Departamento de Álgebra,
Geometría y Topología.
Universidad de Málaga.

Ejercicios de Álgabra Clásica

Relación 8.
Cuerpos finitos.

10 de diciembre de 2009.

Profesor de la asignatura:
José Antonio Cuenca Mira.

8. Cuerpos finitos

8.1 Mostrar que todo cuerpo cuyo grupo multiplicativo es cíclico es necesariamente finito.

8.2 Sea F un cuerpo finito y p su característica. Usar el teorema de Cauchy para demostrar que el cardinal de F es una potencia de p.

8.3 Sea G un grupo abeliano finito de orden n. Comprobar que para todo entero positivo d que divide a n existe un único subgrupo de G de orden d. Demostrar hay exactamente $\varphi(d)$ elementos de G cuyo orden es d, donde $\varphi : \mathbb{N}_> \longrightarrow \mathbb{N}_>$ es la *función φ de Euler* definida por $\varphi(1) = 1$ y siendo $\varphi(n)$ el número de enteros positivos menores que n y primos relativos con él. Mostrar finalmente que

$$\sum_{d|n} \varphi(d) = n.$$

8.4 Sea G un grupo multiplicativo de orden n con la propiedad de que para todo entero positivo d que divide a n existen a lo más d elementos para los que se satisface la igualdad $x^d = 1$. Usar el ejercicio anterior para demostrar que G es cíclico.

8.5 Sea F un cuerpo finito de q elementos. Demostrar que toda aplicación $\chi : F \longrightarrow F$ está representada por un único polinomio de grado estrictamente menor que q y que dicho polinomio es $f(X) = \sum_{a\in F} \chi(a)\Big(1 - (X - a)^{q-1}\Big)$.

8.6 Sean p y n enteros positivos, con p primo y n dividiendo a $p - 1$. Demostrar que la congruencia $x^n \equiv 1 (\text{mód}\, p)$ tiene exactamente n soluciones en $\mathbb{Z}/(p)$.

8.7 ¿Cómo puede generalizarse el ejercicio anterior en el caso de los cuerpos finitos?

8.8 Sea p un primo positivo que es congruente con 3 módulo 4. Demostrar que la congruencia $x^2 \equiv -1 (\text{mód}\, p)$ no tiene soluciones en $\mathbb{Z}/(p)$.

8.9 Demostrar que en un cuerpo finito F todo elemento es suma de dos cuadrados. [Indicación. Considerar separadamente los casos en que F tiene tiene o no característica 2].

8.10 Supóngase que el cuerpo F goza de la propiedad siguiente: si $f \in F[X]$ tiene dos raíces distintas en F entonces su derivada formal f' tiene también alguna raíz en F. Mostrar que F tiene característica cero y que el cuerpo $\mathbb{R}$ de los número reales tiene dicha propiedad.

8.11 Para todo entero $r > 0$, se denota por S_r a la suma de las potencias r-ésimas de los elementos de un cuerpo finito dado de q elementos. Demostrar que

$$S_r = \begin{cases} -1 & \text{si } q - 1 \mid r \\ 0 & \text{en otros casos} \end{cases}$$

[Indicación. En el caso que $q - 1 \not| r$, obsérvese la existencia de algún elemento del cuerpo con potencia r-ésima distinta de 1.]

8.12 Sea F un cuerpo finito de q elementos, p la característica de F y $n \geq 1$ un entero. Supóngase $f_1, \ldots, f_r \in F[X_1, \ldots, X_n]$ tales que $\sum f_i < n$. Sea V el subconjunto de F^n que consta de todas las raíces comunes que tienen los polinomios $f_1, \ldots, f_r$ en F^n. Comprobar que el polinomio $h = \prod_{i=1}^{r}(1 - f_i^{q-1}$ es tal que para todo $x = (x_1, \ldots, x_n) \in F^n$ se tiene

$$h(x) = \begin{cases} 1 & \text{si } x \in V \\ 0 & \text{si } x \notin V \end{cases}$$

Para todo $f \in F[X_1, \ldots, X_n]$, denótese por $S(f)$ a la suma $\sum_{x\in F^n} f(x)$. Demostrar que $S(h)$ es un elemento del cuerpo primo de F que coincide con $|V|1$. Expresando h como combinación lineal de monomios de grado extrictamente menor que $n(q - 1)$ y usando el ejercicio precedente, demostrar que $S(h) = 0$ y que, en consecuencia, se tiene el *teorema de Chevalley-Warning* que asegura que el número de puntos de V es divisible por p.

8.13 Sea F un cuerpo finito. Demostrar que toda forma cuadrática sobre F de a lo menos tres variables se anula en algún punto no nulo y, en particular, toda cónica del plano proyectivo $\mathcal{P}_2(f)$ es no vacía.

8.14 Sea F un cuerpo con la misma propiedad que el cuerpo F del ejercicio anterior. Sean a, $b \in F$. Considerando el polinomio $f(X) = X^3 - 3(a^2+b^2)X + 2a^3 - 6ab^2$, demostrar que cada suma de cuadrados de elementos de F es un cuadrado en F.

8.15 Sea F un cuerpo, Ω una clausura algebraica suya y $f(X)$ un polinomio mónico de $F[X]$ que no tiene raíces múltiples. Demostrar que si las raíces de $f(X)$ constituyen un subcuerpo de Ω entonces F tiene característica p y existe algún entero $r \geq 1$ tal que $f(X) = X^{p^r} - X$.

8.16 Sea K un cuerpo finito y n un entero estrictamente positivo. Demostrar que existe algún polinomio irreducible en $K[X]$ de grado n.

8.17 Mostrar que el producto de los elementos no nulos de un cuerpo finito coincide con -1.

8.18 (Wilson) Comprobar que si p es un número primo entonces $(p-1)! \equiv -1 (\text{mód}\, p)$.

8.19 ¿Es verdad el recíproco del teorema de Wilson enunciado en el ejercicio anterior?

8.20 Demostrar que si p es un primo positivo impar entonces

$$\left(\left(\frac{p-1}{2} \right)! \right) \equiv (-1)^{\frac{p+1}{2}} (\text{mód}\, p)$$

8.21 Hallar el polinomio irreducible de una raíz 7-ésima primitiva de la unidad sobre $\mathbb{Z}/(2)$.

8.22 Sea n un entero positivo y F un cuerpo cuya característica es cero o un primo p distinto de 2 que no divide a $4n+1$. Sea K el cuerpo de descomposición del polinomio $X^{2n+1}-1$ sobre el cuerpo F. Demostrar que K coincide con el cuerpo de dewscomposición de $X^{4n+1} - 1$ sobre F. [Indicación. Pruébese que si ε es una raíz $(2n+1)$-ésima primitiva de la unidad, entonces $\eta = -\varepsilon^n$ es una raíz $(4n+2)$-ésima primitiva de la unidad].

8.23 Sea p un primo positivo y $s > 0$ un entero. Demostrar que el grupo aditivo del cuerpo finito F_{p^s} es isomorfo a una suma directa de s copias de $\mathbb{Z}/(p)$.

8.24 Demostrar que sobre un cuerpo finito polinomios irreducibles del mismo grado tienen el mismo cuerpo de descomposición.

8.25 Sean F_q y $F_{q'}$ cuerpos finitos de cardinales q y q'. Comprobar que $F_{q'}$ tiene un subcuerpo isomorfo a F_q si y sólo si existe un primo positivo p tal que $q = p^d$, $q' = p^n$ con $d|n$.

8.26 Sea F un cuerpo de 81 elementos. Determinar el número de raíces distintas que los polinomios $X^{80} - 1$, $X^{81} - 1$ y $X^{88} - 1$ tienen en F.

8.27 Calcular $\Phi_{15}(X)$.

8.28 Sean n y p enteros positivos, con p primo que no divide a n. Demostrar que si hay algún entero k tal que $p \mid \Phi_n(k)$ entonces $p \equiv 1 (\text{mód}\, n)$. Justificar la existencia de infinitos números primos congruentes con 1 módulo n.

8.29 Sea F un cuerpo finito de q elementos, $n \geq 1$ un entero y $f(X)$ un polinomio irreducible de $F[X]$. Demostrar que el polinomio $f(X)$ divide a $X^{q^n} - X$ si y sólo si $\deg f$ divide a n.

8.30 Sea F_q un cuerpo finito de q elementos , K una extensión finita de F_q y x un elemento de K cuyo polinomio irreducible sobre F_q es $p(X)$. Mostrar que los elementos $x, x^q, \ldots, x^{q^{\deg p - 1}}$ son todos distintos y que el conjunto que constituyen coincide con el de las raíces de $p(X)$ en K.

8.31 Sea K/F_q una extensión finita de un cuerpo finito de q elementos. Sea x un elemento de K que genera al grupo multiplicativo $K^\star$. Demostrar que las restantes raíces del polinomio irreducible de x sobre F_q generan también a $K^\star$ y que el grado de éste divide a $\varphi(q^m - 1)$, donde φ es el indicador de Euler.

8.32 Demostrar que el polinomio $X^4 + 1$ es irreducible sobre $\mathbb{Z}$ pero no lo es sobre ningún cuerpo $\mathbb{Z}/(p)$. [Indicación. Comernzar comprobando que para todo primo $p > 2$ el número $p^2 - 1$ es divisible por 8. Utilizar el ejercicio XXX en el caso en que $p > 2$.]

8.33 Sea K/F una extensión finita de cuerpos y $K = F(x)$. Supóngase que F contiene alguna raíz primitiva n-ésima de la unidad y que $x^n \in F$. Demostrar que entonces $x^{[K:F]} \in F$.

8.34 Sean p y ℓ dos primos positivos distintos. Demostrar que el polinomio $f(X) = X^p - 1$ se descompone en factores lineales de $F_\ell[X]$ si y sólo si $\ell \equiv 1 (\text{mód}\, p)$.

8.35 Pruébese que en un cuerpo finito de q elementos se tiene

$$X^{q^n} - X = \prod_{d|n} \prod_{f_d} f_d(X)$$

donde el producto más interno se toma sobre todos los polinomios irreducibles de grado d cuyo coeficiente líder es 1. Por comparación de grados, demuéstrese que

$$q^n = \sum_{d|n} d\psi(d),$$

donde $\psi(d)$ es el cardinal del conjunto de los polinomios irreducibles de grado d de $F_q[X]$.

8.36 Determinar el número de polinomios mónicos irreducibles de grado 3 que hay en $F_{81}[X]$.

8.37 Sea K un cuerpo de característica distinta de 2, n un entero impar mayor o igual que 1 y $\varepsilon \in K$ una raíz n-ésima primitiva de la unidad. Probar que K contiene alguna raíz $2n$-ésima primitiva de la unidad.

8.38 Sea p un primo positivo que no divide al entero positivo n. Demostrar que el polinomio ciclotómico Φ_n es irreducible sobre F_p si y sólo si la clase de p módulo n tiene orden $\varphi(n)$ en el grupo multiplicativo de los elementos inversibles de $\mathbb{Z}/(n)$. [Indicación: Si ε es una raíz n-ésima primitiva de la unidad, demostrar que el menor entero positivo m para el que se tiene $\varepsilon^{p^m-1} = 1$ coincide con $\varphi(n)$, en el caso en que Φ_n sea irreducible sobre F_p.]