Práctica 2

Retículos y teorema de Minkowski.

1. Sea L un retículo en $\mathbb{R}^2$, $L \subset \mathbb{Z}^2$. Probar que el volumen de un dominio fundamental T es igual al número de puntos de $\mathbb{Z}^2$ que caen dentro de T.

2. (a) Graficar los retículos de $\mathbb{R}^2$ generados por los siguientes pares de vectores:
   i. $(2,1)$ y $(1,1)$
   ii. $(-1,2)$ y $(2,2)$
   iii. $(1,1)$ y $(2,3)$

   (b) Decidir si algunos de los conjuntos de vectores dados en el item anterior, generan el mismo retículo.

   (c) Mostrar, para cada retículo, un dominio fundamental T y calcular su volumen.

3. Escribir a los primos $p = 5, 13$ y 17 como suma de dos cuadrados en $\mathbb{Z}$ usando el teorema de Minkowski (ver demostración en la teórica).

4. Encontrar dos dominios fundamentales distintos para el retículo de $\mathbb{R}^3$ generado por los vectores $(0,0,1), (0,2,0)$ y $(1,1,1)$. Mostrar, por cálculo directo, que los dominios fundamentales hallados tienen el mismo volumen.

5. Probar que el volumen de un dominio fundamental T de un retículo, no depende del dominio T elegido.

Algebraicos, enteros, discriminantes, normas y trazas ...

6. Probar que para todo número algebraico γ existe un $n \in \mathbb{Z}$ tal que $n\gamma$ es *entero* algebraico.

7. Sean $n, m \in \mathbb{Z}$, libres de cuadrados y coprimos. Probar que $\sqrt{m} \notin \mathbb{Q}(\sqrt{n})$.

8. Si K es una extensión algebraica de $\mathbb{Q}$ de grado impar, entonces K no puede contener a una raiz primitiva n-ésima de la unidad ($n > 2$).

9. Decidir si los siguientes números algebraicos son *enteros* algebraicos
   (a) $\sqrt{17} + \sqrt{19}$
   (b) $(1 + \sqrt{17})/(2\sqrt{-19})$

10. Expresar $\mathbb{Q}(\sqrt{2}, \sqrt[3]{5})$ en la forma $\mathbb{Q}(\theta)$.

11. Sea $K = \mathbb{Q}(\sqrt[4]{2})$. Encontrar todos los morfismos $\sigma : K \to \mathbb{C}$. Calcular los polinomios minimal y característico de $\sqrt[4]{2}, \sqrt{2}$ y 2. Compararlos.

12. Calcular el discriminante $\Delta(1, \alpha, \alpha^2)$ relativo a $\mathbb{Q}(\alpha)$, donde α es una raíz de la cúbica $x^3 + px + q$ ($p, q \in \mathbb{Q}$).

13. Mostrar con un ejemplo que $N_K(\alpha)$ y $T_K(\alpha)$ dependen del cuerpo K.

14. Encuentre una base de enteros y el discriminante de $\mathbb{Q}(\sqrt{-7}), \mathbb{Q}(\sqrt{11})$ y $\mathbb{Q}(\sqrt{-6})$.

15. Calcular una base de enteros y el discriminante de
    (a) $\mathbb{Q}(\sqrt{2}, \sqrt{3})$
    (b) $\mathbb{Q}(\sqrt[3]{2})$

16. Sean $\alpha_1, \ldots \alpha_n$ en el anillo de enteros de un cuerpo de números K. Supongamos que $\Delta(\alpha_1, \ldots, \alpha_n) \neq 0$.
    (a) Mostrar que si $\Delta(\alpha_1, \ldots, \alpha_n)$ es libre de cuadrados, entonces $\{\alpha_1, \ldots, \alpha_n\}$ es una base de enteros de K.
    (b) Si $d \in \mathbb{Z}$ es libre de cuadrados y $d \equiv 1(4)$, entonces $\{1, \frac{1+\sqrt{d}}{2}\}$ es una base de enteros de $\mathbb{Q}(\sqrt{d})$.

17. Sean $\alpha_1, \ldots \alpha_n$ enteros algebraicos en $\mathbb{Q}(\theta)$, linealmente independientes sobre $\mathbb{Q}$, tales que
    $$\Delta(\alpha_1, \ldots, \alpha_n) = D$$
    donde D es el discriminante de $\mathbb{Q}(\theta)$.

    Probar que $\{\alpha_1, \ldots \alpha_n\}$ es una base de enteros de $\mathbb{Q}(\theta)$.

18. (a) Sea $R \subsetneq \mathcal{D}_K$ un Z-módulo maximal con base $\{\alpha_1, ..., \alpha_n\}$.
Probar que existen un primo p tal que $p^2 \mid \Delta(\alpha_1, ..., \alpha_n)$ y un elemento

$$\gamma = \frac{1}{p}\sum_{i=1}^{n} c_i\alpha_i \quad c_i \in \mathbb{Z}; 0 \leq c_i < p;$$

de K, tal que $\gamma \in \mathcal{D}_K$.

(b) Hallar una base de $\mathcal{D}_K$ para $K = \mathbb{Q}(\sqrt[3]{5})$.

19. (a) Sea f un polinomio mónico irreducible sobre un cuerpo de números K y sea $\alpha \in \mathbb{C}$ una raíz de f. Probar que

$$f'(\alpha) = \prod_{\beta \neq \alpha}(\alpha - \beta)$$

donde el producto es sobre todas las raíces $\beta \neq \alpha$ de f.

(b) Sean $K = \mathbb{Q}(\alpha)$ y $\alpha_1, ..., \alpha_n$ las conjugadas de α sobre $\mathbb{Q}$. Probar que

$$\Delta(1, \alpha, ..., \alpha^{n-1}) = \pm N_K(f'(\alpha))$$

donde f es el polinomio minimal de α sobre $\mathbb{Q}$ y el signo es $+1$ si y sólo si $n \equiv 0, 1(4)$.

20. Sea $K = Q(\sqrt{7}, \sqrt{10})$ y sea $\alpha \in K$ un entero algebraico. El objetivo de este ejercicio es probar que $\mathcal{D}_K$ no es de la forma $\mathbb{Z}[\alpha]$.

Sea f el polinomio minimal de α sobre $\mathbb{Q}$, ($f \in \mathbb{Z}[x]$). Para cada polinomio $g \in \mathbb{Z}[x]$ denotaremos $\bar{g}$ al polinomio en $\mathbb{F}_3[x]$ que se obtiene de reducir módulo 3 los coeficientes de g.

(a) Probar que $g(\alpha)$ es divisible por 3 en el anillo $\mathbb{Z}[\alpha]$ si y sólo si $\bar{g}$ es divisible por $\bar{f}$ en $\mathbb{F}_3[x]$.

(b) Suponga que $\mathcal{D}_K = \mathbb{Z}[\alpha]$.
Considere los siguientes enteros algebraicos (¿por qué son enteros?):

$$\alpha_1 = (1 + \sqrt{7})(1 + \sqrt{10})$$
$$\alpha_2 = (1 + \sqrt{7})(1 - \sqrt{10})$$
$$\alpha_3 = (1 - \sqrt{7})(1 + \sqrt{10})$$
$$\alpha_4 = (1 - \sqrt{7})(1 - \sqrt{10})$$

Probar que cualquier producto $\alpha_i\alpha_j$ $(i \neq j)$ es divisible por 3 en $\mathbb{Z}[\alpha]$, pero 3 no divide a ninguna potencia de α_i.
Sugerencia: Probar que $\alpha_i^n/3$ no es un entero algebraico. Para ésto considere la traza de α_i^n y pruebe que

$$T_K(\alpha_i^n) = (T_K(\alpha_i))^n = 4^n$$

en $\mathbb{Z}[\alpha]/3\mathbb{Z}[\alpha]$. ¿ Porqué esto implica que $T_K(\alpha_i^n) \equiv 1(3)$ en $\mathbb{Z}$?

(c) Sean $fi(x) \in \mathbb{Z}[x]$ tales que $\alpha_i = fi(\alpha)$. Probar que $\bar{f} \mid \bar{f}_i\bar{f}_j$ en $\mathbb{F}_3[x]$ (con $i \neq j$), pero que $\bar{f} \nmid \bar{f}_i^n$. Deducir que para cada i, $\bar{f}$ tiene un factor irreducible que no divide a $\bar{f}_i$ pero que divide a todos los $\bar{f}_j$ para $j \neq i$ (recuerde que $\mathbb{F}_3[x]$ es un DFU.)

(d) El item anterior implica que $\bar{f}$ tiene al menos cuatro factores irreducibles distintos en $\mathbb{F}_3[x]$. Por otro lado, f tiene grado a lo sumo 4. ¿ orqué ésto es una contradicción?

21. Sea K un cuerpo de números y sea $\alpha \in K$ un entero. Probar que α es una unidad si y sólo si $N_K(\alpha) = \pm 1$.

22. Probar que las únicas unidades de $\mathbb{Z}[\sqrt{-2}]$ son ± 1.

23. Probar que $1+\sqrt{2}$ es una unidad de $\mathbb{Z}[\sqrt{2}]$, pero no es una raíz de la unidad. Usar las potencias de $1+\sqrt{2}$ para general infinitas soluciones de la ecuación $x^2 - 2y^2 = \pm 1$.

24. Sea $K = \mathbb{Q}(\xi)$ con $\xi = e^{2\pi i/3}$. Sea $\alpha = a + b\xi \in \mathbb{Z}[\xi]$, el anillo de enteros de $\mathbb{Q}(\xi)$. Verificar que $N_K(\alpha) = a^2 - ab + b^2$ y deduzca que $\pm 1, \pm\xi$ y $\pm\xi^2$ son las únicas unidades en $\mathbb{Z}[\xi]$.

25. Sea $K = Q(\xi)$ con $\xi = e^{2\pi i/5}$.

    (a) Probar que $-(\xi^2 + \xi^3)$ es una unidad de K.

    (b) Probar que $\mathbb{Q}(\sqrt{5}) \subset K$.

    (c) Probar que en $\mathbb{Q}(\xi)$ hay infinitas unidades.

26. Probar que si $p \equiv 1(4)$, el anillo de enteros de $\mathbb{Q}(\xi_p)$, $\xi_p = e^{2\pi i/p}$ tiene infinitas unidades.

    Sugerencia: Calcular el discriminante del cuerpo y deducir que $\sqrt{p} \in \mathbb{Q}(\xi_p)$.