

Extensión de caracteres definidos en grupos conmutativos finitos

Objetivos. Demostrar el teorema sobre la extensión de caracteres sobre grupos finitos conmutativos.

Prerrequisitos. Caracteres de un grupo conmutativo finito, el grupo dual de un grupo conmutativo finito, subgrupos, grupos cíclicos, construcción de un caracter no trivial sobre un grupo cíclico.

Estos apuntes están basados en el libro Lidl, Niederreiter, “Finite fields”, 2nd. ed., 1997.

Usamos la notación aditiva para el grupo G . Denotamos por 0_G al elemento neutro de G .

Lema 1 (sobre el subgrupo de un grupo conmutativo, generado por un subgrupo y un elemento). *Sean G un grupo conmutativo finito, H un subgrupo de G , $H \neq G$, $a \in G \setminus H$. Denotemos por X al siguiente conjunto:*

$$X := \{x \in G: \exists j \in \mathbb{Z} \quad \exists h \in H \quad x = ja + h.\}$$

Entonces, X es un subgrupo de G . Más aún, X es el mínimo entre todos los subgrupos que contienen $H \cup \{a\}$. En otras palabras, X es el subgrupo de G generado por $H \cup \{a\}$.

Demostración. 1. Mostremos que $H \cup \{a\} \subseteq X$.

$$a = \underbrace{1}_{\in \mathbb{Z}} \cdot a + \underbrace{0_G}_{\in H} \in X.$$

Si $h \in H$, entonces

$$h = \underbrace{0}_{\in \mathbb{Z}} \cdot a + \underbrace{h}_{\in H} \in X.$$

2. Mostremos que X es un subgrupo de G . Si $x = ja + h$, $y = ka + g$, donde $j, k \in \mathbb{Z}$, $h, g \in H$, entonces

$$x + y = (j + k)a + (h + g) \in X.$$

El elemento 0_G pertenece a X :

$$0_G \in H \subseteq X.$$

Mostremos que si $x \in X$, entonces $-x \in X$. Si x es de la forma $j \cdot a + h$, donde $j \in \mathbb{Z}$, $h \in H$, consideremos el elemento

$$y := (-j) \cdot a + (-h).$$

Es fácil ver que $y \in X$ y $x + y = 0_G$.

3. Sea Y un subgrupo de G tal que $H \cup \{a\} \subseteq Y$. Sea $x \in X$. Entenramos j en $\mathbb{Z}$ y h en H tales que $x = j \cdot a + h$. Como $a \in Y$ y $h \in Y$, tenemos que

$$x = j \cdot \underbrace{a}_{\in Y} + \underbrace{h}_{\in Y} \in Y.$$

Hemos demostrado que $X \subseteq Y$. □

Repaso 2. Dado m en $\mathbb{N}$, denotamos por G_m el conjunto $\{0, 1, \dots, m-1\}$. Ya sabemos que G_m se puede ver como un grupo isomorfo a $\mathbb{Z}_m$.

Lema 3 (descripción más precisa del subgrupo de un grupo conmutativo finito, generado por un subgrupo y un elemento). Sean G, H, a, X como en el lema anterior. Sean

$$J := \{j \in \mathbb{N} : j \cdot a \in H\}, \quad m := \min(J).$$

Definimos $f: G_m \times H \rightarrow X$,

$$f(j, h) := j \cdot a + h.$$

Entonces, f es una biyección.

Demostración. 1. Primero, mostremos que $J \neq \emptyset$, $m \in \mathbb{N}$ y $m \geq 2$. Usamos la suposición que G es finito. Ponemos $n := \#G$. Sabemos que

$$n \cdot a = 0_G \in H,$$

así que $n \in J$. Hemos mostrado que $J \neq \emptyset$. Por el principio de inducción, J tiene un elemento mínimo. Denotamos por m este elemento. Como $a \notin H$, tenemos que $1 \notin J$ y $m \geq 2$.

2. Mostremos que f es inyectiva. Sean $j, k \in G_m$, $h, g \in H$ tales que $f(j, h) = f(k, g)$, es decir,

$$j \cdot a + h = k \cdot a + g.$$

Entonces,

$$(j - k) \cdot a = g - h \in H.$$

Si $j > k$, entonces $j - k \in J$ y $j - k \geq m$. Por otro lado, como $j, k \in G_m$, es fácil ver que $j - k < m$. Contradicción.

De manera similar, es fácil ver que el caso $j < k$ no es posible. Concluimos que $j = k$ y luego $g = h$.

3. Mostremos que f es sobre. Sea $x \in X$. Por el Lema 1, ya sabemos que existen $k \in \mathbb{Z}$, $g \in H$ tales que

$$x = k \cdot a + g.$$

Usando el algoritmo de división de números enteros, encontramos q en $\mathbb{Z}$ y j en G_m tales que

$$k = qm + j.$$

Pongamos $h := g + q \cdot (m \cdot a)$. Entonces,

$$x = k \cdot a + g = (qm + j) \cdot a + g = j \cdot a + g + (qm) \cdot a = j \cdot a + g + q \cdot (m \cdot a) = j \cdot a + h.$$

De la definición de m , se sigue que $m \cdot a \in H$. Por lo tanto, $x = f(j, h)$. $\square$

Observación 4. En general, la función f del lema anterior no necesariamente es un homomorfismo de grupos.

Lema 5 (sobre extensión de caracteres). Sean G un grupo conmutativo finito, H un subgrupo de G , $\varphi \in \hat{H}$, $a \in G \setminus H$. Sea X al grupo generado por H y a . Entonces, existe $\psi \in \hat{X}$ tal que $\psi|_H = \varphi$.

Demostración. 1. Definimos m como en el Lema 3. Notamos que $m \cdot a \in H$, así que $\varphi(m \cdot a)$ está definido y pertenece a $\mathbb{T}$. Como $\mathbb{C}$ es un campo algebraicamente cerrado, el polinomio

$$z^m - \varphi(m \cdot a)$$

tiene una raíz. Denotemos una raíz de este polinomio por ω . Podríamos construir ω de manera más explícita, usando alguna representación exponencial de $\varphi(m \cdot a)$, pero no lo necesitamos. Por la definición de ω , tenemos que

$$\omega^m = \varphi(m \cdot a).$$

Notamos que $|\omega|^m = |\omega^m| = 1$, así que $\omega \in \mathbb{T}$.

2. Por el Lema 3, sabemos que cada elemento x de X se representa de manera única en la forma

$$x = ja + h \quad (j \in G_m, h \in H), \quad (1)$$

Definimos $\psi: X \rightarrow \mathbb{T}$ mediante la siguiente regla. Para cada x , representamos x como (1) y pongamos

$$\psi(x) := \omega^j \varphi(h).$$

Esta definición es consistente. Podemos escribir esta definición de manera más formal, usando la biyección f del Lema 3. Notamos que $f^{-1}(x)$ es un par ordenado. Denotamos sus componentes de manera natural y ponemos

$$\psi(x) := \omega^{(f^{-1}(x))_1} \varphi((f^{-1}(x))_2).$$

Esta forma de definir ψ es equivalente a la definición anterior.

3. Probemos que ψ es un homomorfismo. Sean $x, y \in X$, donde x es de la forma (1), y es de la forma

$$y = k \cdot a + g \quad (k \in G_m, g \in H).$$

Si $j + k < m$, entonces

$$\psi(x + y) = \psi((j + k) \cdot a + (h + g)) = \omega^{j+k} \varphi(h + g) = \omega^j \varphi(h) \omega^k \varphi(g) = \psi(x) \psi(y).$$

Si $j + k \geq m$, entonces

$$x + y = (j + k - m) \cdot a + (h + h + m \cdot a),$$

así que

$$\psi(x + y) = \omega^{j+k-m} \varphi(h + g + m \cdot a) = \omega^j \omega^k \omega^{-m} \varphi(h) \varphi(z) \omega^m = \psi(x) \psi(y).$$

4. Cada x en H se representa en la forma (1) con $j = 0$ y $h = x$, así que

$$\psi(x) = \omega^0 \varphi(x) = \varphi(x)$$

Hemos mostrado que $\psi|_H = \varphi$. □

Teorema 6 (sobre extensión de caracteres). *Si G un grupo finito conmutativo, H un subgrupo de G y $\varphi \in \widehat{H}$, entonces existe $\psi \in \widehat{G}$ tal que $\psi|_H = \varphi$.*

Demostración. Demostremos por inducción sobre q la siguiente afirmación $\mathcal{A}(q)$: para cada grupo finito G , cada subgrupo H de G tal que $\#G = q + \#H$ y cada φ en $\widehat{H}$ existe ψ en $\widehat{G}$ tal que $\psi|_H = \varphi$.

La afirmación $\mathcal{A}(0)$ se cumple: si $H = G$, ponemos $\psi = \varphi$.

Supongamos que $q \in \mathbb{N}$, $q \geq 1$, y las afirmaciones $\mathcal{A}(0), \dots, \mathcal{A}(q-1)$ se cumplen. Demostremos $\mathcal{A}(q)$. Sean G , H , φ como en la definición de $\mathcal{A}(q)$. Elijamos $a \in G \setminus H$. Sea X el subgrupo generado por H y a . Aplicando el Lema 5 construimos ξ in $\widehat{X}$ tal que $\xi|_H = \varphi$. Si $X = G$, entonces $\psi := \xi$. Si $X \neq G$, entonces notamos que $\#X > \#H$ y por eso

$$\#G - \#X < q.$$

Aplicamos la suposición $\mathcal{A}(\#G - \#X)$ con G , X y ξ , y encontramos ψ en $\widehat{G}$ tal que $\psi|_X = \xi$. Luego $\psi|_H = \varphi$. $\square$

Proposición 7. *Si G es un grupo conmutativo finito, $z \in G$ y $z \neq 0_G$, entonces existe χ en $\widehat{G}$ tal que $\chi(z) \neq 1$.*

Demostración. Sea H el grupo cíclico generado por z y sea $m = \#H$. La condición $z \neq 0_G$ implica que $m \geq 2$. Definimos $\varphi: H \rightarrow \mathbb{T}$ mediante la regla

$$\varphi(jz) := \varepsilon_m^j \quad (j \in \{0, \dots, m-1\}).$$

Entonces, $\varphi(z) = \varepsilon_m \neq 1$.

Por el Teorema 6, encontramos χ in $\widehat{G}$ tal que $\chi|_H = \varphi$, y obtenemos que

$$\chi(z) = \varphi(z) \neq 1. \quad \square$$

Proposición 8 ($\widehat{G}$ separa los elementos de G). *Si $x, y \in G$, $x \neq y$, entonces existe χ en $\widehat{G}$ tal que $\chi(x) \neq \chi(y)$.*

Demostración. Sea $z := x - y$. Usando la Proposición 7 encontramos χ en $\widehat{G}$ tal que $\chi(z) \neq 1$. Entonces,

$$\chi(x) = \chi(y)\chi(z) \neq \chi(y). \quad \square$$