Teoría de Números - Lista de ejercicios para entregar

2do. Cuatrimestre 2011

1. Sea $K/\mathbb{Q}$ una extensión abeliana finita tal que en K ramifica un único primo p de $\mathbb{Q}$. Probar que entonces hay un único primo $\mathfrak{p}$ de K arriba de p y que es totalmente ramificado (es decir $f = 1$). ¿Qué pasa si la extensión es Galois pero no abeliana? (demostrar o dar un contraejemplo).

2. (a) Sea L/K una extensión finita de cuerpos de números. Probar que los primos de K que ramifican en L son los mismos que los que ramifican en la clausura normal de L.
   (b) Sea nuevamente L/K una extensión finita de cuerpos de números, probar que los primos que se parten completamente en L son los mismos que los que se parten completamente en la clausura normal de L.

3. Sea $d \equiv 1 \pmod 8$ un entero negativo libre de cuadrados. Llamemos $K_d = \mathbb{Q}[\sqrt{d}]$. Probar que $\mathcal{O}_{K_d}$ contiene dos ideales (conjugados) de índice 2. Calcular el orden de estos ideales en el grupo de clases para $d = -7, -15$ y -71. Probar finalmente que

$$\lim_{d\to\infty} h(K_d) = \infty$$

   donde d recorre los enteros negativos libres de cuadrados congruentes a 1 módulo 8.

4. Sea p un primo congruente con 3 modulo 4. Probar que el grupo de clases de $\mathbb{Q}[\sqrt{-p}]$ tiene orden impar.

5. Sea K un cuerpo de números y $R \subseteq \mathcal{O}_K$ un anillo de índice finito (notemos $n = [\mathcal{O}_K/R]$ su índice). Un R-ideal es un R-módulo $\mathfrak{a} \subseteq R$ tal que

$$\{\alpha \in K : \ \alpha\mathfrak{a} = \mathfrak{a}\} = R.$$

   De manera análoga al caso de $\mathcal{O}_K$, si $\mathfrak{a} \subseteq R$ es un R-módulo definimos su norma como $N(\mathfrak{a}) = |R/\mathfrak{a}|$.

   (a) Probar que si $\mathfrak{a}$ es un R-módulo tal que $(N(\mathfrak{a}) : n) = 1$ entonces $R = \mathfrak{a} + n\mathcal{O}_K$. Deducir que $\mathfrak{a}$ es un R-ideal.
   (b) Notemos por $J(R, n) = \{\mathfrak{a} \text{ ideal de R: } (N(\mathfrak{a}), n) = 1\}$. Probar que existen biyecciones entre los conjuntos de ideales

$$J(\mathcal{O}_K, n) \longleftrightarrow J(R, n)$$

   dadas por enviar $\mathfrak{a} \in J(\mathcal{O}_K, n)$ a $\mathfrak{a} \cap R$. Y a un $\mathfrak{b} \in J(R, n)$ a $\mathfrak{b}\mathcal{O}_K$.
   (c) Probar que dado n, todo elemento del grupo de clases de $\mathcal{O}_K$ tiene un representante de norma coprima con n.
   (d) Deducir que el número de clases de R es mayor o igual que el número de clases de $\mathcal{O}_K$.

6. Sea K un cuerpo de números que contiene una raiz n-ésima primitiva de la unidad μ_n. Sea $\mathfrak{p}$ un ideal primo de K tal que $\mathfrak{p} \nmid n$.

   (a) Probar que $\{1, \mu_n, \mu_n^2, \ldots, \mu_n^{n-1}\}$ son todos distintos módulo $\mathfrak{p}$. Deducir que $n \mid N(\mathfrak{p}) - 1$.

(b) Probar que si $a \in \mathcal{O}_k$ y $a \notin \mathfrak{p}$ entonces

$$a^{(N(\mathfrak{p})-1)/n} \equiv \mu_n^i \pmod{\mathfrak{p}}$$

para un único i entre 1 y $n-1$. Luego, definimos el símbolo de Legendre $\left(\frac{a}{\mathfrak{p}}\right)_n$ como la única raiz n-ésima de la unidad tal que

$$a^{(N(\mathfrak{p})-1)/n} \equiv \left(\frac{a}{\mathfrak{p}}\right)_n \pmod{\mathfrak{p}}$$

Extendemos este símbolo a todo $\mathcal{O}_K$ definiendolo como 0 en los elementos de $\mathfrak{p}$.

(c) Probar que $\left(\frac{a}{\mathfrak{p}}\right)_n = 1$ si y solo si a es una potencia n-ésima módulo $\mathfrak{p}$.

7. Probar que existen extensiones de cuerpos de $\mathbb{Q}_p$ de cualquier grado.

8. Sean L_w y K_v completaciones de dos cuerpos de números L/K tales que la extensión L_w/K_v es totalmente ramificada (es decir tiene grado de inercia 1). Sea π_L un uniformizador local de O_w. Probar que $L = K[\pi_L]$. Deducir que $O_w = O_v[\pi_L]$.

9. Sea L_w/K_v una extensión de completaciones de cuerpos de números. Probar que dicha extensión es totalmente ramificada si y solo si $L_w = K_v[\alpha]$ con α raiz de un polinomio de Eisenstein (es decir, un polinomio mónico $\sum \lambda_i x^i$ tal que $v(\lambda_i) > 0$ para todo $0 \leq i < n$ y $v(\lambda_0) = 1$).

10. (a) Sea K una extensión finita y Galois de $\mathbb{Q}_p$ y α, β dos elementos de K. Supongamos β esta "muy cerca" de α en el siguiente sentido: para todo morfismo $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ tal que $\sigma(\alpha) \neq \alpha$ vale que $|\beta - \alpha| < |\sigma(\alpha) - \alpha|$. Probar que entonces $\mathbb{Q}_p(\alpha) \subseteq \mathbb{Q}_p(\beta)$.

(b) Sea $f(x) = \sum a_i x^i \in \mathbb{Q}_p[x]$ un polinomio irreducible de grado n y α una de sus raices. Probar que existe $\epsilon > 0$ tal que para todo $g(x) = \sum b_i x^i \in \mathbb{Q}_p[x]$ tal que $|f - g| = \max |a_i - b_i| < \epsilon$ vale que g es irreducible y hay una raiz β de g tal que $\mathbb{Q}_p[\alpha] = \mathbb{Q}_p[\beta]$. En otras palabras, estamos probando que perturbar los coeficientes de un polinomio no modifica las extensiones que generan sus raices.

(c) Probar que toda extensión finita $K/\mathbb{Q}_p$ es la completación de una extensión finita $L/\mathbb{Q}$ respecto de algun primo $\mathcal{P}|p$.