ÁLGEBRA III

Práctica 5 – Segundo Cuatrimestre de 2007

Cuerpos finitos y raíces de la unidad

Ejercicio 1. Sea K un cuerpo. Notemos $(K, +)$ al grupo aditivo de K y $(K^*, \cdot)$ al grupo multiplicativo. Probar que $(K, +)$ y $(K^*, \cdot)$ nunca son isomorfos como grupos. Caracterizar ambos grupos en el caso en que K sea finito.

Ejercicio 2. Probar que dos cuerpos finitos de igual cardinal son isomorfos.

Ejercicio 3. Sea C una clausura algebraica de $\mathbb{Z}_p$ y sean F_{p^m} y F_{p^n} los cuerpos de p^m y p^n elementos en C. Probar que $F_{p^m} \subset F_{p^n}$ si y sólo si $m \mid n$.

Ejercicio 4. Sea K un cuerpo de q elementos y sea E/K una extensión finita de K. Probar que E/K es cíclica con $G(E/K) =< \sigma >$, donde $\sigma : E \to E$ es el morfismo definido por $\sigma(x) = x^q$.

Ejercicio 5. Sea K un cuerpo finito de q elementos.

i) Sea $f \in K[X]$ irreducible. Probar que f divide a $X^{q^n} - X$ si y sólo si $\deg(f)$ divide a n.

ii) Probar que $X^{q^n} - X = \prod_{d|n} (\prod f_d)$, donde el producto de adentro recorre todos los polinomios irreducibles mónicos de grado d en $K[X]$.

iii) Deducir que $q^n = \sum_{d|n} d.u(d)$, donde $u(d)$ es la cantidad de polinomios irreducibles mónicos de grado d en $K[X]$.

iv) Dar una fórmula para $u(d)$.

v) Calcular la cantidad de polinomios de grado 3 y 4 mónicos e irreducibles que hay en un cuerpo de 2^{12} y 3^{12} elementos.

Ejercicio 6. Sea n un número natural impar y sea K un cuerpo de característica distinta de 2. Probar que K contiene una raíz n-ésima primitiva de 1 si y sólo si K contiene una raíz $2n$-ésima primitiva de 1.

Ejercicio 7. Hallar todos los $m \in \mathbb{N}$ tales que una raíz m-ésima primitiva de 1 tiene grado 2 o 4 sobre $\mathbb{Q}$.

Ejercicio 8.

i) Sea $E/\mathbb{Q}$ una extensión de grado finito. Probar que existe sólo un número finito de raíces de la unidad en E.

ii) Determinar todas las raíces de la unidad contenidas en cada uno de los siguientes cuerpos: $\mathbb{Q}[\,i\,]$, $\mathbb{Q}[\sqrt{-2}\,]$, $\mathbb{Q}[\sqrt{2}\,]$, $\mathbb{Q}[\sqrt{-3}\,]$, $\mathbb{Q}[\sqrt{-5}\,]$, $\mathbb{Q}[\sqrt{2}, \sqrt{-3}\,]$ y $\mathbb{Q}(\xi_9)$.

Ejercicio 9. Para cada $n \in \mathbb{N}$, sea $\phi_n \in \mathbb{Q}[X]$ el polinomio ciclotómico de orden n. Probar que:

i) Si $p \in \mathbb{N}$ es primo, entonces $\phi_p(X) = X^{p-1} + X^{p-2} + \cdots + 1$.

ii) Para cada $r \in \mathbb{N}$ y cada primo $p \in \mathbb{N}$, $\phi_{p^r}(X) = \phi_p(X^{p^{r-1}})$.

iii) Si $n = p_1^{r_1} p_2^{r_2} \ldots p_s^{r_s}$ con $p_1 \ldots, p_s$ primos distintos, $\phi_n(X) = \phi_{p_1 \ldots p_s}\left(X^{p_1^{r_1-1} \cdots p_s^{r_s-1}}\right)$.

iv) Si n es impar, $\phi_{2n}(X) = \phi_n(-X)$.

v) Si p es primo, $(p : n) = 1$, entonces $\phi_{pn}(X) = \dfrac{\phi_n(X^p)}{\phi_n(X)}$.

Ejercicio 10. Sean E/K y F/K extensiones ciclotómicas de índices m y n respectivamente, con $(m : n) = 1$, contenidas en una clausura algebraica C de K. Probar que:

i) EF/K es una extensión ciclotómica de índice mn.

ii) Si $K = \mathbb{Q}$, entonces $E \cap F = \mathbb{Q}$.

Ejercicio 11.

i) Sea $E/\mathbb{Q}$ una extensión cuadrática. Probar que ϕ_n es reducible en $E[X]$ si y sólo si $E \subset \mathbb{Q}(\xi_n)$.

ii) Determinar todas las extensiones cuadráticas $E/\mathbb{Q}$ tales que ϕ_{12} es irreducible en $E[X]$. Idem para ϕ_8 y ϕ_{10}.

Ejercicio 12. Hallar todos los $n \in \mathbb{N}$ tales que ϕ_n es irreducible sobre $\mathbb{Q}(\xi_9)$.

Ejercicio 13. Sea K un cuerpo, sea $\Phi : \mathbb{Z} \to K$ el único morfismo de anillos con unidad y sea $\overline{\Phi} : \mathbb{Z}[X] \to K[X]$ el morfismo de anillos inducido por Φ definido como $\overline{\Phi}\left(\sum a_i X^i\right) = \sum \Phi(a_i) X^i$. Como $\phi_n \in \mathbb{Z}[X]$, podemos pensar a ϕ_n en $K[X]$ vía $\overline{\Phi}$.

i) Probar que:

   a) $\phi_n \in K[X]$ es mónico de grado $\varphi(n)$.

   b) $X^n - 1 = \prod\limits_{d|n} \phi_d$ en $K[X]$.

   c) Si $\mathrm{car}(K) \neq 0$ y n es coprimo con $\mathrm{car}(K)$, entonces ϕ_n tiene todas sus raíces simples.

ii) Sea C/K una clausura algebraica y sea $\xi \in C$ una raíz n-ésima primitiva de 1 (i.e. $\xi^n = 1$ y $\xi^r \neq 1 \,\forall\, r < n$). Probar que, si $\mathrm{car}(K) n$:

   a) $\xi \in C$ es raíz de ϕ_n si y sólo si ξ es raíz n-ésima primitiva de 1.

   b) La cantidad de raíces n-ésimas primitivas de 1 en C es $\varphi(n)$.

   c) Si ξ_n es una raíz n-ésima primitiva de 1 en C, entonces $\xi \in C$ es otra raíz n-ésima primitiva de 1 si y sólo si $\xi = \xi_n^j$ para algún $1 \leq j \leq n$ tal que $(j : n) = 1$.

Ejercicio 14. Sea K un cuerpo y sea $n \in \mathbb{N}$ tal que $\mathrm{car}(K) n$. Probar que ϕ_n se factoriza en $K[X]$ como producto de polinomios irreducibles distintos de igual grado. Más aún, el grado de los factores irreducibles es $[K(\xi_n) : K]$, donde ξ_n es una raíz n-ésima primitiva de 1.

Ejercicio 15. Sea K un cuerpo finito de q elementos, y sea E/K una extensión ciclotómica de índice n, con n coprimo con $\mathrm{car}(K)$. Probar que:

i) E es un cuerpo de q^m elementos, donde m es el menor número natural tal que $n \mid q^m - 1$.

ii) ϕ_n es irreducible en $K[X]$ si y sólo si la clase de q en $\mathcal{U}_n$ tiene orden $\varphi(n)$.

Ejercicio 16. Probar que:

i) Si p es un primo, $p \neq 2,\ 3$, entonces ϕ_{12} es reducible en $\mathbb{Z}_p[X]$.

ii) El polinomio $X^4 + 1$ es reducible en $\mathbb{Z}_p[X]$ para todo primo p.

Ejercicio 17. Probar que $\mathbb{Z}_3$ no contiene raíces 13-ésimas de la unidad distintas de 1. Probar también que si $E/\mathbb{Z}_3$ es una extensión ciclotómica de índice 13, entonces su grado es $3 < \varphi(13)$.

Ejercicio 18.

i) Hallar todos los $n \in \mathbb{N}$ tales que ϕ_n es irreducible sobre un cuerpo de 9 elementos.

ii) Sea $p \in \mathbb{N}$ primo. Hallar todos los $m \in \mathbb{N}$ tales que ϕ_6 es irreducible sobre un cuerpo de p^m elementos.

Ejercicio 19.

i) Sea K un cuerpo de 27 elementos. Factorizar ϕ_7 como producto de polinomios irreducibles en $K[X]$.

ii) Sea t trascendente sobre $\mathbb{Z}_7$ y sea $K = \mathbb{Z}_7(t)$. Factorizar ϕ_9 como producto de polinomios irreducibles en $K[X]$.