Teoría Algebraica de Números - Práctica

2do. Cuatrimestre 2020

Grupo de Clases, Teorema de Minkowski y Aplicaciones.

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

1. Consideremos el grupo $\mathcal{F}(K)$ el grupo de ideales fraccionarios (no nulos) de K. Definimos en $\mathcal{F}(K)$ la siguiente relación de equivalencia: dados $\mathfrak{a}, \mathfrak{b} \in \mathcal{F}(K)$, $\mathfrak{a} \sim \mathfrak{b}$ si y sólo si existe $\alpha \in K^\times$ tal que $\mathfrak{a} = \mathfrak{b}\alpha$. Probar que esto es una relación de equivalencia, que $\mathcal{F}(K)/\sim$ es un grupo abeliano y es isomorfo a $\mathrm{Cl}(\mathcal{O}_K)$ (donde $\mathrm{Cl}(\mathcal{O}_K)$ denota el grupo de clases de $\mathcal{O}_K$).

2. Probar que:

   (a) $\mathrm{Cl}(\mathbb{Q}[\sqrt{10}]) \cong \mathbb{Z}/2\mathbb{Z}$.

   (b) $\mathbb{Q}[\sqrt{6}]$ es un DIP.

   (c) $\mathrm{Cl}(\mathbb{Q}[\sqrt{223}]) \cong \mathbb{Z}/3\mathbb{Z}$.

   (d) $\mathrm{Cl}(\mathbb{Q}[\sqrt{-14}]) \cong \mathbb{Z}/4\mathbb{Z}$.

   (e) $\mathrm{Cl}(\mathbb{Q}[\sqrt{-21}]) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

3. Probar que el cuerpo $\mathbb{Q}[\sqrt{-6}]$ tiene grupo de clases isomorfo a $\mathbb{Z}/2\mathbb{Z}$, y que el cuerpo $\mathbb{Q}[\sqrt{-6}, \sqrt{2}]$ es un DIP.

4. En este ejercicio daremos una manera (no muy efectiva) de construir unidades fundamentales para cuerpos cuadráticos reales $\mathbb{Q}[\sqrt{d}]$ (con d libre de cuadrados). Consideremos los casos según el discriminante d:

   - Supongamos que $d \equiv 2, 3 \pmod 4$. Consideremos los números $db^2 \pm 1$ con $b \in \mathbb{N}$ y tomemos el b mas pequeño tal que $db^2 \pm 1$ es un cuadrado perfecto, digamos $db^2 \pm 1 = a^2$ con $a > 0$ (sabemos que tal elemento existe por el Teorema de las Unidades). Luego el elemento $\eta = a + b\sqrt{d}$ es una unidad. Probar que η es una unidad fundamental (i.e. toda unidad es del tipo $\pm\eta^r$ con $r \in \mathbb{Z}$).
   - Dar un método similar para el caso en que $d \equiv 1 \pmod 4$.

5. Encontrar una unidad fundamental para el cuerpo $K = \mathbb{Q}(\sqrt{6})$. La búsqueda anterior puede ser muy tediosa, por ejemplo, la unidad fundamental de $\mathbb{Q}(\sqrt{94})$ es $2143295 + 221064\sqrt{94}$.

6. Probar que si $n \in \mathbb{N}$ entonces $\frac{n^n}{n!} \geq 2^n - 1$. Deducir que toda extensión de $\mathbb{Q}$ tiene un primo ramificado.

7. Veamos una aplicación del Teorema de Minkowski para demostrar el Teorema de Lagrange: todo número natural es suma de 4 cuadrados. Por la fórmula:

$$\begin{aligned}(x_1^2+x_2^2+x_3^2+x_4^2)(y_1^2+y_2^2+y_3^2+y_4^2) &= (x_1y_1+x_2y_2+x_3y_3+x_4y_4)^2 \\ &\quad +(x_1y_2-x_2y_1+x_3y_4-x_4y_3)^2 \\ &\quad +(x_1y_3-x_2y_4-x_3y_1+x_4y_2)^2 \\ &\quad +(x_1y_4+x_2y_3-x_3y_2-x_4y_1)^2,\end{aligned}$$

basta probar que todo primo es suma de 4 cuadrados. Tomemos p un primo impar (claramente 2 es suma de 4 cuadrados).

- Probar que existen enteros r, s tales que $r^2+s^2+1 \equiv 0 \pmod{p}$.
- Consideremos el retículo

  $$L = \langle (p,0,0,0), (0,p,0,0), (r,s,1,0), (s,-r,0,1) \rangle.$$

  Verificar que si $\mathbf{v} \in L$ entonces $v_1^2+v_2^2+v_3^2+v_4^2 \equiv 0 \pmod{p}$.
- Tomemos $B = \left\{ (x_1,x_2,x_3,x_4) \in \mathbb{R}^4 \ : \ \sum_{i=1}^4 x_i^2 < 2p \right\}$ la bola de radio $\sqrt{2p}$. Probar que B satisface las condiciones del Teorema de Minkowski con lo existe $\mathbf{v} \neq \mathbf{0}$ tal que $\mathbf{v} \in L \cap B$. Probar que $\mathbf{v}$ sirve.