# Capítulo 2
# El álgebra de grupo

## 2.1. Nociones básicas

Sea $K$ un cuerpo y sea $G$ un grupo. El **álgebra de grupo** $K[G]$ es el $K$-espacio vectorial con base $\{g : g \in G\}$ con la estructura de álgebra dada por el producto

$$\left(\sum_{g\in G} \lambda_g g\right)\left(\sum_{h\in G} \mu_h h\right) = \sum_{g,h\in G} \lambda_g \mu_h (gh).$$

Es fácil ver que $K[G]$ nunca es un álgebra simple: el conjunto

$$I(G) = \left\{\sum_{g\in G} \lambda_g g \in K[G] : \sum_{g\in G} \lambda_g = 0\right\}$$

es un ideal propio y no nulo de $K[G]$ (pues $\dim I(G) = \dim K[G] - 1$). Este conjunto se conoce como el **ideal de aumentación** de $K[G]$.

**Ejercicio 2.1.1.** Sea $G = C_n$ el grupo ciclico de orden $n$ (escrito multiplicativamente). Demuestre que $K[G] \simeq K[X]/(X^n - 1)$.

**Ejercicio 2.1.2.** Sea $G$ un grupo finitamente generado abeliano y sin torsión. Demuestre que $K[G]$ es un dominio.

**Ejercicio 2.1.3.** Sea $G$ un grupo y $H$ un subgrupo de $G$. Sea $\alpha \in K[H]$. Demuestre que $\alpha$ es inversible (resp. divisor de cero a izquierda) en $K[H]$ si y sólo si $\alpha$ es inversible (resp. divisor de cero a izquierda) en $K[G]$.

**Ejercicio 2.1.4.** Sean $G$ un grupo y $\alpha = \sum_{g\in G} \lambda_g g \in K[G]$. Se define el **soporte** de $\alpha$ como el conjunto

$$\operatorname{supp}\alpha = \{g \in G : \lambda_g \neq 0\}.$$

Demuestre que si $g \in G$, entonces $\operatorname{supp}(g\alpha) = g(\operatorname{supp}\alpha)$ y $\operatorname{supp}(\alpha g) = (\operatorname{supp}\alpha)g$.

## 2.2. El teorema de Maschke

El objetivo de esta sección es calcular el radical de Jacobson del álgebra de grupo de un grupo finito. Comenzamos con un ejemplo:

**Ejemplo 2.2.1.** Sea $G = C_2 = \langle g \rangle \simeq \mathbb{Z}/2$ el grupo de dos elementos escrito multiplicativamente. Todo elemento de $K[G]$ es de la forma $\alpha = a1 + bg$ para escalares $a, b \in K$ y el producto de $K[G]$ está dado por

$$(a1+bg)(c1+dg) = (ac+bd)1 + (ad+bc)g.$$

Si la característica de $K$ es distinta de dos, la función

$$K[G] \to K \times K, \quad a1+bg \mapsto (a+b, a-b),$$

es un isomorfismo de álgebras. Si en cambio $K$ es de característica dos, la función

$$K[G] \to \begin{pmatrix} K & K \\ 0 & K \end{pmatrix}, \quad a1+bg \mapsto \begin{pmatrix} a+b & b \\ 0 & a+b \end{pmatrix},$$

es un isomorfismo de álgebras.

Veamos otros ejemplo un poco más difíciles. La idea a utilizar es la siguiente: Si $A$ es una $K$-álgebra y $\rho \colon G \to U(A)$ es un morfismo de grupos, donde $U(A)$ es el grupo de unidades de $A$, entonces la función $K[G] \to A$, $\sum_{g \in G} \lambda_g g \mapsto \sum_{g \in G} \lambda_g \rho(g)$, es un morfismo de álgebras.

**Ejemplo 2.2.2.** Sea $G = C_3$ el grupo cíclico de orden tres (escrito multiplicativamente). Entonces

$$\mathbb{R}[G] \simeq \mathbb{R} \times \mathbb{C}.$$

Escribamos $G = \langle g : g^3 = 1 \rangle$ y sea

$$\varphi \colon \mathbb{R}[G] \to \mathbb{R} \times \mathbb{C}, \quad g \mapsto (1, \omega),$$

donde $\omega$ es una raíz cúbica primitiva de la unidad. Entonces $\varphi$ es inyectivo pues $0 = \varphi(a1 + bg + cg^2) = (a+b+c, a+b\omega+c\omega^2)$ implica que $a = b = c = 0$. Luego $\varphi$ es un isomorfismo pues $\dim_{\mathbb{R}} \mathbb{R}[G] = \dim_{\mathbb{R}}(\mathbb{R} \times \mathbb{C}) = 3$.

**Ejemplo 2.2.3.** Sea $G = \langle r, s : r^3 = s^2 = 1, srs = r^{-1} \rangle$ el grupo diedral de seis elementos. Vamos a demostrar que $\mathbb{C}[G] \simeq \mathbb{C} \times \mathbb{C} \times M_2(\mathbb{C})$. Sea $\omega$ una raíz cúbica de la unidad y sean

$$R = \begin{pmatrix} \omega & 0 \\ 0 & \omega^2 \end{pmatrix}, \quad S = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Un cálculo sencillo muestra que $R^2 = S^2 = I$ y que $SRS = R^{-1}$. Sea

$$\varphi \colon \mathbb{C}[G] \to \mathbb{C} \times \mathbb{C} \times M_2(\mathbb{C}), \quad r \mapsto (1,1,R), \quad s \mapsto (1,-1,S).$$

Es fácil ver que $\varphi$ es un morfismo de álgebras. Veamos que es biyectivo. Como $\dim_{\mathbb{C}} \mathbb{C}[G] = \dim_{\mathbb{C}}(\mathbb{C}\times\mathbb{C}\times M_2(\mathbb{C})) = 6$, basta ver que $\varphi$ es inyectivo. Si

$$\alpha = a_0 + a_1 r + a_2 r^2 + (b_0 + b_1 r + b_2 r^2)s \in \ker\varphi,$$

entonces

$$0 = \varphi(\alpha) = \left(u, v, \begin{pmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{pmatrix}\right),$$

donde

$$\begin{aligned} u &= a_0 + a_1 + a_2 + b_0 + b_1 + b_2, & v &= a_0 + a_1 + a_2 - b_0 - b_1 - b_2,\\ \alpha_{11} &= a_0 + a_1\omega + a_2\omega^2, & \alpha_{12} &= b_0 + b_1\omega + b_2\omega^2,\\ \alpha_{21} &= b_0 + b_2\omega + b_1\omega^2, & \alpha_{22} &= a_0 + a_2\omega + a_1\omega^2. \end{aligned}$$

Un cálculo sencillo muestra que estas ecuaciones implican que $\alpha = 0$ y luego $\varphi$ es inyectiva.

**Ejercicio 2.2.4.** Demuestre que si $G$ es el grupo diedral de seis elementos entonces

$$\mathbb{Q}[G] \simeq \mathbb{Q}\times\mathbb{Q}\times M_2(\mathbb{Q}),$$

donde $\omega$ es una raíz cúbica primitiva de la unidad.

**Teorema 2.2.5 (Maschke).** *Sea $G$ un grupo finito. Entonces $J(K[G]) = 0$ si y sólo si $K$ es de característica cero o la característica de $K$ no divide al orden de $G$.*

*Demostración.* Supongamos que $G = \{g_1, \dots, g_n\}$ con $g_1 = 1$. Sea $\rho\colon K[G] \to K$ dada por $\alpha \mapsto \text{traza}(L_\alpha)$, donde $L_\alpha(\beta) = \alpha\beta$. Tenemos $\rho(g_1) = n$ y $\rho(g_i) = 0$ para todo $i \in \{2, \dots, n\}$ pues, como $L_{g_i}(g_j) = g_i g_j \neq g_j$, la matriz de $L_{g_i}$ en la base $\{g_1, \dots, g_n\}$ tiene ceros en la diagonal.

Supongamos que $J = J(K[G])$ es no nulo y sea $\alpha = \sum_{i=1}^n \lambda_i g_i \in J \setminus \{0\}$. Sin pérdida de generalidad podemos suponer que $\lambda_1 \neq 0$ (pues si $\lambda_1 = 0$ hay algún $\lambda_i \neq 0$ y alcanza con tomar $g_i^{-1}\alpha \in J$). Entonces

$$\rho(\alpha) = \sum_{i=1}^n \lambda_i \rho(g_i) = n\lambda_1.$$

Como $G$ es un grupo finito, $K[G]$ es un álgebra de dimensión finita y luego $K[G]$ es artiniana a izquierda. Como el radical de Jacobson $J$ es un ideal nilpotente, en particular $\alpha$ es un elemento nil. Luego $L_\alpha$ es nilpotente y entonces $0 = \rho(\alpha) = n\lambda_1$. Esto implica que la característica del cuerpo $K$ divide a $n$.

Recíprocamente, supongamos que la característica de $K$ es un número primo que divide a $n$ y sea $\alpha = \sum_{i=1}^n g_i$. Como $\alpha g_j = g_j\alpha = \alpha$ para todo $j \in \{1, \dots, n\}$, el conjunto $I = K[G]\alpha$ es un ideal de $K[G]$. Como además

$$\alpha^2 = \sum_{i=1}^n g_i\alpha = n\alpha = 0,$$

se concluye que $I$ es un ideal no nulo y nilpotente. Luego $J(K[G]) \neq 0$ pues por la proposición 1.3.7 sabemos que $I \subseteq J(K[G])$.

cor:GfinitoNOnil **Corolario 2.2.6.** *Sea $G$ un grupo finito. Entonces $K[G]$ no contiene ideales a izquierda nil no nulos.*

*Demostración.* Es consecuencia inmediata del teorema de Maschke ya que $J(K[G])$ contiene a todo ideal a izquierda nil.

## 2.3. El teorema de Herstein

El objetivo de esta sección responderemos la siguiente pregunta: ¿Cuándo un álgebra de grupo es un álgebra algebraica? Una respuesta parcial está dada por el teorema de Herstein.

**Definición 2.3.1.** Un grupo $G$ se dice **localmente finito** si todo subgrupo de $G$ finitamente generado es finito.

Si $G$ es un grupo localmente finito, entonces todo $g \in G$ tiene orden finito (pues el subgrupo $\langle g \rangle$ es finito por ser finitamente generado).

**Ejemplo 2.3.2.** Todo grupo finito es obviamente localmente finito.

**Ejemplo 2.3.3.** El grupo $\mathbb{Z}$ no es localmente finito pues es libre de torsión.

**Ejemplo 2.3.4.** Sea $p$ un primo. El **grupo de Prüfer**

$$\mathbb{Z}(p^\infty) = \{z \in \mathbb{Z} : z^{p^n} = 1 \text{ para algún } n \in \mathbb{N}\}$$

de todas las raíces $p$-ésimas de uno es localmente finito.

**Ejemplo 2.3.5.** Sean $X$ un conjunto infinito y $\mathbb{S}_X$ el conjunto de biyecciones $X \to X$ que mueven únicamente una cantidad finita de elementos de $X$. Entonces $\mathbb{S}_X$ es localmente finito.

Antes de demostrar el teorema de Herstein vamos a dar una familia de ejemplos de grupos localmente finitos. Para eso necesitamos un lema:

lem:solvable_torsion=>lf **Lema 2.3.6.** *Sea $G$ un grupo y sea $N$ un subgrupo normal de $G$. Si $N$ y $G/N$ son localmente finitos, entonces $G$ es localmente finito.*

*Demostración.* Sea $\pi\colon G \to G/N$ el morfismo canónico. Sea $\{g_1, \dots, g_n\}$ un subconjunto finito de $G$. Como $G/N$ es localmente finito, el subgrupo $Q$ de $G/N$ generado por $\pi(g_1), \dots, \pi(g_n)$ es finito, digamos

$$Q = \{\pi(g_1), \dots, \pi(g_n), \pi(g_{n+1}), \dots, \pi(g_m)\}.$$

Para cada $i, j \in \{1, \dots, n\}$ sabemos que existen $u_{ij} \in N$ y $k \in \{1, \dots, m\}$ tales que $g_i g_j = u_{ij} g_k$. Sea $U$ el subgrupo de $G$ generado por los $u_{ij}$. Como $N$ es localmente finito, $U$ es un subgrupo finito. Como además cada elemento $g_i g_j g_l$ puede escribirse como

$$g_i g_j g_l = u_{ij} g_k g_l = u_{ij} u_{kl} g_t = u g_t$$

para algún $u \in U$ y algún $t \in \{1, \dots, m\}$, se concluye que el subgrupo $H$ de $G$ generado por $\{g_1, \dots, g_n\}$ es finito pues $|H| \leq m|U|$.

Veamos una aplicación a los grupos resolubles. Recordemos que un grupo $G$ se dice **resoluble** si existe una sucesión de subgrupos

$$1 = G_0 \subsetneq G_1 \subsetneq \cdots \subsetneq G_n = G \tag{2.1}$$ eq:resoluble

donde cada $G_i$ es normal en $G_{i+1}$ y cada cociente $G_i/G_{i-1}$ es abeliano.

**Proposición 2.3.7.** *Si G es un grupo resoluble y de torsión, entonces G es localmente finito.*

*Demostración.* Procederemos por inducción en la longitud $n$ de la sucesión de resolubilidad (2.1). Si $n = 1$ entonces $G$ es finito por ser abeliano y de torsión. Supongamos que el resultado vale para grupos resolubles de longitud $n-1$ y sea $G$ un grupo resoluble tal que (2.1). Por hipótesis inductiva, el subgrupo normal $G_{n-1}$ de $G$ es localmente finito. Entonces, como $G/G_{n-1}$ es localmente finito por ser abeliano y de torsión, el resultado se obtiene del lema 2.3.6.

**Teorema 2.3.8 (Herstein).** *Si $G$ es un grupo localmente finito, entonces $K[G]$ es algebraica. Recíprocamente, si $K[G]$ es algebraica y $K$ es de característica cero, entonces $G$ es localmente finito.*

*Demostración.* Supongamos que $G$ es localmente finito y sea $\alpha \in K[G]$. El subgrupo $H = \langle \operatorname{supp} \alpha \rangle$ es finitamente generado y luego finito. Como $\alpha \in K[H]$ y $\dim_K K[H] < \infty$, el conjunto $\{1, \alpha, \alpha^2, \dots\}$ es linealmente dependiente. Luego $\alpha$ es algebraico sobre $K$.

Sea $\{x_1, \dots, x_m\}$ un subconjunto finito de $G$. Si agregamos los inversos, podemos suponer que $\{x_1, \dots, x_m\}$ genera al subgrupo $H = \langle x_1, \dots, x_m \rangle$ como semigrupo. Si $\alpha = x_1 + \cdots + x_m \in K[G]$, entonces, como $\alpha$ es algebraico sobre $K$,

$$\alpha^{n+1} = a_0 + a_1 \alpha + \cdots + a_n \alpha^n$$

para algún $n \geq 0$ y escalares $a_0, \dots, x_n \in K$. Sea $w = x_{i_1} \cdots x_{i_{n+1}} \in H$ una palabra de longitud $n+1$. Observemos que existen enteros positivos $c_{i_1 \cdots i_m}$ tales que

$$\alpha^{n+1} = (x_1 + \cdots + x_m)^{n+1} = \sum_{\substack{i_1 + \cdots + i_m = n+1 \\ i_j \text{ enteros positivos}}} c_{i_1 \cdots i_m} x_1^{i_1} \cdots x_m^{i_m}.$$

Como $K$ es de característica cero, se concluye que $w \in \operatorname{supp}(\alpha^{n+1})$. Pero como además $\alpha^{n+1} = \sum_{j=0}^{n} a_j \alpha^j$, entonces $w \in \operatorname{supp}(\alpha^j)$ para algún $j \in \{0, \dots, n\}$. Demostramos entonces que toda palabra en las $x_j$ de longitud $n+1$ puede escribirse como una palabra en las $x_j$ de longitud a lo sumo $n$. Luego $H$ es finito y entonces $G$ es localmente finito.

## 2.4. El teorema de Formanek

Veremos un resultado de Formanek que puede entenderse como una generalización del teorema de Herstein.

**Ejercicio 2.4.1.** Sea $A$ un álgebra algebraica y sea $a \in A$. Demuestre las siguientes afirmaciones:

1. $a$ es un divisor de cero a izquierda si y sólo si $a$ es un divisor de cero a derecha.
2. $a$ es inversible a izquierda si y sólo si $a$ es inversible a derecha.
3. $a$ es inversible si y sólo si $a$ no es un divisor de cero.

exa:norma **Ejercicio 2.4.2.** Si $\alpha = \sum_{g \in G} \alpha_g g \in \mathbb{C}[G]$ se define $|\alpha| = \sum_{g \in G} |\alpha_g| \in \mathbb{R}$. Demuestre que valen las siguientes propiedades:

1. $|\alpha + \beta| \leq |\alpha| + |\beta|$, y
2. $|\alpha\beta| \leq |\alpha||\beta|$

para todo $\alpha, \beta \in \mathbb{C}[G]$.

thm:FormanekQ **Teorema 2.4.3 (Formanek, primera versión).** *Sea $G$ un grupo y supongamos que todo elemento de $\mathbb{Q}[G]$ es inversible o un divisor de cero. Entonces $G$ es localmente finito.*

*Demostración.* Sea $\{x_1, \dots, x_n\}$ un subconjunto finito de $G$. Si agregamos los inversos, podemos suponer que $\{x_1, \dots, x_n\}$ genera al subgrupo $H = \langle x_1, \dots, x_n \rangle$ como semigrupo. Sea
$$\alpha = \frac{1}{2n}(x_1 + \cdots + x_n) \in \mathbb{Q}[G]$$

Veamos que $1 - \alpha \in \mathbb{Q}[G]$ es inversible. Si no, entonces es un divisor de cero. Si existe $\delta \in \mathbb{Q}[G]$ tal que $\delta(1-\alpha) = 0$, entonces $\delta = \delta\alpha$ y luego, como
$$|\delta| = |\delta\alpha| \leq |\delta||\alpha| = |\delta|/2,$$
se concluye que $\delta = 0$. Similarmente se demuestra que $(1-\alpha)\delta = 0$ implica que $\delta = 0$.

Sea $\beta = (1-\alpha)^{-1} \in \mathbb{Q}[G]$. Para cada $k$ definimos
$$\gamma_k = (1 + \alpha + \cdots + \alpha^k) - \beta.$$

Entonces
$$\begin{aligned}\gamma_k(1-\alpha) &= (1 + \alpha + \cdots + \alpha^k - \beta)(1-\alpha)\\ &= (1 + \alpha + \cdots + \alpha^k)(1-\alpha) - \beta(1-\alpha) = -\alpha^{k+1}\end{aligned}$$

y luego $\gamma_k = -\alpha^{k+1}\beta$. Como

$$|\gamma_k| = |-\alpha^{k+1}\beta| \leq |\beta||\alpha^{k+1}| = \frac{|\beta|}{2^{k+1}},$$

se concluye que $\lim_{k\to\infty} |\gamma_k| = 0$.

Para terminar veamos que $H \subseteq \operatorname{supp}\beta$. Si $H \not\subseteq \operatorname{supp}\beta$, sea $h \in H \setminus \operatorname{supp}\beta$. Supongamos que $h = x_{i_1}\cdots x_{i_m}$ es una palabra de longitud $m$ en los $x_j$. Sea $c_j$ el coeficiente de $h$ en $\alpha^j$. Entonces $c_0 + \cdots + c_k$ es el coeficiente de $h$ en $\gamma_k$, pero

$$|\gamma_k| \geq c_0 + c_1 + \cdots + c_k \geq c_m > 0$$

para todo $k \geq m$ pues cada $c_j$ es no negativo, una contradicción pues demostramos que $|\gamma_k| \to 0$ si $k \to \infty$.

A continuación explicaremos por qué el teorema de Formanek se considera una generalización del teorema de Herstein. En el teorema 2.4.3 nos concentramos en álgebras de grupo sobre los números racionales. ¿Cómo podemos extender este resultado a álgebras de grupo sobre cuerpos de característica cero? Para extender el cuerpo de base sobre el que se trabaja necesitamos definir el producto tensorial de espacios vectoriales y el producto tensorial de álgebras.

**Definición 2.4.4.** El **producto tensorial** de los $K$-espacios vectoriales $U$ y $V$ es el espacio vectorial cociente $K[U\times V]/T$, donde $K[U\times V]$ es el espacio vectorial con base $\{(u,v) : u \in U, v \in V\}$ y $T$ es el subespacio generado por los elementos de la forma

$$(\lambda u + \mu u', v) - \lambda(u,v) - \mu(u',v), \quad (u, \lambda v + \mu v') - \lambda(u,v) - \mu(u,v')$$

para $\lambda, \mu \in K$, $u, u' \in U$ y $v, v' \in V$.

El producto tensorial de $U$ y $V$ será denotado por $U \otimes_K V$ o por $U \otimes V$ si la referencia al cuerpo $K$ puede omitirse. Dados $u \in U$ y $v \in V$ escribiremos $u \otimes v$ para denotar a la coclase $(u,v) + T$.

**Teorema 2.4.5.** *Sean $U$ y $V$ espacios vectoriales. Existe entonces una función bilineal $U\times V \to U\otimes V$, $(u,v) \mapsto u\otimes v$, tal que todo elemento de $U \otimes V$ es una suma finita de la forma*

$$\sum_{i=1}^{N} u_i \otimes v_i$$

*para $u_1,\dots,u_N \in U$ y $v_1,\dots,v_N \in V$. Más aún, dado un espacio vectorial $W$ y una función bilineal $\beta\colon U\times V \to W$, existe una función lineal $\overline{\beta}\colon U\otimes V \to W$ tal que $\overline{\beta}(u\otimes v) = \beta(u,v)$ para todo $u \in U$ y $v \in V$.*

*Demostración.* Por la definición del producto tensorial, la función

$$U\times V \to U\otimes V, \quad (u,v) \mapsto u\otimes v,$$

es bilineal. También de la definición se deduce inmediatamente que todo elemento de $U \otimes V$ es una combinación lineal finita de elementos de la forma $u \otimes v$, donde $u \in U$ y $v \in V$. Como $\lambda(u \otimes v) = (\lambda u) \otimes v$ para todo $\lambda \in K$, la primera afirmación queda demostrada.

Como $U \times V$ es base de $K[U \times V]$, existe una transformación lineal

$$\gamma\colon K[U \times V] \to W, \quad \gamma(u,v) = \beta(u,v).$$

Como $\beta$ es bilineal por hipótesis, $T \subseteq \ker \gamma$. Existe entonces una transformación lineal $\overline{\beta}\colon U \otimes V \to W$ tal que

$$\begin{tikzcd} K[U \times V] \arrow[r] \arrow[d] & W \\ U \otimes V \arrow[ur, dashed] & \end{tikzcd}$$

conmuta. En particular, $\overline{\beta}(u \otimes v) = \beta(u,v)$.

xca:tensorial_unicidad

**Ejercicio 2.4.6.** Demuestre que las propiedades mencionadas en el teorema anterior caracterizan el producto tensorial salvo isomorfismo.

Veamos algunas propiedades del producto tensorial de espacios vectoriales.

**Lema 2.4.7.** *Sean $\varphi\colon U \to U'$ y $\psi\colon V \to V'$ transformaciones lineales. Existe entonces una única transformación lineal $\varphi \otimes \psi\colon U \otimes V \to U' \otimes V'$ tal que*

$$(\varphi \otimes \psi)(u \otimes v) = \varphi(u) \otimes \psi(v)$$

*para todo $u \in U$ y $v \in V$.*

*Demostración.* Como la función $U \times V \to U \otimes V$, $(u,v) \mapsto \varphi(u) \otimes \psi(v)$, es bilineal, existe una transformación lineal $U \otimes V \to U \otimes V$, $u \otimes v \to \varphi(u) \otimes \psi(v)$. Luego la función

$$\sum u_i \otimes v_i \mapsto \sum \varphi(u_i) \otimes \psi(v_i)$$

está bien definida.

**Ejercicio 2.4.8.** Demuestre las siguientes afirmaciones:

1. $(\varphi \otimes \psi)(\varphi' \otimes \psi') = (\varphi\varphi') \otimes (\psi\psi')$.
2. Si $\varphi$ y $\psi$ son isomorfismos, entonces $\varphi \otimes \psi$ es un isomorfismo.
3. $(\lambda\varphi + \lambda'\varphi') \otimes \psi = \lambda\varphi \otimes \psi + \lambda'\varphi' \otimes \psi$.
4. $\varphi \otimes (\lambda\psi + \lambda'\psi') = \lambda\varphi \otimes \psi + \lambda'\varphi \otimes \psi'$.
5. Si $U \simeq U'$ y $V \simeq V'$, entonces $U \otimes V \simeq U' \otimes V'$.

**Lema 2.4.9.** *Si $U$ y $V$ son espacios vectoriales, entonces $U \otimes V \simeq V \otimes U$.*

*Demostración.* Como la función $U \times V \to V \otimes U$, $(u,v) \mapsto v \otimes u$, existe una transformación lineal $U \otimes V \to V \otimes U$, $u \otimes v \mapsto v \otimes u$. Similarmente se demuestra que existe una transformación lineal $V \otimes U \to U \otimes V$, $v \otimes u \mapsto u \otimes v$. Luego $U \otimes V \simeq V \otimes U$.

xca:UxVxW **Ejercicio 2.4.10.** Demuestre que $(U \otimes V) \otimes W \simeq U \otimes (V \otimes W)$.

xca:UxK **Ejercicio 2.4.11.** Demuestre que $U \otimes K \simeq K \simeq K \otimes U$.

lem:U_LI **Lema 2.4.12.** *Sea $\{u_1, \dots, u_n\} \subseteq U$ un conjunto linealmente independiente y sean $v_1, \dots, v_n \in V$ tales que $\sum_{i=1}^{n} u_i \otimes v_i = 0$. Entonces $v_i = 0$ para todo $i \in \{1, \dots, n\}$.*

*Demostración.* Sea $i \in \{1, \dots, n\}$ y sea $f_i \colon U \to K$, $f_i(u_j) = \delta_{ij}$. Como la función $U \times V \to V$, $(u, v) \mapsto f_i(u)v$, es bilineal, existe una función $\alpha_i \colon U \otimes V \to V$ lineal tal que $\alpha_i(u \otimes v) = f_i(u)v$. Luego

$$v_i = \sum_{j=1}^{n} \alpha_i(u_j \otimes v_j) = \alpha_i \left( \sum_{j=1}^{n} u_j \otimes v_j \right) = 0.$$

xca:uxv=0 **Ejercicio 2.4.13.** Demuestre que si $u \otimes v = 0$ y $v \neq 0$, entonces $u = 0$.

**Teorema 2.4.14.** *Si $\{u_i : i \in I\}$ es una base de $U$ y $\{v_j : j \in J\}$ es una base de $V$, entonces $\{u_i \otimes v_j : i \in I, j \in J\}$ es una base de $U \otimes V$.*

*Demostración.* Los $u_i \otimes v_j$ forman un conjunto de generadores pues si $u = \sum_i \lambda_i u_i$ y $v = \sum_j \mu_j v_j$, entonces $u \otimes v = \sum_{i,j} \lambda_i \mu_j u_i \otimes v_j$. Veamos ahora que los $u_i \otimes v_j$ son linealmente independientes. Para eso, queremos ver que cualquier subconjunto finito de los $u_i \otimes v_j$ es linealmente independiente. Si $\sum_k \sum_l \lambda_{kl} u_{i_k} \otimes v_{j_l} = 0$, entonces $0 = \sum_k u_{i_k} \otimes \left( \sum_l \lambda_{kl} v_{j_l} \right)$ y luego, como los $u_{i_k}$ son linealmente indepentientes, el lema 2.4.12 implica que $\sum_l \lambda_{kl} v_{j_l} = 0$. Luego $\lambda_{kl} = 0$ para todo $k, l$ pues los $v_{j_l}$ son linealmente independientes.

El teorema anterior implica inmediatamente que si $U$ y $V$ son espacios vectoriales de dimensión finita entonces

$$\dim(U \otimes V) = (\dim U)(\dim V).$$

**Corolario 2.4.15.** *Si $\{u_i : i \in I\}$ es base de $U$, entonces todo elemento de $U \otimes V$ se escribe unívocamente como una suma finita $\sum_i u_i \otimes v_i$.*

*Demostración.* Sabemos que todo elemento de $U \otimes V$ es una suma finita $\sum_i x_i \otimes y_i$, donde $x_i \in U$ y $y_i \in V$. Si escribimos $x_i = \sum_j \lambda_{ij} u_j$, entonces

$$\sum_i x_i \otimes y_i = \sum_i \left( \sum_j \lambda_{ij} u_j \right) \otimes y_i = \sum_j u_j \otimes \left( \sum_i \lambda_{ij} y_i \right).$$

El siguiente lema nos permite definir el **producto tensorial de álgebras**.

**Lema 2.4.16.** *Si $A$ y $B$ son álgebras, entonces $A \otimes B$ es un álgebra con el producto*

$$(a \otimes b)(x \otimes y) = ax \otimes by.$$

*Demostración.* Para $x \in A$, $y \in B$ consideramos $R_x \otimes R_y \in \mathrm{End}_K(A \otimes B)$. Como la función $A \times B \to \mathrm{End}_K(A \otimes B)$, $(x,y) \mapsto R_x \otimes R_y$, es bilineal, existe una función lineal $\varphi \colon A \otimes B \to \mathrm{End}_K(A \otimes B)$, $\varphi(x \otimes y) = R_x \otimes R_y$. Para $u, v \in A \otimes B$ definimos

$$uv = \varphi(v)(u).$$

Esta operación es bilineal pues por ejemplo

$$u(v+w) = \varphi(v+w)(u) = (\varphi(v) + \varphi(w))(u) = \varphi(v)(u) + \varphi(w)(u) = uv + uw.$$

Además $(a \otimes b)(x \otimes y) = \varphi(x \otimes y)(a \otimes b) = (R_x \otimes R_y)(a \otimes b) = ax \otimes by$. Un cálculo sencillo muestra que este producto es asociativo.

**Ejercicio 2.4.17.** Demuestre que para álgebras valen las siguientes afirmaciones:

1. $A \otimes B \simeq B \otimes A$.
2. $(A \otimes B) \otimes C \simeq A \otimes (B \otimes C)$.
3. $A \otimes K \simeq A \simeq K \otimes A$.
4. Si $A \otimes A'$ y $B \otimes B'$ entonces $A \otimes B \simeq A' \otimes B'$.

Veamos algunos ejemplos:

**Proposición 2.4.18.** *Si $G$ y $H$ son grupos, entonces $K[G] \otimes K[H] \simeq K[G \times H]$.*

*Demostración.* Sabemos que $\{g \otimes h : g \in G, h \in H\}$ es una base de $K[G] \otimes K[H]$ y que $G \times H$ es una base de $K[G \times H]$. Tenemos entonces un isomorfismo lineal

$$K[G] \otimes K[H] \to K[G \times H], \quad g \otimes h \mapsto (g,h),$$

que además es multiplicativo. Luego $K[G] \otimes K[H] \simeq K[G \times H]$ como álgebras.

**Proposición 2.4.19.** *Si $A$ es un álgebra, entonces $A \otimes K[X] \simeq A[X]$.*

*Demostración.* Todo elemento de $A \otimes K[X]$ se escribe unívocamente como una suma finita de la forma $\sum a_i \otimes X^i$. Un cálculo sencillo muestra que $A \otimes K[X] \mapsto A[X]$, $\sum a_i \otimes X^i \mapsto \sum a_i X^i$, es un isomorfismo de álgebras.

**Ejercicio 2.4.20.** Demuestre que si $A$ es un álgebra, $A \otimes M_n(K) \simeq M_n(A)$. En particular, $M_n(K) \otimes M_m(K) \simeq M_{nm}(K)$.

Estos últimos dos ejemplos son casos particulares de una construcción importante que involucra productos tensoriales y se conoce como **extensión de escalares**.

**Teorema 2.4.21.** *Sea $A$ un álgebra sobre $K$ y sea $E$ una extensión de $K$. Entonces $A^E = E \otimes_K A$ es un álgebra sobre $E$ con respecto a la multiplicación por escalares dada por*

$$\lambda(\mu \otimes a) = (\lambda\mu) \otimes a,$$

*para $\lambda, \mu \in E$ y $a \in A$.*

*Demostración.* Sea $\lambda \in E$. Como la función $E \times A \to E \otimes_K A$, $(\mu, a) \mapsto (\lambda\mu) \otimes a$, es $K$-bilineal, existe una transformación lineal $E \otimes_K A \to E \otimes_K A$, $\mu \otimes a \mapsto (\lambda\mu) \otimes a$. Queda bien definida entonces la multiplicación por escalares y además

$$\lambda(u+v) = \lambda u + \lambda v$$

para $\lambda \in E$ y $u, v \in E \otimes_K A$. Un cálculo directo muestra que además

$$(\lambda + \mu)u = \lambda u + \mu u, \quad (\lambda\mu)u = \lambda(\mu u), \quad \lambda(uv) = (\lambda u)v = u(\lambda v)$$

valen para todo $u, v \in E \otimes_K A$ y $\lambda, \mu \in E$.

**Ejercicio 2.4.22.** Demuestre que valen las siguientes afirmaciones:

1. $1 \otimes A$ es una subálgebra de $A^E$ isomorfa a $A$.
2. Si $\{a_i : i \in I\}$ es base de $A$, entonces $\{1 \otimes a_i : i \in I\}$ es base de $A^E$.

**Ejercicio 2.4.23.** Demuestre que si $G$ es un grupo y $K$ es un subcuerpo de $E$, entonces $E \otimes_K K[G] \simeq E[G]$.

Estamos en condiciones de demostrar el teorema de Formanek:

**Teorema 2.4.24 (Formanek).** *Sea $K$ un cuerpo de característica cero y sea $G$ un grupo. Si todo elemento de $K[G]$ es inversible o un divisor de cero, entonces $G$ es localmente finito.*

*Demostración.* Como $K$ es de característica cero, $\mathbb{Q} \subseteq K$ y $K[G] \simeq K \otimes_{\mathbb{Q}} \mathbb{Q}[G]$. Todo $\beta \in K \otimes_{\mathbb{Q}} \mathbb{Q}[Q]$ se escribe unívocamente como

$$\beta = 1 \otimes \beta_0 + \sum k_i \otimes \beta_i,$$

donde $\{1, k_1, k_2, \dots,\}$ es una base de $K$ como $\mathbb{Q}$-espacio vectorial. Sea $\alpha \in \mathbb{Q}[G]$ y sea $\beta \in K[G]$ tal que $\alpha\beta = 1$. Como entonces

$$1 \otimes 1 = (1 \otimes \alpha)\beta = 1 \otimes \alpha\beta_0 + \sum k_i \otimes \alpha\beta_i,$$

la unicidad de la escritura nos dice que $\alpha\beta_0 = 1$. De la misma forma, si $\alpha\beta = 0$, entonces $\alpha\beta_j = 0$ para todo $j$. Luego, como todo $\alpha \in \mathbb{Q}[G]$ es inversible o un divisor de cero, el resultado se obtiene al usar el teorema 2.4.3 de Formanek para $\mathbb{Q}$.

## 2.5. El teorema de Rickart

En esta sección vamos a demostrar que para cualquier grupo $G$ el radical de Jacobson de $\mathbb{C}[G]$ es cero. Demostraremos también que el radical de Jacobson de $\mathbb{R}[G]$ es cero.

**Definición 2.5.1.** Sea $R$ un anillo. Una **involución** del anillo $R$ es un morfismo aditivo $R \to R$, $x \mapsto x^*$, tal que $x^{**} = x$ y $(xy)^* = y^*x^*$ para todo $x, y \in R$.

De la definición se deduce inmediatamente que si $R$ es unitario, entonces $1^* = 1$.

**Ejemplo 2.5.2.** La conjugación $z \mapsto \overline{z}$ es una involución de $\mathbb{C}$.

**Ejemplo 2.5.3.** La trasposición $X \mapsto X^T$ es una involución del anillo $M_n(K)$.

**Ejemplo 2.5.4.** Sea $G$ un grupo. Entonces $\left(\sum_{g\in G} \alpha_g g\right)^* = \sum_{g\in G} \overline{\alpha_g} g^{-1}$ es una involución de $\mathbb{C}[G]$.

Dado un grupo $G$, se define la **traza** de un elemento $\alpha = \sum_{g\in G} \alpha_g g \in K[G]$ como $\operatorname{traza}(\alpha) = \alpha_1$. Es fácil ver que traza: $K[G] \to K$, $\alpha \mapsto \operatorname{traza}(\alpha)$ es una función $K$-lineal tal que $\operatorname{traza}(\alpha\beta) = \operatorname{traza}(\beta\alpha)$.

**Ejercicio 2.5.5.** Sea $G$ un grupo finito y $K$ un cuerpo tal que su característica no divide al orden de $G$. Demuestre las siguientes afirmaciones:

1. Si $\alpha \in K[G]$ es nilpotente, entonces $\operatorname{traza}(\alpha) = 0$.
2. Si $\alpha \in K[G]$ es idempotente, entonces $\operatorname{traza}(\alpha) = \dim K[G]\alpha/|G|$.

**Ejercicio 2.5.6.** Demuestre que $\langle \alpha, \beta \rangle = \operatorname{traza}(\alpha\beta^*)$, $\alpha, \beta \in \mathbb{C}[G]$, define un producto interno en $\mathbb{C}[G]$.

lem:algebraico

**Lema 2.5.7.** *Sea $G$ un grupo. Si $J(\mathbb{C}[G]) \neq 0$, entonces existe $\alpha \in J(\mathbb{C}[G])$ tal que* $\operatorname{traza}(\alpha^{2^m}) \in \mathbb{R}_{\geq 1}$ *para todo $m \geq 1$.*

*Demostración.* Sea $\alpha = \sum_{g\in G} \alpha_g g \in \mathbb{C}[G]$. Entonces

$$\operatorname{traza}(\alpha^*\alpha) = \sum_{g\in G} \overline{\alpha_g}\alpha_g = \sum_{g\in G} |\alpha_g|^2 \geq |\alpha_1|^2 = |\operatorname{traza}(\alpha)|^2.$$

Al usar esta fórmula para algún $\alpha$ tal que $\alpha^* = \alpha$ y usar inducción se obtiene que $\operatorname{traza}(\alpha^{2^m}) \geq |\operatorname{traza}(\alpha)|^{2^m}$ para todo $m \geq 1$.

Sea $\beta = \sum_{g\in G} \beta_g g \in J(\mathbb{C}[G])$ tal que $\beta \neq 0$. Como $\operatorname{traza}(\beta^*\beta) = \sum_{g\in G} |\beta_g|^2 \neq 0$ y $J(\mathbb{C}[G])$ es un ideal,

$$\alpha = \frac{\beta^*\beta}{\operatorname{traza}(\beta^*\beta)} \in J(\mathbb{C}[G]).$$

Este elemento $\alpha$ cumple que $\alpha^* = \alpha$ y $\operatorname{traza}(\alpha) = 1$. Luego $\operatorname{traza}(\alpha^{2^m}) \geq 1$ para todo $m \geq 1$.

El ejercicio 2.4.2 implica que $\mathbb{C}[G]$ con $\operatorname{dist}(\alpha, \beta) = |\alpha - \beta|$ es un espacio métrico. En este espacio métrico, la función $\mathbb{C}[G] \to \mathbb{C}$, $\alpha \mapsto \operatorname{traza}(\alpha)$, es una función continua.

lem:phi_diferenciable

**Lema 2.5.8.** *Sea $\alpha \in J(\mathbb{C}[G])$. La función*

$$\varphi\colon \mathbb{C} \to \mathbb{C}[G], \quad \varphi(z) = (1 - z\alpha)^{-1},$$

*es continua, diferenciable y $\varphi(z) = \sum_{n\geq 0} \alpha^n z^n \in \mathbb{C}[G]$ si $|z|$ es suficientemente pequeño.*

*Demostración.* Sean $y, z \in \mathbb{C}$. Como $\varphi(y)$ y $\varphi(z)$ conmutan,

$$\begin{aligned} \varphi(y) - \varphi(z) &= ((1 - z\alpha) - (1 - y\alpha))\,(1 - y\alpha)^{-1}(1 - z\alpha)^{-1} \\ &= (y - z)\alpha\varphi(y)\varphi(z). \end{aligned} \tag{2.2}$$

eq:Rickart

Entonces $|\varphi(y)| \leq |\varphi(z)| + |y - z||\alpha\varphi(y)||\varphi(z)|$ y luego

$$|\varphi(y)|\,(1 - |y - z||\alpha\varphi(z)|) \leq |\varphi(z)|.$$

Fijado $z$ podemos elegir $y$ suficientemente cerca de $z$ de forma tal que se cumpla que $1 - |y - z||\alpha\varphi(z)| \geq 1/2$. Luego $|\varphi(y)| \leq 2|\varphi(z)|$. De la igualdad (2.2) se obtiene entonces $|\varphi(y) - \varphi(z)| \leq 2|y - z||\alpha||\varphi(z)|^2$ y luego $\varphi$ es una función continua. Por la expresión (2.2),

$$\varphi'(z) = \lim_{y \to z} \frac{\varphi(y) - \varphi(z)}{y - z} = \lim_{y \to z} \alpha\varphi(y)\varphi(z) = \alpha\varphi(z)^2$$

para todo $z \in \mathbb{C}$.

Si $z$ es tal que $|z||\alpha| = |z\alpha| < 1$, entonces

$$\varphi(z) - \sum_{n=0}^{N} z^n\alpha^n = \varphi(z)\left(1 - (1 - z\alpha)\sum_{n=0}^{N} z^n\alpha^n\right) = \varphi(z)(z\alpha)^{N+1}$$

y luego

$$\left|\varphi(z) - \sum_{n=0}^{N} z^n\alpha^n\right| \leq |\varphi(z)||z\alpha|^{N+1}.$$

Como $\varphi(z)$ está acotada cerca de $z = 0$, se concluye que $\left|\varphi(z) - \sum_{n=0}^{N} z^n\alpha^n\right| \to 0$ si $N \to \infty$.

Estamos en condiciones de demostrar el teorema de Rickart:

**Teorema 2.5.9 (Rickart).** *Si $G$ es un grupo, entonces $J(\mathbb{C}[G]) = 0$.*

*Demostración.* Sea $\alpha \in J(\mathbb{C}[G])$ y sea $\varphi(z) = (1 - \alpha z)^{-1}$. Sea $f\colon \mathbb{C} \to \mathbb{C}$ dada por $f(z) = \operatorname{traza}\varphi(z) = \operatorname{traza}\big((1 - z\alpha)^{-1}\big)$. Por el lema 2.5.8, $f(z)$ es una función entera tal que $f'(z) = \operatorname{traza}(\alpha\varphi(z)^2)$ y

$$f(z) = \sum_{n=0}^{\infty} z^n \operatorname{traza}(\alpha^n) \tag{2.3}$$

eq:Taylor

si $|z|$ es suficientemente pequeño. En particular, la igualdad (2.3) es la expansión en serie de Taylor para $f(z)$ en el origen. Esto implica que esta serie tiene radio de convergencia infinito y converge a $f(z)$ para todo $z \in \mathbb{C}$. En particular,

$$\lim_{n \to \infty} \operatorname{traza}(\alpha^n) = 0. \tag{2.4}$$

eq:limite

Por otro lado, si $\alpha \neq 0$ el lema 2.5.7 implica que traza$(\alpha^{2^m}) \geq 1$ para todo $m \geq 0$, lo que contradice el límite calculado en (2.4). Luego $\alpha = 0$.

Para demostrar un corolario necesitamos dos lemas:

lem:Nakayama **Lema 2.5.10 (Nakayama).** *Sea $R$ un anillo unitario y sea $M$ un $R$-módulo finitamente generado. Si $J(R)M = M$, entonces $M = 0$.*

*Demostración.* Supongamos que $M$ está generado por los elementos $x_1, \dots, x_n$. Como $x_n \in M = J(R)M$, existen $r_1, \dots, r_n \in J(R)$ tales que $x_n = r_1x_1 + \cdots + r_nx_n$, es decir $(1 - r_n)x_n = \sum_{j=1}^{n-1} r_jx_j$. Como $1 - r_n$ es inversible, existe $s \in R$ tal que $s(1 - r_n) = 1$. Luego $x_n = \sum_{j=1}^{n-1} sr_jx_j$ y entonces $M$ está generado por $x_1, \dots, x_{n-1}$. Al repetir este procedimiento una cierta cantidad finita de veces, se obtiene que $M = 0$.

lem:Rickart **Lema 2.5.11.** *Sea $\iota \colon R \to S$ un morfismo de anillos unitarios. Si*

$$S = \iota(R)x_1 + \cdots + \iota(R)x_n,$$

*donde cada $x_j$ cumple que $x_jy = yx_j$ para todo $y \in \iota(R)$, entonces $\iota(J(R)) \subseteq J(S)$.*

*Demostración.* Veamos que $J = \iota(J(R))$ actúa trivialmente en cada $S$-módulo simple $M$. Si $M$ es un $S$-módulo simple, escribimos $M = Sm$ para algún $m \neq 0$. Es claro que $M$ es un $R$-módulo con $r \cdot m = \iota(r)m$. Como

$$M = Sm = (\iota(R)x_1 + \cdots + \iota(R)x_n)m = \iota(R)(x_1m) + \cdots + \iota(R)(x_nm),$$

$M$ es finitamente generado como $\iota(R)$-módulo. Además $J(R) \cdot M = JM = \iota(J)M$ es un $S$-submódulo de $M$ pues

$$x_j(JM) = (x_jJ)M = (Jx_j)M = J(x_jM) \subseteq JM.$$

Como $M \neq 0$, el lema de Nakayama implica que $J(R) \cdot M \subsetneq M$. Luego, como $M$ es un $S$-módulo simple, se concluye que $J(R)M = 0$.

**Corolario 2.5.12.** *Si $G$ es un grupo, entonces $J(\mathbb{R}[G]) = 0$.*

*Demostración.* Sea $\iota \colon \mathbb{R}[G] \to \mathbb{C}[G]$ la inclusión canónica. Como

$$\mathbb{C}[G] = \mathbb{R}[G] + i\mathbb{R}[G],$$

el lema 2.5.11 y el teorema de Rickart implican que $\iota(J(\mathbb{R}[G])) \subseteq J(\mathbb{C}[G]) = 0$. Luego $J(\mathbb{R}[G]) = 0$ pues $\iota$ es inyectiva.