Teoría de números algebraicos
Tarea 2

Alexey Beshenov (alexey.beshenov@cimat.mx)

26 de agosto de 2020

Fecha límite: viernes, 4 de septiembre.

Ejercicio 2.1. Demuestre que para $\alpha \in \mathbb{Z}[i]$ no nulo se tiene

$$N_{\mathbb{Q}(i)/\mathbb{Q}}(\alpha) = \#(\mathbb{Z}[i]/(\alpha)).$$

(Más adelante veremos un resultado general.)

Solución. Pongamos $\alpha = a + bi$. Tenemos

$$(\alpha) = \{(c + di)\,(a + bi) \mid c, d \in \mathbb{Z}\}.$$

Podemos escribir

$$(c + di)\,(a + bi) = c \cdot (a + bi) + d \cdot (-b + ai),$$

así que como $\mathbb{Z}$-módulo se tiene

$$(\alpha) = (a + bi)\mathbb{Z} \oplus (-b + ai)\mathbb{Z}.$$

Nos interesa el cociente de $\mathbb{Z}[i]$ por (α), o de manera equivalente, el cociente de $\mathbb{Z}[i]$ por el subgrupo generado por (a, b) y $(-b, a)$. El número de elementos en el cociente será igual a[(*)]

$$\det \begin{pmatrix} a & -b \\ b & a \end{pmatrix} = a^2 + b^2 = N(\alpha).$$

Esta es la prueba elemental que tenía en mente. Otra opción es la siguiente: para $\alpha \notin \mathbb{Z}[i]^\times$ podemos tomar la factorización en primos de Gauss

$$\alpha \sim \pi_1^{e_1} \cdots \pi_s^{e_s}.$$

[(*)]Este es un caso particular del siguiente resultado general: para $v_1, \ldots, v_n \in \mathbb{Z}^n$ denotemos por A la matriz formada por los v_i. Luego, si $\det A \neq 0$, entonces

$$[\mathbb{Z}^n : \langle v_1, \ldots, v_n \rangle] = \det A$$

(y si $\det A = 0$, el índice no es finito).

La multiplicatividad de la norma nos da

$$N(\alpha) = N(\pi_1)^{e_1} \cdots N(\pi_s)^{e_s}.$$

Además, por el teorema chino del resto,

$$\mathbb{Z}[i]/(\alpha) \cong \mathbb{Z}[i]/(\pi_1^{e_1}) \times \cdots \times \mathbb{Z}[i]/(\pi_s^{e_s}).$$

Así el problema se reduce al probar que para un primo de Gauss π se cumple $\#(\mathbb{Z}[i]/(\pi^e)) = N(\pi)^e$. Ya lo observamos para $e = 1$, y por el lema que vimos al inicio de clase 8, se tiene $\#(\mathbb{Z}[i]/(\pi^e)) = \#(Z[i]/(\pi))^e$. $\square$

Ejercicio 2.2. Para $R = \mathbb{Z}[\sqrt{-5}]$ encuentre todos los ideales maximales $\mathfrak{p} \subset R$ tales que $R/\mathfrak{p} \cong \mathbb{F}_{23}$.

Solución. Hay varios modos de hacerlo. Por ejemplo, podemos ocupar la idea de Kummer–Dedekind. Si $\mathbb{Z}[\sqrt{-5}]/\mathfrak{p} \cong \mathbb{F}_{23}$, entonces $23 \in \mathfrak{p}$. Estos ideales corresponden a los ideales maximales en el anillo cociente

$$\begin{gathered} \mathbb{Z}[\sqrt{-5}]/(23) \xrightarrow{\cong} \mathbb{F}_{23}[x]/(x^2+5), \\ a + b \mapsto \sqrt{-5} \text{ mód } 23 \mapsto \overline{a+bx}. \end{gathered}$$

De la factorización $x^2 + 5 = (x+8)(x-8)$ en $\mathbb{F}_{23}[x]$ podemos concluir que los ideales en cuestión son $(23, \pm 8 + \sqrt{-5})$, o mejor dicho, $\mathfrak{p} = (23, 8 + \sqrt{-5})$, $\overline{\mathfrak{p}} = (23, 8 - \sqrt{-5})$. De hecho, estos ideales no son principales. $\square$

Ejercicio 2.3. Demuestre que el ideal $(23, x)$ no es invertible en el anillo $\mathbb{Z}[x]$.

Solución. El número 23 no tiene mucho que ver con el ejercicio, podemos poner en su lugar cualquier primo p y considerar el ideal $\mathfrak{m} = (p, x)$.

$$\mathfrak{m}^{-1} = \{f \in \mathbb{Q}(x) \mid pf, xf \in \mathbb{Z}[x]\}.$$

La condición $pf \in \mathbb{Z}[x]$ significa que en el denominador de f a lo sumo puede estar p, mientras que la condición $xf \in \mathbb{Z}[x]$ significa que en el denominador a lo sumo puede estar x. Todo esto implica que $\mathfrak{m}^{-1} = \mathbb{Z}[x]$, y entonces $\mathfrak{m}\mathfrak{m}^{-1} = \mathfrak{m} \neq \mathbb{Z}[x]$.

Otra manera de verlo sería la siguiente: notamos que $\mathfrak{m}^2 = (p^2, px, x^2)$, y para el ideal $I = (p, x^2)$ se tiene $\mathfrak{m}^2 \subsetneq I \subsetneq \mathfrak{m}$. Las inclusiones son estrictas: por ejemplo, no es difícil comprobar que $p \notin \mathfrak{m}^2$ y $x \notin I$. Si $\mathfrak{m}$ fuera invertible, tendríamos $\mathfrak{m} \subsetneq I\mathfrak{m}^{-1} \subsetneq \mathbb{Z}[x]$, pero el ideal $\mathfrak{m}$ es maximal. $\square$

Ejercicio 2.4. Consideremos el anillo $\mathbb{Z}[\sqrt{5}]$ y los ideales

$$\mathfrak{p}_2 = (2, 1+\sqrt{5}), \quad \mathfrak{p}_{11} = (11, 4+\sqrt{5}).$$

Determine si son invertibles y encuentre I^{-1} en cada caso.

Solución. En cada caso se puede calcular I^{-1} a mano y luego multiplicar II^{-1}, pero esto es algo aburrido... Podemos notar que

$$\mathfrak{p}_2^2 = (4, 2+2\sqrt{5}, 6+2\sqrt{5}) = (2)\cdot(2, 1+\sqrt{5}) = 2\mathbb{Z}[\sqrt{5}]\cdot\mathfrak{p}_2.$$

Ahora si $\mathfrak{p}_2$ fuera invertible, esto implicaría que $\mathfrak{p}_2 = 2\mathbb{Z}[\sqrt{5}]$, pero $1+\sqrt{5}\notin 2\mathbb{Z}[\sqrt{5}]$. Entonces, el ideal no es invertible.

Respecto al ideal $\mathfrak{p}_{11}$, en realidad este es principal: $11 = (4+\sqrt{5})\,(4-\sqrt{5})$. Entonces, $\mathfrak{p}_{11} = (4+\sqrt{5})$, $\mathfrak{p}_{11}^{-1} = \left(\frac{1}{4+\sqrt{5}}\right)$.

Ahora calculamos

$$\mathfrak{p}_2^{-1} = \{\alpha\in\mathbb{Q}(\sqrt{5}) \mid 2\alpha, (1+\sqrt{5})\alpha\in\mathbb{Z}[\sqrt{5}]\}.$$

De la primera condición tenemos $\alpha = \frac{a}{2}+\frac{b}{2}\sqrt{5}$, donde $a,b\in\mathbb{Z}$. Para la segunda condición, primero calculamos $(1+\sqrt{5})\,\alpha = \frac{a+5b}{2}+\frac{a+b}{2}\sqrt{5}$, así que $a\equiv b \pmod 2$, y luego $\mathfrak{p}_2^{-1} = \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$. Solo para comprobar otra vez más que el ideal no es invertible, podemos calcular

$$\mathfrak{p}_2\mathfrak{p}_2^{-1} = (2, 1+\sqrt{5})\left(1, \frac{1+\sqrt{5}}{2}\right) = (2, 1+\sqrt{5}, 3+\sqrt{5}) = \mathfrak{p}_2 \neq \mathbb{Z}[\sqrt{5}]. \quad \square$$

Ejercicio 2.5. Asumiendo que $\operatorname{Pic}(\mathbb{Z}[\sqrt{-37}])\cong\mathbb{Z}/2\mathbb{Z}$, demuestre que la curva elíptica $y^2 = x^3-37$ no tiene puntos enteros.

Solución. Reduciendo la ecuación módulo 4, notamos que y debe ser par. Escribamos $x^3 = (y+\sqrt{-37})\,(y-\sqrt{-37})$. Usando que y es par, podemos ver que el ideal $(y+\sqrt{-37}, y-\sqrt{-37})$ contiene $2y$ e

$$37 = \left(\frac{y}{2}-\sqrt{-37}\right)(y+\sqrt{-37}) - \frac{y}{2}\,(y-\sqrt{-37}).$$

De la ecuación $y^2 = x^3-37$ se ve que $37\nmid y$, así que $\operatorname{mcd}(2y, 37) = 1$. Esto demuestra que $(y+\sqrt{-37})+(y-\sqrt{-37}) = \mathbb{Z}[\sqrt{-37}]$. Dado que los ideales son coprimos, tenemos $(y+\sqrt{-37}) = I^3$ para algún ideal I. Pero $\operatorname{Pic}(\mathbb{Z}[\sqrt{-37}]) = \mathbb{Z}/2\mathbb{Z}$ implica que el mismo I es principal. Escribamos $I = (a+b\sqrt{-37})$. Tenemos

$$y+\sqrt{-37} = a\,(a^2-111b^2) + b\,(3a^2-37b^2)\sqrt{-37}.$$

Se ve que la ecuación $b\,(3a^2-37b^2) = \pm 1$ no tiene soluciones $a,b\in\mathbb{Z}$, y entonces nuestra ecuación $y^2 = x^3-37$ tampoco tiene soluciones enteras. $\square$

Ejercicio adicional. Encuentre el anillo de enteros $\mathcal{O}_K$ para $K = \mathbb{Q}(\sqrt{3},\sqrt{5})$. (Hay modos listos de hacerlo, pero también se pueden ocupar cálculos directos como veremos el lunes para los campos cuadráticos; véase *Kenneth S. Williams, Integers of biquadratic fields, Canad. Math. Bull. 13 (1970), 519–526.*)

Solución. Este ejercicio no es muy instructivo porque más adelante veremos otro modo mejor de hacerlo.(*)

$$\begin{tikzcd}[column sep=small] & \mathbb{Q}(\sqrt{3},\sqrt{5}) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\ \mathbb{Q}(\sqrt{3}) \arrow[dr, dash] & \mathbb{Q}(\sqrt{5}) \arrow[d, dash] & \mathbb{Q}(\sqrt{15}) \arrow[dl, dash] \\ & \mathbb{Q} & \end{tikzcd}$$

Tomemos $1, \sqrt{3}, \sqrt{5}, \sqrt{15}$ como una base de $K/\mathbb{Q}$ y consideremos un elemento genérico $\alpha \in \mathcal{O}_K \setminus \mathbb{Q}$ y sus conjugados $\alpha', \alpha'', \alpha''' \in \mathcal{O}_K \setminus \mathbb{Q}$:

$$\begin{aligned} \alpha &= a + b\sqrt{3} + c\sqrt{5} + d\sqrt{15}, \\ \alpha' &= a - b\sqrt{3} + c\sqrt{5} - d\sqrt{15}, \\ \alpha'' &= a + b\sqrt{3} - c\sqrt{5} - d\sqrt{15}, \\ \alpha''' &= a - b\sqrt{3} - c\sqrt{5} + d\sqrt{15}. \end{aligned}$$

La integralidad de estos elementos implica que

$$\alpha + \alpha'' \in \mathbb{Z}[\sqrt{3}], \quad \alpha + \alpha' \in \mathbb{Z}\Big[\frac{1+\sqrt{5}}{2}\Big], \quad \alpha + \alpha''' \in \mathbb{Z}[\sqrt{15}].$$

Como consecuencia,

$$\alpha = \frac{1}{2}(a' + b'\sqrt{3} + c'\sqrt{5} + d'\sqrt{15}),$$

donde $a', b', c', d' \in \mathbb{Z}$.

Primero, analizando los casos cuando α está en uno de los tres subcampos cuadráticos, notamos que necesariamente se cumple

$$a' \equiv c', \; b' \equiv d' \pmod{2}. \tag{*}$$

Ahora empieza la verdadera pesadilla: si α no está en los subcampos cuadráticos, vamos a escribir su polinomio mínimo que coincide con el polinomio característico. Lo calculé en PARI/GP.

```
? K = nfinit(t^2-3);
? L = rnfinit(K, x^2-5);
? u = rnfeltreltoabs(L,t);
? v = rnfeltreltoabs(L,x);
? f = charpoly ((a + b*u + c*v + d*u*v)/2)
```

(*)Respuesta breve: $K = \mathbb{Q}(\sqrt{3})$ y $K' = \mathbb{Q}(\sqrt{5})$ son campos linealmente disjuntos con $\operatorname{mcd}(\Delta_K, \Delta_{K'}) = 1$. Esto será explicado más adelante.

```
% = .....
? r = a^2 - 15*d^2;
? s = a^2 - 3*b^2 - 5*c^2 + 15*d^2;
? t = 2*(a*d - b*c);
? f == x^4 - 2*a*x^3 + (r+s/2)*x^2
+ (15*d*t - a*s)/2*x + (s^2-15*t^2)/16
% = 1
```

El resultado es

$$x^4 - 2a'x^3 + \left(r + \frac{s}{2}\right)\, x^2 + \frac{15d't - a's}{2}\, x + \frac{s^2 - 15\, t^2}{16},$$

donde

$$r = a'^2 - 15d'^2, \quad s = a'^2 - 3b'^2 - 5c'^2 + 15d'^2, \quad t = 2\,(a'd' - b'c').$$

Se puede ver que los coeficientes del polinomio mínimo son enteros si y solamente si $s \equiv t \equiv 0 \pmod 4$, y esto sucede si y solamente si se cumple la condición (*). Entonces,

$$\begin{aligned}
\mathcal{O}_K &= \left\{ \frac{1}{2}(a' + b'\sqrt{3} + c'\sqrt{5} + d'\sqrt{15}) \;\middle|\; a' \equiv c',\ b' \equiv d'\ (2) \right\} \\
&= \mathbb{Z}\Big[\sqrt{3}, \frac{1+\sqrt{5}}{2}\Big] \\
&= \mathbb{Z} \oplus \sqrt{3}\mathbb{Z} \oplus \frac{1+\sqrt{5}}{2}\mathbb{Z} \oplus \frac{\sqrt{3}+\sqrt{15}}{2}\,\mathbb{Z}.
\end{aligned}$$

Los elementos de arriba son claramente enteros, y uno podría adivinar desde el principio que la respuesta es $\mathbb{Z}\Big[\sqrt{3}, \frac{1+\sqrt{5}}{2}\Big]$, pero todavía no sabríamos cómo probarlo de manera lista... La moraleja de estos cálculos: trabajando solamente con la definición de $\mathcal{O}_K$, sin usar ninguna idea especial, no se puede llegar muy lejos... $\square$