Teoría de Números - Práctica 3
2do. Cuatrimestre 2005
Factorización en extensiones y Teoría de Galois

(1) Sea $K = \mathbb{Q}[\alpha]$ donde α es ua raíz del polinomio $x^3 - x^2 - 2x + 1$.
- Calcular el anillo de enteros y el grupo de clases de $\mathcal{O}_K$. Calcular como factorizan los primos $p \leq 100$.
- Probar que $K/\mathbb{Q}$ es Galois (luego su grupo de Galois es isomorfo a $\mathbb{Z}/3\mathbb{Z}$). Usar este hecho para verificar las factorizaciones obtenidas. Notar que en este ejemplo sucede lo mismo que en extensiones cuadráticas, a saber los primos no ramificados son inertes o se parten completamente.

(2) Sea K un cuerpo de números y E su clausura normal. Probar que $\mathbb{Q}[\sqrt{\mathrm{D}_K}] \subset E$. Deducir que una extensión de $\mathbb{Q}$ con grupo de Galois cíclico de grado 3 tiene discriminante un cuadrado perfecto.

(3) Sea K un cuerpo de números. Un primo $p \in \mathbb{Z}$ ramifica completamente si $p\mathcal{O}_K = \mathfrak{q}^n$, donde $n = [K : \mathbb{Q}]$.
- Probar que si p es totalmente ramificado en $\mathcal{O}_K$ entonces lo es en cualquier cuerpo intermedio, o sea si $\mathbb{Q} \subset L \subset K$ entonces p es totalmente ramificado en $\mathcal{O}_L$.
- Probar que si K,K' son dos extensiones de $\mathbb{Q}$ y $p \in \mathbb{Z}$ es tal que p es totalmente ramificado en K y es no ramificado en K' entonces $K \cap K' = \mathbb{Q}$.
- Utilizando el item anterior, probar que si $p_1, \ldots, p_r$ son primos distintos de $\mathbb{Z}$ entonces $\mathbb{Q}[\sqrt{p_1}, \ldots, \sqrt{p_r}]$ es una extensión de grado 2^r de $\mathbb{Q}$.

(4) Sea K una extensión normal de $\mathbb{Q}$ con grupo de Galois G. Probar que si $p \in \mathbb{Z}$ es inerte en $\mathcal{O}_K$ entonces G es cíclico.

(5) Sean m y n dos enteros libres de cuadrados y $\neq 1$. El cuerpo bicuadrático $K = \mathbb{Q}[\sqrt{m}, \sqrt{n}]$ es una extensión normal de $\mathbb{Q}$ con grupo de Galois $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. Luego hay tres subextensiones de grado dos de $\mathbb{Q}$ (¿cual es la tercera?). Sea p un primo de $\mathbb{Z}$.
- Supongamos que p ramifica en cada subextensión cuadrática de $\mathcal{O}_K$. ¿Que pasa con p en $\mathcal{O}_K$? Dar un ejemplo.
- Supongamos que p se parte en cada subextensión cuadrática de $\mathcal{O}_K$, ¿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?