Revisión Domiciliaria - Segunda Parte

1. Probar que $\mathbb{Q}(\sqrt{-31})$ tiene número de clases de ideales $h = 3$ y exhibir un generador del grupo de clases.

2. Sea x la raíz real del polinomio $X^3 - X + 1$ y sean $y, \bar{y}$ sus dos otras raíces en $\mathbb{C}$. Sea K el cuerpo cúbico $\mathbb{Q}(x)$.

   (a) Observar que $y + \bar{y} = -x$, $y\bar{y} = -\frac{1}{x}$ y calcular $\Delta(1, x, x^2)$.

   (b) Probar que el anillo $\mathcal{D}$ de enteros de K es $\mathbb{Z}[x]$ y que este anillo es principal.

   (c) Probar que $p = 23$ es el único primo en $\mathbb{Z}$ que ramifica en $\mathcal{D}$ y usar (a) para hallar la descomposición de (23) como producto de ideales primos (principales) en K.

   (d) Sea $L = \mathbb{Q}(x, \sqrt{-23}) = \mathbb{Q}(x, y, \bar{y})$. Decidir qué tipo de descomposición tiene (23) en L (cuántos ideales primos intervienen en su factorización, y cuáles son sus índices de ramificación y grados residuales).

3. Sea $K \subset \mathbb{R}$ una extensión cúbica de $\mathbb{Q}$ con una única inmersión real en $\mathbb{C}$. Sea u la unidad fundamental de $\mathcal{D}_K$. Luego $u > 1$ y toda unidad de $\mathcal{D}_K$ es de la forma $\pm u^n$ con $n \in \mathbb{Z}$.

   En los items siguientes buscaremos una cota inferior para u.

   (a) Sean u, $\rho e^{i\theta}$ y $\rho e^{-i\theta}$ los conjugados de u. Probar que $u = \rho^{-2}$ y que

   $$D = \Delta(1, u, u^2) = -4 \operatorname{sen}^2 \theta \, (\rho^3 + \rho^{-3} - 2\cos\theta)^2$$

   (b) Probar que

   $$|D| < 4(u^3 + u^{-3} + 6)$$

   sugerencia: Llamar $x = \rho^3 + \rho^{-3}$, $c = \cos\theta$ y buscar el máximo de la función

   $$f(x) = (1 - c^2)(x - 2c)^2 - x^2.$$

   (c) Si Δ denota el discriminante de K, probar que $u^3 > \frac{|\Delta|}{4} - u^{-3} - 6 > \frac{|\Delta|}{4} - 7$.

   En los items siguientes calcularemos la unidad fundamental de $K = \mathbb{Q}(\sqrt[3]{2})$. Usar, sin demostrar, que $\mathcal{D}_K = \mathbb{Z}[\sqrt[3]{2}]$ y que $\Delta = -108$.

   (d) Si u es la unidad fundamental, probar que $u^3 > 20$.

   (e) Sea $\alpha = \sqrt[3]{2}$. Probar que $1 + \alpha + \alpha^2$ es una unidad en K y que es la unidad fundamental.

4. Calcular el grupo de puntos de la curva elíptica $y^2 = x^3 + x$ sobre el cuerpo finito $\mathbb{F}_{37}$.

   Sugerencia: Hallar todos los puntos de orden 2^k ($k \in \mathbb{N}$) (ver, por ejemplo, si los puntos de orden 2 son "dobles" de otros puntos); hallar los puntos de orden 3, usando el polinomio $\psi_3(x)$ (ver el ejercicio 3 de la práctica 5). Argumentar por qué no puede haber más puntos.

5. Sea E la curva elíptica

$$y^2 = x(x-1)(x+3).$$

   Probar que el grupo de puntos $E(\mathbb{Q}) \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_4$.

   sugerencia: Calcular la imagen en $\mathbb{Q}^*/(\mathbb{Q}^*)^2 \times \mathbb{Q}^*/(\mathbb{Q}^*)^2$ de $E(\mathbb{Q})/2E(\mathbb{Q})$ via el morfismo $\varphi = \varphi_\alpha \times \varphi_\beta$ dado por

$$\varphi(x,y) = \begin{cases} (x-\alpha, x-\beta) & x \neq \alpha, \beta \\ ((\alpha-\beta)(\alpha-\gamma), \alpha-\beta) & x = \alpha \\ (\beta-\alpha, (\beta-\alpha)(\beta-\gamma)) & x = \beta \\ (1,1) & P = \mathcal{O} \end{cases}$$

   donde $\alpha < \beta < \gamma$ son las tres raíces racionales de f en $y^2 = f(x)$ y probar que el rango $r = 0$. Para $E(\mathbb{Q})_{\texttt{Tors}}$ reducir módulo 5 y usar la información obtenida anteriormente.

   Nota: El discriminante de $f(x) = (x-\alpha)(x-\beta)(x-\gamma)$ es $((\alpha-\beta)(\alpha-\gamma)(\beta-\gamma))^2$