Reto 4

Rafa Granero

Lema 1 *El grupo de clase de $\mathbb{Q}(\xi_{11})$ con ξ_{11} raíz 11-ésima de la unidad es el trivial.*

Demostración:

Tenemos que

$$n = [\mathbb{Q}(\xi_{11}) : \mathbb{Q}] = 10; \quad t = 5; \quad \Delta_{\mathbb{Q}(\xi_{11})} = -1^{(11-1)/2} 11^{11-2} = -11^9$$

y

$$\mathcal{O}_K = \mathbb{Z}[\xi_{11}]$$

por los teoremas 3.5 y 3.6 de [1].

Calculamos M_K.

$$M_K = \left(\frac{4}{\pi}\right)^5 \frac{10!}{10^{10}} \sqrt{11^9} \approx 58{,}96...$$

es decir, podemos tener ideales hasta de norma 58. Debemos ahora factorizar

$$< p > \quad \forall p < 58$$

y primo, pues sea $n < 59$ la norma de un cierto ideal J, entonces $n \in J$, con lo que $< n > \subset J \Rightarrow J| < n > = < \prod p_i^{e_i} > = \prod < p_i >^{e_i}$ y todo queda reducido a los primos. Utilizando `SAGE` [1] comprobamos que para 2 el polinomio mínimo de ξ_{11} es irreducible en $\mathbb{Z}/2\mathbb{Z}$ por lo que el ideal $< 2 >$ ya es primo y tiene norma 2^{10}. Esto me asegura que no hay ningún ideal de norma 2, si exisitiese I de norma 2 tendríamos que $2 \in I$, pero el único ideal que contiene a 2 es el generado por este, al no descomponer $< 2 >$ como producto de ideales, que no tiene norma 2. Lo mismo ocurre para $p = 7, 13, 17, 19, 29$ y 41. Seguimos así para los demás primos encontrando los polinomios en los cuales factoriza nuestro polinomio ciclotómico.

Para el caso $p = 3$ tenemos que factoriza como producto dos polinomios

$$p_1(x) = x^5 + x^4 + 2x^3 + x^2 + 2$$

y

$$p_2(x) = x^5 + 2x^3 + x^2 + 2x + 2$$

aplicando el teorema 10.1 de [1] logramos

$$< 3 > = < 3, \xi_{11}^5 + \xi_{11}^4 + 2\xi_{11}^3 + \xi_{11}^2 + 2 >< 3, \xi_{11}^5 + 2\xi_{11}^3 + \xi_{11}^2 + 2\xi_{11} + 2 > = P_{1,3} P_{2,3}$$

Cuyo producto tiene norma 3^{10}. No podemos asegurar nada más de la norma de estos de momento, aunque lo que uno espera, que es que ambos tengan la misma norma 3^5 (con lo que no habrá ningún ideal de norma 3) es verdad. El tercer teorema de isomorfía nos dice que si R es un anillo e I y J son ideales de R entonces $(R/I)/(J/I) \cong R/J$. Ahora si I, B son ideales de R se tiene $(I + B)/I \cong B$. Así los dos hechos juntos dicen que

$$(R/I)/J \cong R/(I + B)$$

[1] Utilizando el comando **cyclotomic_polynomial(11).factor_mod(p)** factorizaramos el polinomio mínimo de ξ_{11} módulo un primo p.

y basta tomar $I =< 3 >$ y $B =< \xi_{11}^5 + \xi_{11}^4 + 2\xi_{11}^3 + \xi_{11}^2 + 2 >$, tenemos que

$$\mathcal{N}_{\mathbb{Q}(\xi_{11})}(P_{i,3}) = |\mathbb{Z}[\xi_{11}]/ < 3, p_i(\xi_{11}) > | = |\mathbb{F}_3[\xi_{11}]/ < p_i(\xi_{11}) > | \quad i = 1, 2$$

pues son isomorfos, pero el cardinal de este cuerpo (pues p_i es irreducible) es $3^{gr\ p_i} = 3^5$.

Para el caso 5 tenemos que factoriza como producto de

$$x^5 + 2x^4 + 4x^3 + x^2 + x + 4$$

y

$$x^5 + 4x^4 + 4x^3 + x^2 + 3x + 4$$

por lo que tendremos

$$< 5 >=< 5, \xi_{11}^5 + 2\xi_{11}^4 + 4\xi_{11}^3 + \xi_{11}^2 + \xi_{11} + 4 >< 5, \xi_{11}^5 + 4\xi_{11}^4 + 4\xi_{11}^3 + \xi_{11}^2 + 3\xi_{11} + 4 >$$

Como antes, el producto tiene norma 5^{10} y con razonamientos idénticos a los anteriores tenemos que cada uno tiene norma 5^5, con lo que tampoco hay ideales de norma 5.

Módulo 11 este polinomio factoriza como producto de

$$(x + 10)^{10}$$

con lo que se tiene, ya que al ser lineal podemos eliminar el término independiente racional,

$$< 11 >=< 11, (\xi_{11} + 10) >^{10}$$

y cada uno de estos tiene norma 11.

Módulo 23 este polinomio factoriza como producto de 10 polinomios lineales

$$(x + 17)(x + 7)(x + 19)(x + 15)(x + 21)(x + 10)(x + 20)...$$

$$(x + 5)(x + 14)(x + 11)$$

por lo que tenemos

$$< 23 >=< 23, \xi_{11} + 17 >< 23, \xi_{11} + 7 >< 23, \xi_{11} + 19 > 23, \xi_{11}x + 15 >< 23, \xi_{11} + 21 >$$

$$< 23, \xi_{11} + 10 >< 23, \xi_{11} + 20 >< 23, \xi_{11} + 5 >< 23, \xi_{11} + 14 >< 23, \xi_{11} + 11 >$$

donde cada uno de estos tiene norma 23.

Ahora toca $p = 31$, donde el polinomio factoriza como producto de

$$x^5 + 10x^4 + 30x^3 + x^2 + 9x + 30$$

y

$$x^5 + 22x^4 + 30x^3 + x^2 + 21x + 30$$

$$< 31 >=< 31, \xi_{11}^5+10\xi_{11}^4+30\xi_{11}^3+\xi_{11}^2+9\xi_{11}+30 >< 31, \xi_{11}^5+22\xi_{11}^4+30\xi_{11}^3+\xi_{11}^2+21\xi_{11}+30 >$$

donde el producto tiene norma 31^{10}. Los mismos razonamientos anteriores nos muestran que no hay ideales de norma 31.

Para el número 37 se tiene que factoriza como producto de

$$(x^5 + 24x^4 + 36x^3 + x^2 + 23x + 36)$$

y

$$(x^5+14x^4+36x^3+x^2+13x+36)$$

con lo que

$$<37>=<37, \xi_{11}^5+24\xi_{11}^4+36\xi_{11}^3+\xi_{11}^2+23\xi_{11}+36><37, \xi_{11}^5+14\xi_{11}^4+36\xi_{11}^3+\xi_{11}^2+13\xi_{11}+36>$$

Y el producto tiene norma 37^{10}. Merced de las afirmaciones previas no hay ideales de norma 37.

Si $p=43$ tenemos una descomposición en 5 polinomios cuadráticos

$$x^2+7x+1, \quad x^2+29x+1, \quad x^2+34x+1, \quad x^2+39x+1, \quad x^2+21x+1$$

y entonces tenemos

$$<43>=<43, (\xi_{11}^2+7\xi_{11}+1)><43, \xi_{11}^2+29\xi_{11}+1><43, \xi_{11}^2+34\xi_{11}+1> ...$$

$$<43, \xi_{11}^2+39\xi_{11}+1><43, \xi_{11}^2+21\xi_{11}+1>$$

donde el producto tiene norma 43^{10}. Si seguimos las ideas anteriores llegamos a que cada uno tiene norma $43^2 > M_k$ por lo que tampoco hay ideales de norma 43.

Ya vamos acabando con la factorización. En el caso $p=47$ el polinomio factoriza como producto de

$$x^5+21x^4+46x^3+x^2+20x+46$$

y

$$x^5+27x^4+46x^3+x^2+26x+46$$

con lo que obtenemos los ideales primos

$$<47>=<47, \xi_{11}^5+21\xi_{11}^4+46\xi_{11}^3+\xi_{11}^2+20\xi_{11}+46><47, \xi_{11}^5+27\xi_{11}^4+46\xi_{11}^3+\xi_{11}^2+26\xi_{11}+46>$$

con norma del producto 47^{10}. Idénticamente a lo ya dicho cada uno tiene norma 47^5 y, consecuentemente, no hay ideales de norma 47.

Y el último, $p=53$, donde nuestro polinomio ciclotómico factoriza como producto de

$$x^5+41x^4+52x^3+x^2+40x+52$$

y

$$x^5+13x^4+52x^3+x^2+12x+52$$

con lo que nos quedan los ideales primos

$$<53>=<53, \xi_{11}^5+41\xi_{11}^4+52\xi_{11}^3+\xi_{11}^2+40\xi_{11}+52><53, \xi_{11}^5+13\xi_{11}^4+52\xi_{11}^3+\xi_{11}^2+12\xi_{11}+52>$$

Con norma del producto 53^{10}. Repetimos por última vez lo anterior y obtenemos que no hay ideales de norma 53, por ser la norma de cada uno de estos ideales en los que hemos descompuesto $53^5 >> M_k$.

Entonces debemos mirar los casos $p=11$ y $p=23$, pues hemos descartado todos los demás. Si vemos que son equivalentes a un principal entonces tendríamos que nuestro grupo buscado es isomorfo al grupo trivial, por lo que nuestro anillo sería D.I.P y consecuentemente D.F.U.

Utilizando `SAGE`[2], comprobamos que 11 y $\xi_{11}+10$ pertenecen al ideal $<\xi_{11}^8+\xi_{11}>$, distinto del total, pues

$$11=(3\xi_{11}^9+6\xi_{11}^8+9\xi_{11}^7+\xi_{11}^6+4\xi_{11}^5+7\xi_{11}^4+10\xi_{11}^3+2\xi_{11}^2+5\xi_{11}+8)(\xi_{11}^8+\xi_{11})$$

y

$$\xi_{11}+10=(3\xi_{11}^9+6\xi_{11}^8+8\xi_{11}^7+\xi_{11}^6+4\xi_{11}^5+7\xi_{11}^4+9\xi_{11}^3+2\xi_{11}^2+5\xi_{11}+7)(\xi_{11}^8+\xi_{11})$$

pero como era primo era maximal, con lo que tenemos que el contenido es igualdad.

Por lo mismo tenemos que todos los ideales de norma 23 primos son principales. Listamos las igualdades, escribiendo como segundo multiplicando el generador del ideal principal en cuestión.

$$\begin{gathered}23=(3\xi_{11}^9+16\xi_{11}^8+11\xi_{11}^7-3\xi_{11}^6+13\xi_{11}^5+21\xi_{11}^4+2\xi_{11}^3+4\xi_{11}^2+5\xi_{11}+17)*\\(\xi_{11}^9+\xi_{11}^8+2\xi_{11}^7+2\xi_{11}^6+\xi_{11}^5+\xi_{11}^4+\xi_{11}^3+\xi_{11}^2+\xi_{11}+1)\\ \xi_{11}+11=(2\xi_{11}^9+8\xi_{11}^8+5\xi_{11}^7-\xi_{11}^6+7\xi_{11}^5+10\xi_{11}^4+\xi_{11}^3+2\xi_{11}^2+3\xi_{11}+8)*\\(\xi_{11}^9+\xi_{11}^8+2\xi_{11}^7+2\xi_{11}^6+\xi_{11}^5+\xi_{11}^4+\xi_{11}^3+\xi_{11}^2+\xi_{11}+1)\end{gathered}$$

$$23=(-4\xi_{11}^9+6\xi_{11}^8+4\xi_{11}^7+9\xi_{11}^6+8\xi_{11}^5-\xi_{11}^4+10\xi_{11}^3-6\xi_{11}^2+11\xi_{11}+3)*(-\xi_{11}^9-\xi_{11}^2-\xi_{11})$$

$$\xi_{11}+14=(-2\xi_{11}^9+4\xi_{11}^8+3\xi_{11}^7+6\xi_{11}^6+5\xi_{11}^5+6\xi_{11}^3-3\xi_{11}^2+7\xi_{11}+2)*(-\xi_{11}^9-\xi_{11}^2-\xi_{11})$$

$$23=(-17\xi_{11}^9-\xi_{11}^8-12\xi_{11}^7-3\xi_{11}^6-2\xi_{11}^5-7\xi_{11}^4-5\xi_{11}^3-15\xi_{11}^2-11\xi_{11}-8)*$$

[2]Para definir el cuerpo de números la instrucción es

K.<a>=NumberField(cyclotomic_polynomial(11));K

Una vez definido el cuerpo de números, definimos el ideal como

I=ideal(generadores)

Por ejemplo

I=ideal(23,a+7)

Cuando le pidamos que escriba I, nos devolverá un único generador, pues es principal. En el mismo ejemplo anterior, si tecleamos I nos da

Fractional ideal $(-a^9-a^6-a^5-a^4-a^2-a)$ **of Number Field in a with defining polynomial** $x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1$

Así logramos el generador del ideal I. Si además queremos la expresión de los dos generadores anteriores, en el ejemplo 23 y a+7, como un elemento por el nuevo generador, lo único que tenemos que hacer es dividir normalmente. En el ejemplo anterior y para a+7 la instrucción es

r=(a+7)/$(-a^9-a^6-a^5-a^4-a^2a)$**;**
Lo único que falta ahora es hacer esto muchas veces, de hecho dos por cada ideal.

$$(\xi_{11}^8 - \xi_{11}^7 + \xi_{11}^6 + \xi_{11}^5 + \xi_{11}^4 + \xi_{11}^3 + \xi_{11} + 1)$$

$$\xi_{11}+5 = (-3\xi_{11}^9 - 2\xi_{11}^7 - \xi_{11}^4 - \xi_{11}^3 - 3\xi_{11}^2 - 2\xi_{11} - 1) * (\xi_{11}^8 - \xi_{11}^7 + \xi_{11}^6 + \xi_{11}^5 + \xi_{11}^4 + \xi_{11}^3 + \xi_{11} + 1)$$

$$23 = (-2\xi_{11}^9 - 8\xi_{11}^8 - 3\xi_{11}^7 - 11\xi_{11}^6 - 12\xi_{11}^5 - 15\xi_{11}^4 - \xi_{11}^3 - 5\xi_{11}^2 - 17\xi_{11} - 6) *$$
$$(\xi_{11}^9 + \xi_{11}^8 + \xi_{11}^6 + \xi_{11}^4 + \xi_{11}^3 + \xi_{11}^2 + \xi_{11} + 1)$$
$$\xi_{11} + 20 = (-2\xi_{11}^9 - 7\xi_{11}^8 - 3\xi_{11}^7 - 10\xi_{11}^6 - 11\xi_{11}^5 - 13\xi_{11}^4 - \xi_{11}^3 - 5\xi_{11}^2 - 15\xi_{11} - 6) *$$
$$(\xi_{11}^9 + \xi_{11}^8 + \xi_{11}^6 + \xi_{11}^4 + \xi_{11}^3 + \xi_{11}^2 + \xi_{11} + 1)$$

$$23 = (-7\xi_{11}^9 - 6\xi_{11}^8 - 16\xi_{11}^7 - 8\xi_{11}^6 + 4\xi_{11}^5 - \xi_{11}^4 + 3\xi_{11}^3 - 14\xi_{11}^2 - 5\xi_{11} - 3) *$$
$$(-\xi_{11}^9 - \xi_{11}^5 - \xi_{11}^4 - \xi_{11}^2 - \xi_{11})$$
$$\xi_{11} + 10 = (-3\xi_{11}^9 - 3\xi_{11}^8 - 7\xi_{11}^7 - 3\xi_{11}^6 + 2\xi_{11}^5 + \xi_{11}^3 - 6\xi_{11}^2 - 2\xi_{11} - 1) *$$
$$(-\xi_{11}^9 - \xi_{11}^5 - \xi_{11}^4 - \xi_{11}^2 - \xi_{11})$$

$$23 = (-5\xi_{11}^9 + 8\xi_{11}^8 + 11\xi_{11}^7 - 6\xi_{11}^6 + 6\xi_{11}^5 + 7\xi_{11}^4 + 9\xi_{11}^3 - 10\xi_{11}^2 - 2\xi_{11} + 14) *$$
$$(\xi_{11}^8 + \xi_{11}^7 + 2\xi_{11}^6 + \xi_{11}^5 + \xi_{11}^4 + \xi_{11}^3 + \xi_{11}^2 + \xi_{11} + 1)$$
$$\xi_{11} + 21 = (-4\xi_{11}^9 + 8\xi_{11}^8 + 10\xi_{11}^7 - 5\xi_{11}^6 + 6\xi_{11}^5 + 7\xi_{11}^4 + 8\xi_{11}^3 - 9\xi_{11}^2 - \xi_{11} + 13) *$$
$$(\xi_{11}^8 + \xi_{11}^7 + 2\xi_{11}^6 + \xi_{11}^5 + \xi_{11}^4 + \xi_{11}^3 + \xi_{11}^2 + \xi_{11} + 1)$$

$$23 = (-5\xi_{11}^9 + 2\xi_{11}^8 + 6\xi_{11}^7 - 8\xi_{11}^6 + 5\xi_{11}^5 - 4\xi_{11}^4 + 4\xi_{11}^3 - \xi_{11}^2 + 5\xi_{11} + 7) * (-\xi_{11}^7 - \xi_{11}^5 - \xi_{11}^2)$$
$$\xi_{11} + 15 = (-6\xi_{11}^9 + 2\xi_{11}^8 + 4\xi_{11}^7 - 5\xi_{11}^6 - 3\xi_{11}^5 - 2\xi_{11}^4 + 3\xi_{11}^3 + 4\xi_{11} + 5) * (-\xi_{11}^7 - \xi_{11}^5 - \xi_{11}^2)$$

$$23 = (5\xi_{11}^9 + 2\xi_{11}^8 - 10\xi_{11}^7 - 12\xi_{11}^6 + 3\xi_{11}^5 - 6\xi_{11}^4 + 4\xi_{11}^3 - 2\xi_{11}^2 - 3\xi_{11} - 7) * (-\xi_{11}^7 - \xi_{11}^5 - \xi_{11}^4)$$
$$\xi_{11} + 19 = (4\xi_{11}^9 + \xi_{11}^8 - 9\xi_{11}^7 - 10\xi_{11}^6 + 2\xi_{11}^5 - 5\xi_{11}^4 + 3\xi_{11}^3 - 2\xi_{11}^2 - 3\xi_{11} - 6) * (-\xi_{11}^7 - \xi_{11}^5 - \xi_{11}^4)$$

$$23 = (-10\xi_{11}^9 - \xi_{11}^8 - 16\xi_{11}^7 - 14\xi_{11}^6 - 2\xi_{11}^5 + \xi_{11}^4 - 4\xi_{11}^3 - 11\xi_{11}^2 - 7\xi_{11} - 6) * (-\xi_{11}^5 - \xi_{11}^4 - \xi_{11}^2)$$
$$\xi_{11} + 17 = (-7\xi_{11}^9 - \xi_{11}^8 - 12\xi_{11}^7 - 14\xi_{11}^6 - \xi_{11}^5 + \xi_{11}^4 - 3\xi_{11}^3 - 8\xi_{11}^2 - 5\xi_{11} - 4) * (-\xi_{11}^5 - \xi_{11}^4 - \xi_{11}^2)$$

$$23 = (2\xi_{11}^9 + 11\xi_{11}^8 - 6\xi_{11}^7 - 2\xi_{11}^6 - 7\xi_{11}^5 + 5\xi_{11}^4 + 13\xi_{11}^3 + 3\xi_{11}^2 + 4\xi_{11} - 3) * (-\xi_{11}^9 - \xi_{11}^6 - \xi_{11}^5 - \xi_{11}^4 - \xi_{11}^2 - \xi_{11})$$
$$\xi_{11} + 7 = (\xi_{11}^9 + 3\xi_{11}^8 - 2\xi_{11}^7 - \xi_{11}^6 - 2\xi_{11}^5 + 2\xi_{11}^4 + 4\xi_{11}^3 + \xi_{11}^2 + \xi_{11} - 1) * (-\xi_{11}^9 - \xi_{11}^6 - \xi_{11}^5 - \xi_{11}^4 - \xi_{11}^2 - \xi_{11})$$

Todo esto nos da el siguiente corolario

Corolario 1 *El anillo de enteros de* $\mathbb{Q}(\xi_{11})$, $\mathbb{Z}[\xi_{11}]$, *es un dominio de ideales principales, y por tanto de factorización única.*

Referencias

[1] Stewart, Ian y Tall, David *Algebraic number theory and Fermat's last theorem.* (Third edition). A K Peters, Ltd., Natick, MA, 2002.