Revisión Domiciliaria

1. Sea $a \in \mathbb{Z}$ un no cuadrado. En el siguiente ejercicio se prueba que existen infinitos primos p tales que a es un no residuo cuadrático módulo p.

   Observar que se puede suponer que a es libre de cuadrados.

   (a) Suponga primero que a es divisible por algún primo impar q y sea $\{q = q_1, ..., q_n\}$ el conjunto de primos impares que dividen a a.

   Sea $P = \{p_1, p_2, ..., p_k\}$ un conjunto cualquiera de primos impares que no dividen a a. Sea s un no residuo cuadrático módulo q. Por el teorema chino del resto existe $b \in \mathbb{Z}$ tal que:

   $b \equiv 1\,(8)$ $\qquad$ $b \equiv 1\,(p_i)$ $\;(i = 1, ..., k)$
   $b \equiv s\,(q)$ $\qquad$ $b \equiv 1\,(q_i)$ $\;(i = 2, ..., k)$

   i. Calcular $\left(\frac{a}{b}\right)$.

   ii. Probar que existe $p \neq 2$ y $p \neq p_i$ tal que $p \mid b$ y $\left(\frac{a}{p}\right) = -1$.

   iii. Probar el enunciado.

   (b) Suponga $a = 2$.

   Sea $P = \{p_1, p_2, ..., p_k\} \not\ni 3$ un conjunto de primos tales que $\left(\frac{2}{p_i}\right) = -1$. Considere $b = 8p_1p_2...p_k + 3$.

   Probar que $\left(\frac{2}{b}\right) = -1$ y que existe un primo $p \neq 3$ y $p \notin P$ tal que $\left(\frac{2}{p}\right) = -1$.

2. Sean $L \supset K$ dos cuerpos de números. Sea $n = [L : K]$.

   Hay exactamente n morfismos $\sigma_i : L \to \mathbb{C}$ tales que $\sigma_i(x) = x$ para todo $x \in K$. Describirlos (recordar que $L = K(\theta)$).

   Para $\alpha \in L$ se definen

$$N_{L|K}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha)$$

$$T_{L|K}(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha).$$

   Observar que si $K = \mathbb{Q}$, $N_{L|\mathbb{Q}} = N_L$ y $T_{L|\mathbb{Q}} = T_L$.

   Probar:

   (a) $N_{L|K}(\alpha)$ y $T_{L|K}(\alpha) \in K$,
   (b) $N_{L|K}(\alpha_1\alpha_2) = N_{L|K}(\alpha_1)N_{L|K}(\alpha_2)$,
   (c) $T_{L|K}(\alpha_1 + \alpha_2) = T_{L|K}(\alpha_1) + T_{L|K}(\alpha_2)$.

3. Sea $K = \mathbb{Q}(\sqrt{m}, \sqrt{n})$, con m y n enteros distintos y libres de cuadrados ($m, n \neq 1, 0$). Sea $\mathcal{D}$ el anillo de enteros de K.

   Sea $s = \frac{mn}{(m,n)^2}$. Luego $K \supset \mathbb{Q}(\sqrt{s})$.

   Nota: En este ejercicio de calculan el anillo de enteros de K y el discriminante del cuerpo. El enunciado está completo y cubre todos los casos. Puede hacer uno sólo de los dos items (b) y (c).

   (a) Sea $\alpha \in K$. Probar que $\alpha \in \mathcal{D}$ si y sólo si $N_{K/\mathbb{Q}(\sqrt{m})}(\alpha)$ y $T_{K/\mathbb{Q}(\sqrt{m})}(\alpha)$ son enteros algebraicos.

   (b) Suponga que $m \equiv 3\,(4)$ y $n \equiv s \equiv 2\,(4)$.

   - Pruebe que todo $\alpha \in \mathcal{D}$ se escribe en la forma

     $$\frac{a + b\sqrt{m} + c\sqrt{n} + d\sqrt{s}}{2}$$

     con $a, b, c, d \in \mathbb{Z}$.
     Sugerencia: Escribir a α como combinación lineal de $1, \sqrt{m}, \sqrt{n}, \sqrt{s}$ con coeficientes en $\mathbb{Q}$ y considerar las tres trazas relativas.
   - Considerando la $N_{K/\mathbb{Q}(\sqrt{m})}(\alpha)$ probar que a y b son pares y que $c \equiv d\,(2)$.
   - Concluir que una base de enteros de $\mathcal{D}$ es

     $$\left\{1, \sqrt{m}, \sqrt{n}, \frac{\sqrt{n} + \sqrt{s}}{2}\right\}.$$

   (c) Suponga que $m \equiv 1(4)$ y $n \equiv s \equiv 2, 3\,(4)$.
   Igual que en el item (b), probar que si $\alpha \in \mathcal{D}$, α es de la forma $(a + b\sqrt{m} + c\sqrt{n} + d\sqrt{s})/2$, con $a, b, c, d \in \mathbb{Z}$. Probar que $a \equiv b\,(2)$ y $c \equiv d\,(2)$. Concluir que

   $$\left\{1, \frac{1 + \sqrt{m}}{2}, \sqrt{n}, \frac{\sqrt{n} + \sqrt{s}}{2}\right\}$$

   es una base de enteros de $\mathcal{D}$.

   (d) Suponga que $m \equiv n \equiv s \equiv 1\,(4)$.

   - Pruebe que todo $\alpha \in \mathcal{D}$ se escribe en la forma

     $$\frac{a + b\sqrt{m} + c\sqrt{n} + d\sqrt{s}}{4}$$

     con $a, b, c, d \in \mathbb{Z}$ y $a \equiv b \equiv c \equiv d\,(2)$.
   - Probar que sumando un múltiplo apropiado de

     $$\left(\frac{1 + \sqrt{m}}{2}\right)\left(\frac{1 + \sqrt{s}}{2}\right)$$

     se puede obtener un entero en $\mathcal{D}$ de la forma

     $$\frac{x + y\sqrt{m} + z\sqrt{n}}{2}$$

     con $x, y, z \in \mathbb{Z}$. Probar que, además, $x + y + z \equiv 0\,(2)$.

- Concluir que una base de enteros de $\mathcal{D}$ es

$$\left\{1, \frac{1+\sqrt{m}}{2}, \frac{1+\sqrt{n}}{2}, \left(\frac{1+\sqrt{m}}{2}\right)\left(\frac{1+\sqrt{s}}{2}\right)\right\}.$$

(e) Probar que (b), (c) y (d) cubren todos los casos posibles, salvo reordenamientos de m, n, s.

(f) Comparar, en cada caso, el discriminante de $\mathcal{D}$ con el discriminante $\Delta(1, \sqrt{m}, \sqrt{n}, \sqrt{mn})$ y, calculando este último, probar que:

- $\mathrm{Disc}(K) = 64mns$ en (b),
- $\mathrm{Disc}(K) = 16mns$ en (c),
- $\mathrm{Disc}(K) = mns$ en (d).

Observar que, en cualquiera de los tres casos, el discriminante del cuerpo K es el producto de los discriminantes de los tres subcuerpos cuadráticos.

4. Sea $\mathcal{D} = \mathbb{Z}[\sqrt{-29}]$. Se tiene la siguiente factorización en $\mathcal{D}$:

$$30 = 2 \cdot 3 \cdot 5 = (1 + \sqrt{-29})(1 - \sqrt{-29}). \tag{1}$$

(a) Probar que $(30) \subset (2, 1 + \sqrt{-29})$.

(b) Sea $\mathcal{P}_1 = (2, 1 + \sqrt{-29})$. Calcular $N(\mathcal{P}_1)$ y probar que $\mathcal{P}_1$ es un ideal primo de $\mathcal{D}$.

(c) Ver que $1 - \sqrt{-29} \in \mathcal{P}_1$ y que $(30) \subset \mathcal{P}_1^2$.

(d) Hallar ideales primos $\mathcal{P}_2$, $\mathcal{P}_2'$, $\mathcal{P}_3$, $\mathcal{P}_3'$, de norma 3 o 5 tales que

$$(30) \subset \mathcal{P}_i \mathcal{P}_i'$$

para $i = 2, 3$.

(e) Probar que $(30) = \mathcal{P}_1^2 \mathcal{P}_2 \mathcal{P}_2' \mathcal{P}_3 \mathcal{P}_3'$.

(f) ¿Cómo se relaciona la factorización de (30) en ideales primos con las dos factorizaciones indicadas en (1)?

(g) Hallar todos los ideales de $\mathcal{D}$ que tienen a 30 entre sus elementos.