Teoría Algebraica de Números - Práctica 4

2do. Cuatrimestre 2020

Anillos de enteros e ideales primos

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. Sean $p_1, \ldots, p_r$ primos distintos de $\mathbb{Z}$. Probar que $[\mathbb{Q}[\sqrt{p_1}, \ldots, \sqrt{p_r}] : \mathbb{Q}] = 2^r$, y $\mathrm{Gal}(\mathbb{Q}[\sqrt{p_1}, \ldots, \sqrt{p_r}]/\mathbb{Q}) \simeq (\mathbb{Z}/2)^r$.

2. Sean m y n dos enteros distintos, libres de cuadrados y distintos de 1. Sean $K_1 = \mathbb{Q}(\sqrt{m})$, $K_2 = \mathbb{Q}(\sqrt{n})$ y $K = \mathbb{Q}[\sqrt{m}, \sqrt{n}]$. Luego $K/\mathbb{Q}$ es una extensión Galoisiana de $\mathbb{Q}$ con grupo de Galois $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. En particular, existen tres subextensiones de K de grado dos sobre $\mathbb{Q}$ (¿cual es la tercera?). Tomemos p un primo de $\mathbb{Z}$.

   - Supongamos que p ramifica en $K_i/\mathbb{Q}$, $i = 1, 2$. ¿Que pasa con p en $\mathcal{O}_K$? Dar un ejemplo.
   - Supongamos que p se parte en $K_i/\mathbb{Q}$, ¿que pasa con p en $\mathcal{O}_K$? Dar un ejemplo.
   - Supongamos que p es inerte en cada subextensión cuadrática de $\mathcal{O}_K$, ¿que pasa con p en $\mathcal{O}_K$? ¿Puede esto suceder?

3. Probar que todo polinomio $f(x) \in \mathbb{Z}[x]$ tiene una raíz módulo p para infinitos primos p (Sugerencia si $f(0) = 1$, mirar $f(n!)$, y hacer algo parecido en el caso general). Deducir las siguientes propiedades:

   - Si $K/\mathbb{Q}$ es un cuerpo de números, entonces existen infinitos primos $\mathcal{P} \subset \mathcal{O}_K$ arriba de un primo $p \in \mathbb{Z}$ tales que $f(\mathcal{P}|p) = 1$.
   - Probar que si K, L son cuerpos de números con $K \subset L$, entonces existen infinitos primos de K que se parte completamente en L, o sea primos $\mathcal{P}_K \subset \mathcal{O}_K$ tales que para todo primo $\mathcal{P}_L \subset \mathcal{O}_L$ arriba de $\mathcal{P}_K$ se tiene que $f(\mathcal{P}_L|\mathcal{P}_K) = 1$ (recordar que si $K \subset L$, existe siempre una estensión M arriba de L que es Galois sobre K; en el caso de extensiones de $\mathbb{Q}$, si $L = K[\alpha]$, M se obtiene adjuntándole a L todas las raíces del minimal de α).
   - Deducir que si $f(x) \in \mathbb{Z}[x]$ existen infinitos primos p tales que $\bar{f} \in \mathbb{F}_p[x]$ tiene todas sus raíces en $\mathbb{F}_p$.

4. Probar que si K es una extensión Galois de $\mathbb{Q}$ entonces $\mathbb{Q}[\sqrt{\mathcal{D}(\mathcal{O}_K)}] \subset K$. Deducir que una extensión de Galois de orden impar tiene discriminante un cuadrado perfecto. ¿Qué pasa si $K/\mathbb{Q}$ no es Galois?

5. Probar con un argumento similar al de la teórica que

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{si } p \equiv \pm 1 \pmod 8 \\ -1 & \text{si } p \equiv \pm 3 \pmod 8 \end{cases}$$

6. Sea K la extensión de $\mathbb{Q}$ dada por adjuntar una raíz del polynomio $x^3 + x^2 - 2x - 1$. Probar que $K/\mathbb{Q}$ ramifica solamente en el primo $p = 7$, y dar una descripción explícita de como factoriza un primo $q \neq 7$ en la extensión $K/\mathbb{Q}$.

7. Recordar que si R es un dominio íntegro, y S es un conjunto multiplicativo (o sea cerrado para el producto) que no contiene el 0, entonces la *localización* de R en S es el conjunto

$$R_S := \left\{ \frac{a}{b} \ : \ a \in R, b \in S \right\} / \sim,$$

donde $\sim$ es la relación de equivalencia dada por $\frac{a}{b} \sim \frac{c}{d}$ si $ad = bc$. En el caso particular en que K es un cuerpo, y $R = \mathcal{O}_K$, R_S es un subanillo de K.

- Probar que si $\mathfrak{p} \subset \mathcal{O}_K$ es un ideal primo no nulo, y tomamos $S = \mathcal{O}_K \setminus \mathfrak{p}$ (ver que dicho conjunto es multiplicativo) entonces $(\mathcal{O}_K)_{(\mathfrak{p})} := (\mathcal{O}_K)_S$ es un dominio de Dedeking.
- Probar que $(\mathcal{O}_K)_{(\mathfrak{p})}$ es un DIP (o sea todo ideal es principal).
- Probar que si L/K es una extensión finita, y $\mathfrak{p} \subset \mathcal{O}_K$ es un ideal primo no nulo, entonces $(\mathcal{O}_K)_{(\mathfrak{p})} \cdot \mathcal{O}_L$ es un dominio de Dedekind (notar que este anillo no es en general una localización). ¿Quiénes son todos los ideales primos?

8. Sea L/K una extensión de cuerpos de números de grado n. Definimos el *discriminante relativo* de L/K como el ideal

$$\mathcal{D}(L/K) = \langle \mathcal{D}(\alpha_1, \ldots, \alpha_n) \ : \ \alpha_i \in \mathcal{O}_L \rangle_{\mathcal{O}_K}.$$

(a) Probar que $\mathcal{D}(L/K)$ es un ideal no nulo de $\mathcal{O}_K$.

(b) Probar que si $K = \mathbb{Q}$ entonces el discriminante relativo de $L/\mathbb{Q}$ es el ideal de $\mathbb{Z}$ generado por $\mathcal{D}(L/\mathbb{Q})$.

(c) Probar que $\mathfrak{p}$ ramifica en L/K si y sólo si $\mathfrak{p} \mid \mathcal{D}(L/K)$. (sugerencia: comparar el discriminante de la extensión $\mathcal{O}_L/\mathcal{O}_K$ con el de la extensión $(\mathcal{O}_K)_{(\mathfrak{p})} \cdot \mathcal{O}_L/(\mathcal{O}_K)_{(\mathfrak{p})}$, y como factoriza el ideal generado por $\mathfrak{p}$ en ambas. Luego convencerse de que la demostración dada en la teórica para una extensión $K/\mathbb{Q}$ se generaliza trivialmente a cualquier caso donde el dominio de Dedekind en la extensión de abajo es un DIP).