TEORIA DE NUMEROS

Ejercicio 5 $*$ 1er. Cuatrimestre 2003

A entregar para el martes 17 de junio

El objetivo del ejercicio es probar que (el anillo de enteros $\mathcal{D}_K := \mathbb{Z}[\xi_{31}]$ de) $K := \mathbb{Q}[\xi_{31}]$, donde ξ_{31} es una raíz primitiva de orden 31 de la unidad, no es un dominio de factorización única.

- Determinar una extensión cuadrática E de $\mathbb{Q}$ con $E \subset K$. Factorizar el ideal $2\,\mathcal{D}_E$ en producto de ideales primos de $\mathcal{D}_E$, y determinar el orden de esos primos en el grupo de clases $\mathcal{H}(E)$.
- Determinar la forma de la factorización en ideales primos de $2\,\mathcal{D}_K$ en $\mathcal{D}_K$, cantidad de primos, ramificación y grados residuales. Deducir la forma de la la factorización en ideales primos de $\mathcal{Q}\,\mathcal{D}_K$ en $\mathcal{D}_K$, donde $\mathcal{Q}$ es un ideal primo de $\mathcal{D}_E$ que contiene al 2 (verificar que es del tipo $\mathcal{Q}\,\mathcal{D}_K = \mathcal{P}_1 \ldots \mathcal{P}_r$, con $\mathcal{P}_i \neq \mathcal{P}_j$ para $i \neq j$, y determinar r).
- Para primos $\mathcal{P}_i$ y $\mathcal{Q}$ como arriba, se define la "norma" relativa:

$$\widetilde{N}_{K/E}(\mathcal{P}_i) := \mathcal{Q}^{n/r} \ \subset\ \mathcal{D}_E,$$

  donde $n = [K : E]$ (observar que efectivamente $r|n$).
  (i) Calcular $\widetilde{N}_{K/E}(\mathcal{P})$ para cada ideal primo $\mathcal{P}$ de $\mathcal{D}_K$ que contiene al 2.
  (ii) Probar que en este caso,

$$\widetilde{N}_{K/E}(\mathcal{P}) = \mathcal{D}_E \cap \prod_{\sigma \in G(K/E)} \sigma(\mathcal{P}),$$

  donde $G(K/E) := \{\, \sigma : K \to K \text{ tal que } \sigma|_E = \mathrm{Id}_E \,\}$.
  (iii) Mostrar que entonces, si $\mathcal{P}$ es un ideal principal en $\mathcal{D}_K$, su "norma" relativa es un ideal principal en $\mathcal{D}_E$ (los que no hicieron Algebra III (o no la están haciendo) pueden asumir que si $\alpha \in K$, entonces $\prod_{\sigma \in G(K/E)} \sigma(\alpha) \in E$).
- Mostrar que un ideal primo en $\mathcal{D}_K$ que contiene a 2 no puede ser principal y concluir.