No 2

UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE CIENCIAS

ANILLOS DE GRUPO EN LOS CUALES CADA IDEAL IZQUIERDO ES UN IDEAL DERECHO

TESIS

Que para obtener el titulo de

MATEMATICO

Presenta

GERARDO RIOQUINTO AGUILAR SANCHEZ.

MEXICO, D.F. 1982

TESIS CON FALLA DE ORIGEN

Introducción

En este trabajo se dará una clasificación de aquellos anillos de grupo que cumplen la condición de que cada ideal izquierdo es también un ideal derecho - (iiid). No pretende de ninguna manera ser un trabajo original, es simplemente una versión del artículo debido a P. Menal " Group Rings in which every left ideal is a right ideal" Publ. Mat. U.A.B. nº 6 des. 1977 pags. 97 - 105. La notación está tomada de dicho artículo la que a su vez está tomada de [1].

Los principales resultados están en los teoremas 3 y 4. El Teorema 4 (debido a P. Menal) - nos dice que un anillo de grupo $K[G]$ cumpla la condición iiid, es equivalente para G no conmutativo (si el grupo G es conmutativo, el anillo de grupo $K[G]$ es conmutativo y la condición iiid se satisface trivialmente), a pedir que $K[G]$ cumpla la condición de que solo los anuladores izquierdos sean ideales derechos (aiid) y que G sea localmente finito. Es equivalente además, a que el grupo G sea localmente finito y que si el producto de dos elementos es cero, entonces al conmutar dicho producto sigue siendo cero. Combinando estas equivalencias con los resultados del Teorema 3 (también debido a P. Menal), obtenemos condiciones necesarias y suficientes para

- que un anillo de grupo tenga la condición iiid.

El lema 1 inciso i), nos dice que para demostrar que el anillo de grupo $K[G]$ cumple la condición iiid y G es un grupo localmente finito, basta considerar el caso en que G es un grupo finito. Los incisos ii) y iii) del lema 1 son un ejemplo interesante de como es que pedir ciertas condiciones sobre el anillo de grupo $K[G]$, implican condiciones sobre el grupo G, pues nos dicen que pedir que $K[G]$ tenga la condición iiid ó las condiciones Iiid y G localmente finito, implican en cualquier caso que el grupo G es hamiltoniano para G no-conmutativo.

El lema 2 nos da la equivalencia, bajo la hipótesis de que G sea localmente finito, de que el anillo de grupo $K[G]$ tenga la condición aiid, a la condición de pedir que si el producto de dos elementos es cero, al conmutar tal producto sigue siendo cero (de hecho nos da la equivalencia entre ii) y iii) del Teorema 4).

Los teoremas 1 y 2 son dos importantes resultados que se usan en la demostración del Teorema 3. El Teorema 1 es la clasificación de los grupos hamiltonianos, y la demostración está tomada de [2]. Tal demostración se hace por partes que indicadas están con números romanos.

Si la característica $(K) \nmid \cdot (G)$ entonces $K[G]$ es semisimple, tal es el importante resultado debido a

- Maschke y que enunciamos como el Teorema 2. La demostración está tomada de [3], pero ésta demostración no nos dice como es la descomposición de $K[G]$ como suma de anillos simples. Tal descomposición, para el caso en que G es abeliano, puede encontrarse en [4].

Finalmente si usamos el antiautomorfismo de $K[G]$ dado por

$$\sum_{x\in G} a_x x \longmapsto \sum_{x\in G} a_x x^{-1},$$

vemos que $K[G]$ tiene la condición iiid (aiid) $\iff$ $K[G]$ cumple la condición idii (adii) esto es, que cada ideal derecho de $K[G]$ es también un ideal izquierdo (respectivamente cada anulador derecho de $K[G]$ es un ideal izquierdo).

__Agradecimiento__.

Deseo expresar mi mas profundo agradecimiento al Dr. Fransisco Raggi C. por su ayuda y paciencia en la dirección de esta tésis.

Definiciones :

i) Se dice que un grupo G es hamiltoniano ó de Hamilton si G no es abeliano y todos sus subgrupos son normales.

ii) Un grupo G se dice que es localmente finito si todo subgrupo finitamente generado de G es finito.

iii) Un anillo A se dice que tiene la condición iiid ó que es iiid si cada ideal izquierdo de A, es un ideal derecho de A y se dice que A tiene la condición aiid ó bién que es aiid, si cada anulador izquierdo de A es un ideal derecho de A.

Notación :

i) En este trabajo K denotará un campo, G un grupo multiplicativo y $K[G]$ el anillo de grupo.

ii) Si H es un subgrupo de G entónces denotaremos con π_H la función

$$\begin{aligned} \pi_H : K[G] &\longrightarrow K[H] \\ \sum_{x\in G} a_x x &\longmapsto \sum_{x\in H} a_x x \end{aligned}$$

iii) Para $H \triangleleft G$ ρ_H denotará el morfismo de anillos

$$\begin{aligned} \rho_H : K[G] &\longrightarrow K[G/H] \\ \sum_{x\in G} a_x x &\longmapsto \sum_{x\in G} a_x \bar{x} \end{aligned}$$

iv) Para H subgrupo finito de G, escribimos $\hat{H}$ para denotar $\sum_{h\in H} h \in K[G]$

v) Finalmente $\left(\frac{-1,-1}{F}\right)$ denotará el algebra de cuaternios sobre el campo F.

<u>Proposición 1</u>.- Sean G un grupo multiplicativo y H un subgrupo de G y Y un conjunto representativo de clases laterales izquierdas para H en G. Entonces cada elemento $\alpha \in K[G]$ se puede escribir en forma única como una suma finita de la forma:

$$\alpha = \sum_{y \in Y} y \alpha_y \quad , \text{ donde } \alpha_y \in K[H] .$$

<u>Demostración</u> :

Sea $\alpha \in K[G]$, $\alpha = \sum_{x \in G} a_x x$. Como sop α es finito está contenido en un número finito de clases laterales izquierdas de H, digamos $y_1 H, y_2 H, \ldots, y_n H$ con $y_i \in Y$.

Sea ahora, α_i la suma de aquellos elementos $a_x x$ con $x \in y_i H$. Observamos que

$x \in y_i H \Rightarrow y_i^{-1} x \in H$, así tenemos la expresión

$$\alpha = \sum_{i=1}^{n} y_i (y_i^{-1} \alpha_i) ,$$

donde $y_i^{-1}\alpha_i \in K[H]$. Para la unicidad supongamos que $\alpha = \sum_{y \in Y} y \alpha_y$ y sea $\alpha_0 \in Y$. Entónces consideramos

$$y_0^{-1} \alpha = \sum_{y \in Y} y_0^{-1} y \alpha_y \quad ,$$

y como $y_0^{-1} y \in H \iff y = y_0$, tenemos que

$$\pi_H (y_0^{-1} \alpha) = \sum y_0^{-1} y \alpha_y \; ,$$

$\therefore \ \forall\, y \in Y,\ \alpha_y = \pi_H(y^{-1}\alpha)$, es decir, la expresión

$$\alpha = \sum_{y \in Y} y\,\alpha_y \quad , \text{ donde } \alpha_y \in K[H] \text{ es única.} \qquad \square$$

<u>Proposición 2</u>.- Si H es un subgrupo normal del grupo G, entonces

$$Ker\ \varepsilon_H = W(K[H])\,K[G] \quad ,$$

donde $W(K[H]) = \left\{ \sum_{x \in H} a_x\, x \in K[H] \;\middle|\; \sum a_x = 0 \right\}$.

<u>Demostración</u>:

Sea X un conjunto representativo de clases laterales derechas para H en G y sea $\alpha \in K[G]$. Por la proposición 1 podemos escribir

$$\alpha = \sum_{x \in X} \alpha_x\, x \quad ,$$

con $\alpha_x \in K[H]$, entónces

$$\varepsilon_H(\alpha) = \sum_{x \in X} \varepsilon_H(\alpha_x)\,\varepsilon_H(x) \quad \text{y} \quad \varepsilon_H(\alpha_x) \in K \quad ,$$

además (por definición) $\{\varepsilon_H(x) \mid x \in X\}$ es una base de $K[G/H]$

$\therefore\ \alpha \in Ker\ \varepsilon_H \iff \varepsilon_H(\alpha_x) = 0 \quad \forall\, x \in X$ y como $\varepsilon_H(H) = 1$ entónces $\forall\, x \in X$ tenemos

$$\varepsilon_H(\alpha_x) = 0 \iff \alpha_x \in W(K[H])$$

$$\therefore\ Ker\ \varepsilon_H = W(K[H])\,K[G].$$

$\square$

Proposición 3.- Sean G y H grupos multiplicativos. Entónces $K[G\times H] \cong K[G]\otimes_K K[H]$.

Demostración:

Consideremos la función

$$\bar{\varphi}: G\times H \longrightarrow \mathcal{U}(K[G]\otimes_K K[H]),$$
$$(g,h)\longmapsto g\otimes h$$

(donde $\mathcal{U}(K[G]\otimes_K K[H])$ es el grupo de unidades de $K[G]\otimes_K K[H]$). Por las propiedades del producto tensorial $\bar{\varphi}$ es un morfismo de grupos, entónces $\bar{\varphi}$ se extiende linealmente a un morfismo de K-álgebras

$$\bar{\varphi} = K[G\times H] \longrightarrow K[G]\otimes_K K[H].$$

Pero $\bar{\varphi}$ es un morfismo de la base de $K[G\times H]$ a la base de $K[G]\otimes_K K[H]$

$\therefore$ φ es un isomorfismo de K-álgebras.

□

Proposición 4.- Sea H un subgrupo del grupo multiplicativo G. Si H es finito, entonces $\ell(\hat{H}) = K[G]\,W(K[H])$.

Demostración:

Sea $\alpha\in\ell(\hat{H})$ y sea X un conjunto representativo de clases laterales izquierdas para H en G. Por la proposición 1 escribimos

$$\alpha = \sum_{x\in X} x\alpha_x, \quad \text{con } \alpha_x\in K[H],$$

por tanto

$$0 = \alpha \hat{H} = \sum_{x \in X} x \alpha_x \hat{H} \iff \alpha_x \hat{H} = 0 \ \forall\, x \in X.$$

Ahora, si $\alpha_x = \sum_{h \in H} a_h^x h$, entónces,

$$\alpha_x \hat{H} = (\sum a_h^x) \hat{H}$$

$$\therefore \ \alpha_x \hat{H} = 0 \iff \sum a_h^x = 0 \iff \alpha_x \in W(K[H])$$

$$\therefore \ \alpha \in \ell(\hat{H}) \iff \alpha \in K[G]\, W(K[H]).$$

$\square$

Proposición 5.- Si K es un campo de característica y G es un p-grupo finito no trivial, entónces $W(K[G])$ es nilpotente.

Demostración:

Inducción en el órden de G.

i) a) Si $G = \langle 1 \rangle$ el resultado es inmediato.

b) Si $G = \langle x \rangle$ cíclico de órden p, entónces como $W(K[\langle x \rangle])$ está generado por términos de la forma $x^i - 1$ y como $x^i - 1 = (x-1)(1 + x + \cdots + x^{i-1})$, entónces $W(K[\langle x \rangle])$ es principal generado por $x-1$ y como $K[\langle x \rangle]$ es conmutativo $(x-1)^p = x^p - 1 = 0$ el resultado se sigue.

ii) Si $G \neq \langle 1 \rangle$ es un p-grupo, sea H un subgrupo central de orden p, entónces

$$\rho_H(W(K[G])) \subset W(K[G/H])$$

y, por inducción tenemos $W(K[G/H])^n = 0$ para algún $n \in \mathbb{N}$.

$$\therefore \ \rho_H(W(K[G])^n) = [\rho_H(W(K[G]))]^n$$

$$\subseteq \omega(K[G/H])^n = 0$$

$\therefore\ \omega[K[G]]^n \subseteq \operatorname{Ker} \varepsilon_H$, pero por la proposición 2 — $\operatorname{Ker} \varepsilon_H = \omega(K[H])K[G]$. Ahora, como $\omega(K[H])$ es nilpotente y central en $K[G]$,

$\therefore\ \omega(K[G])$ es nilpotente complementando así la demostración.

<u>Corolario</u>: Si K es campo de característica p y G es un p-grupo finito entonces $K[G]$ es un anillo local con $\{\alpha \in K[G] \mid |\alpha| = 0\}$ el ideal máximo.

<u>Demostración</u>:

Consideremos el morfismo de anillos

$$\varphi : K[G] \longrightarrow K$$

$$\sum_{x\in G} a_x x \longmapsto \sum_{x\in G} a_x .$$

φ tiene como núcleo precisamente a $\omega(K[G])$ y es claramente suprayectivo,

$$\therefore\ K[G]/\omega(K[G]) \cong K \qquad K \text{ campo}$$

$\therefore\ \omega(K[G])$ es un ideal máximo.

Ahora bien, por la proposición anterior $\omega(K[G])$ es nilpotente, $\therefore\ \omega(K[G])^n = 0$ para cierto $n \in \mathbb{N}$ y si $\mathfrak{m} \subseteq K[G]$ es un ideal máximo, entonces

$$\omega(K[G])^n \subseteq \mathfrak{m} \text{ y } \therefore\ \omega(K[G]) \subseteq \mathfrak{m}$$

y por la maximalidad

$$\omega(K[G]),\ \omega(K[G]) = \mathfrak{m}$$, es decir, $\omega(K[G])$ es el único ideal máximo de $K[G]$. □

<u>Proposición 6.</u>- Sean K un campo, Q el grupo cuaternio (generado por a y b con las relaciones $a^4 = 1$, $b^2 = a^2$, $aba = b$), y sea ξ_n una raiz n-ésima primitiva de la unidad, entonces

$$K[Q] \otimes_K K(\xi_n) \cong K(\xi_n)[Q].$$

<u>Demostración:</u>

Consideremos las siguientes inclusiones

$$\begin{array}{l} K[Q] \hookrightarrow \\ \qquad\qquad\qquad K(\xi_n)[Q] \\ K[\xi_n] \hookrightarrow \end{array}$$

$$\therefore \text{ sea } \varphi : K[Q] \times K[\xi_n] \longrightarrow K(\xi_n)[Q]$$
$$(\alpha, \beta) \longmapsto \alpha\beta.$$

φ es K-bilineal, entónces por la propiedad universal del producto tensorial, $\exists!\ f : K[Q] \otimes_K K(\xi_n) \longrightarrow K(\xi_n)[Q]$ tal que el triángulo

$$\begin{tikzcd} K[Q] \otimes_K K(\xi_n) \arrow[r, "f"] & K(\xi_n)[Q] \\ K[Q] \times K(\xi_n) \arrow[u, "\Gamma"] \arrow[ur, "\varphi"'] & \end{tikzcd}$$

(donde Γ es la función canónica al producto tensorial), conmuta. Por otra parte sea

$g = K(\xi_n)[Q] \longrightarrow K[Q] \otimes_K K(\xi_n)$ la extensión $K(\xi_n)$-lineal del morfismo de grupos $\bar{g}$ de Q al grupo de unidades del $K(\xi_n)$-álgebra $K[Q] \otimes_K K(\xi_n)$, dado por -

$$x \overset{\bar{g}}{\longmapsto} x \otimes 1$$

$$\therefore \text{ si } \sum_{x \in Q} a_x x \in K(\xi_n)[Q], \text{ entónces}$$

$$g\left(\sum_{x\in Q} a_x x\right) = \sum_{x\in Q}(x\otimes a_x).$$

Demostraremos que $fg = 1_{K(\xi_n)[Q]}$, $gf = 1_{K[Q]\otimes_K K(\xi_n)}$ con lo cual $K[Q]\otimes_K K(\xi_n)$ y $K(\xi_n)[Q]$ serán isomorfos como $K(\xi_n)$-álgebras.

i) Para ver que $f\cdot g = 1$, basta mostrarlo en la base, $\therefore$ sea $x\in Q$ y consideremos

$$\begin{aligned}(f\cdot g)(x) &= f(x\otimes 1)\\ &= f(\Gamma(x,1))\\ &= \varphi(x,1)\\ &= x\end{aligned}$$

$$\therefore\ f\cdot g = 1$$

ii) Para mostrar $g\cdot f = 1$ basta mostrar que las funciones son iguales aplicadas a cualquier generador de $K[Q]\otimes_K K(\xi_n)$,

$\therefore$ sea $\alpha\otimes\beta \in K[Q]\otimes_K K(\xi_n)$ con $\alpha = \sum_{x\in Q} a_x x$, $a_x\in K$ $\forall\, x\in Q$ y consideramos

$$\begin{aligned}(g\circ f)(\alpha\otimes\beta) &= g(f(\Gamma(\alpha,\beta)))\\ &= g(\varphi(\alpha,\beta))\\ &= g(\alpha\beta)\\ &= g\left(\left(\sum_{x\in Q} a_x x\right)\beta\right)\\ &= g\left(\sum_{x\in Q} a_x\beta x\right)\\ &= \sum_{x\in Q}(x\otimes a_x\beta)\\ &= \sum_{x\in Q}(a_x x\otimes\beta)\\ &= \alpha\otimes\beta\end{aligned}$$

$$\therefore\ g\circ f = 1_{K[Q]\otimes_K K(\xi_n)} \quad \square.$$

Nótese que en forma análoga se demuestra que también $\left(\frac{-1,-1}{K}\right)\otimes_K K(\xi_n)$ y $\left(\frac{-1,-1}{K(\xi_n)}\right)$ son isomorfos como $K(\xi_n)$-álgebras.

Lema 1.- i) $K[G]$ es iiid $\Leftrightarrow$ $K[H]$ lo es para cada subgrupo finitamente generado H de G.

ii) Si $K[G]$ es iiid entonces los subgrupos de G son normales.

iii) Supongamos que G es localmente finito. Si $K[G]$ es aiid, entonces todo subgrupo de G es normal.

Demostración:

i) Supongamos que $K[H]$ es iiid $\forall$ H subgrupo finitamente generado de G y sea $I \subseteq K[G]$ un ideal izquierdo.

Tomamos $\alpha \in I$, $g \in G$ y consideremos $H = \langle g, \operatorname{sop} \alpha \rangle$, entonces H es finitamente generado y por hipótesis $K[H]$ es iiid $\therefore$ $I \cap K[H]$ es un ideal bilateral de $K[H]$ y además $\alpha \in I \cap K[H]$, $g \in K[H]$

$\therefore$ $\alpha g \in I \cap K[H] \subseteq I$

$\therefore$ I es también ideal derecho de $K[G]$

$\therefore$ $K[G]$ es iiid.

Inversamente supongamos que $K[G]$ es iiid y sean H un subgrupo de G é $I \subseteq K[H]$ un ideal izquierdo. Sea $\{x_i\}_{\mho}$ un conjunto representativo de clases laterales izquierdas para H en G. Por la proposición 1, $K[G]$ es un $K[H]$ módulo libre derecho con base $\{x_i\}_{\mho}$.

$\therefore$ $K[G] = \dot{\sum} x_i K[H]$. Sea $J = \dot{\sum} x_i I$, es claro que J es un ideal izquierdo de $K[G]$ que es iiid por hipótesis, $\therefore$ J es también un ideal derecho de $K[G]$.

Sea $h \in H$, entonces

$$Ih \subseteq Jh \cap K[H] \subseteq J \cap K[H] = I$$

$\therefore$ I es ideal derecho de $K[H]$

$\therefore$ $K[H]$ es $iiid$.

ii) observamos que para probar que todos los subgrupos de G son normales, es suficiente ver que todos los subgrupos cíclicos de G son normales. Así pues, sean $a, g \in G$. Consideremos el ideal izquierdo $I = K[G](1-a)$. Como por hipótesis $K[G]$ es $iiid$, I es un ideal derecho,

$\therefore$ $g^{-1}(1-a)g \in I$

$\therefore$ $1 - g^{-1}ag = \alpha(1-a)$ para cierto $\alpha \in K[G]$.

Usando el $K[\langle a \rangle]$ - morfismo

$$\theta : K[G] \longrightarrow K[G]$$
$$\sum_{x \in G} a_x x \longmapsto \sum_{x \in \langle a \rangle} a_x x$$, obtenemos

$1 - \theta(g^{-1}ag) = \theta(\alpha)(1-a)$ y como $1-a$ no es invertible, $\theta(g^{-1}ag) \neq 0$ $\therefore$ $g^{-1}ag \in \langle a \rangle$

$\therefore$ $\langle a \rangle$ es normal en G.

iii) supongamos que $K[G]$ es $aiid$ y G localmente finito y sea H un subgrupo finito de G. Por la proposición 4 tenemos

$\ell(\hat{H}) = K[G]\,\omega(K[H])$ y por hipótesis $\ell(\hat{H})$ es un ideal de $K[G]$.

Por otra parte tenemos que

$H = \{x \in G \mid x-1 \in \ell(\hat{H})\}$, pues si $h \in H$, entonces $(h-1)\hat{H} = h\hat{H} - \hat{H} = \hat{H} - \hat{H} = 0$ $\therefore$ $h \in \{x \in G \mid x-1 \in \ell(\hat{H})\}$ y si $x \in G$ es tal que $x-1 \in \ell(\hat{H})$, entonces $(x-1)\hat{H} = 0$

$\therefore$ $x\hat{H} = \hat{H} \in K[G]$ y por la unicidad en la escritura de los elementos de $K[G]$, $x \in H$,

$\therefore$ $H = \{x \in G \mid x-1 \in K[G]\,\omega(K[H])\}$.

Sean ahora $g \in G$ y $h \in H$ entonces $h-1 \in \ell(\hat{A})$ y como $\ell(\hat{A})$ es un ideal de $K[G]$, $g^{-1}(h-1)g \in \ell(\hat{A})$

$$\therefore\ g^{-1}hg \in H$$

$\therefore$ H es normal en G $\forall$ $H \leq G$ subgrupo finito y como G es localmente finito, todo subgrupo cíclico de G es normal en G. $\square$

<u>Lema 2.</u>- Sea G un grupo localmente finito. Entonces $K[G]$ es a.i.i.d $\Longleftrightarrow$ $\forall\, \alpha, \beta \in K[G]$.>. $\alpha\beta = 0 \Rightarrow \beta\alpha = 0$.

<u>Demostración</u>:

$\Leftarrow$) Inmediato.

$\Rightarrow$) Si G es abeliano el resultado es trivial.

Si G no es abeliano, por el lema 1 inciso iii), G es un grupo hamiltoniano y por el teorema 1, escribimos $G = Q \times A \times B$, donde Q es un grupo de cuaternios (generado por a y b con $a^4 = 1$, $a^2 = b^2$, $aba = b$), A es un grupo abeliano donde cada elemento tiene orden impar y B es un grupo abeliano de exponente dos.

Como $\langle a^2 \rangle$ es el centro de Q, $H = \langle a^2 \rangle \times A \times B$ es el centro de G.

Calculamos ahora con la función:

$$\pi_H : K[G] \longrightarrow K[H]$$

$$\sum_{x \in G} a_x x \longmapsto \sum_{x \in H} a_x x, \text{ para } \alpha = \sum_{x \in G} a_x x \in K[G]$$

$$\pi_H(\alpha) = \sum_{\substack{x_2 \in A \\ x_3 \in B}} a_x (1, x_2, x_3) + \sum_{\substack{x_2 \in A \\ x_3 \in B}} a_x (a^2, x_2, x_3)$$

$$\pi_H(a^{-1}\alpha)a = \sum_{x_2,x_3} a_x(a^3, x_2, x_3) + \sum_{x_2,x_3} a_x(a, x_2, x_3),$$

$$\pi_H(b^{-1}\alpha)b = \sum_{x_2,x_3} a_x(b, x_2, x_3) + \sum_{x_2,x_3} a_x(a^2 b, x_2, x_3),$$

$$\pi_H(b^{-1}a^{-1}\alpha)ab = \sum_{x_2,x_3} a_x(ab, x_2, x_3) + \sum_{x_2,x_3} a_x(a^3 b, x_2, x_3)$$

$$\therefore \ \alpha = \pi_H(\alpha) + \pi_H(a^{-1}\alpha)a + \pi_H(b^{-1}\alpha)b + \pi_H(b^{-1}a^{-1}\alpha)ab \ \text{---}(*)$$

Supongamos que $\alpha\beta = 0$. Tenemos que $\pi_H(\alpha\beta) = \pi_H(\beta\alpha)$ pues si $x = (x_1, x_2, x_3)$, $y = (y_1, y_2, y_3) \in G$, entónces $xy \in H \iff x_1 y_1 \in \langle a^2 \rangle$

$$\iff \begin{cases} x_1 = y_1^{-1} \\ x_1 = a^2 y_1^{-1} \end{cases} \text{ó}$$

$\therefore \ x_1 y_1 = y_1 x_1$, $\therefore \ yx \in H$. Análogamente si $yx \in H \Rightarrow xy \in H$,

$$\therefore \ \pi_H(\alpha\beta) = \sum_{xy \in H} a_x b_y \, xy = \sum_{yx \in H} b_y a_x \, yx = \pi_H(\beta\alpha).$$

$\therefore$ Si $\pi_H(\alpha\beta) = 0$, $\pi_H(\beta\alpha) = 0 \ \forall \alpha, \beta \in K[G]$.

Como por hipótesis $\alpha\beta = 0$ y $\ell(\beta)$ es un ideal de $K[G]$, tenemos que $(\alpha x)\beta = 0 \ \forall x \in G$. Así,

$$0 = \pi_H((\alpha x)\beta) = \pi_H(\alpha(x\beta))$$
$$= \pi_H(x\beta\alpha) \quad \forall x \in G.$$

Consideremos ahora la expresión $(*)$ correspondiente para $\beta\alpha$:

$$\beta\alpha = \pi_H(\beta\alpha) + \pi_H(a^{-1}\beta\alpha)a + \pi_H(b^{-1}\beta\alpha)b + \pi_H(b^{-1}a^{-1}\beta\alpha)ab,$$

y como cada término del lado derecho de la igualdad es cero, tenemos que

$$\beta\alpha = 0$$

$\square$.

Lema 3.- Sea K un campo de característica dos. Supongamos que K no contiene ninguna raíz cúbica primitiva de la unidad y sea $Q = \langle a, b \rangle$ el grupo cuaternio. Entonces si $\alpha = \sum_{x \in \langle a \rangle} a_x x$, $\alpha \in K[\langle a \rangle]$ con $|\alpha| = 1$, tenemos

$$1 + (\alpha b)^2 = (1 + a^2)\mu, \text{ donde } \mu \in K[\langle a \rangle] \text{ es una}$$

unidad.

Demostración:

$$\text{Sea } \alpha = \sum_{i=1}^{4} k_i a^i \in K[\langle a \rangle], \text{ con } \sum_{i=1}^{4} k_i = 1.$$

Entonces

$$1 + (\alpha b)^2 = (1 + a^2)(1 + (k_1 + k_3)(k_2 + k_4)a)$$

Como Q es un 2-grupo finito y la característica de K es 2, el corolario a la proposición 5 nos dice que $K[Q]$ es un anillo local cuyo ideal máximo es

$$\omega(K[Q]) = \{\alpha \in K[Q] \mid |\alpha| = 0\}.$$

Supongamos que $\mu = 1 + (k_1 + k_3)(k_2 + k_4)a$ no es unidad, entonces $\mu \in \omega(K[Q])$

$$\therefore (k_1 + k_3)(k_2 + k_4) + 1 = 0$$

$$\therefore (k_1 + k_3)(k_2 + k_4) = 1.$$

Como $\sum_{i=1}^{4} k_i = 1$ y caract $(K) = 2$, tenemos $(k_2 + k_4)^2 = 1 + (k_1 + k_3)^2$ y como $(k_1 + k_3)(k_2 + k_4) = 1$

$$\begin{aligned} \therefore k_2 + k_4 &= (k_1 + k_3)(k_2 + k_4)^2 \\ &= (k_1 + k_3)[1 + (k_1 + k_3)^2] \\ &= (k_1 + k_3) + (k_1 + k_3)^3 \end{aligned}$$

$$\therefore (k_1 + k_3)^3 = k_1 + k_2 + k_3 + k_4 = 1$$

$\therefore k_1 + k_3$ es una raíz cúbica primitiva de la unidad, contradiciendo la hipótesis,

$\therefore \mu$ es unidad $\square$.

Teorema 1 .- Sea G un grupo. Entonces G hamiltoniano $\Leftrightarrow$ G es el producto directo de un grupo de cuaternios con un grupo abeliano en el que todo elemento es de orden (finito) impar y un grupo abeliano de exponente 2.

Demostración:

I.- Primero mostramos que todo elemento de G es de orden finito:

Sean $a, b \in G$. Entonces el conmutador

$$c = (a,b) = a^{-1}b^{-1}ab = (a^{-1}b^{-1}a)b = b^{s} = a^{-1}(b^{-1}ab) = a^{r}$$

ya que $\langle a \rangle$, $\langle b \rangle$ son por hipótesis subgrupos normales de G. En particular c conmuta con a y con b.

Tenemos que la siguiente igualdad vale $\forall n \in \mathbb{N}$: $(a^n, b) = (a,b)^n$, pues para $n=1$ $(a,b) = c$ y si suponemos cierta la igualdad para $n>1$ y consideramos

$$\begin{aligned}(a^{n+1}, b) &= a^{-1}a^{-n}b^{-1}a^{n}ab \\ &= a^{-1}(a^{-n}b^{-1}a^{n}b)b^{-1}ab \\ &= a^{-1}(a^{n}, b)b^{-1}ab \\ &= a^{-1}(a,b)^{n}b^{-1}ab \\ &= (a,b)^{n}a^{-1}b^{-1}ab \\ &= (a,b)^{n+1},\end{aligned}$$

hemos mostrado por inducción la igualdad.

Ahora bién, si a y b no conmutan, entonces $c = a^r \neq 1$ y con $i = r$ ó $i = -r$ (el que sea positivo) tenemos que (a^i, b) es (c, b) ó bién (c^{-1}, b) y en cualquier caso $(a^i, b) = 1$ ya que c conmuta con b.

$$\therefore\ (a^i, b) = (a,b)^i = c^i = 1$$

$\therefore\ a^{ri} = 1$, $b^{si} = 1$, es decir, dos elementos en G que no conmutan son de orden finito. Ahora, si $x \in G$ conmuta con a y b, entónces xa no conmuta con b (pues en tal caso $(xa)b = bxa = xba \Rightarrow ab = ba$ ¡)

$\therefore\ xa$ es de orden finito

$\therefore\ x$ es de orden finito

$\therefore$ Todo elemento de G es de orden finito.

II.- Mostramos a continuación que cualquier subgrupo no abeliano de G contiene un subgrupo de cuaternios.

Sean $a, b \in G$ dos elementos que no conmuten con $N, M \in \mathbb{N}$ mínimos $\ni\cdot$ $a^N = b^M = 1$, (es decir, dos elementos de orden mínimo que no conmutan). Si p es primo que divide a N entonces $a^p b = b a^p$ por la "minimalidad" de N,

$$\therefore\ (a^p, b) = (a,b)^p = c^p = 1 .$$

Análogamente si q es primo que divide a M, entónces $(a, b^q) = c^q = 1$ y como $c = (a,b) \neq 1$, $o(c) \mid p$ y $o(c) \mid q$

$\therefore\ p = q$ $\therefore\ p$ es el único primo que divide a N y a M,

$$\therefore\ N = p^n, \quad M = p^m, \quad n, m \in \mathbb{N}$$

$$\therefore\ a^{p^n} = b^{p^m} = 1, \quad c^p = 1$$

Por simetría podemos suponer $n \geq m$. Como $c \in \langle a \rangle$, $c \in \langle b \rangle$, $c = a^{jp^{n-1}} = b^{kp^{m-1}}$, donde $j, k \not\equiv 0 \pmod p$.

Probamos ahora por inducción la fórmula

$$(ab)^i = a^i b^i (b,a)^{\frac{i(i-1)}{2}} \quad --- (*) .$$

a) si $i=1$ la fórmula es válida.

b) Supongamos que $(*)$ vale para $i>1$ y consideremos:

$$(ab)^{i+1} = (ab)^i ab$$

$$
\begin{aligned}
(ab)^{i+1} &= a^i b^i (b,a)^{\frac{i(i-1)}{2}} ab \\
&= a^i b^i\, ab\, (b,a)^{\frac{i(i-1)}{2}} \\
&= a^i a b^i (b^i,a) b\, (b,a)^{\frac{i(i-1)}{2}} \\
&= a^{i+1} b^i (b,a)^i b\, (b,a)^{\frac{i(i-1)}{2}} \\
&= a^{i+1} b^{i+1} (b,a)^{\frac{i(i+1)}{2}} .
\end{aligned}
$$

Sea $b_1 = a^{\mu} b^k$, donde $\mu = -jp^{n-m}$, entonces $\langle a, b_1 \rangle = \langle a, b \rangle$, $\therefore$ b_1 no conmuta con a $\therefore$ $o(b_1) \geq o(b)$. Aplicamos la fórmula $(*)$ de arriba y tenemos:

$$
\begin{aligned}
b_1^{p} &= (a^{\mu} b^k)^p \\
&= a^{\mu p} b^{kp} (b^k, a^{\mu})^{\frac{p(p-1)}{2}} \\
&= a^{\mu p} b^{kp}\; c^{-\mu k \frac{p(p-1)}{2}}
\end{aligned}
$$

$$\therefore \; b_1^{p^{m-1}} = a^{-jp^{n-1}}\, b^{kp^{m-1}}\, c^{jkp^{n-1}\frac{(p-1)}{2}}$$

$$\therefore \; b_1^{p^{m-1}} = c^{jkp^{n-1}\frac{(p-1)}{2}}$$

Como $b_1^{p^{m-1}} \neq 1$ pero $c^p = 1$, entonces $p = 2$, $n = 2$, es decir para a y b tenemos

$$a^2 = b^2 = a^{-1}b^{-1}ab = c \;, \quad c^2 = 1$$

$\therefore$ $\langle a, b \rangle$ es el grupo cuaternio.

$\therefore$ Todo subgrupo no conmutativo de G contiene un grupo de cuaternios.

Sea $Q = \langle a, b \rangle$ el grupo cuaternio con las relaciones $a^4 = 1$, $a^2 = b^2$, $aba = b$ y sea

$$Z = \{ x \in G \mid x \text{ centraliza } Q \} .$$

III.- Demostraremos que G es el producto de Q y Z:

Si $x \in H$ no conmuta con a, entonces

$$x^{-1} a x = a^3$$

$$\therefore\ x^{-1}(axb) = a^3 b = ba = x^{-1}(xba)$$

$$\therefore\ a(xb) = (xb)a.$$

Análogamente si x (ó xb) no conmuta con b, entonces xa (ó xba) conmuta con a, por lo tanto, uno de los elementos x, xb, xa, xba, está en Z,

$$\therefore\ G = QZ$$

IV.- Vemos ahora que en Z no hay elementos de orden cuatro:

Si $x \in Z$ y $o(x) = 4$, entonces $(bx)^4 = 1$

$$\therefore\ a^{-1}(bx)a = (bx)^{-1}$$

$$\therefore\ a^{-1}bax = b^{-1}x^{-1}$$

$$\therefore\ a^{-1}bax^2 = b^{-1}, \text{ pero } a^{-1}ba = b^{-1}$$

$$\therefore\ x^2 = 1 \text{ contradiciendo } o(x) = 4.$$

$\therefore$ Z no puede contener un grupo de cuaternios, y así por la parte II Z es abeliano. Por lo tanto podemos escribir

$Z = Z_2 \oplus Z'$, donde Z_2 es la parte 2-primaria de Z.

Ahora, $\langle a^2 \rangle \subset Z_2$ es un subespacio vectorial y por lo tanto es sumando directo, es decir,

$$Z_2 = \langle a^2 \rangle \oplus Z''$$

$$\therefore\ Z = \langle a^2 \rangle \oplus (Z' \oplus Z'').$$

Sea $Z_1 = Z' \oplus Z''$. Tenemos

$$Q \cap Z_1 \subseteq Q \cap Z = \langle a^2 \rangle$$

$$\therefore\ Q \cap Z_1 \subseteq \langle a^2 \rangle \cap Z_1 = \{e\}$$

$$\therefore\ Q \cap Z_1 = \{e\}$$

$$\therefore\ G = Q \times Z' \times Z''.$$

$\Leftarrow$): Recíprocamente si G es de la forma $G = Q \times A \times B$, donde

$Q = \langle a, b \rangle$ es un grupo de cuaternios con las relaciones $a^4 = 1$, $a^2 = b^2$, $aba = b$, A es un grupo abeliano donde todo elemento es de orden impar y B es un grupo abeliano de exponente dos, entonces para mostrar que G es un grupo hamiltoniano es suficiente mostrar que todo subgrupo cíclico de G es normal en G, pues Q no es abeliano.

Como A y B estan en el centro de G solo necesitamos mostrar que a y b transforman a cualquier grupo cíclico en si mismo.

Sea $(q, u, v) \in G$. Entónces

$a^{-1}(q, u, v)a = (q^i, u, v)$, donde $i = 1$ ó 3.

Ahora, como $n = o(u)$ es impar y $o(v) = 2$, el sistema de congruencias

$$\begin{cases} r \equiv i \pmod 4 \\ r \equiv 1 \pmod n \end{cases}$$, tiene solución.

$\therefore a^{-1}(q, u, v)a = (q, u, v)^r$.

Análogamente b transforma a $\langle (q, u, v) \rangle$ en si mismo, $\therefore \langle (q, u, v) \rangle$ es normal en G

$\therefore$ G es un grupo hamiltoniano. $\square$

<u>Teorema 2 (Haschke)</u>.- Si la característica del campo K no divide al orden del grupo G, entonces el anillo de grupo $K[G]$ es semisimple

<u>Demostración</u>:

Sea $G = \{g_1, g_2, \ldots, g_n\}$.

Para ver que $K[G]$ es semisimple, basta ver que to-

-do $K[G]$-módulo izquierdo es semisimple.

Sea M un $K[G]$-módulo izquierdo. Para mostrar que M es semisimple basta mostrar que todo $K[G]$-submódulo de M es sumando directo de M, $\therefore$ sea M' un $K[G]$-submódulo de M.

Considerando M y M' como espacios vectoriales sobre K, M' es sumando directo de M

$\therefore \exists\ F : M \to M'$ un K-morfismo $\cdot\ni\cdot$ $F|M' = 1_{M'}$.

Sea $N(F) : M \to M'$ el $K[G]$-morfismo dado por
$x \longmapsto \sum_{i=1}^{n} g_i F(g_i^{-1}x)$

Sea $x \in M'$, entonces $g_i x \in M'$

$$\therefore N(F)(x) = \sum_{i=1}^{n} g_i F(g_i^{-1}x)$$
$$= \sum_{i=1}^{n} g_i (g_i^{-1}x)$$
$$= nx.$$

Pero según la hipótesis n tiene inverso en K,
$\therefore N(F)|_{M'}$ es un $K[G]$-isomorfismo.

$\therefore M'$ es sumando directo de M como $K[G]$-módulo, $\therefore K[G]$ es semisimple. $\square$

<u>Teorema 3</u>.- Sean K un campo y G un grupo no abeliano localmente finito. Entonces si $K[G]$ es aiid, sucede alguna de las siguientes cosas:

i) La característica de K es cero y G es hamiltoniano tal que si n es el orden de un elemento en G, n impar, entonces el álgebra de los cuaternios sobre el campo $K(\xi_n)$, donde ξ_n es una raíz n-ésima primitiva de la unidad, es un anillo con división.

ii) La característica de K es dos y K no contiene ninguna raíz cúbica primitiva de la unidad. Además $G \cong Q \times A$, donde Q es el grupo de cuaternios de orden 8 y A es un grupo abeliano en el cual cada elemento tiene orden finito impar y si n es el orden de un elemento en A, entonces el mínimo entero $m \geq 1$ tal que $2^m \equiv 1 \pmod{n}$, es impar.

Inversamente, si K y G cumplen i) ó ii), entónces $K[G]$ es iiid y en particular es aiid.

<u>Demostración</u>:

Sea G un grupo localmente finito no abeliano y supongamos que $K[G]$ es aiid.

Por el lema 1- iii) G es hamiltoniano

$\therefore G \cong Q \times A \times B$ (con la notación del teorema 1)

Si $K[G]$ es aiid, $K[Q]$ lo es también, pues si $S \subseteq Q$, consideramos $\ell_{K[G]}(S)$ que es por ser $K[G]$ aiid un ideal bilateral de $K[G]$, pero

$$\ell_{K[G]}(S) \cap K[Q] = \ell_{K[Q]}(S)$$

$\therefore \ell_{K[Q]}(S)$ es un ideal de $K[Q]$ y así $K[Q]$ es aiid.

Ahora bien, si característica de $K > 2$ tenemos

$$K[Q] \cong K \times K \times K \times K \times M_2(K),$$

y como $M_2(K)$ no es aiid y un producto de anillos es aiid $\Leftrightarrow$ cada factor lo es, entonces $K[Q]$ no es aiid, por lo tanto caract $(K) \neq 2$.

i) Supongamos primero que caract$(K) = 0$. Sea n el orden de un elemento $x \in A$ y consideremos $K[\langle x \rangle]$ que por el teorema de Maschke es semisimple,

$$\therefore\ K[\langle x \rangle] \cong K(\xi_n) \times L \times \dots \times L_m,$$

donde ξ_n es una raíz n-ésima primitiva de la unidad.

Por otra parte tenemos:

$$K[Q] \cong K \times K \times K \times K \times \left(\frac{-1,-1}{K}\right),$$

donde $\left(\frac{-1,-1}{K}\right)$ denota el álgebra de los cuaternios sobre el campo K.

Consideremos ahora

$$\begin{aligned} K[Q \times \langle x \rangle] &\cong K[Q] \otimes_K K[\langle x \rangle] \\ &\cong \left[K \times K \times K \times K \times \left(\tfrac{-1,-1}{K}\right)\right] \otimes_K \left[K(\xi_n) \times L_1 \times \dots \times L_m\right] \end{aligned}$$

$\therefore\ \left(\frac{-1,-1}{K}\right) \otimes_K K(\xi_n)$ es un factor directo de $K[Q \times \langle x \rangle]$ que es aiid pues $Q \times \langle x \rangle \leq G$ y $K[G]$ es aiid por hipótesis. Pero

$$\left(\frac{-1,-1}{K}\right) \otimes_K K(\xi_n) \cong \left(\frac{-1,-1}{K(\xi_n)}\right)$$

$\therefore\ \left(\frac{-1,-1}{K(\xi_n)}\right)$ es aiid, pero además es simple, pues sus únicos idempotentes centrales son triviales.

Sea $\alpha \in \left(\frac{-1,-1}{K(\xi_n)}\right)$, $\alpha \neq 0$ y consideremos:

$\ell(\alpha)$ que es un ideal por ser $\left(\frac{-1,-1}{K(\xi_n)}\right)$ aiid y como es simple, $\ell(\alpha) = 0 \qquad \therefore\ \alpha\bar{\alpha} \neq 0$

$\therefore\ \exists\ \alpha^{-1} = \dfrac{\bar{\alpha}}{\alpha\bar{\alpha}}, \qquad \therefore\ \left(\frac{-1,-1}{K(\xi_n)}\right)$ es con división.

Inversamente supongamos ahora que K y G satisfacen i). Demostraremos que $K[G]$ es iiid y así, en particular, aiid. Para esto, es suficiente por el lema 1-i), considerar G finito

$$\therefore G \cong Q \times A \times \underbrace{\mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2}_{m\text{-veces}}$$

$$\therefore K[G] \cong K[Q \times A \times \underbrace{\mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2}_{m\text{-veces}}]$$

$$\cong K[Q \times A] \otimes_K \underbrace{K[\mathbb{Z}_2] \otimes_K \cdots \otimes_K K[\mathbb{Z}_2]}_{m\text{-veces}},$$

pero tenemos que $K[\mathbb{Z}_2] \cong K \times K$, pues sea $\mathbb{Z}_2 = \langle \alpha \rangle$ como grupo multiplicativo y consideremos

$$\mathbb{Z}_2 \xrightarrow{\bar{\varphi}} \mathcal{U}(K \times K) = \text{unidades de } K \times K$$

$$1 \longmapsto (1,1)$$

$$\alpha \longmapsto (1,-1),$$

extendemos linealmente $\bar{\varphi}$ a un morfismo de K-álgebras

$$\varphi : K[\mathbb{Z}_2] \longrightarrow K \times K,$$

para el cual es fácil dar su inverso

$$\psi : K \times K \longrightarrow K[\mathbb{Z}_2]$$

$$(x,y) \longmapsto \left(\tfrac{x+y}{2} \cdot 1 + \tfrac{x-y}{2}\alpha\right),$$

$\therefore \varphi$ es isomorfismo de K-álgebras, y así tenemos

$$K[\mathbb{Z}_2] \cong K \times K,$$

$$\therefore K[G] \cong K[Q \times A] \otimes_K \underbrace{K[\mathbb{Z}_2] \otimes_K \cdots \otimes_K K[\mathbb{Z}_2]}_{m\text{-veces}}$$

$$\cong K[Q \times A] \otimes_K \underbrace{(K \times K) \otimes_K \cdots \otimes_K (K \times K)}_{m\text{-veces}}$$

$$\cong K[Q \times A] \otimes_K \underbrace{(K \times K \times \cdots \times K)}_{2^m\text{-veces}}$$

$$\cong \underbrace{K[Q \times A] \times \cdots \times K[Q \times A]}_{2^m\text{-veces}}$$

Por tanto, basta suponer $G \cong Q \times A$ y entonces

$$K[G] \cong K[Q \times A]$$
$$\cong K[Q] \otimes_K K[A] \qquad \text{(Proposición 3)}$$
$$\cong [K \times K \times K \times K \times (\tfrac{-1,-1}{K})] \otimes_K K[A]$$
$$\cong K[A] \times K[A] \times K[A] \times K[A] \times [(\tfrac{-1,-1}{K}) \otimes_K K[A]],$$

pero $K[A] \cong \prod_{i|(A)} K(\xi_{d_i})^{a_i}$, y como

$$\left(\tfrac{-1,-1}{K}\right) \otimes_K K(\xi_d) \cong \left(\tfrac{-1,-1}{K(\xi_d)}\right) \quad \text{tenemos}$$

$$K[G] \cong K[A] \times K[A] \times K[A] \times K[A] \times \prod_i \left(\tfrac{-1,-1}{K(\xi_i)}\right)$$

$\therefore$ $K[G]$ es un producto directo de anillos iiid, ($\prod_i \left(\tfrac{-1,-1}{K(\xi_i)}\right)$ es iiid pues por hipótesis cada factor $\left(\tfrac{-1,-1}{K(\xi_i)}\right)$ es un anillo con división).

$\therefore$ $K[G]$ es iiid.

ii) Supongamos ahora que caract$(K) = 2$. Afirmamos que K no contiene ninguna raíz cúbica primitiva de la unidad, pues en caso de contener alguna, digamos ξ, tenemos los siguientes elementos de $K[G]$:

$$\alpha = [1 + \xi(1 + \xi a) b]$$
$$\beta = [1 + \xi(1 + \xi a) b](1 + a) b$$

(donde $Q = \langle a, b \rangle$). Un cálculo muestra $\alpha\beta = 0$, pero $\beta\alpha \neq 0$ $\therefore$ de acuerdo con el lema 2, $K[G]$ no es aiid, contradiciendo así la hipótesis de que $K[G]$ es aiid.

Probamos ahora que $G \cong Q \times A$. Ahora bien, si este no es el caso, $\exists\, x \in G - Q$, de orden dos, el cual centraliza a G. Por el lema 2 basta exhibir dos elementos $\alpha, \beta \in K[G]$ tales que $\alpha\beta = 0$ pero $\beta\alpha \neq 0$, para obtener así una contradicción. Sean

$$\alpha = 1 + (a + b + ab)x$$
$$\beta = (a + b + ab)(1 + x) + (1 + a)x, \text{ entonces}$$

$\alpha\beta = 0$ y $\beta\alpha \neq 0$ $\therefore$ $K[G]$ no es aiid !

$$\therefore \; G \cong Q \times A$$

Sea $x \in A$ un elemento de orden n. Como la característica de K es dos y n es impar, $K[\langle x \rangle]$ es semisimple.

$$\therefore \; K[\langle x \rangle] \cong K(\xi_n) \times \cdots \times L_m,$$

donde ξ_n es una raiz n-ésima primitiva de la unidad.

$$\therefore \; K[Q] \otimes_K K(\xi_n)$$

es un factor directo de $K[Q \times \langle x \rangle]$ que es aiid y como

$$K[Q] \otimes_K K(\xi_n) \cong K(\xi_n)[Q]$$

$$\therefore \; K(\xi_n)[Q] \text{ es aiid}$$

Con el argumento del principio, vemos que $K(\xi_n)$ no contiene ninguna raiz cúbica primitiva de la unidad,

$$\therefore \; 2 \nmid m,$$

donde $m = [\mathbb{Z}_2(\xi_n) : \mathbb{Z}_2]$ (si $m = 2s$, $\exists$ L campo tal que

$$\mathbb{Z}_2(\xi_n) \supset L \supset \mathbb{Z}_2 \;\text{ y }\; [L : \mathbb{Z}_2] = 2$$

$\therefore$ se satisface el polinomio irreducible $x^2 + x + 1$, como

$$(x+1)(x^2+x+1) = x^3+1$$

$\exists$ una raiz cúbica de la unidad ! $\therefore$ $2 \nmid m$). Pero m es precisamente el mínimo entero ≥ 1 $\ni$ $2^m \equiv 1 \pmod{n}$.

Inversamente, supongamos que K y G satisfacen ii). Veremos que $K[G]$ es iiid. Para esto, nuevamente (por el lema 1-i), podemos considerar G finito

$$\therefore \; K[A] = \prod_{d \mid e(A)} K(\xi_d)^{a_d}$$

$$\begin{aligned} \therefore \; K[Q \times A] &\cong K[Q] \otimes_K K[A] \\ &\cong K[Q] \otimes_K \prod_{d \mid e(A)} K(\xi_d)^{a_d} \\ &\cong \prod_{d \mid e(A)} K[Q] \otimes_K K(\xi_d)^{a_d} \end{aligned}$$

$$\cong \prod_{d|\iota(n)} (K[Q] \otimes_K K(\xi_d))^{a_d} \cong \prod_{d|\iota(n)} (K(\xi_d)[Q])^{a_d} \quad \text{(prop. 6)}$$

Por hipótesis el campo $K(\xi_d)$ no contiene ninguna raíz cúbica primitiva de la unidad y como un producto de anillos iiid es iiid, solo tenemos que probar que si un campo K de característica igual a 2 no contiene ninguna raíz cúbica primitiva de la unidad, entonces $K[Q]$ es iiid, para haber probado que $K[Q]$ es iiid. Así pues, sea K un tal campo y sea $I \leq K[Q]$ un ideal izquierdo y tomemos $\alpha \in I$. Escribimos $\alpha = \alpha_1 + \alpha_2 b$, con $\alpha_1, \alpha_2 \in K[\langle a \rangle]$.

Demostraremos que $\alpha_i(1+a^2) \in I$. Primero notamos que si $\alpha_1(1+a^2) \in I$, entonces dado que $1+a^2$ es central $(1+a^2)\alpha = \alpha(1+a^2) = \alpha_1(1+a^2) + \alpha_2 b(1+a^2) \in I$, $\therefore$ $\alpha_2 b(1+a^2) \in I$. Nuevamente $\alpha_2(1+a^2)$ es central $\therefore$ $b\alpha_2(1+a^2) \in I$ y como I es ideal izquierdo $\alpha_2(1+a^2) \in I$ por lo tanto basta probar $\alpha_1(1+a^2)$ para tener también $\alpha_2(1+a^2) \in I$.

Si α es unidad $I = K[Q]$, por lo tanto podemos suponer α no es unidad y como como caract$(K) = 2$ y Q es un 2-grupo finito por el corolario a la proposición 5, $K[G]$ es local con $\omega(K[Q])$ máximo.

$$\therefore \alpha \in \omega(K[Q])$$
$$\therefore |\alpha| = |\alpha_1| + |\alpha_2| = 0$$

a) Suponemos que α_1 es unidad, entonces

$$1 + \alpha_1^{-1}\alpha_2 b = \alpha_1^{-1}(\alpha_1 + \alpha_2 b) = \alpha_1^{-1}\alpha \in I$$
$$\therefore (1 + \alpha_1^{-1}\alpha_2 b)^2 = 1 + (\alpha_1^{-1}\alpha_2 b)^2 \in I$$

Como $|\alpha_1| + |\alpha_2| = 0$, entonces

$$0 = |\alpha_1^{-1}|\,(|\alpha_1| + |\alpha_2|)$$
$$= 1 + |\alpha_1^{-1}\alpha_2| \text{, es decir, } |\alpha_1^{-1}\alpha_2| = 1 .$$

Podemos así aplicar el lema 3 a $1+(\alpha_1^{-1}\alpha_2)b$ y obtenemos que

$\mu(1+a^2) = (1+a^2)\mu = 1+(\alpha_1^{-1}\alpha_2 b)^2 \in I$, μ unidad en $K[\langle a\rangle]$

$$\therefore\ (1+a^2) \in I$$
$$\therefore\ \alpha_1(1+a^2) \in I$$

b) Supongamos α_1 no es unidad:

$$\therefore\ |\alpha_1| = 0 \quad \text{y} \quad \therefore\ |\alpha_2| = 0$$

$\therefore$ Si $\alpha_1 = k_0 + k_1 a + k_2 a^2 + k_3 a^3$, $\sum_{i=0}^{3} k_i = 0$, entonces

$$\alpha_1 = \alpha_1 + \sum_{i=0}^{3} k_i = k_1(1+a) + k_2(1+a^2) + k_3(1+a^3)$$
$$= \beta_1(1+a), \quad \beta_1 \in K[\langle a\rangle]$$

Análogamente:

$$\alpha_2 = \beta_2(1+a), \quad \beta_2 \in K[\langle a\rangle].$$

$$\therefore\ (\beta_1 + \beta_2 ab)(1+a) = \beta_1(1+a) + \beta_2(ab + aba)$$
$$= \alpha_1 + \beta_2(ab+b)$$
$$= \alpha_1 + \beta_2(1+a)b$$
$$= \alpha_1 + \alpha_2 b$$
$$= \alpha \in I$$

Si $\beta_1 + \beta_2 ab$ es unidad, tenemos entonces que $1+a \in I$ $\therefore$ $\alpha_1(1+a^2) \in I$. Así pues, podemos considerar $|\beta_1| + |\beta_2| = 0$

Si β_1 es unidad, entonces

$$(1+\beta_1^{-1}\beta_2 ab)(1+a) = \beta_1^{-1}(\beta_1 + \beta_2 ab)(1+a) = \beta_1^{-1}\alpha \in I .$$
$$\therefore\ [1+(\beta_1^{-1}\beta_2 ab)^2](1+a) \in I$$

Nuevamente $|\beta_1| + |\beta_2| = 0$ y β_1 unidad implica $|\beta_1^{-1}\beta_2| = 1$ y por el lema 3 tenemos

$1+(\beta_1^{-1}\beta_2 ab)^2 = (1+a^2)\mu$, μ unidad y como $1+a^2$ es central, μ unidad, I es ideal izquierdo y $(1+\beta_1^{-1}\beta_2 ab)(1+a) \in I$, tenemos $(1+a^2)(1+a) \in I$

$$\therefore\ \alpha_1(1+a^2) = \beta_1(1+a)(1+a^2) \in I.$$

Finalmente si β_1 no es unidad, tenemos

$\beta_1 = \gamma'_1(1+a)$, con $\gamma'_1 \in K[\langle a \rangle]$

$$\begin{aligned}\therefore\ \alpha_1(1+a^2) &= \beta_1(1+a)(1+a^2)\\ &= \gamma'_1(1+a)(1+a)(1+a^2)\\ &= \gamma'_1(1+a^4)\\ &= \gamma'_1(1+1) = \gamma'(0) = 0 \in I\end{aligned}$$

$$\therefore\ \alpha_1(1+a^2) \in I.$$

Ahora probaremos que $\alpha x \in I$, $\forall x \in G$ con lo cual habremos probado que I es un ideal derecho y $\therefore$ $K[G]$ iiid. Como $G = \langle a, b \rangle$ es suficiente con probar que $\alpha a, \alpha b \in I$ y por la simetría que hay entre a y b basta probar, digamos $\alpha a \in I$, pero

$$\begin{aligned}\alpha a &= \alpha_1 a + \alpha_2 ba\\ &= a\alpha + ab(\alpha_2(1+a^2))\end{aligned}$$

(esto pues $ab\alpha_2(1+a^2) + a\alpha_2 b = \alpha_2 ba$)

$$\therefore\ \alpha a \in I \quad \therefore\ K[G] \text{ es iiid}.$$

$\square$

<u>Teorema 4 (P. Menal)</u>.- Sea $K[G]$ el anillo de grupo sobre un grupo no abeliano. Entónces es equivalente:

i) $K[G]$ es iiid

ii) G es localmente finito y si $\alpha, \beta \in K[G]$ son tales que $\alpha\beta = 0$, entonces $\beta\alpha = 0$

iii) G es localmente finito y $K[G]$ es aiid.

<u>Demostración</u>:

i) $\Rightarrow$ ii) Por el lema 1 ii), G es un grupo hamiltoniano (pues no es abeliano) $\therefore$ G es localmente finito.

Ahora como $K[G]$ es iiid, en particular es aiid y por el lema 2, siempre que tengamos $\alpha, \beta \in K[G]$, $\alpha\beta = 0$ entonces $\beta\alpha = 0$.

ii) $\Rightarrow$ iii) es trivial y

iii) $\Rightarrow$ i) si suponemos que se cumple iii) entonces por el Teorema I sucede Teo. I-i) ó Teo. I-ii)

$\therefore K[G]$ es iiid. $\square$

<u>Observación</u>.- Supongamos caract$(K) > 2$ y que G es localmente finito, entonces si $K[G]$ es aiid por el Teorema I, G no debe ser abeliano. Inversamente, si G es abeliano entonces $K[G]$ es iiid y por lo tanto aiid tenemos así que en caract.$(K) > 2$ y G localmente finito,

$K[G]$ es aiid $\Leftrightarrow$ G es abeliano. $\square$

Bibliografía

[1] Passman, D. S. "The algebraic structure of group rings", Wiley - Interscience, New York, 1977.

[2] Marshall Hall, Jr. "Teoría de los grupos", Trillas, México D.F., 1979, pags 202-204.

[3] Cárdenas H, Lluis E, "Módulos semisimples y representación de grupos finitos", Trillas, México D.F., 1970, pags. 79-80.

[4] Perlis S., Walker G. L., "Abelian group algebras of finite order", Math. Soc., 1949, vol.