Teoría de números algebraicos
Examen final

Alexey Beshenov (alexey.beshenov@cimat.mx)

9 de diciembre de 2020

Fecha límite: 16 de diciembre de 2020.

Ejercicio 1. Consideremos el polinomio $f = x^3 + 5x^2 - x - 4$.

0) Demuestre que f es irreducible en $\mathbb{Q}[x]$. Sea $K = \mathbb{Q}[x]/(f)$.

1) Calcule el anillo de enteros $\mathcal{O}_K$ y discriminante Δ_K.

2) Demuestre que $u_1 = \alpha + 1$ y $u_2 = \alpha - 1$, donde $\alpha = x \mod f$, son unidades en $\mathcal{O}_K^\times$. Asumiendo que u_1 y u_2 generan la parte libre de $\mathcal{O}_K^\times$, calcule el regulador.

3) Calcule el grupo de clases $\mathrm{Cl}(K)$.

4) Usando la fórmula analítica del número de clases[*], compruebe que u_1 y u_2 son efectivamente unidades fundamentales.

Solución. Basta ver que el polinomio es irreducible en $\mathbb{Z}[x]$, y para esto basta notar que al reducir f mód 3 nos queda un polinomio cúbico irreducible (= que no tiene raíces mód 3).

Ahora calculamos que

$$\Delta(\mathbb{Z}[\alpha]) = \Delta(f) = 1957 = 19 \cdot 103.$$

Tenemos

$$\Delta(\mathbb{Z}[\alpha]) = [\mathcal{O}_K : \mathbb{Z}[\alpha]]^2 \cdot \Delta_K,$$

y $\Delta(\mathbb{Z}[\alpha])$ es libre de cuadrados, así que $\mathcal{O}_K = \mathbb{Z}[\alpha]$ y $\Delta_K = \Delta(\mathbb{Z}[\alpha])$.

Notamos que el polinomio f tiene tres raíces reales. Esto se ve de los cambios de signos:

$$f(-6) = -34, \quad f(-5) = 1, \quad f(0) = -4, \quad f(1) = 1.$$

Los valores aproximados de estas raíces (calculados en PARI/GP usando la función `polroots`) son

$$x_1 = -5{,}040964\ldots, \quad x_2 = -0{,}870538\ldots, \quad x_3 = 0{,}911503\ldots.$$

Se sigue que hay tres encajes reales $\sigma\colon K \hookrightarrow \mathbb{R}$. En particular, el grupo de unidades $\mathcal{O}_K^\times$ tiene rango 2. Dado que el campo es totalmente real, las raíces de la unidad son $\mu_K = \{\pm 1\}$, y debe haber dos unidades fundamentales u_1, u_2 tales que

$$\mathcal{O}_K^\times = \{\pm 1\} \times \langle u_1 \rangle \times \langle u_2 \rangle.$$

El ejercicio nos sugiere considerar $u_1 = \alpha + 1$ y $u_2 = \alpha - 1$. Para ver que estas son unidades, basta calcular que $N_{K/\mathbb{Q}}(u_1) = N_{K/\mathbb{Q}}(u_2) = -1$. El regulador correspondiente será

$$\det \begin{pmatrix} \log|x_1 + 1| & \log|x_1 - 1| \\ \log|x_2 + 1| & \log|x_2 - 1| \end{pmatrix} = 4{,}551450\ldots$$

[*] El residuo de $\zeta_K(s)$ en $s = 1$ puede ser calculado en PARI/GP.

Para calcular el grupo de clases, empezamos por la cota de Minkowski

$$M_K = \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2}\sqrt{|\Delta_K|} = \frac{3!}{3^3}\sqrt{1957} = 9{,}83\ldots$$

Esta nos dice que todo elemento del grupo de clases está representado por un ideal entero de norma ≤ 9. Para encontrar estos ideales, consideremos los ideales primos que están arriba de $p = 2, 3, 5, 7$. Esto es fácil porque $\mathcal{O}_K = \mathbb{Z}[\alpha] = \mathbb{Z}[x]/(f)$, y basta considerar las factorizaciones de f mód p (teorema de Kummer–Dedekind).

Primero notamos que f queda irreducible mód 3 y mód 7, lo que nos da ideales primos $\mathfrak{p}_3 \mid 3$ y $\mathfrak{p}_7 \mid 7$ de norma 3^3 y 7^3 respectivamente. Esta excede la cota de Minkowski. Por otra parte, mód 2 se obtiene factorización de la forma

$$f \equiv x\,(x^2 + x + 1),$$

lo que nos da dos ideales primos:

$$\mathfrak{p}_2 = (2, \alpha), \quad \mathfrak{p}_2' = (2, 1 + \alpha + \alpha^2),$$

de norma 2 y 4 respectivamente. En fin, mód 5 nos salen de nuevo un factor lineal y otro cuadrático:

$$f \equiv (x + 2)\,(x^2 + 3x + 3).$$

El factor cuadrático corresponde a un ideal primo de norma 5^2 que no nos interesará, mientras que el factor lineal nos da el ideal primo

$$\mathfrak{p}_5 = (5, 2 + \alpha)$$

de norma 5.

Primero afirmo que $\mathfrak{p}_5$ y $\mathfrak{p}_2'$ representan el mismo elemento en el grupo de clases. Para esto podemos calcular que

$$(1 + \alpha/2)\,\mathfrak{p}_2' = \mathfrak{p}_5.$$

Por otra parte, calculamos que $\mathfrak{p}_2^2 = (\alpha)$, así que $\mathfrak{p}_2$ tiene orden 2 en el grupo de clases, y en particular $[\mathfrak{p}_2'] = [\mathfrak{p}_2]^{-1} = [\mathfrak{p}_2]$.

Nos quedan entonces dos posibilidades: si $\mathfrak{p}_2 = (2, \alpha)$ es un ideal principal, entonces el grupo de clases es trivial. Por otra parte, si el ideal $\mathfrak{p}_2$ no es principal, entonces el grupo de clases tiene orden 2. Afirmo que estamos en la segunda situación.

Vamos a ocupar la relación $\mathfrak{p}_2^2 = (\alpha)$. Si el ideal $\mathfrak{p}_2$ fuera principal, tendríamos $\mathfrak{p}_2 = (\beta)$ para algún $\beta \in \mathcal{O}_K$, y luego $\beta^2 = u\,\alpha$, donde $u \in \mathcal{O}_K^\times$. La última relación no se ve muy interesante: ¡todavía no hemos calculado el grupo de unidades! Sin embargo, podemos observar que si $u = vw^2$, entonces $(\beta\,w^{-1})^2 = v\alpha$, así que bastaría probar que $u\alpha$ no es un cuadrado para todos u que representan diferentes elementos del grupo cociente $\mathcal{O}_K^\times/(\mathcal{O}_K^\times)^2$.

Si u_1, u_2 son unidades fundamentales, entonces $\mathcal{O}_K^\times = \{\pm 1\} \times \langle u_1\rangle \times \langle u_2\rangle$, y luego $\mathcal{O}_K^\times/(\mathcal{O}_K^\times)^2 = \{\pm 1\, u_1^{e_1}\, u_2^{e_2}\}$, donde $e_{1,2} = 0, 1$. No conocemos las unidades fundamentales, pero tenemos dos buenos candidatos para estas: $u_1 = \alpha + 1$ y $u_2 = \alpha - 1$. Para verificar que estos números representan los elementos de $\mathcal{O}_K^\times/(\mathcal{O}_K^\times)^2$, tenemos que ver que entre

$$-1,\ u_1,\ u_1u_2,\ u_2,\ -u_1,\ -u_1u_2,\ -u_2$$

no hay cuadrados.

Dado que nuestro campo es totalmente real, si x es un cuadrado en K, entonces para cualquier encaje $\sigma_{1,2,3}\colon K \hookrightarrow \mathbb{R}$ la imagen $\sigma_i(x)$ debe ser un número positivo. Hagamos una tabla:

x	$\sigma_1(x)$	$\sigma_2(x)$	$\sigma_3(x)$
-1	-1	-1	-1
$u_1 = \alpha + 1$	$-4{,}040965$	$+0{,}129461$	$+1{,}911503$
$u_2 = \alpha - 1$	$-6{,}040965$	$-1{,}870539$	$-0{,}088497$
$u_1 u_2 = \alpha^2 - 1$	$+24{,}411324$	$-0{,}242162$	$-0{,}169162$
$-u_1 = -\alpha - 1$	$+4{,}040965$	$-0{,}129461$	$-1{,}911503$
$-u_2 = -\alpha + 1$	$+6{,}040965$	$+1{,}870539$	$+0{,}088497$
$-u_1 u_2 = -\alpha^2 + 1$	$-24{,}411324$	$+0{,}242162$	$+0{,}169162$

De aquí podemos concluir que todos los números de arriba no son cuadrados, con la única posible excepción de $-u_2 = -\alpha + 1$, que tiene todos los encajes positivos. Para ver que $-\alpha + 1$ tampoco es un cuadrado, bastaría encontrar un ideal primo $\mathfrak{p}$ tal que $\overline{-\alpha + 1}$ no es un cuadrado en el campo finito $\mathcal{O}_K/\mathfrak{p}$. Por ejemplo, $\mathfrak{p} = (5, 2 + \alpha)$ nos da $\mathcal{O}_K/\mathfrak{p} \cong \mathbb{F}_5$. Tenemos $-\alpha + 1 \equiv 3 \pmod{\mathfrak{p}}$, y este no es un cuadrado mód 5.

Ahora bien, nuestro cálculo hasta ahora nos dice que los elementos de $\mathcal{O}_K^\times/(\mathcal{O}_K^\times)^2$ pueden ser representados por

$$1,\ u_1,\ u_1u_2,\ u_2,\ -1,\ -u_1,\ -u_1u_2,\ -u_2.$$

Para concluir, hay que ver que αu no es un cuadrado para todos los u de arriba. Esto se sigue de la tabla de abajo.

x	$\sigma_1(x)$	$\sigma_2(x)$	$\sigma_3(x)$
α	$-5{,}040965$	$-0{,}870539$	$0{,}911503$
$\alpha u_1 = \alpha^2 + \alpha$	$+20{,}370359$	$-0{,}112701$	$+1{,}742342$
$\alpha u_1 u_2 = -5\alpha^2 + 4$	$-123{,}056620$	$+0{,}210812$	$-0{,}154191$
$\alpha u_2 = \alpha^2 - \alpha$	$+30{,}452289$	$+1{,}628376$	$-0{,}080665$
$-\alpha$	$+5{,}040965$	$+0{,}870539$	$-0{,}911503$
$-\alpha u_1 = -\alpha^2 - \alpha$	$-20{,}370359$	$+0{,}112701$	$-1{,}742342$
$-\alpha u_1 u_2 = 5\alpha^2 - 4$	$+123{,}056620$	$-0{,}210812$	$+0{,}154191$
$-\alpha u_2 = -\alpha^2 + \alpha$	$-30{,}452289$	$-1{,}628376$	$+0{,}080665$

Entonces, el ideal $\mathfrak{p}_2$ no es principal, y por lo tanto el grupo de clases es isomorfo a $\mathbb{Z}/2\mathbb{Z}$.

En fin, usando PARI/GP, calculamos que

$$\lim_{s \to 1^+} (s-1)\,\zeta_K(s) = 0{,}8230844\ldots$$

Por otra parte,

$$\lim_{s \to 1^+} (s-1)\,\zeta_K(s) = \frac{2^{r_1}\,(2\pi)^{r_2}\ \mathrm{Reg}_K\ h_k}{\#\mu_K\ \sqrt{|\Delta_K|}} = \frac{2^3 \cdot \mathrm{Reg}_K \cdot 2}{2 \cdot \sqrt{1957}}.$$

Comparando las dos expresiones, se obtiene $\mathrm{Reg}_K = 4{,}551450\ldots$ Este es el regulador que fue calculado arriba, así que podemos concluir que u_1, u_2 son unidades fundamentales. □

Ejercicio 2. Para un campo de números $K/\mathbb{Q}$ demuestre que la cerradura de Galois L/K contiene como subcampo $\mathbb{Q}(\sqrt{\Delta_K})$. Dé un ejemplo particular cuando Δ_K no es un cuadrado y $K \neq \mathbb{Q}(\sqrt{\Delta_K})$.

Solución. Recordemos la fórmula para el discriminante

$$\Delta_K = \det(\sigma_i(\alpha_j))_{i,j}^2,$$

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

$$\sqrt{\Delta_K} = \pm \det(\sigma_i(\alpha_j))_{i,j} \in L,$$

donde los números $\sigma_i(\alpha_j)$ pueden ser vistos como elementos de la cerradura de Galois L/K.

Para dar un ejemplo, el campo cúbico real $K = \mathbb{Q}(\sqrt[3]{2})$ tiene discriminante $\Delta_K = -2^2 \cdot 3^3$. La cerradura de Galois es $L = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$, y esta contiene $\sqrt{-3} = 1 + 2\zeta_3$. □

Ejercicio 3. Sea $k > 0$ un entero positivo libre de cuadrados. Supongamos que $k \equiv 1, 2 \pmod 4$ y k no tiene forma $3a^2 \pm 1$ para $a \in \mathbb{Z}$. Demuestre que si $3 \nmid h_{\mathbb{Q}(\sqrt{-k})}$, entonces la ecuación $y^2 = x^3 - k$ no tiene soluciones enteras.

Punto extra: encuentre un contraejemplo para $3 \mid h_{\mathbb{Q}(\sqrt{-k})}$.

Solución. Considerando la ecuación mód 4 y usando que $k \equiv 1, 2 \pmod 4$, notamos que x es necesariamente impar. Además, x e y deben ser coprimos: si $p \mid x$ y $p \mid y$, entonces $p^2 \mid k$, pero k es libre de cuadrados por nuestra hipótesis.

Dado que $k \equiv 1, 2 \pmod 4$, para el campo cuadrático imaginario $K = \mathbb{Q}(\sqrt{-k})$ se tiene $\mathcal{O}_K = \mathbb{Z}[\sqrt{-k}]$. Factoricemos la ecuación como

$$x^3 = y^2 + k = (y + \sqrt{-k})\,(y - \sqrt{-k}). \tag{*}$$

Sea $\mathfrak{p} \subset \mathbb{Z}[\sqrt{-k}]$ un ideal primo que divide a ideales $(y + \sqrt{-k})$ e $(y - \sqrt{-k})$ (y por lo tanto a (x)). En este caso $\mathfrak{p}$ divide al ideal $(2y)$. Puesto que x es impar, tenemos $\mathfrak{p} \nmid 2$, y luego $\mathfrak{p} \mid y$. Pero esto contradice el hecho de que x e y son coprimos.

Entonces, los ideales $(y + \sqrt{-k})$ e $(y - \sqrt{-k})$ son coprimos. Usando esto, podemos concluir de (*) que se tiene

$$(y + \sqrt{-k}) = I^3$$

para algún ideal $I \subset \mathbb{Z}[\sqrt{-k}]$. Por nuestra hipótesis $3 \nmid h_K$, y en este caso el hecho de que I^3 es un ideal principal implica que I es también principal. Escribamos $I = (a + b\sqrt{-k})$. Tenemos

$$y + \sqrt{-k} = u\,(a + b\sqrt{-k})^3$$

para alguna unidad $u \in \mathbb{Z}[\sqrt{-k}]^\times$. De todos modos, por nuestra hipótesis $k \neq 1$, así que $u = \pm 1$, y siempre podemos asumir que $u = +1$, dado que $-1 = (-1)^3$. Analicemos la expresión

$$y + \sqrt{-k} = (a + b\sqrt{-k})^3 = (a^2 - 3k\,b^2)\,a + (3a^2 - kb^2)\,b\,\sqrt{-k}.$$

De aquí necesariamente $b = \pm 1$, y luego $k = 3a^2 \pm 1$, pero esto contradice nuestra hipótesis sobre k. Hemos obtenido una contradicción, así que la ecuación no tiene soluciones enteras.

Revisando la tabla de grupos de clases para los campos cuadráticos imaginarios, encontramos que el primer numero de clases divisible por 3 aparece para $k = 23$, donde $h_{\mathbb{Q}(\sqrt{-23})} = 3$. Este k no tiene forma $3a^2 \pm 1$. La ecuación $y^2 = x^3 - 23$ sí tiene solución $(x, y) = (3, \pm 2)$. □

Ejercicio 4. Dada una extensión ciclotómica $\mathbb{Q}(\zeta_m)$, sean $X \subseteq \widehat{(\mathbb{Z}/m\mathbb{Z})^\times}$ un grupo de caracteres de Dirichlet y $K \subseteq \mathbb{Q}(\zeta_m)$ el subcampo correspondiente. Demuestre que K es un campo real (es decir, $r_2 = 0$) si y solamente si $\chi(-1) = +1$ para todo $\chi \in X$.

Solución. Un subcampo $K \subseteq \mathbb{Q}(\zeta_m)$ es real si y solamente si los elementos de K están fijos por la conjugación compleja; es decir, por el subgrupo

$$H = \{\pm 1\} \subset (\mathbb{Z}/m\mathbb{Z})^\times \cong \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}).$$

El subcampo de $\mathbb{Q}(\zeta_m)$ fijo por H es $L = \mathbb{Q}(\zeta_m + \zeta_m^{-1})$. En términos de caracteres de Dirichlet, a L corresponde el grupo de caracteres mód m que cumplen $\chi(-1) = +1$:

$$Y = H^\perp = \{\chi \in \widehat{(\mathbb{Z}/m\mathbb{Z})^\times} \mid \chi(-1) = +1\}.$$

Ahora K es real si y solamente si $K \subseteq L$, si y solamente si $X \subseteq Y$. □

Ejercicio 5. Consideremos el campo cuadrático real $K = \mathbb{Q}(\sqrt{3})$.

1) Calcule el residuo de $\zeta_K(s)$ en $s = 1$.
2) Exprese $\zeta_K(s)$ como un producto de series L de Dirichlet.
3) Calcule los valores $\zeta_K(0)$, $\zeta_K(-1)$, $\zeta_K(-2)$, $\zeta_K(-3)$.
4) Calcule los valores $\zeta_K(2)$ y $\zeta_K(4)$.

Solución. El residuo en $s = 1$ viene dado por la fórmula analítica del número de clases:

$$\frac{2^{r_1}\,(2\pi)^{r_2}\,\mathrm{Reg}_K\;h_K}{\#\mu_K\,\sqrt{|\Delta_K|}}.$$

En este caso $r_1 = 2$, $r_2 = 0$. La unidad fundamental de K es $2 + \sqrt{3}$, así que $\mathrm{Reg}_K = \log(2 + \sqrt{3})$. Hemos calculado en clase que $h_K = 1$. En fin, $\mu_K = \{\pm 1\}$ y $\Delta_K = 12$. Tenemos entonces el residuo

$$\zeta_K^*(1) = \frac{\log(2 + \sqrt{3})}{\sqrt{3}} = 0{,}760345\ldots$$

De la misma manera, en $s = 0$ habrá un cero simple de residuo

$$\zeta_K^*(0) = -\frac{\mathrm{Reg}_K\;h_K}{\#\mu_K} = -\frac{\log(2 + \sqrt{3})}{2} = -0{,}658478\ldots$$

Por lo que vimos en clase, se tiene

$$\zeta_K(s) = \zeta(s)\,L(s, \chi),$$

donde χ es el carácter de Dirichlet mód 12 dado por

$$\chi\colon 1 \mapsto +1, \quad 5 \mapsto -1, \quad 7 \mapsto -1, \quad 11 \mapsto +1.$$

Tenemos

$$\begin{aligned}
\zeta_K(-1) &= \frac{B_2}{2}\,\frac{B_{2,\chi}}{2},\\
\zeta_K(-2) &= 0,\\
\zeta_K(-3) &= \frac{B_4}{4}\,\frac{B_{4,\chi}}{4},
\end{aligned}$$

Aquí

$$B_{k,\chi} = 12^{k-1} \sum_{(a,12)=1} \chi(a)\,B_k(a/12).$$

Usando esta fórmula, calculamos que

$$B_{2,\chi} = 4, \quad B_{4,\chi} = -184.$$

Dado que

$$B_2 = \frac{1}{6}, \quad B_4 = -\frac{1}{30},$$

se obtiene

$$\zeta_K(-1) = \frac{1}{6}, \quad \zeta_K(-3) = \frac{23}{60}.$$

En fin, de la ecuación funcional, para k par se obtiene

$$\zeta_K(k) = \frac{(2\pi)^{2k}}{12^{k-1/2} \cdot 4 \cdot ((k-1)!)^2}\, \zeta_K(1-k),$$

En particular, para $k = 2$

$$\zeta_K(2) = \frac{\pi^4}{2 \cdot 3^{3/2}}\, \zeta_K(-1) = \frac{\pi^4}{36\sqrt{3}} = 1{,}562199\ldots$$

y para $k = 4$

$$\zeta_K(4) = \frac{\pi^8}{8 \cdot 3^{11/2}}\, \zeta_K(-3) = \frac{23\,\pi^8}{116640\sqrt{3}} = 1{,}080236\ldots \qquad \square$$