Práctica 5: Cuerpos finitos - Extensiones ciclotómicas

1 Sean $E/\mathbb{F}_q$ una extensión algebraica y $\alpha \in E$. Probar que $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = \min\{n \in \mathbb{N} \mid \alpha^{q^n} = \alpha\}$.

2 Sea $f \in \mathbb{F}_q[X]$ un polinomio irreducible de grado n.

(*a*) ¿Para qué valores de $k \in \mathbb{N}$ ocurre que f sigue siendo irreducible en $\mathbb{F}_{q^k}[X]$?

(*b*) En el caso general, ¿qué grado tienen los factores irreducibles de f en $\mathbb{F}_{q^k}[X]$?

3 Probar que $\mathbb{F}_{p^m} \cap \mathbb{F}_{p^n} = \mathbb{F}_{p^{(m:n)}}$ y $\mathbb{F}_{p^m}\mathbb{F}_{p^n} = \mathbb{F}_{p^{[m:n]}}$, donde $(m : n)$ y $[m : n]$ denotan máximo común divisor y mínimo común múltiplo respectivamente.

4 Probar que $\bigcup_{m\in\mathbb{N}} \mathbb{F}_{p^m} = \overline{\mathbb{F}_p}$.

5 **(Criterio de irreducibilidad de Rabin)** Sean $n > 1$ un entero y $p_1, p_2, \ldots, p_k$ sus divisores primos. Para cada i entre 1 y k, definimos $n_i = \frac{n}{p_i}$.

Sea $f \in \mathbb{F}_q[X]$ un polinomio de grado n. Probar que f es irreducible si y sólo si f divide a $X^{q^n} - X$ y es coprimo con $X^{q^{n_i}} - X$ para todo i.

6 Probar que toda extensión algebraica $E/\mathbb{F}_q$ es una extensión de Galois.

7 Sea $\mathbb{F}_q$ un cuerpo finito. ¿Para qué valores de k la función de $\mathbb{F}_q$ en $\mathbb{F}_q$ dada por $x \mapsto x^k$ es biyectiva?

8 Consideremos el polinomio $f = X^p - X - a \in \mathbb{F}_p[X]$, con $a \neq 0$.

(*a*) Probar que f no tiene raíces en $\mathbb{F}_p$.

(*b*) Probar que f es irreducible en $\mathbb{F}_p[X]$.

Sugerencia. Sea $\alpha \in \overline{\mathbb{F}_p}$ una raíz de f. ¿Cuáles son las otras raíces?

(*c*) ¿Para cuáles cuerpos finitos $\mathbb{F}_q$ es cierto que $X^q - X - a$ es irreducible en $\mathbb{F}_q[X]$?

9 Dado un cuerpo finito $\mathbb{F}_q$, sea $\mathrm{Aff}(\mathbb{F}_q)$ el conjunto de todas las funciones de $\mathbb{F}_q$ en sí mismo que tienen la forma $t \mapsto at + b$, donde $a, b \in \mathbb{F}_q$, $a \neq 0$.

(*a*) Probar que todas las funciones de $\mathrm{Aff}(\mathbb{F}_q)$ son biyectivas.

(*b*) Probar que $\mathrm{Aff}(\mathbb{F}_q)$, con la composición de funciones, es un grupo.

(*c*) Probar que $\mathrm{Aff}(\mathbb{F}_q) \cong \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \;\middle|\; a, b \in \mathbb{F}_q,\ a \neq 0 \right\}$.

10 Calcular los grados de los factores irreducibles del polinomio $X^{13} - 3X - 1 \in \mathbb{F}_{13}[X]$.

11 (*a*) Probar que -1 es un cuadrado en $\mathbb{F}_p$ si y sólo si $p = 2$ o $p \equiv 1 \pmod 4$.

(*b*) Deducir que si $p \equiv 3 \pmod 4$ entonces $\mathbb{F}_{p^2} = \mathbb{F}_p(i)$, donde $i^2 = -1$.

(*c*) Con esta última identificación, ¿cómo actúa el morfismo de Frobenius correspondiente a la extensión $\mathbb{F}_{p^2}/\mathbb{F}_p$?

12 Sea $\mathbb{F}_q$ un cuerpo finito cuya característica no es 2 (es decir, con q impar).

(*a*) Probar que hay exactamente $\frac{q+1}{2}$ elementos de $\mathbb{F}_q$ que son cuadrados en $\mathbb{F}_q$.

(*b*) Probar que para todo $x \in \mathbb{F}_q$ existen $a, b \in \mathbb{F}_q$ tales que $x = a^2 + b^2$.

Sugerencia. Esto ocurre si y sólo si el conjunto $\{x - a^2 : a \in \mathbb{F}_q\}$ contiene algún cuadrado.

13 Sean K un cuerpo finito, $f \in K[X]$ un polinomio de grado n y E el cuerpo de descomposición de f sobre K. Sabiendo que $[E : K] = 2021$, determinar el mínimo valor posible de n.

Sugerencia. 2021 se factoriza como 43×47.

14 (*a*) Probar que todo polinomio $f \in \mathbb{F}_q[X]$ de grado 2 se factoriza linealmente en $\mathbb{F}_{q^2}[X]$.

(*b*) Dar un ejemplo de un polinomio $f \in \mathbb{F}_q[X]$ de grado 3 que no se factorice linealmente en $\mathbb{F}_{q^3}[X]$.

(*c*) ¿Cómo podríamos generalizar entonces el enunciado de (*a*)?

15 Sea n un entero positivo tal que $q \equiv 1 \pmod{n}$. Probar que para todo $a \in \mathbb{F}_q$, el polinomio $X^n - a$ se factoriza linealmente en $\mathbb{F}_{q^n}[X]$.

16 Sea $q = p^m$ con p impar. Sea $G = SL(2, \mathbb{F}_q)$ el grupo de matrices de 2×2 con coeficientes en $\mathbb{F}_q$ cuyo determinante es 1.

(*a*) Probar que $|G| = (q-1)q(q+1)$.

(*b*) Probar que G contiene elementos de orden d si y sólo si d divide a $q-1$, $q+1$ o $2p$.

Sugerencia. Dada $A \in G$ hay 3 casos según cómo sean las raíces de χ_A. ¿Les suena?

Sea K un cuerpo tal que la característica de K no divide a n. Podemos tomar entonces $\xi_n \in \overline{K}$ una raíz n-ésima primitiva de la unidad. La extensión $K(\xi_n)/K$ se llama *extensión ciclotómica* de índice n.

17 Calcular el grado de la extensión ciclotómica en cada uno de los siguientes casos:

(*a*) $K = \mathbb{Q}, \quad n = 120$

(*b*) $K = \mathbb{Q}(i), \quad n = 120$

(*c*) $K = \mathbb{Q}\left(\sqrt{3}\right), \quad n = 12$

(*d*) $K = \mathbb{Q}\left(\sqrt[3]{2}\right), \quad n = 100$

18 (*a*) Sea $E/\mathbb{Q}$ una extensión de grado 2. Probar que Φ_n es reducible en $E[X]$ si y sólo si $E \subset \mathbb{Q}(\xi_n)$.

(*b*) Determinar todas las extensiones $E/\mathbb{Q}$ de grado 2 tales que Φ_{12} es irreducible en $E[X]$. Ídem para Φ_8 y Φ_{10}.

19 Determinar todos los $n \in \mathbb{N}$ tales que el polinomio ciclotómico Φ_n es irreducible sobre $\mathbb{Q}(\xi_9)$.

20 (*a*) Probar que $\lim_{n\to\infty} \varphi(n) = +\infty$.

(*b*) Deducir que si $E/\mathbb{Q}$ es una extensión finita, entonces E contiene sólo finitas raíces de la unidad.

21 Probar las siguientes propiedades de los polinomios ciclotómicos:

(*a*) Si p es primo y $r \in \mathbb{N}$, entonces $\Phi_{p^r}(X) = \Phi_p\left(X^{p^{r-1}}\right)$.

(*b*) Si n es impar, entonces $\Phi_{2n}(X) = \Phi_n(-X)$.

(*c*) Si p es primo y $p \nmid n$, entonces $\Phi_{pn}(X) = \dfrac{\Phi_n(X^p)}{\Phi_n(X)}$.

22 Sea $q = p^m$ donde p es un primo que no divide a n. Probar que el grado de la extensión ciclotómica $\mathbb{F}_q(\xi_n)/\mathbb{F}_q$ coincide con el orden de q en el grupo $\mathscr{U}(\mathbb{Z}/n\mathbb{Z})$, es decir, el mínimo $d \in \mathbb{N}$ tal que $q^d \equiv 1 \pmod{n}$.

23 Probar que $\Phi_8 = X^4 + 1$ es reducible en $\mathbb{F}_p[X]$ para todo primo p.

Nota. Esto responde una pregunta de la Práctica 1.

24 Dados $n, m \in \mathbb{Z}$, probar que el polinomio $X^6 + (5n+1)X^3 + (5m+1)$ es irreducible en $\mathbb{Q}[X]$.

Nota. En alguna guía anterior probaron que $X^6 - 4X^3 + 1$ era irreducible. Ahora es más fácil.

25 Sea $a \in \mathbb{Z}$ y sea p un primo tal que $p \mid \Phi_n(a)$. Probar que entonces $p \mid n$ o bien $p \equiv 1 \pmod{n}$.

26 **(Teorema de Dirichlet, versión débil)** Probar que para todo $n \in \mathbb{N}$ existen infinitos primos congruentes a 1 módulo n.

Sugerencia. Suponer que hay sólo finitos, y usar el ejercicio anterior para llegar a un absurdo "a la Euclides".

Nota. Más en general, el *Teorema de Dirichlet* afirma que dados $a, b \in \mathbb{N}$ coprimos, existen infinitos primos de la forma $am + b$.