrak{q}_3\mathfrak{p}_2$. Como $\mathfrak{p}_2$ no es principal no podemos tener que $\mathfrak{p}_5$ sea equivalente $\mathfrak{p}_2\mathfrak{p}_5$. Si fuese equivalente a $\mathfrak{p}_2\mathfrak{q}_5$ entonces tendríamos $\mathfrak{p}_2\mathfrak{q}_5^2$ sería principal. Como su norma es $2 * 25 = 50$ debe, si esto es verdad, haber un elemento de norma 50. Esto no ocurre. Si fuese equivalente a $\mathfrak{q}_3^2$ entonces $\mathfrak{q}_5\mathfrak{q}_3^2$ sería principal con norma 45, pero ningun elemento tiene esta norma. Lo dicho también sirve para $\mathfrak{p}_3^2$.

Continuamos con $\mathfrak{q}_5$. Si fuese equivalente a $\mathfrak{q}_3\mathfrak{p}_2$ entonces habría un elemento de norma $3 * 2 * 5$ y no ocurre. Lo mismo es aplicable a $\mathfrak{p}_3\mathfrak{p}_2$. Son válidos los mismos argumentos que para $\mathfrak{p}_5$.

Si $\mathfrak{q}_3\mathfrak{p}_2$ fuese equivalente a $\mathfrak{p}_3\mathfrak{p}_2$ entonces tendríamos $\mathfrak{p}_2$ equivalente a $\mathfrak{p}_2\mathfrak{p}_3^2$, que sólo es posible si $\mathfrak{p}_3^2$ es principal, pero esto no ocurre. Si fuese equivalente a $\mathfrak{p}_2\mathfrak{p}_5$ tendríamos[3]

$$\mathfrak{p}_2^2\mathfrak{q}_3 \ \mathcal{E} \ \mathfrak{p}_2^2\mathfrak{p}_5 \Leftrightarrow \mathfrak{q}_3 \ \mathcal{E} \ \mathfrak{p}_5$$

que sabemos que es mentira. Lo mismo vale para $\mathfrak{p}_2\mathfrak{q}_5$. Si fuese equivalente a $\mathfrak{p}_3^2$ entonces

$$\mathfrak{p}_3^3 \ \mathcal{E} \ \mathfrak{p}_2$$

Lo que nos dice que $\mathfrak{p}_3^6$ es principal. Por lo tanto ha de existir un elemento de norma 3^6. El único que lo cumple es 27. Entonces obligatoriamente se ha de tener que $\mathfrak{p}_3^6 =< 27 >$. Sabemos que

$$\mathfrak{p}_3^3 =< 27, \sqrt{-74} + 13 >$$

de donde

$$\mathfrak{p}_3^6 =< 729, 27(\sqrt{-74} + 13), 95 + 26\sqrt{-74}) >$$

y vemos que el último generador no está contenido en el ideal principal. Como hemos visto antes que $\mathfrak{p}_2$ no era equivalente a $\mathfrak{q}_3$ concluímos.

Se procede igual para $\mathfrak{p}_2\mathfrak{p}_3$.

Si $\mathfrak{p}_2\mathfrak{p}_5$ fuese equivalente a $\mathfrak{p}_2\mathfrak{q}_5$ se tendría que $\mathfrak{p}_5 \ \mathcal{E} \ \mathfrak{q}_5$. Si fuese equivalente a $\mathfrak{p}_3^2$ entonces

$$\mathfrak{p}_2\mathfrak{p}_5\mathfrak{q}_5 \ \mathcal{E} \ \mathfrak{p}_2 \Rightarrow \mathfrak{p}_3^4\mathfrak{q}_5^2 \ \mathcal{E} \ O$$

y por lo tanto habría al menos un elemento de norma $3^4 * 5^2$. Hay varias posibilidades

$$\{a = 29, b = -4\}, \{b = 0, a = -45\}, \{a = -29, b = -4\}, \{a = -29, b = 4\}, \{a = 45, b = 0\}, \{a = 29, b = 4\}$$

Si calculamos nuestro ideal observamos que

$$\mathfrak{p}_3^4\mathfrak{q}_5^2 =< 29 - 4\sqrt{-74} >$$

Merced de esto tenemos una equivalencia.

Lo mismo ocurre con $\mathfrak{q}_3^2$. Sólo que en este caso tenemos que el ideal es

$$\mathfrak{q}_3^4\mathfrak{p}_5^2 =< 29 + 4\sqrt{-74} >$$

Si $\mathfrak{p}_3^2$ fuese equivalente a $\mathfrak{q}_3^2$ entonces $\mathfrak{q}_3^4$ sería principal, y existiría un elemento de norma 3^4, este elemento es el 9. Así, el ideal sería $< 9 >$, pero si calculamos los generadores de $\mathfrak{p}_3^4$ vemos que el último no esta en el principal generado por el nueve.

La tabla de lo que hemos demostrado aparece en el cuadro 1.

Entonces nuestro grupo tiene los siguientes elementos

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

[3]Denoto 'ser equivalente' por $\mathcal{E}$.

	$\mathfrak{p}_2$	$\mathfrak{p}_3$	$\mathfrak{q}_3$	$\mathfrak{p}_5$	$\mathfrak{q}_5$	$\mathfrak{p}_2\mathfrak{q}_3$	$\mathfrak{p}_2\mathfrak{p}_3$	$\mathfrak{p}_2\mathfrak{p}_5$	$\mathfrak{p}_2\mathfrak{q}_5$	$\mathfrak{p}_3^2$	$\mathfrak{q}_3^2$	O
$\mathfrak{p}_2$	1	0	0	0	0	0	0	0	0	0	0	0
$\mathfrak{p}_3$	0	1	0	0	0	0	0	0	0	0	0	0
$\mathfrak{q}_3$	0	0	1	0	0	0	0	0	0	0	0	0
$\mathfrak{p}_5$	0	0	0	1	0	0	0	0	0	0	0	0
$\mathfrak{q}_5$	0	0	0	0	1	0	0	0	0	0	0	0
$\mathfrak{p}_2\mathfrak{q}_3$	0	0	0	0	0	1	0	0	0	0	0	0
$\mathfrak{p}_2\mathfrak{p}_3$	0	0	0	0	0	0	1	0	0	0	0	0
$\mathfrak{p}_2\mathfrak{p}_5$	0	0	0	0	0	0	0	1	0	1	0	0
$\mathfrak{p}_2\mathfrak{q}_5$	0	0	0	0	0	0	0	0	1	0	1	0
$\mathfrak{p}_3^2$	0	0	0	0	0	0	0	1	0	1	0	0
$\mathfrak{q}_3^2$	0	0	0	0	0	0	0	0	1	0	1	0
O	0	0	0	0	0	0	0	0	0	0	0	1

Cuadro 1: Relaciones (1 si equivalen y 0 si no lo hacen).

Tenemos el grupo C_{10} pues es el único grupo abeliano finito con ese número de elementos. Calculamos las primeras potencias de $\mathfrak{p}_5$

$$\mathfrak{p}_5^2 =< 25, \sqrt{-74} + 1 >, ..., \mathfrak{p}_5^5 =< 3125, \sqrt{-74} + 2776 >$$

El ideal $\mathfrak{p}_5$ no tiene orden ni 2 ni 5, así que su orden debe ser 10. Uno de los generadores es $\mathfrak{p}_5$. Los demás generadores podemos sacarlos fácilmente sin más que calcular sus cuadrados y sus quintas potencias, si no son principales son generadores.