Teoría de Números - Práctica 1

2do. Cuatrimestre 2011

Anillo de enteros y discriminante

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

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

2. Sea K un cuerpo tal que $[K : \mathbb{Q}] = 2$. Probar que existe $d \in \mathbb{Z}$ libre de cuadrados tal que $K = \mathbb{Q}[\sqrt{d}]$. Demostrar además que si $d \neq d'$ son enteros libres de cuadrados entonces $\mathbb{Q}[\sqrt{d}] \neq \mathbb{Q}[\sqrt{d'}]$.

3. Hallar dos cuerpos de grado 3 sobre $\mathbb{Q}$ tales que el cuerpo de composición de ambos (i.e. si $K_i = \mathbb{Q}[\alpha_i]$ con $i = 1, 2$, mirar el cuerpo $\mathbb{Q}[\alpha_1, \alpha_2]$) tiene grado 6.

4. Si $\alpha \in K$, probar que existe $n \in \mathbb{N}$ tal que $n\alpha \in \mathcal{O}_K$.

5. Si $K = \mathbb{Q}[\sqrt{m}]$ es un cuerpo cuadrático (con $m \in \mathbb{Z}$ libre de cuadrados), calcular una base (como $\mathbb{Z}$-módulo) de $\mathcal{O}_K$ y calcular el discriminante en cada caso.

6. Sea $R \subsetneq \mathcal{O}_K$ un $\mathbb{Z}$-módulo maximal con base $\{\alpha_1, \ldots, \alpha_n\}$. Probar que existe un primo p tal que $p^2 \mid \delta(R)$ y un elemento $\gamma = \frac{1}{p}(\sum_{i=1}^{n} c_i\alpha_i)$ de K con $c_i \in \mathbb{Z}$ y $0 \leq c_i < p$ tal que $\gamma \in \mathcal{O}_K$.

7. 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).

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

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

10. 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:

    - $m, n \equiv 1 \bmod 4$
    - $m \equiv 1 \bmod 4, n \not\equiv 1 \bmod 4$.

11. Consideremos el cuerpo $K = \mathbb{Q}[\sqrt{7}, \sqrt{10}]$ y fijemos cualquier entero algebraico $\alpha \in K$, vamos a probar que $\mathbb{Z}[\alpha] \subsetneq \mathcal{O}_K$. Consideremos el cuerpo $\mathbb{F}_3 = \mathbb{Z}/3\mathbb{Z}$ y la función reducción

$$^{-}: \mathbb{Z}[x] \to \mathbb{F}_3[x], \qquad f(x) \mapsto \bar{f}(x) := f(x) \pmod 3$$

(a) Probar que $g(\alpha)$ es divisible por 3 en $\mathbb{Z}[\alpha]$ (o sea $g(\alpha) = 3h(\alpha)$ con $h[x] \in \mathbb{Z}[x]$) si y sólo si $\bar{g}(x)$ es dividible por $\overline{m_\alpha}(x)$ en $\mathbb{F}_3[x]$.

(b) Consideremos los siguientes enteros algebraicos (¿por qué son enteros?)

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

Probar que los productos $\alpha_i\alpha_j$ (con $i \neq j$) son divisibles por 3 en $\mathcal{O}_K$, pero 3 no divide a ninguna potencia de α_i (i.e. $\alpha_i^r/3$ no es entero algebraico para ningún r). Sugerencia: considerar la traza de tal elemento. ¿Cuánto vale la traza de α_i?

(c) Supongamos que $\mathcal{O}_K = \mathbb{Z}[\alpha]$, luego existen polinomios $f_i(x) \in \mathbb{Z}[x]$ tales que $\alpha_i = f_i(\alpha)$. Probar que $\bar{m_\alpha}(x) \mid \bar{f}_i(x)\bar{f}_j(x)$ en $\mathbb{F}_3[x]$ (con $i \neq j$), pero $\bar{m_\alpha}(x) \nmid \bar{f}_i^{\,r}(x)$. Como $\mathbb{F}_3[x]$ es euclídeo (¿por qué?), concluir que para cada $1 \leq i \leq 4$, $\bar{m_\alpha}(x)$ debe tener un factor irreducible en $\mathbb{F}_3[x]$ que no divide a $\bar{f}_i(x)$ y todos los otros factores irreducibles sí lo dividen.

(d) El ítem anterior implica que $\bar{m_\alpha}(x)$ debe tener al menos cuatro factores irreducibles en $\mathbb{F}_3[x]$, pero como $m_\alpha(x)$ tiene grado 4, debe tener exáctamente cuatro factores irreducibles en $\mathbb{F}_3[x]$, ¿puede pasar esto?