Teoría Algebraica de Números - Práctica 3

2do. Cuatrimestre 2020

Anillos de Enteros y Discriminante

En esta práctica la letra K denotará un cuerpo de números, y $\mathcal{O}_K$ denotará su anillo de enteros. Por $\mathcal{D}(K)$ denotamos el discriminante de $\mathcal{O}_K$.

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

2. Sea $R \subsetneq \mathcal{O}_K$ un $\mathbb{Z}$-módulo de rango $n = [K : \mathbb{Q}]$ con base $\{\alpha_1, \ldots, \alpha_n\}$. Probar que existe un primo p tal que $p^2 \mid \mathcal{D}(R)$ 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 $\gamma \in \mathcal{O}_K$. Dar a partir de este hecho un algoritmo para calcular el anillo de enteros de K.

3. 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).

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

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

6. El objetivo de este ejercicio es probar el siguiente resultado: sean L, K dos extensiones de cuerpos de $\mathbb{Q}$, y sea $L \cdot K$ su composición. ¿Existe alguna relación entre $\mathcal{O}_K$, $\mathcal{O}_L$, $\mathcal{O}_{KL}$? Supongamos que $L \cap K = \mathbb{Q}$, con lo cual $[K \cdot L : \mathbb{Q}] = [K : \mathbb{Q}] \cdot [L : \mathbb{Q}]$ (por el ejercicio 6 de la práctica 2). Denotemos por $n = [K : \mathbb{Q}]$ y $m = [L : \mathbb{Q}]$.

   (a) Probar que si $\mathcal{O}_K = \langle \alpha_1, \ldots, \alpha_n \rangle_{\mathbb{Z}}$ y $\mathcal{O}_L = \langle \beta_1, \ldots, \beta_m \rangle_{\mathbb{Z}}$ entonces $\mathcal{O}_L \cdot \mathcal{O}_K = \langle \alpha_i\beta_j \rangle_{\mathbb{Z}} \subset \mathcal{O}_{LK}$ es un $\mathbb{Z}$-módulo de rango $n \cdot m$.

   (b) Supongamos que $\gamma \in \mathcal{O}_{LK} \setminus \mathcal{O}_L \cdot \mathcal{O}_K$, luego

   $$\gamma = \sum_{i,j} \frac{a_{ij}}{d} \alpha_i\beta_j,$$

   para algún $d \in \mathbb{Z}$. Todo $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ se puede extender (de forma única) a $\mathrm{Gal}(L \cdot K/L)$ pues ambos grupos son isomorfos (ejercicio 6 de la práctica 2). Luego

   $$\sigma(\gamma) = \sum_{i,j} \frac{a_{ij}}{d} \sigma(\alpha_i)\beta_j.$$

   Para $1 \leq i \leq n$ denotemor por $x_i = \sum_{j=1}^{m} \frac{a_{ij}}{d}\beta_j$ con lo cual $\sigma(\gamma) = \sum_i \sigma(\alpha_i)x_i$. Si $\{\sigma_1, \ldots, \sigma_n\} = \mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C})$ entonces los elementos x_i satisfacen un sistema de n-ecuaciones con n-incógnitas. Probar (usando la regla de Cramer) que $\mathcal{D}(K)x_i$ es un entero algebraico.

   (c) Deducir del hecho que $\{\beta_1, \ldots, \beta_m\}$ es una base de anillo de enteros de L que $d \mid \mathcal{D}(K)$. Probar que $\mathcal{O}_{LK} \subset \frac{1}{\gcd(\mathcal{D}(L), \mathcal{D}(K))}\mathcal{O}_L \cdot \mathcal{O}_K$.

7. 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:

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

8. Consideremos el cuerpo $K = \mathbb{Q}[\sqrt{7}, \sqrt{10}]$ y fijemos cualquier entero algebraico $\alpha \in K$. Probaremos que $\mathbb{Z}[\alpha] \subsetneq \mathcal{O}_K$ (con lo cual $\mathcal{O}_K$ no es monogénica). Consideremos el cuerpo $\mathbb{F}_3 = \mathbb{Z}/3\mathbb{Z}$ y la función reducción

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

   (a) Sea $g(x) \in \mathbb{Z}[x]$ un polinomio cualquiera. 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 módulo 3.

   (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 $\overline{m_\alpha}(x) \mid \bar{f}_i(x)\bar{f}_j(x)$ en $\mathbb{F}_3[x]$ (con $i \neq j$), pero $\overline{m_\alpha}(x) \nmid \bar{f}_i{}^r(x)$.
   En particular, $\bar{f}_i \neq \bar{f}_j$ si $i \neq j$. Como $\mathbb{F}_3[x]$ es Euclídeo, concluir que para cada $1 \leq i \leq 4$, $\overline{m_\alpha}(x)$ debe tener al menos un factor irreducible en $\mathbb{F}_3[x]$ que no divide a $\bar{f}_i(x)$ pero si a los otros polinomios.

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

9. $(*)$ Sean $K \subset L \subset M$ extensiones de cuerpos de números con $[M : L] = n$ y $[L : K] = m$.

   (a) Probar que si $\{\alpha_1, \ldots, \alpha_n\}$ son elementos de M, tiene sentido definir su dicriminante $\mathcal{D}(\alpha_1, \ldots, \alpha_n)$ como lo hemos hecho en la teórica, y valen las mismas propiedades (o sea no es preciso suponer $L = \mathbb{Q}$).

(b) Probar que si $\{\alpha_1, \ldots, \alpha_n\}$ son elementos de M y $\{\beta_1, \ldots, \beta_m\}$ son elementos de L entonces vale la siguiente fórmula:

$$\mathcal{D}_{M/K}(\alpha_1\beta_1, \ldots, \alpha_n\beta_m) = \mathcal{D}_{L/K}(\beta_1, \ldots, \beta_m)^n \cdot \mathcal{N}_{L/K}(\mathcal{D}_{M/L}(\alpha_1, \ldots, \alpha_n)).$$

(c) Deducir que si L y K son extensiones de $\mathbb{Q}$ tales que $L \cap K = \mathbb{Q}$ y $\gcd(\mathcal{D}(L), \mathcal{D}(K)) = 1$ entonces $\mathcal{D}(K \cdot L) = \mathcal{D}(K)^{[L:\mathbb{Q}]}\mathcal{D}(L)^{[K:\mathbb{Q}]}$.