

Cuerpos de números.

1. ¿Cuáles de los siguientes números complejos son números algebraicos?:

$$\frac{355}{133}, e^{\frac{2\pi i}{23}}, \sqrt{17} + \sqrt{19}, \frac{1 + \sqrt{17}}{2\sqrt{-19}}, \sqrt{1 + \sqrt{2}} + \sqrt{1 - \sqrt{2}}, \pi^k \text{ con } k \in \mathbb{Q}.$$

2. Sean $\alpha_1, \dots, \alpha_n$ enteros algebraicos de $\mathbb{Q}(\theta)$ que son \mathbb{Q} -linealmente independientes. Sea $n = [\mathbb{Q}(\theta) : \mathbb{Q}]$ y sea Δ el discriminante de $\mathbb{Q}(\theta)$. Demostrar que si $\Delta[\alpha_1, \dots, \alpha_n] = \Delta$, entonces $\{\alpha_1, \dots, \alpha_n\}$ es una base entera de $\mathbb{Q}(\theta)$.

3. a) Si $[K : \mathbb{Q}] = n$ y $\alpha \in \mathbb{Q}$, demostrar $N_K(\alpha) = \alpha^n$ y $\text{Tr}_K(\alpha) = n\alpha$.

b) Dar un ejemplo que demuestre que para un α fijo, $N_K(\alpha)$ y $\text{Tr}_K(\alpha)$ dependen de K , y que por tanto no se puede hablar de *norma* de α ni de *traza* de α sin hacer referencia a una extensión $\mathbb{Q} \subset K$.

4. Sea $\zeta = e^{2\pi i/3}$.

a) Demostrar que $\mathbb{Q}(\zeta) = \{a + b\zeta : a, b \in \mathbb{Q}\}$ y que $\mathbb{Z}[\zeta] = \{a + b\zeta : a, b \in \mathbb{Z}\}$.

b) Demostrar que si $N : \mathbb{Z}[\zeta] \rightarrow \mathbb{Z}$ es la norma en $\mathbb{Q}(\zeta)$ restringida a $\mathbb{Z}[\zeta]$, entonces $N(a + b\zeta) = a^2 - ab + b^2$. Probar que si $a + b\zeta = u + vi$ con $u, v \in \mathbb{R}$ (todo elemento de $\mathbb{Z}[\zeta]$ se puede escribir así de manera única) entonces $N(a + b\zeta) = u^2 + v^2$.

c) Demostrar que si α divide a β en $\mathbb{Z}[\zeta]$, entonces $N(\alpha)$ divide a $N(\beta)$ en \mathbb{Z} .

d) Sea $\alpha \in \mathbb{Z}[\zeta]$. Probar que α es una unidad si y sólo si $N(\alpha) = 1$. Encontrar todas las unidades de $\mathbb{Z}[\zeta]$. (Son sólo 6).

e) Demostrar que $1 - \zeta$ es irreducible en $\mathbb{Z}[\zeta]$ y que $3 = u(1 - \zeta)^2$ para una cierta unidad u .

5. Encontrar bases enteras y los discriminantes de los siguientes cuerpos:

$$\mathbb{Q}(\sqrt{3}), \mathbb{Q}(\sqrt{-7}), \mathbb{Q}(\sqrt{11}), \mathbb{Q}(\sqrt{-11}), \mathbb{Q}(\sqrt{6}), \mathbb{Q}(\sqrt{-6}).$$

6. Sea $K = \mathbb{Q}(\zeta)$ donde $\zeta = e^{2\pi i/5}$. Calcular $N_K(\alpha)$ y $\text{Tr}_K(\alpha)$ para los siguientes valores de α :

$$\zeta^2, \zeta + \zeta^2, 1 + \zeta + \zeta^2 + \zeta^3 + \zeta^4.$$

7. Sea $K = \mathbb{Q}(\zeta)$ donde $\zeta = e^{2\pi i/5}$.

a) Demostrar que si $\alpha \in \mathbb{Z}[\zeta]$, entonces $N_K(\alpha)$ es de la forma $(a^2 - 5b^2)/4$ con $a, b \in \mathbb{Z}$.

b) Probar que $\mathbb{Z}[\zeta]$ tiene un número infinito de unidades.

c) Demostrar que para $a, b \in \mathbb{Q}, a \neq -b$, se tiene $N_K(a + b\zeta) = (a^5 + b^5)/(a + b)$.

d) Calcular $N_K(\alpha)$ para $\alpha = \zeta + 2, \zeta - 2, \zeta + 3, \zeta - 3, \zeta + 4$.

e) Demostrar que $\zeta + 2, \zeta - 2, \zeta + 3$ son irreducibles en $\mathbb{Z}[\zeta]$.

f) Factorizar 11, 31 y 61 en $\mathbb{Z}[\zeta]$.

g) Probar que todos los divisores propios de $\zeta + 4$ tienen norma 5 ó 41, y, sabiendo que $\zeta - 1$ es un factor de $\zeta + 4$, encontrar otro.

8. Encontrar todas las soluciones enteras de las ecuaciones $y^2 + 4 = x^3$ (puede convenir distinguir el caso de y par del de y impar), $y^2 + 19 = x^3$ e $y^2 + 3 = x^3$. (Ayuda: Factorizar).

9. Ramanujan observó que 1729 es el menor entero positivo que se puede escribir como suma de dos cubos de dos maneras distintas. Demostrar que, efectivamente, la ecuación $x^3 + y^3 = 1729$ tiene dos soluciones distintas en enteros positivos (excluyendo intercambiar x e y). (Ayuda: factorizar ambos lados.) La misma idea permitiría, quizá con ayuda de un ordenador, comprobar caso a caso que ningún $n < 1729$ tiene esta propiedad. O sin utilizar el ordenador, elegir un n tal que $100 < n < 1729$ y tal que n sea suma de dos cubos, y demostrar que la ecuación $x^3 + y^3 = n$ tiene una única solución con x e y enteros positivos (excluyendo intercambiar x e y).

10. Sea $K = \mathbb{Q}(\zeta)$ donde $\zeta = e^{2\pi i/5}$. Si α es un primo en $\mathbb{Z}[\zeta]$, probar que el conjunto de enteros racionales que son divisibles por α es precisamente un ideal $\langle q \rangle$ de $\mathbb{Z}[\zeta]$ para un primo racional q . Esto es, que $(\alpha\mathbb{Z}[\zeta]) \cap (\mathbb{Z}) = q\mathbb{Z}$ para algún primo racional q . (Ayuda: Demostrarlo en general).

11. Sea K un cuerpo de números con anillo de enteros \mathcal{O} . Sea $x \in \mathcal{O}$ un elemento primo, demostrar que $N_K(x) = \pm q^r$, para un primo racional q y un $r \leq [K : \mathbb{Q}]$.

12. a) Sea \mathbb{Q}_2 el conjunto formado por los números racionales a/b con $a, b \in \mathbb{Z}$ tales que b es impar.

Probar que \mathbb{Q}_2 es un dominio en el que los únicos irreducibles son 2 y sus asociados.

b) Generalizar el resultado anterior al anillo \mathbb{Q}_Σ (donde Σ es un conjunto finito de números enteros primos) formado por racionales a/b con $a, b \in \mathbb{Z}$ tales que b es primo con todos los elementos de Σ .

13. Sea $\zeta_p = e^{2\pi i/p}$, p primo impar. Demostrar que $\mathbb{Z}[\zeta_p]$ contiene a \sqrt{p} si $p \equiv 1 \pmod{4}$, y contiene a $\sqrt{-p}$ si $p \equiv 3 \pmod{4}$. (Ayuda: ¿Cuál es el discriminante de $\mathbb{Q}(\zeta_p)$?) Expresar $\sqrt{-3}$ y $\sqrt{5}$ como polinomios en el correspondiente ζ_p .

14. Utilizar las siguientes igualdades para demostrar que los anillos de enteros de los correspondientes cuerpos cuadráticos no son D.F.U.:

a) $\mathbb{Q}(\sqrt{-5})$: $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$,

b) $\mathbb{Q}(\sqrt{-6})$: $6 = 2 \cdot 3 = \sqrt{-6}\sqrt{-6}$,

c) $\mathbb{Q}(\sqrt{-10})$: $14 = 2 \cdot 7 = (2 + \sqrt{-10})(2 - \sqrt{-10})$,

d) $\mathbb{Q}(\sqrt{-13})$: $14 = 2 \cdot 7 = (1 + \sqrt{-13})(1 - \sqrt{-13})$,

e) $\mathbb{Q}(\sqrt{-14})$: $15 = 3 \cdot 5 = (1 + \sqrt{-14})(1 - \sqrt{-14})$,

f) $\mathbb{Q}(\sqrt{-15})$: $4 = 2 \cdot 2 = \left(\frac{1+\sqrt{-15}}{2}\right) \left(\frac{1-\sqrt{-15}}{2}\right)$,

g) $\mathbb{Q}(\sqrt{-17})$: $18 = 2 \cdot 3 \cdot 3 = (1 + \sqrt{-17})(1 - \sqrt{-17})$,

h) $\mathbb{Q}(\sqrt{-21})$: $22 = 2 \cdot 11 = (1 + \sqrt{-21})(1 - \sqrt{-21})$,

i) $\mathbb{Q}(\sqrt{-22})$: $26 = 2 \cdot 13 = (2 + \sqrt{-22})(2 - \sqrt{-22})$,

j) $\mathbb{Q}(\sqrt{-23})$: $6 = 2 \cdot 3 = \left(\frac{1+\sqrt{-23}}{2}\right) \left(\frac{1-\sqrt{-23}}{2}\right)$,

k) $\mathbb{Q}(\sqrt{-26})$: $27 = 3 \cdot 3 \cdot 3 = (1 + \sqrt{-26})(1 - \sqrt{-26})$,

l) $\mathbb{Q}(\sqrt{-29})$: $30 = 2 \cdot 3 \cdot 5 = (1 + \sqrt{-29})(1 - \sqrt{-29})$,

m) $\mathbb{Q}(\sqrt{-30})$: $34 = 2 \cdot 17 = (2 + \sqrt{-30})(2 - \sqrt{-30})$,

n) $\mathbb{Q}(\sqrt{10})$: $6 = 2 \cdot 3 = (4 + \sqrt{10})(4 - \sqrt{10})$,

ñ) $\mathbb{Q}(\sqrt{15})$: $10 = 2 \cdot 5 = (5 + \sqrt{15})(5 - \sqrt{15})$,

o) $\mathbb{Q}(\sqrt{26})$: $10 = 2 \cdot 5 = (6 + \sqrt{26})(6 - \sqrt{26})$,

p) $\mathbb{Q}(\sqrt{30})$: $6 = 2 \cdot 3 = (6 + \sqrt{30})(6 - \sqrt{30})$.

15. En $\mathbb{Z}[\sqrt{-5}]$ definimos los ideales

$$\begin{aligned}\mathfrak{p} &= \langle 2, 1 + \sqrt{-5} \rangle, \\ \mathfrak{q} &= \langle 3, 1 + \sqrt{-5} \rangle, \\ \mathfrak{r} &= \langle 3, 1 - \sqrt{-5} \rangle.\end{aligned}$$

- a) Demostrar que son ideales maximales, por lo tanto primos.
b) Mostrar que

$$\begin{aligned}\mathfrak{p}^2 &= \langle 2 \rangle, \\ \mathfrak{q} \cdot \mathfrak{r} &= \langle 3 \rangle, \\ \mathfrak{p} \cdot \mathfrak{q} &= \langle 1 + \sqrt{-5} \rangle, \\ \mathfrak{p} \cdot \mathfrak{r} &= \langle 1 - \sqrt{-5} \rangle.\end{aligned}$$

- c) Demostrar que las factorizaciones de 6:

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}),$$

proviene de diferentes agrupamientos de la factorización en ideales primos:

$$\langle 6 \rangle = \mathfrak{p}^2 \mathfrak{q} \cdot \mathfrak{r}.$$

- d) Calcular las normas de los ideales \mathfrak{p} , \mathfrak{q} y \mathfrak{r} .
e) Demostrar que \mathfrak{p} , \mathfrak{q} y \mathfrak{r} no son principales.
f) Demostrar que los ideales $\langle 2 \rangle$ y $\langle 3 \rangle$ están generados por elementos irreducibles pero que los ideales no son primos.

16. Encontrar todos los ideales de $\mathbb{Z}[\sqrt{-5}]$ que contienen el elemento 6.

17. Encontrar todos los ideales de $\mathbb{Z}[\sqrt{2}]$ con norma 18.

18. En $\mathbb{Z}[\sqrt{-29}]$ tenemos

$$30 = 2 \cdot 3 \cdot 5 = (1 + \sqrt{-29})(1 - \sqrt{-29}).$$

- a) Demostrar que

$$\langle 30 \rangle \subseteq \mathfrak{p} := \langle 2, 1 + \sqrt{-29} \rangle$$

y que \mathfrak{p} es un ideal primo de norma 2.

- b) Ver que $1 - \sqrt{-29} \in \mathfrak{p}$ y deducir que $\langle 30 \rangle \subseteq \mathfrak{p}^2$.
c) Calcular ideales primos $\mathfrak{q}, \mathfrak{q}', \mathfrak{r}, \mathfrak{r}'$ con normas 3 y 5 tales que

$$\langle 30 \rangle \subseteq \mathfrak{q} \cdot \mathfrak{q}' \quad \text{y} \quad \langle 30 \rangle \subseteq \mathfrak{r} \cdot \mathfrak{r}'.$$

- d) Deducir que $\mathfrak{p}^2 \cdot \mathfrak{q} \cdot \mathfrak{q}' \cdot \mathfrak{r} \cdot \mathfrak{r}' \mid \langle 30 \rangle$ y calculando normas, o de otro modo, demostrar que

$$\langle 30 \rangle = \mathfrak{p}^2 \cdot \mathfrak{q} \cdot \mathfrak{q}' \cdot \mathfrak{r} \cdot \mathfrak{r}'.$$

- e) Comentar como está esto relacionado con las dos factorizaciones:

$$\begin{aligned}\langle 30 \rangle &= \langle 2 \rangle \langle 3 \rangle \langle 5 \rangle, \\ \langle 30 \rangle &= \langle 1 + \sqrt{-29} \rangle \langle 1 - \sqrt{-29} \rangle.\end{aligned}$$

- f) Calcular todos los ideales de $\mathbb{Z}[\sqrt{-29}]$ conteniendo al elemento 30.

19. En $\mathbb{Z}[\sqrt{-5}]$ definimos, como en el ejercicio (15) los ideales

$$\begin{aligned}\mathfrak{p} &= \langle 2, 1 + \sqrt{-5} \rangle, \\ \mathfrak{q} &= \langle 3, 1 + \sqrt{-5} \rangle, \\ \mathfrak{r} &= \langle 3, 1 - \sqrt{-5} \rangle.\end{aligned}$$

Sea \mathcal{H} el grupo de clase. Demostrar que en \mathcal{H} se tiene:

$$[\mathfrak{p}]^2 = [\mathcal{O}], \quad [\mathfrak{p}][\mathfrak{q}] = [\mathcal{O}], \quad [\mathfrak{p}][\mathfrak{r}] = [\mathcal{O}],$$

y deducir que $\mathfrak{p}, \mathfrak{q}$ y \mathfrak{r} son equivalentes. Demostrar también que $\mathfrak{p}, \mathfrak{q}$ y \mathfrak{r} son equivalentes haciendo los cálculos explícitos.

20. En $\mathbb{Z}[\sqrt{-6}]$:

a) Demostrar que todo ideal es equivalente a uno de norma menor o igual que 3.

b) Comprobar que $\langle 2 \rangle = \langle 2, \sqrt{-6} \rangle^2$, $\langle 3 \rangle = \langle 3, \sqrt{-6} \rangle^2$ y concluir que los únicos ideales de normas 2 y 3 son $\langle 2, \sqrt{-6} \rangle$ y $\langle 3, \sqrt{-6} \rangle$ respectivamente.

c) Deducir de lo anterior que $h \leq 3$ y utilizar que $\langle 2 \rangle = \langle 2, \sqrt{-6} \rangle^2$, o cualquier otro modo, para probar que $h = 2$.

d) Encontrar ideales principales \mathfrak{p} y \mathfrak{q} tales que

$$\mathfrak{p} \langle 2, \sqrt{-6} \rangle = \mathfrak{q} \langle 3, \sqrt{-6} \rangle.$$

21. Para cada uno de los cuerpos siguientes, factorizar los ideales que se indican en sus respectivos anillos de enteros:

a) $\mathbb{Q}(\sqrt{3}) : \langle 2 \rangle, \langle 3 \rangle, \langle 5 \rangle, \langle 10 \rangle, \langle 30 \rangle$.

b) $\mathbb{Q}(\sqrt{5}) : \langle 2 \rangle, \langle 3 \rangle, \langle 5 \rangle, \langle 12 \rangle, \langle 25 \rangle$.

c) $\mathbb{Q}(e^{2\pi i/5}) : \langle 2 \rangle, \langle 5 \rangle, \langle 20 \rangle, \langle 50 \rangle$.

22. Encontrar la estructura del grupo de clase para cada uno de los cuerpos cuadráticos $\mathbb{Q}(\sqrt{d})$ con d libre de cuadrados y $-30 < d < 30$. La Tabla siguiente indica los valores de h (donde h^+ es el número de clase de $\mathbb{Q}(\sqrt{d})$ y h^- el de $\mathbb{Q}(\sqrt{-d})$).

d	h^+	h^-	d	h^+	h^-
1	—	1	14	1	4
2	1	1	15	2	2
3	1	1	17	1	4
5	1	2	19	1	1
6	1	2	21	1	4
7	1	1	22	1	2
10	2	2	23	1	3
11	1	1	26	2	6
13	1	2	29	1	6