Álgebra III

Práctica 6 – Segundo Cuatrimestre de 2018

Cuerpos finitos y extensiones ciclotómicas

Ejercicio 1. Sea K un cuerpo finito. Probar que el grupo multiplicativo K^* es cíclico. Concluir que toda extensión finita de un cuerpo finito es simple.

Ejercicio 2. Sea $p \in \mathbb{N}$ un primo y sean $n, m \in \mathbb{N}$. Probar que $\mathbb{F}_{p^n} \subseteq \mathbb{F}_{p^m}$ si y solo si $n|m$.

Ejercicio 3. Sea K un cuerpo de q elementos.

1. Sea $f \in K[X]$ irreducible. Probar que $f|X^{q^n} - X$ si y solo si $\mathrm{gr}(f)|n$.
2. Probar que $X^{q^n} - X = \prod_{d|n}(\prod f)$, donde el producto de adentro recorre todos los $f \in K[X]$ irreducibles mónicos de grado d.
3. Probar que $q^n = \sum_{d|n} u(d)d$, donde $u(d)$ es la cantidad de polinomios mónicos irreducibles de grado d en $K[X]$.
4. Calcular cuántos polinomios irreducibles de grados 3 y 4 hay en un cuerpo de 2^{12} elementos. Lo mismo en un cuerpo de 3^{12} elementos.
5. * Obtener una fórmula cerrada para $u(n)$ para todo $n \in \mathbb{N}$.

Ejercicio 4. Sea $f \in \mathbb{F}_q[X]$ irreducible de grado n y sea $k \in \mathbb{N}$. Probar que f se factoriza en $\mathbb{F}_{q^k}[X]$ como producto de polinomios irreducibles de grado n/d, donde $d = (n : k)$. Concluir que f sigue siendo irreducible en $\mathbb{F}_{q^k}[X]$ si y solo si n y k son coprimos.

Ejercicio 5. Sea $p \in \mathbb{N}$ primo. Sea C una clausura algebraica de $\mathbb{F}_p$. Probar que existe un elemento en $\mathrm{Gal}(C/\mathbb{F}_p)$ que no es una potencia del automorfismo de Frobenius $\sigma : C \to C$ dado por $\sigma(x) = x^p$. Mas aún, caracterizar el grupo de Galois $\mathrm{Gal}(C/\mathbb{F}_p)$.

Ejercicio 6. Sea $n \in \mathbb{N}$ impar, y sea K un cuerpo de característica distinta de 2. Probar que K contiene a una raíz n-ésima primitiva de la unidad si y solo si contiene una raíz $2n$-ésima primitiva de la unidad.

Ejercicio 7.

1. Sea $K/\mathbb{Q}$ una extensión finita. Probar que hay sólo un número finito de raíces de la unidad en K.
2. Hallar todas las raíces de la unidad en K cuando K es uno de los siguientes cuerpos: $\mathbb{Q}[i]$, $\mathbb{Q}[\sqrt{-2}]$, $\mathbb{Q}[\xi_9]$, $\mathbb{Q}[\sqrt{2}, \sqrt{-3}]$, $\mathbb{Q}[\sqrt[p]{2}]$.

Ejercicio 8. Hallar todos los $n \in \mathbb{N}$ tales que Φ_n es irreducible sobre $\mathbb{Q}(\xi_9)$.

Ejercicio 9. Para cada $n \in \mathbb{N}$ sea Φ_n el polinomio ciclotómico de orden n sobre $\mathbb{Q}$. Probar que

1. Si p es primo y $r \in \mathbb{N}$ entonces $\Phi_{p^r}(X) = \Phi_p(X^{p^{r-1}})$.
2. Si p es primo y p no divide a n entonces $\Phi_{pn}(X)\Phi_n(X) = \Phi_n(X^p)$.
3. Calcular explícitamente Φ_{18} y Φ_{30}.

Ejercicio 10. Sea K un cuerpo de q elementos y sea $n \in \mathbb{N}$ coprimo con $\mathrm{car}(K)$. Sea $E = K[\xi_n]$, donde ξ_n es una raíz primitiva n-ésima de la unidad.

1. Probar que $[E : K] = m$, donde $m \in \mathbb{N}$ es el menor natural tal que $n|q^m - 1$.
2. Probar que Φ_n se factoriza en $K[X]$ como producto de polinomios irreducibles de grado m.
3. Deducir que Φ_n es irreducible en $K[X]$ si y solo si q tiene orden $\varphi(n)$ en $\mathcal{U}_n$.

Ejercicio 11. Probar que $f = X^4 + 1$ es reducible en $\mathbb{F}_p[X]$ para todo $p \in \mathbb{N}$ primo. Es f reducible en $\mathbb{Z}[X]$?

Ejercicio 12. Probar que:

1. $\mathbb{F}_3$ no contiene raices 13-ésimas de la unidad distintas de 1.
2. Si $\xi_{13} \in \overline{\mathbb{F}_3}$ es una raíz 13-ésima primitiva de la unidad, entonces $[\mathbb{F}_3[\xi_{13}] : \mathbb{F}_3] = 3 < \varphi(13)$.

Ejercicio 13. Sea $n, m \in \mathbb{Z}$. Probar que el polinomio $x^6 - (5n+1)x^3 + (5m+1)$ es irreducible en $\mathbb{Q}[X]$.

Ejercicio 14. Hallar todos los $n \in \mathbb{N}$ tales que Φ_n es irreducible en $\mathbb{F}_9[X]$.

Ejercicio 15. Sea $p \in \mathbb{N}$ primo. Hallar todos los $n \in \mathbb{N}$ tales que Φ_6 es irreducible en $\mathbb{F}_{p^n}$.

Ejercicio 16. Factorizar $\Phi_7(X)$ en $\mathbb{F}_{27}[X]$ y $\Phi_9(X)$ en $\mathbb{F}_7(t)[X]$.

Ejercicio 17. Sea K un cuerpo de q elementos y sea n coprimo con q. Sea $\xi_n \in \overline{K}$ una raíz primitiva n-ésima de la unidad. Probar que

$$\xi_n + {\xi_n}^{-1} \in K \iff q \equiv \pm 1 \text{ mód } n.$$

Ejercicio 18. Decimos que $f \in \mathbb{F}_q[X]$ irreducible es *primitivo* si alguna de sus sus raíces genera multiplicativamente su cuerpo de descomposición (es decir, es raiz primitiva de $\mathbb{F}_q^\times$).

1. Probar que todas las raíces de un f primitivo son raíces primitivas.
2. Hallar la cantidad de polinomios primitivos de grado n en $\mathbb{F}_q[X]$.

Ejercicio 19. (Test de Rabin) Sean $p_1, \dots, p_k$ los divisores primos de n. Notamos $n_i = n/p_i$ para $i = 1, \dots, k$. Un polinomio $f \in \mathbb{F}_q[X]$ de grado n es irreducible si y sólo si $\gcd(f, X^{q^{n_i}} - X) = 1$ para todo $i = 1, \dots, k$, y f divide a $X^{q^n} - X$.

Ejercicio 20. (Algoritmo de Berlekamp) Sea $f \in \mathbb{F}_q[X]$ libre de cuadrados. Sea $K \subseteq \mathbb{F}_q[X]/f\mathbb{F}_q[X]$ el núcleo del endomorfismo $g \mapsto g^q - g$.

1. Probar que K es una $\mathbb{F}_q-$subálgebra de $\mathbb{F}_q[X]/f\mathbb{F}_q[X]$.
2. Probar que la cantidad de factores irreducibles de f coincide con $\dim_{\mathbb{F}_q} K$.
3. Probar que $f(X) = \prod_{a\in\mathbb{F}_q} \gcd(f(X), g(X) - a)$ para todo $g \in K$.

Ejercicio 21. Sea $\xi = \xi_p$ una raíz $p-$ésima primitiva de la unidad con p primo. Probar que $\mathbb{Z}[\xi]/(1-\xi)\mathbb{Z}[\xi] \simeq \mathbb{F}_p$.

Ejercicio 22. Sea $P \in \mathbb{Z}[X_1, \dots, X_n]$. Supongamos que para cierta $n-$upla $(\xi_1, \dots, \xi_n) \in \mu_p(\mathbb{C})^n$ de raíces $p-$ésimas de la unidad (no necesariamente primitivas) se tiene que $P(\xi_1, \dots, \xi_n) = 0$. Probar que $P(1, \dots, 1) \equiv 0 \pmod{p}$.

Ejercicio 23. Sea $g \in \mathbb{F}_p[X] \setminus \{0\}$ de grado menor que p. Sea $\alpha \in \mathbb{F}_p^\times$ un elemento no nulo de $\mathbb{F}_p$. Probar que la nultiplicidad de α como raíz de g es menor que la cantidad de coeficientes no nulos de g.

$*$ **Ejercicio 24.** (Principio finito de incertidumbre) Sea $A \in \mathbb{C}^{p\times p}$ la matriz de Vandemonde definida por las raíces $p-$ésimas de la unidad. Probar que todos sus menores son invertibles. Sugerencia: usar los ejercicios anteriores.

Ejercicio 25. (Chevalley–Warning) Sean p primo y $q = p^m$ para cierto $m \geq 1$.

1. Probar que para todo $k = 1, \dots, q-2$ se tiene que $\displaystyle\sum_{x\in\mathbb{F}_q} x^k = 0$.
2. Si $f \in \mathbb{F}_q[X_1, \dots, X_n]$ de grado total menor que $n(q-1)$ entonces $\displaystyle\sum_{x\in\mathbb{F}_q^n} f(x) = 0$.
3. Sean $\{f_i\}_{i=1}^r \subseteq \mathbb{F}_q[X_1, \dots, X_n]$ Probar que el número de soluciones de $f_1(x) = \ldots = f_r(x) = 0$ es congruente módulo p a $\displaystyle\sum_{x\in\mathbb{F}_q^n} \prod_{i=1}^r (1 - f_i^{q-1}(x))$.
4. Supongamos además que f_i tiene grado total d_i y $\sum d_i < n$. Probar que el número de soluciones de $f_1(x) = \ldots = f_r(x) = 0$ es múltiplo de p.

Ejercicio 26. Sean $a, b, c \in \mathbb{F}_q^\times$ con q impar. Probar que existen $x, y \in \mathbb{F}_q$ tales que $ax^2 + by^2 = c$. Sugerencia: homogeneizar.

Ejercicio 27. Sean $p > 2$ primo y $g \in \mathbb{F}_p^\times$ una raíz primitiva (es decir, un generador del grupo multiplicativo de los restos módulo p). Para $x \in \mathbb{F}_p^\times$ notamos $\log_g(x)$ al menor entero no negativo k tal que $g^k = x$. Probar que

$$\log_g(x) \equiv -1 + \sum_{i=1}^{p-2} \frac{x^i}{g^{-i} - 1}.$$

En particular, el polinomio que interpola al logaritmo discreto módulo p tiene por coeficientes una permutación de $\mathbb{F}_p^\times$.

Ejercicio 28. (Lucas–Lehmer) Sean $p \geq 3$ primo, $q = 2^p - 1$ y r el menor divisor primo de q. Se define recursivamente la sucesión $s_0 = 4$, $s_{k+1} = s_k^2 - 2$.

1. Probar que $s_k = (2+\sqrt{3})^{2^k} + (2-\sqrt{3})^{2^k}$.
2. Probar que 2 es resto cuadrático $\mod (r)$.
3. Probar que el grupo de unidades de $R := \mathbb{F}_r[X]/(X^2-3)$ tiene orden a lo sumo $r^2 - 1$.
4. Probar que si q es primo entonces 3 no es un cuadrado en $\mathbb{F}_q$.
5. $*$ Probar que q es primo si y sólo si $s_{p-2} \equiv 0 \mod (q)$.

$*$ **Ejercicio 29.** Con ayuda de una computadora probar que $M_{127} := 2^{127} - 1$ es primo.

Ejercicio 30. Sea $p \equiv 3 \mod (4)$ primo. Probar que $2p+1$ es también primo si y sólo si $2p+1$ divide a $2^p - 1$.

Ejercicio 31. (Teorema de Kronecker) Sea $f = \prod_{i=1}^{n}(X - \alpha_i)$ la factorización en $\mathbb{C}$ de un $f \in \mathbb{Z}[X]$ mónico. Supongamos que $0 < |\alpha_i| \leq 1$ para todo $i = 1, \ldots, n$. Probar que:

i) $f_m := \prod_{i=1}^{n}(X - \alpha_i^m) \in \mathbb{Z}[X]$.

ii) los coeficientes de f_m están acotados.

iii) $\{f_m\}_{m\geq 1}$ sólo recorre un número finito de polinomios.

iv) f es un producto de ciclotómicos.

v) existe $\alpha \in \overline{\mathbb{Q}} \setminus \overline{\mathbb{Z}}$ con la propiedad de tener todos sus conjugados de módulo 1.

Ejercicio 32. Sea $K/\mathbb{Q}$ de grado finito. Probar que K sólo tiene finitas raíces de la unidad.

Ejercicio 33. Sea $f = (X^2 + X + 1)^2 - 2X^2$. Probar que:

a) f es irreducible en $\mathbb{Q}[X]$.

b) sólo tiene dos raíces de módulo 1.

Ejercicio 34. Sean $\alpha, \beta \in \mathbb{C}$ raíces primitivas de la unidad de órdenes p y $p-1$ respectivamente, con $p > 2$ primo. Elegimos un $g \in \mathbb{F}_p^{\times}$ de orden $p-1$. Para $j = 1, \ldots, p-1$ sea $t_j := \sum_{k=1}^{p-1} \alpha^{g^k}\beta^{jk}$.

(i) Hallar $\mathrm{Gal}(\mathbb{Q}[\alpha,\beta]/\mathbb{Q}[\beta])$.

(ii) Probar que $\alpha = \dfrac{1}{p-1}(t_1 + \ldots + t_{p-1})$.

(iii) Probar que $(t_j)^{p-1} \in \mathbb{Q}[\beta]$.

(iv) Probar que $t_j(t_1)^{p-1-j} \in \mathbb{Q}[\beta]$.

Ejercicio 35. (Suma de Gauss) Sean $g := \sum_{k=0}^{p-1} \xi_p^{k^2}$ donde $\xi_p \in \mathbb{C}$ es una raíz primitiva de orden p y σ un generador de $\mathrm{Gal}(\mathbb{Q}[\xi_p]/\mathbb{Q})$. Probar que:

1) $g = \displaystyle\sum_{k=0}^{p-2} (-1)^k \sigma^k(\xi_p)$.

2) $g^2 = (-1)^{(p-1)/2} p$.

Ejercicio 36. Sea $A \in \mathrm{GL}_n(\mathbb{F}_q)$.

1. Probar que el orden de A es a lo sumo $q^n - 1$.
2. Hallar el orden de $\mathrm{GL}_n(\mathbb{F}_q)$.

Ejercicio 37. Sean $p_1, \ldots, p_n$ números primos positivos distintos y $f \in \mathbb{Q}[X]$ el minimal de $\sqrt{p_1} + \ldots + \sqrt{p_n}$. Probar que para todo primo p la reducción de f módulo p se factoriza como producto de polinomios de grado 1 o 2.

Ejercicio 38. Para cada $n \geq 1$ notamos $B_n \subseteq \mu_n(\mathbb{C})$ al conjunto de raíces primitivas $n-$ésimas de la unidad.

(a) Hallar $\displaystyle\sum_{\xi \in B_n} \xi$.

(b) Probar que B_n es una base normal de $\mathbb{Q}[\xi_n]/\mathbb{Q}$ si y sólo si n es libre de cuadrados.

Ejercicio 39. Veamos a $\mathbb{F}_{q^n}$ como $\mathbb{F}_q[X]-$módulo donde X actúa como el Frobenius $X \cdot \alpha := \alpha^q$.

I) Probar que los submódulos de $\mathbb{F}_{q^n}$ admiten un *vector cíclico* (i.e.: son monogeneados).

II) Probar que $\mathbb{F}_{q^n}$ admite una base normal.

$*$ **Ejercicio 40.** Sea $q = 2^p - 1$ un primo de Mersenne. Supongamos que $X^p + X + 1 \in \mathbb{F}_2[X]$ es irreducible. Probar que $X^q + X + 1 \in \mathbb{F}_2[X]$ es irreducible. Sugerencia: ejercicio anterior.

Ejercicio 41. Para $f \in \mathbb{F}_q[X]$ notamos $\varphi_q(f)$ a la cantidad de polinomios en $\mathbb{F}_q[X]$ de grado menor que f coprimos con f. Probar que

1. $\varphi_q(f) = 1$ si $\mathrm{gr}(f) = 0$.
2. $\varphi_q(fg) = \varphi_q(f)\varphi_q(g)$ si $(f, g) = 1$.
3. si $\mathrm{gr}(f) = n$ entonces
$$\varphi_q(f) = q^n \prod (1 - q^{-n_i})$$
donde n_i son los grados de los factores mónicos irreducibles que dividen a f.

Ejercicio 42. Probar que $\mathbb{F}_{q^m}/\mathbb{F}_q$ tiene exactamente $\frac{1}{m}\varphi_q(X^m - 1)$ bases normales.

$*$ **Ejercicio 43.** Probar que

$$X^{2^{2^{2^{2^2-1}-1}-1}-1} + X + 1 \in \mathbb{F}_2[X]$$

es irreducible (recuerde que 170141183460469231731687303715884105727 es primo).