Teoría de Números - Práctica 4

2do. Cuatrimestre 2011

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. ¿Es Galoisiana la extensión de $\mathbb{Q}$ dada por adjuntar una raíz del polinomio $x^3 + x + 1$?

2. Consideremos el grupo $\mathfrak{F}(K)$ el grupo de ideales fraccionarios (no nulos) de K. Definimos en $\mathfrak{F}(K)$ la siguiente relación de equivalencia: dados $\mathfrak{a}, \mathfrak{b} \in \mathfrak{F}(K)$, $\mathfrak{a} \sim \mathfrak{b}$ 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 $\mathfrak{F}(K)/\sim$ 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 $\mathcal{O}_K$).

3. Dado K un cuerpo de números, probar que existe un cuerpo de números L que contienen a K tal que todo ideal de K se vuelve principal en L. ¿Tiene L grupo de clases trivial?

4. En este ejercicio probaremos el segundo caso del Teorema de Fermat para primos regulares. La demostración es similar al primer caso. Por ξ_p denotamos una raíz p-ésima primitiva de 1. Supongamos que (x_0, y_0, z_0) es una solución primitiva (i.e. coprimos dos a dos) de $x^p + y^p = z^p$ con p un primo regular. Denotemos por $\mathcal{P}$ al ideal $\mathcal{P} = (1 - \xi_p)$.

   (a) Probar que sin pérdida de generalidad podemos suponer que $p \mid z_0$ pero $p \nmid x_0 y_0$. En tal caso probar que (como ideales)

   $$(x_0 + y_0\xi_p^i : x_0 + y_0\xi_p^j) = \mathcal{P}$$

   para todo par de elementos i, j tales que $i \not\equiv j \pmod{p}$.

   (b) Deducir del ítem anterior que en la factorización de $x_0^p + y_0^p$ todos los factores $x_0 + \xi_p^i y_0$ son divisibles por $\mathcal{P}$ a potencia uno salvo quizás uno de ellos. Más aún, probar que si $\mathcal{P}^2$ divide a algún elemento, necesariamente es $(x_0 + y_0)$.

   (c) Como en el primer caso, usando que p es regular, probar que si $p \nmid i$ entonces

   $$\frac{x_0 + \xi_p^i y_0}{1 - \xi_p} \equiv a_i u_i \pmod{p}$$

   donde $a_i \in \mathbb{Z}$ y u_i es una unidad.

   (d) Siguiendo las cuentas del primer caso, concluir que $2x_0^p \equiv 0 \pmod{p}$ con lo cual $p = 2$.

5. Probar que:

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

- $\mathbb{Q}[\sqrt{6}]$ es un DIP.
- $\mathrm{Cl}(\mathbb{Q}[\sqrt{223}]) \cong \mathbb{Z}/3\mathbb{Z}$.
- $\mathrm{Cl}(\mathbb{Q}[\sqrt{-14}]) \cong \mathbb{Z}/4\mathbb{Z}$.
- $\mathrm{Cl}(\mathbb{Q}[\sqrt{-21}]) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

6. 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.

7. 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.

8. Probar que todo retículo es discreto (i.e. que no hay puntos de acumulación o equivalentemente que toda sucesión de Cauchy de elementos del retículo es constante a partir de un lugar).

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

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

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.