Práctica 4

Notación: A lo largo de esta práctica $[\cdot]$ denotará la clase de un ideal, y h el número de clases de ideales (class number).

1. Hallar la inversa de los siguientes ideales en los anillos indicados:

   (a) $(1+i)$ en $\mathbb{Z}[i]$,

   (b) $(3, 1+2\sqrt{-5})$ en $\mathbb{Z}[\sqrt{-5}]$.

2. Sean $K = \mathbb{Q}(\sqrt{-5})$ y $\mathcal{D}$ su anillo de enteros. Considere los siguientes ideales primos de $\mathcal{D}$:
$$\mathcal{P} = (2, 1+\sqrt{-5}), \quad \mathcal{Q} = (3, 1+\sqrt{-5}), \quad \mathcal{R} = (3, 1-\sqrt{-5}).$$
   Pruebe que
$$[\mathcal{P}^2] = [\mathcal{D}], \quad [\mathcal{P}][\mathcal{Q}] = [\mathcal{D}], \quad [\mathcal{P}][\mathcal{R}] = [\mathcal{D}].$$
   Probar que $h = 2$.

3. Probar que en $\mathbb{Q}(\sqrt{-6})$, todo ideal es equivalente a uno de norma a lo sumo 3. Verificar que
$$(2) = (2, \sqrt{-6})^2, \quad (3) = (3, \sqrt{-6})^2$$
   y probar que $h = 2$.

   Encuentre ideales principales (γ) y (δ) en $\mathbb{Z}[\sqrt{-6}]$ tales que
$$(\gamma)(2, \sqrt{-6}) = (\delta)(3, \sqrt{-6}).$$

4. Encuentre h para cada $\mathbb{Q}(\sqrt{d})$, con $d \in \mathbb{Z}$ libre de cuadrados y $-10 < d < 10$.

5. Probar que el anillo de enteros de $K = \mathbb{Q}(\sqrt{2}, \sqrt{-3})$ es un dominio principal. Notar que K contiene a $\mathbb{Q}(\sqrt{-6})$ cuyo número de clases es $h = 2$.

6. Sean K un cuerpo de números y $\mathcal{D}$ su anillo de enteros. Suponga que el número de clases $h = 2$.

   Probar que si $\pi \in \mathcal{D}$ es irreducible y (π) no es primo, entonces
$$(\pi) = \mathcal{P}_1\mathcal{P}_2$$
   con $\mathcal{P}_i$ ideales primos no necesariamente distintos.

7. Sea $K = \mathbb{Q}(\sqrt{3})$. Factorizar los ideales principales (2), (3) y (5) en el anillo de enteros $\mathcal{D}$ de K.

8. Factorizar los ideales principales (2), (3) y (5) en el anillo de enteros $\mathcal{D}$ de $\mathbb{Q}(\sqrt{5})$.

9. Factorizar los ideales (2) y (5) en $\mathbb{Z}[\xi_5]$, donde ξ_5 denota una raíz quinta primitiva de la unidad.

10. Sean $K \subset F \subset E$ cuerpos de números. Probar que los índices de ramificación y de inercia son multiplicativos en torres de extensiones: si $\mathcal{P} \subset \mathcal{Q} \subset \mathcal{L}$ son ideales primos de $\mathcal{D}_K$, $\mathcal{D}_F$ y $\mathcal{D}_E$ respectivamente, entonces:
$$e(\mathcal{L} \mid \mathcal{P}) = e(\mathcal{L} \mid \mathcal{Q})e(\mathcal{Q} \mid \mathcal{P}),$$
$$f(\mathcal{L} \mid \mathcal{P}) = f(\mathcal{L} \mid \mathcal{Q})f(\mathcal{Q} \mid \mathcal{P}).$$

11. Sean $m \neq n$ enteros libres de cuadrados > 1, $K = \mathbb{Q}(\sqrt{m}, \sqrt{n})$ y $\mathcal{D}_K$ su anillo de enteros. Observar que K tiene tres subextensiones cuadráticas distintas, ¿cuáles son? Sea $p \in \mathbb{Z}$ primo.
    (a) Si p ramifica en cada subextensión cuadrática de K, ¿qué pasa con p en $\mathcal{D}_K$? Dar un ejemplo.
    (b) Si p se parte en cada subextensión cuadrática de K, ¿qué pasa con p en $\mathcal{D}_K$? Dar un ejemplo.
    (c) Si p es inerte en cada subextensión cuadrática de K, ¿qué pasa con p en $\mathcal{D}_K$? ¿Puede dar un ejemplo?

12. Sea E una extensión normal de grado n, de un cuerpo de números K. Sea $\mathcal{P}$ un ideal primo de K y sean $\mathcal{Q}_1$, $\mathcal{Q}_2$ ideales primos de E arriba de $\mathcal{P}$. Probar que:
    (a) existe $\sigma \in \mathrm{Gal}(E/K)$, tal que $\sigma(\mathcal{Q}_1) = \mathcal{Q}_2$
    (b) $e(\mathcal{Q}_1 \mid \mathcal{P}) = e(\mathcal{Q}_2 \mid \mathcal{P})$ y $f(\mathcal{Q}_1 \mid \mathcal{P}) = f(\mathcal{Q}_2 \mid \mathcal{P})$.
    (c) Todos los índices de ramificación y de inercia son iguales y se tiene la relación $efr = n$, donde r es la cantidad de ideales primos distintos arriba de $\mathcal{P}$.

13. Sea K un cuerpo de números de grado n. Probar que
$$|\Delta| \geq \left(\frac{\pi}{4}\right)^n \left(\frac{n^n}{n!}\right)^2.$$

14. Sea K un cuerpo cuadrático real. Probar que si en K hay un elemento de norma -1, entonces ningún primo en $\mathbb{Z}$ congruente con 3 módulo 4 ramifica en K.

15. Probar que el grupo de unidades de un cuerpo de números K es finito si y sólo si K es $\mathbb{Q}$ o un cuerpo cuadrático imaginario.

16. Si K es un cuerpo de números de grado impar, K contiene sólo dos raíces de la unidad.