Teoría de Números - Práctica 1

2do. Cuatrimestre 2005

Anillo de enteros y discriminante

Por K denotaremos un cuerpo de numeros. Dado un cuerpo K, su anillo de enteros sera denotado $\mathcal{O}_K$.

(1) Sea K un cuerpo de grado 2 sobre $\mathbb{Q}$. Probar que $K = \mathbb{Q}[\sqrt{m}]$ para algún m libre de cuadrados.

(2) Sea $K = \mathbb{Q}[\sqrt{3}, \sqrt[3]{5}]$. Hallar un α tal que $K = \mathbb{Q}[\alpha]$ y hallar el polinomio minimal de α sobre $\mathbb{Q}$.

(3) Dar un ejemplo de un cuerpo K y un elemento $\alpha \in K$ tal que $\mathcal{N}(\alpha) \in \mathbb{Z}$ y $\mathrm{Tr}(\alpha) \in \mathbb{Z}$ pero α no es un entero algebraico.

(4) Sea $\mathfrak{a}$ el ideal $\mathfrak{a} = \langle 2, 1+\sqrt{-3}\rangle$ en el anillo $R = \{a + b\sqrt{-3} \,:\, a, b \in \mathbb{Z}\}$. Probar que $\mathfrak{a} \neq \langle 2\rangle$, pero $\mathfrak{a}^2 = 2\mathfrak{a}$. Concluir que R no tiene factorización única en ideales (más aún, $\mathfrak{a}$ es el único ideal primo que contiene a $\langle 2\rangle$, con lo cual $\langle 2\rangle$ no tiene factorización en ideales primos). ¿Contradice esto el teorema de factorización única demostrado?

(5) Sea $K = \mathbb{Q}[\sqrt{-2}]$.
- Probar que $\mathcal{O}_K$ es un Dominio Integro Principal (DIP).
- Hallas TODAS las soluciones enteras de la ecuación $y^2 + 2 = x^3$. (correspondiente a la curva elíptica 1728V, ¿como se explica que esta curva tiene rango 1?)

(6) Probar que $1 + \sqrt{2}$ es una unidad en $\mathbb{Z}[\sqrt{2}]$. ¿Es una raíz de la unidad? Concluir que $\mathbb{Z}[\sqrt{2}]$ tiene infinitas unidades.

(7) Sean G y H dos grupos abelianos de rango n tal que $H \subset G$. Probar que $\Delta(H) = |G/H|^2\Delta(G)$. Deducir que si $R = \sum_{i=1}^n \mathbb{Z}\alpha_i \subset \mathcal{O}_K$ es tal que $\Delta(R) = \Delta(\mathcal{O}_K)$ entonces $R = \mathcal{O}_K$.

(8) Sea $R = \sum_{i=1}^n \mathbb{Z}\alpha_i$, con $R \subsetneq \mathcal{O}_K$. Probar que existe un primo p tal que $p^2 \mid \Delta(R)$ y $\gamma = \frac{1}{p}(\sum_{i=1}^n c_i\alpha_i)$ con $c_i \in \mathbb{Z}$ y $0 \leq c_i < p$ tal que $\gamma \in \mathcal{O}_K$.

(9) Hallar una base de $\mathcal{O}_K$ para $K = \mathbb{Q}[\sqrt[3]{5}]$. (sugerencia: elegir un candidato a base para $\mathcal{O}_K$, calcular su discriminante y usar el ejercicio anterior).

(10) Si $K = \mathbb{Q}[\sqrt{2}, \sqrt{-1}]$, probar que $\mathcal{O}_K = \mathbb{Z} \oplus \mathbb{Z}\sqrt{2} \oplus \mathbb{Z}\sqrt{-1} \oplus \mathbb{Z}\frac{\sqrt{2}(1+\sqrt{-1})}{2}$.

(11) Sea $K = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$. Calcular una base para $\mathcal{O}_K$.

(12) Sea K el cuerpo bicuadrático $K = \mathbb{Q}[\sqrt{m}, \sqrt{n}]$, donde m y n son enteros libres de cuadrados coprimos. Hallar la una base de enteros de K en los casos:
- $m, n \equiv 1 \bmod 4$
- $m \equiv 1 \bmod 4, n \not\equiv 1 \bmod 4$.

(sugerencia: usar que si L, K son dos extensiones finitas de $\mathbb{Q}$ tales que $\gcd(\Delta(\mathcal{O}_L), \Delta(\mathcal{O}_K)) = 1$ entonces $\Delta(\mathcal{O}_{KL}) = \Delta(\mathcal{O}_K)^{[L:\mathbb{Q}]}\Delta(\mathcal{O}_L)^{[K:\mathbb{Q}]}$).