Cuerpos de números

1. Sea $K = \mathbb{Q}(\theta)$ un cuerpo de números y $\alpha \in K$. Definimos:

$$m_\alpha : K \to K\,, \qquad m_\alpha(x) = \alpha \cdot x$$

Demostrar:

a) m_α es una aplicación de $\mathbb{Q}$-espacios vectoriales.

b) Si $f_{m_\alpha}(x)$ denota el polinomio característico de m_α, entonces $f_{m_\alpha}(\alpha) = 0$.

c) Si $f_\theta(x)$ denota el polinomio mínimo de θ, entonces $f_{m_\theta} = f_\theta$.

d) $\mathrm{Traza}(m_\alpha) = \mathrm{Tr}_K(\alpha)$ y $\mathrm{Det}(m_\alpha) = \mathrm{N}_K(\alpha)$.

2. Sea K un cuerpo de números y $\alpha \in K$. Demostrar:

a) Si $[K : \mathbb{Q}] = 2$, $\alpha \in \mathcal{O}_K$ si y sólo si $\mathrm{Tr}_K(\alpha), \mathrm{N}_K(\alpha) \in \mathbb{Z}$.

b) Si $[K : \mathbb{Q}] > 2$, entonces la anterior equivalencia no es cierta.

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

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

4. Sea K un cuerpo de números y $\alpha, \beta \in \mathcal{O}_K$ no nulos. Demostrar que si $\alpha \,|\, \beta$, entonces $\langle \beta \rangle \subseteq \langle \alpha \rangle$. ¿En que caso se da $\langle \beta \rangle = \langle \alpha \rangle$?

5. 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 $\mathrm{N} : \mathbb{Z}[\zeta] \to \mathbb{Z}$ es la norma en $\mathbb{Q}(\zeta)$ restringida a $\mathbb{Z}[\zeta]$, entonces

$$\mathrm{N}(a + b\,\zeta) = a^2 - a\,b + b^2.$$

c) Probar que todo elemento $\alpha \in \mathbb{Q}(\zeta)$ se puede escribir como $\alpha = u + vi$ con $u, v \in \mathbb{R}$ únicos.

d) Sea $a + b\,\zeta = u + v\,i$ con $u, v \in \mathbb{R}$ entonces $\mathrm{N}(a + b\,\zeta) = u^2 + v^2 = \|u + vi\|^2$.

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

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

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

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

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

7. 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: ¿Cúal es el discriminante de $\mathbb{Q}(\zeta_p)$?) Expresar $\sqrt{-3}$ y $\sqrt{5}$ como polinomios en el correspondiente ζ_p.

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

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

d) Calcular $\mathrm{N}_K(\alpha)$ 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.

9. Sea $\theta \in \overline{\mathbb{Q}}$ tal que $\theta^3 + \theta + 1 = 0$ y $K = \mathbb{Q}(\theta)$.

a) Calcula $\Delta[1, \theta, \theta^2]$.

b) Calcula una base entera de $\mathcal{O}_K$.

10. Sea K un cuerpo de números y $\alpha \in \mathcal{O}_K$ un primo. Demostrar que existe un primo racional $p \in \mathbb{Z}$ tal que:

a) $\alpha\mathcal{O}_K \cap \mathbb{Z} = p\mathbb{Z}$.

b) $\mathrm{N}_K(\alpha) = \pm p^r$, donde $r \leq [K : \mathbb{Q}]$.

11. Sea K un cuerpo de números y $\mathfrak{P} \subset \mathcal{O}_K$ un ideal primo. Demostrar:

a) Existe un único primo $p \in \mathbb{Z}$ tal que $p \in \mathfrak{P}$.

b) Existe un entero positivo $f \in \mathbb{Z}$ tal que $\mathrm{N}_K(\mathfrak{P}) = p^f$.

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

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

14. 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.

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

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

Sea $\mathcal{H}$ el grupo de clase de $\mathbb{Z}[\sqrt{-5}]$. 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 explicitos.

16. En el grupo de clases de $\mathbb{Z}[\sqrt{-6}]$:

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

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

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

18. 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

19. Encontrar todas las soluciones enteras de las siguientes ecuaciones diofánticas:

a) $y^2 + 4 = x^3$,

b) $y^2 + 19 = x^3$,

c) $y^2 + 3 = x^3$.