Práctica 3

Factorización en extensiones

---

1. Sea K un cuerpo cuadrático (real). Probar que si $-1 \in N_{K/\mathbb{Q}}(K^\times)$ entonces todo primo $p \in \mathbb{Z}$ con $p \equiv 3 (\mathrm{mod}\, 4)$ es no ramificado en K.

2. Sea $K = \mathbb{Q}(\alpha)$, con $\alpha^3 + \alpha^2 - 2\alpha - 1 = 0$.

a) Probar que $p = 7$ es el único primo de $\mathbb{Z}$ que ramifica en K.
b) Hallar la factorización de $p\mathcal{O}_K$ para $p = 2, 3, 5$.

3. Sea $K = \mathbb{Q}(\alpha)$, con $\alpha^3 + \alpha + 1 = 0$.

Sea p un primo de $\mathbb{Z}$, y sea $\varepsilon = \left(\frac{-31}{p}\right)$. Probar que:

a) Si $\varepsilon = -1$, entonces p es producto de dos primos en K.
b) Si $\varepsilon = 1$, entonces o bien p es inerte o bien se parte completamente en K. Mostrar ejemplos de ambos tipos.

4. Sea $\zeta_5 \in \overline{\mathbb{Q}}^\times$ de orden 5, y sea $K = \mathbb{Q}(\zeta_5)$. Factorizar los ideales $2\mathcal{O}_K$ y $5\mathcal{O}_K$.

5. Consideremos $AKMC$ con A Dedekind, y $M/L/K$ un cuerpo intermedio. Denotemos por B la clausura entera de A en L[1].

Dado R un ideal primo de C, sean $Q = R \cap B$ y $P = Q \cap A$. Probar que:

a) $e(R|P) = e(R|Q)\ e(Q|P)$.
b) $f(R|P) = f(R|Q)\ f(Q|P)$.

Esto es, que el índice de ramificación y el grado de inercia son multiplicativos en torres.

6. Sean m, n enteros libres de cuadrados con $m \neq n$. Sea $K = \mathbb{Q}(\sqrt{m}, \sqrt{n})$. *Observar que $K/\mathbb{Q}$ tiene exactamente tres subextensiones cuadráticas.*

Sea $p \in \mathbb{Z}$ un primo.

a) Dar ejemplos en los que:
   i. p se parta completamente en K.
   ii. $p\mathcal{O}_K = P_1^2 P_2^2$, con $P_1, P_2 \trianglelefteq \mathcal{O}_K$ primos.

b) Probar que no puede suceder que:
   i. p sea inerte en K.
   ii. p sea impar y totalmente ramificado en K.

7. Sean $n_1, ..., n_r$ enteros coprimos dos a dos.

Probar que $\left[\mathbb{Q}\left(\sqrt{n_1}, ..., \sqrt{n_r}\right) : \mathbb{Q}\right] = 2^r$.

8. a) Sea K un cuerpo de números de grado n.

Probar que si existe un primo $p < n$ que se parte completamente en K, entonces $\mathcal{O}_K$ no es monógeno.

b) Probar que si $K = \mathbb{Q}\left(\sqrt{7}, \sqrt{13}\right)$, entonces $\mathcal{O}_K$ no es monógeno.

9. Sea K un cuerpo de números, y sean L, L' extensiones de K. Sea $\mathfrak{p}$ un primo de K.

a) Probar que $\mathfrak{p}$ se parte completamente en LL' si y solo si se parte completamente en L y en L'.
b) Probar que si $\mathfrak{p}$ ramifica completamente en L y no ramifica en L', entonces $L \cap L' = K$.

10. Sea $f \in \mathbb{Z}[X]$ no constante.

a) Probar que existen infinitos primos p tal que $\overline{f} \in \mathbb{F}_p[X]$ tiene *al menos una* raíz en $\mathbb{F}_p$.

Sugerencia: probarlo primero en el caso en que $f(0) = 1$, notando que en tal caso para todo $m \geq 2$ se tiene que $f(km) \equiv 1 (\mathrm{mod}\, m)$ para todo $k \in \mathbb{Z}$.

b) i. Probar que si $K/\mathbb{Q}$ es un cuerpo de números, existen infinitos primos P de $\mathcal{O}_K$ tales que $f(P|P \cap \mathbb{Z}) = 1$.
ii. Probar que si $K \subseteq L$ son cuerpos de números, existen infinitos primos P de $\mathcal{O}_K$ tales para todo primo Q de $\mathcal{O}_L$ con $Q \cap \mathcal{O}_K = P$ se tiene que $f(Q|P) = 1$.

Sugerencia: probarlo primero para el caso en que L/K es de Galois.

c) Probar que existen infinitos primos p tal que $\overline{f} \in \mathbb{F}_p[X]$ tiene *todas* sus raíces en $\mathbb{F}_p$.

Teoría de la ramificación de Hilbert

11. Sea A un dominio de Dedekind, y sea $K = \mathrm{Frac}(A)$. Sean L, L extensiones separables de K

Sea p un primo de K. Probar que si p se parte completamente en L y en L', entonces se parte completamente en LL'.

12. Sea L/K una extensión galoisiana de cuerpos de números tal que $\mathrm{Gal}(L/K)$ *no* es cíclico.

a) Probar que si p es un primo de K que no ramifica en L, entonces p se parte en L.
b) Concluir que el conjunto de primos de K que no se parten en L es finito.

13. Sea L/K una extensión galoisiana de cuerpos de números, y sea $G = \mathrm{Gal}(L/K)$. Por *cuerpos intermedios* nos referimos a aquellos cuerpos E con $K \subsetneq E \subsetneq L$.

Sea p un primo de K.

a) Supongamos, o bien:
i. que p es totalmente ramificado en cada cuerpo intermedio, pero que no es totalmente ramificado en L, o bien
ii. que p no se parte en cada cuerpo intermedio, pero se parte en L.

Probar que G tiene orden primo.

b) Supongamos, o bien:
i. que p es no ramificado en cada cuerpo intermedio, pero ramificado en L, o bien
ii. que p se parte completamente en cada cuerpo intermedio, pero no en L.

Probar que G tiene un (único) subgrupo propio no trivial contenido en todos los subgrupos propios de G, y deducir que G tiene orden potencia de un primo.

[1] de manera que C es la clausura entera de B en M.

14. Sean e, f, r enteros positivos.

a) Probar que existen primos enteros p y q tales que p se parte como producto de r primos *distintos* en $\mathbb{Q}(\zeta_q)$

b) Probar que p y q pueden ser elegidos de manera que $\mathbb{Q}(\zeta_q)$ contenga una subextensión de grado rf sobre $\mathbb{Q}$. ¿Cómo se factoriza p en esta subextensión?

c) Probar que, además, p puede ser elegido de manera que $p \equiv 1 (\mathrm{mod}\, e)$.

d) Probar que, para p y q como arriba, $\mathbb{Q}(\zeta_{pq})$ contiene una subextensión en la que p se parte como producto de r primos, con ramificación e e inercia f.

e) Hallar un ejemplo de p y q para $e = 2, f = 3, r = 5$.

15. Sea m un entero positivo. Identifiquemos $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ con $\mathbb{Z}_m^\times$.

a) Sea K un subcuerpo de $\mathbb{Q}(\zeta_m)$, y sea H el subgrupo de $\mathbb{Z}_m^\times$ que corresponde a K. Sea f el orden de $\overline{p}$ en $\mathbb{Z}_m^\times/H$.

Probar que para todo primo P de K con $P \mid p$ se tiene que $f(P|p) = f$.

b) Determinar cómo se factoriza p en $\mathbb{Q}(\zeta_m + \zeta_m^{-1})$.

c) Sea $K = \mathbb{Q}\left(\sqrt{d}\right) \subseteq \mathbb{Q}(\zeta_m)$ una subextensión cuadrática, y sea H como arriba.

i. Probar que si p es impar, entonces $\overline{p} \in H$ si y solo si $\left(\frac{d}{p}\right) = 1$.

ii. Probar que $\overline{2} \in H$ si y solo si $d \equiv 1 (\mathrm{mod}\, 8)$.

16. Sea L/K una extensión galoisiana de cuerpos de números, y sea $G = \mathrm{Gal}(L/K)$. Sea P un primo de L. Definimos los *grupos de ramificación superior* de P por

$$G_m = \left\{\sigma \in G : \sigma x \equiv x \ \left(\mathrm{mod}\, P^{m+1}\right)\ \forall x \in \mathcal{O}_L\right\}, \quad m \geq 1.$$

a) Probar que $G_m \trianglelefteq D_P$ para todo m.

b) Probar que $\cap_{m\geq 1} G_m = \{1\}$, y deducir que $G_m = \{1\}$ para m suficientemente grande.