Práctica 5: Cuerpos finitos - Extensiones ciclotómicas

Dado un anillo A, siempre existe un único morfismo de anillos $f : \mathbb{Z} \to A$. Como $\mathbb{Z}$ es un DIP, sabemos que existe un único entero no negativo n tal que $\ker f = n\mathbb{Z}$. Este número n se llama la *característica* del anillo A.
Notar que también se podría definir la característica de A como el menor entero positivo n tal que $\underbrace{1+\ldots+1}_{n \text{ sumandos}} = 0$ en A, o 0 en caso de que no exista tal n.

1 Probar que si A es un dominio íntegro entonces la característica de A es 0 o un número primo.

2 Sea $p \in \mathbb{N}$ un número primo. Probar que existe un único cuerpo de p elementos salvo isomorfismo, al cual llamaremos $\mathbb{F}_p$.

En adelante, cada vez que usemos la frase "característica p" estaremos suponiendo tácitamente que $p \in \mathbb{N}$ es un número primo.

3 Sea K un cuerpo de característica p. Probar que $\sigma : K \to K$ dado por $\sigma(x) = x^p$ es morfismo de cuerpos.

4 Sea K un cuerpo de característica p. Probar que K contiene un subcuerpo isomorfo a $\mathbb{F}_p$. Deducir que si K es un cuerpo finito entonces la cantidad de elementos de K es de la forma p^m con p primo y $m \in \mathbb{N}$.

5 Sea K un cuerpo de p^m elementos. Probar que $x^{p^m} = x$ para todo $x \in K$.

Sugerencia. Considerar el grupo $K^\times = (K - \{0\}, \cdot)$.

A partir de ahora, fijamos una clausura algebraica de $\mathbb{F}_p$ y la llamamos $\overline{\mathbb{F}_p}$.

6 Sea $q = p^m$, con p primo y $m \in \mathbb{N}$.

(a) Probar que el polinomio $X^q - X \in \mathbb{F}_p[X]$ es separable.

(b) Sea $\mathbb{F}_q = \{\alpha \in \overline{\mathbb{F}_p} \mid \alpha^q = \alpha\}$. Probar que $\mathbb{F}_q$ es un subcuerpo de $\overline{\mathbb{F}_p}$ que tiene q elementos. Más aún, es el único tal subcuerpo.

(c) Usando la unicidad de los cuerpos de descomposición, probar que todo cuerpo de q elementos es isomorfo a $\mathbb{F}_q$.

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

8 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 $\mathbb{F}_{q^k}[X]$?

9 (a) Probar que $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$ si y sólo si m divide a n.

(b) Deducir 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.

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

11 Probar que $X^{q^n} - X$ es igual al producto de todos los polinomios mónicos irreducibles en $\mathbb{F}_q[X]$ cuyo grado divide a n.

12 **(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.

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

14

(*a*) Sea $(G, \cdot)$ un grupo abeliano de orden n, y sea $d = \max\{\mathrm{ord}(x) : x \in G\}$. Probar que $x^d = 1$ para todo $x \in G$. ¿Es cierto esto si el grupo no es abeliano?

(*b*) Sea K un cuerpo y sea G un subgrupo finito de $K^\times$. Probar que G es cíclico.

(*c*) Deducir que para todo $n \in \mathbb{N}$ existen polinomios irreducibles en $\mathbb{F}_q[X]$ de grado n.

15 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?

16 Sea $\mathbb{F}_{q^n}/\mathbb{F}_q$ una extensión de cuerpos finitos. Sea $\sigma : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ dado por $\sigma(x) = x^q$ (se llama el **morfismo de Frobenius**).

(*a*) Probar que $\sigma \in \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$.

(*b*) Probar que el orden de σ en el grupo de Galois es n.

(*c*) Concluir que toda extensión de cuerpos finitos es cíclica, con grupo de Galois generado por el morfismo de Frobenius.

17 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 $\mathbb{F}_q[X]$?

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

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

20 (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 $\mathbb{F}_{p^2}/\mathbb{F}_p$?

21 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.

22 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.

23 (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)?

24 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 $\mathbb{F}_{q^n}[X]$.

25 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?

Fijemos un cuerpo algebraicamente cerrado L. Sea $G_n(L) = \{x \in L \mid x^n = 1\}$. Los elementos de G_n se llaman *raíces n-ésimas de la unidad*.

26 (a) Probar que G_n es un subgrupo finito de $L^\times$, y por lo tanto es cíclico.

(b) Probar que si la característica de L no divide a n, entonces $|G_n(L)| = n$. (En particular notar que esto pasa para todo n si L tiene característica 0.)

En este caso, un generador de $G_n(K)$ se llama una *raíz n-ésima **primitiva** de la unidad*.

(c) Probar que si L tiene característica p y $n = p^m \cdot s$ con $p \nmid s$, entonces $G_n(L) = G_s(L)$, y por lo tanto $|G_n(K)| = s$.

Ahora, sea K un cuerpo cualquiera 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.

27 Probar que $K(\xi_n)/K$ es una extensión de Galois, y su grupo de Galois es isomorfo a **un subgrupo de** $\mathscr{U}(\mathbb{Z}/n\mathbb{Z})$. En particular, es una extensión abeliana.

28 A través del único morfismo de anillos $f : \mathbb{Z} \to K$, podemos pensar al polinomio ciclotómico Φ_n con coeficientes en $K[X]$.

(a) Probar que (al igual que pasaba en $\mathbb{C}$) las raíces de Φ_n en $\overline{K}$ son exactamente las raíces n-ésimas primitivas de la unidad.

(b) Probar que son equivalentes:

(i) Φ_n es irreducible en $K[X]$,

(ii) $[K(\xi_n) : K] = \varphi(n)$,

(iii) $\mathrm{Gal}(K(\xi_n)/K) \cong \mathcal{U}(\mathbb{Z}/n\mathbb{Z})$.

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

30 (a) Probar que $\lim\limits_{n\to\infty} \varphi(n) = +\infty$.

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

31 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 $\Phi_{pn}(X) = \dfrac{\Phi_n(X^p)}{\Phi_n(X)}$.

32 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 $\mathcal{U}(\mathbb{Z}/n\mathbb{Z})$, es decir, el mínimo $d \in \mathbb{N}$ tal que $q^d \equiv 1 \pmod{n}$.

33 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.

34 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.

35 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 $p \equiv 1 \pmod{n}$.

Nota. En la primera clase de polinomios ciclotómicos, Agus usó este lema para probar un caso particular del *Teorema de Dirichlet*: para todo n hay infinitos primos congruentes a 1 módulo n.