# Representaciones lineales de grupos

Pedro Sancho

15-12-2003

# Índice General

# Capítulo 1

# Anillos semisimples

## 1.1 Módulos semisimples

Supondremos que $A$ es un anillo no conmutativo con unidad.

**1. Ejemplo:** El álgebra de matrices cuadradas de orden $n$ (es decir, el anillo de endomorfismos lineales de un espacio vectorial de dimensión $n$).

Dado un grupo $G$, sea $k[G] := \bigoplus_{g\in G} k\cdot g$ la $k$-álgebra no conmutativa, de operaciones

$$(\sum_{g\in G}\lambda_g g)+(\sum_{g\in G}\lambda'_g g) := \sum_{g\in G}(\lambda_g+\lambda'_g)g$$

$$(\sum_{g\in G}\lambda_g g)\cdot(\sum_{g\in G}\lambda'_g g) := \sum_{g\in G}(\sum_{g'\cdot g''=g}\lambda_{g'}\lambda'_{g''}g)$$

La $k$-álgebra $k[G]$ es conmutativa si y sólo si $G$ es un grupo abeliano.

**2. Definición:** Diremos que un $A$-módulo es simple si no contiene submódulos propios. Diremos que un $A$-módulo es semisimple si es suma directa de $A$-módulos simples.

**3. Ejemplo:** Los $k$-espacios vectoriales simples son los de dimensión 1. En anillos conmutativos $A$, los $A$-módulos simples son isomorfos a $A/\mathfrak{m}$, siendo $\mathfrak{m}$ un ideal maximal. Si $E$ es un $k$-espacio vectorial y $A=\mathrm{End}(E)$ entonces $E$ es un $A$-módulo simple porque $A\cdot e = E$, para todo $e\in E$, no nulo.

**4. Proposición:** *Si $M = N+\sum_{i\in I}S_i$, siendo $S_i$ $A$-módulos simples, entonces existe un subconjunto $J\subseteq I$ de modo que $M = N\oplus\bigoplus_{j\in J}S_j$.*

*Demostración.* Sea $J\subseteq I$ un subconjunto maximal de $I$, que existe por el lema de Zorn, con la condición de que $\{N,S_j\}_{j\in J}$ estén en suma directa. Veamos que $M = N\oplus\bigoplus_{j\in J}S_j$: Dado $m\in S_i$ si $m\in M-(N\oplus\bigoplus_{j\in J}S_j)$, entonces $S_i$ está en suma directa con $\{N,S_j\}_{j\in J}$, porque $S_i\cap(N\oplus\bigoplus_{j\in J}S_j)=0$, pues $S_i$ es simple. Esto contradice la maximalidad de $J$, pues $\{N,S_j,S_i\}_{j\in J}$ están en suma directa. En conclusión, $m\in N\oplus\bigoplus_{j\in J}S_j$ y $S_i\subseteq N\oplus\bigoplus_{j\in J}S_j$, para todo $i$, luego $M = N\oplus\bigoplus_{j\in J}S_j$. □

**5. Corolario:** *Las siguientes condiciones son equivalentes:*

1. *$M$ es semisimple.*
2. *$M$ es suma de simples.*
3. *Todo submódulo de $M$ es un sumando directo en $M$.*

*Demostración.* La proposición anterior implica la equivalencia entre 1. y 2.

Veamos que 1. (o 2.) implica 3.: Sabemos que $M = \sum_{i\in I} S_i$, $S_i$ simples. Sea $N$ un submódulo de $M$. Obviamente $M = N + \sum_{i\in I} S_i$. Por la proposición anterior, $M = N \oplus \bigoplus_{j\in J} S_j$, luego $N$ es un sumando directo en $M$.

Veamos que 3. implica 1. En primer lugar veamos que todo que los submódulos $N$ de $M$ verifican la misma propiedad que $M$. Sea $N' \subseteq N$ un submódulo. $M = N' \oplus R'$, pues bien, $N = N' \oplus (R' \cap N)$. Veamos que existen submódulos simples en $M$. Sea $m \in M$ no nulo, y $M' \subset \langle m\rangle$ un submódulo propio maximal. Por la maximalidad de $M'$, los suplementarios de $M'$ en $\langle m\rangle$ son simples. Tenemos pues un submódulo $S$ simple en $M$. Sea $N$ un submódulo máximo de $M$, con la condición de ser suma directa de submódulos simples. Tenemos que $M = N \oplus R$. Sea $R' \subseteq R$ simple. $N \oplus R'$ es suma directa de simples, contradicción, salvo que $M = N$. □

**6. Corolario:** *Los submódulos y cocientes de un módulo semisimple son semisimples.*

**7. Lema de Schur:** *Si $M$ es un $A$-módulo simple entonces* $\operatorname{End}_A M$ *es un cuerpo no conmutativo, es decir, todo endomorfismo de $M$ no nulo es un isomorfismo. Si $M$ y $M'$ son $A$-módulos simples desisomorfos entonces* $\operatorname{Hom}_A(M, M') = 0$.

Supongamos $M = \bigoplus_{i\in I} S_i$, $S_i$ simples. Sea $S$ un submódulo simple de $M$. Como $0 \neq \operatorname{Hom}_A(S, \bigoplus_{i\in I} S_i) = \bigoplus_{i\in I} \operatorname{Hom}_A(S, S_i)$, por el lema de Schur $S$ ha de ser isomorfo a alguno de los $S_i$.

**8. Definición:** Diremos que un módulo es homogéneo si es suma directa de módulos simples isomorfos.

El "número" de sumandos simples en los que se expresa un módulo homogéneo no depende de la expresión concreta: Si $M = \bigoplus_J N$, $N$ simple, tenemos que $\operatorname{Hom}_A(N, M) = \bigoplus_J \operatorname{Hom}_A(N, N)$. Así, si denotamos $K = \operatorname{End}_A N$ entonces

$$\#J = \dim_K \operatorname{Hom}_A(N, M)$$

**9. Definición:** Diremos que un módulo homogéneo $M$ es de tipo $S$ si $M$ es suma de submódulos simples isomorfos a $S$.

**10. Teorema:** *Todo módulo semisimple es suma directa de modo único de submódulos homogéneos de tipo distinto.*

*Demostración.* Sea $I$ el conjunto de los submódulos simples del módulo semisimple $M$. Dado un elemento $i \in I$, denotémoslo $N_i$ cuando lo queremos pensar como submódulo de $M$. Diremos $i \sim i'$ si $N_i$ y $N_{i'}$ son $A$-módulos isomorfos. Sea $M_{[i]} = \sum_{i'\sim i} N_{i'}$, que es el máximo submódulo homogéneo de tipo $N_i$ de $M$. Se cumple que $M = \bigoplus_{[i]\in I/\sim} M_{[i]}$. Al lector, esto y el resto.

□

## 1.2 Anillos simples y semisimples

**1. Definición:** Se dice que un anillo $A$ es simple si es un $A$-módulo homogéneo.

Como el $1 \in A = \bigoplus_I S$ pertenece a la suma de un número finito de los submódulos simples $S$ y genera el $A$-módulo $A$, $I$ es un conjunto finito. Como todo módulo es cociente de un módulo libre, si $A$ es simple todo $A$-módulo es suma directa de módulos simples isomorfos, además todos los módulos simples son isomorfos.

**2. Teorema de Wedderburn:** *Sea $A$ un anillo simple, $S$ un $A$-módulo simple (único salvo isomorfismos) y $K = \mathrm{End}_A(S)$. La categoría de $A$-módulos finito generados es (anti)-equivalente a la categoría de $K$-espacios vectoriales de dimensión finita. Los funtores contravariantes que dan la equivalencia son $M \rightsquigarrow \mathrm{Hom}_A(M,S)$, $E \rightsquigarrow \mathrm{Hom}_K(E,S)$.*

*Demostración.* El morfismo canónico $M \to Hom_K(\mathrm{Hom}_A(M,S),S)$, $m \mapsto \tilde{m}$, $\tilde{m}(f) := f(m)$, es un isomorfismo, pues basta comprobarlo para $M = S$ y en este caso es fácil verlo.

El morfismo canónico $E \to \mathrm{Hom}_A(\mathrm{Hom}_K(E,S),S)$, $e \mapsto \tilde{e}$, $\tilde{e}(T) := T(e)$, es isomorfismo cómo es fácil ver cuando $E = K$.

En conclusión los dos funtores del teorema son inversos entre sí. □

Dado un anillo $A$ denotaremos por $A^o$ al anillo cuyos elementos son los de $A$, la suma es la de $A$ y el producto $*$ está definido por $a * b := b \cdot a$.

**3. Ejercicio:** Sea $A$ un anillo simple, $S$ un $A$-módulo simple (único salvo isomorfismos) y $K = \mathrm{End}_A(S)^o$. La categoría de $A$-módulos es equivalente a la categoría de $K$-espacios vectoriales. Los funtores covariantes que dan la equivalencia son $M \rightsquigarrow \mathrm{Hom}_A(S,M)$, $E \rightsquigarrow S \otimes_K E$.

**4. Teorema:** *$A$ es un anillo simple si y sólo si es isomorfo a un álgebra de matrices sobre un cuerpo no conmutativo.*

*Demostración.* Supongamos que $A$ es simple. Sea $I$ un $A$-módulo simple y escribamos $A = I^n$. Entonces

$$A = \mathrm{End}_A(A)^o = \mathrm{End}_A(I^n)^o = M_n(K)^o = M_n(K^o)$$

Otra demostración: Por el teorema de Wedderburn

$$A = \mathrm{Hom}_K(\mathrm{Hom}_A(A,I),I) = \mathrm{Hom}_K(I,I)$$

Explícitamente, el isomorfismo $A = \mathrm{Hom}_K(I,I)$, asigna a cada $a \in A$, la homotecia de razón $a$. Luego $A = \mathrm{Hom}_K(I,I) = M_n(K)^o = M_n(K^o)$.

Recíprocamente, $E$ un $K$-espacio vectorial de dimensión finita y $A = \mathrm{End}_K(E)$. Sea $\{e_1,\ldots,e_n\}$ una base de $E$. Consideremos el isomorfismo de $A$-módulos

$$\mathrm{End}_K(E) \to E \oplus \overset{n}{\ldots} \oplus E,\ T \mapsto (T(e_1),\ldots,T(e_n))$$

$E$ es un $A$-módulo simple, pues para todo $e \in E$ no nulo, $A \cdot e = E$. En conclusión, $A$ es simple. □

Llamaremos centro de $A$, que denotaremos $Z(A)$ al conjunto de los elementos de $A$ que conmutan con todos los elementos de $A$. Se cumple que $Z(A)$ es una subálgebra conmutativa de $A$.

Si $A = End_B(B^n)$, entonces $Z(A) = Z(B) \cdot \mathrm{Id}$: Dado $T \in Z(A)$, si $T(e_i) = e'$, de modo que $e' \notin \langle e_i \rangle$, sea $T'$ tal que $T'(e_i) = e_i$ y $T'(e') \neq e'$, entonces $(T' \circ T \circ T'^{-1})(e_i) \neq T(e_i)$ y llegamos a contradicción. Ahora ya, es fácil concluir.

**5. Corolario :** *Sea $k$ un cuerpo algebraicamente cerrado. $A$ es una $k$-álgebra finita simple, con $k \subseteq Z(A)$ entonces $A = M_n(k)$.*

*Demostración.* Sabemos que $A = M_n(K)$, con $K = \operatorname{End}_A I$, siendo $I$ un $A$-módulo simple. Tenemos que $k \hookrightarrow \operatorname{End}_A(I) = K$. Sólo hay que ver que si $K$ es una $k$-álgebra finita íntegra no conmutativa entonces $K = k$. Sea $a \in K$, entonces $k[a]$ es una $k$-álgebra finita conmutativa íntegra, luego $k[a] = k$ y $K = k$. □

**6. Proposición :** *Sea $K$ un cuerpo no conmutativo, $E$ un $K$ espacio vectorial de dimensión finita y $A = \operatorname{End}_K(E)$. Cada ideal de $A$ es el conjunto de endomorfismos de $E$ que se anulan en cierto subespacio vectorial de $E$.*

*Demostración.* $E$ es un $A$-módulo simple y tenemos el isomorfismo natural

$$A = \operatorname{Hom}_K(\operatorname{Hom}_A(A, E), E) = \operatorname{Hom}_K(E, E)$$

Dado un ideal $I \subset A$, tenemos $I = \operatorname{Hom}_K(\operatorname{Hom}_A(I, E), E)$, donde $\operatorname{Hom}_A(I, E) = E'$ es un cociente de $\operatorname{Hom}_A(A, E) = E$, luego $I$ son los endomorfismos de $E$ que factorizan a través de $E'$, es decir los que se anulan en el núcleo del epimorfismo $E \to E'$. □

**7. Definición :** Siempre que digamos ideal entenderemos ideal por la izquierda. Diremos que $I \subset A$ es un ideal bilátero si y sólo si $A \cdot I \cdot A = I$.

**8. Teorema :** *Un anillo es simple si y sólo si no contiene ideales biláteros propios y contiene algún ideal simple.*

*Demostración.* Supongamos que $A$ es simple. Sea $I$ un ideal simple. Sabemos que $A \simeq I \oplus \overset{n}{\ldots} \oplus I$. Entonces $I \cdot A \simeq I^2 \oplus \overset{n}{\ldots} \oplus I^2$. Tenemos $0 \subseteq I^2 \subseteq I$, luego $I^2$ o es cero o es $I$. Luego $I \cdot A$ o es 0 o $A$. Ahora bien, $I \subseteq I \cdot A$, luego $I \cdot A = A$. Todo ideal bilátero no nulo contiene a un ideal mínimo $I$, luego contiene a $I \cdot A = A$, luego es $A$.

Si $A$ no tiene ideales biláteros e $I$ es un ideal simple, entonces $A = I \cdot A$, luego es simple.

□

Observemos que si $A$ es una álgebra finita sobre un cuerpo no conmutativo entonces existen ideales simples.

**9. Definición :** Se dice que un anillo $A$ es semisimple si como $A$-módulo es un $A$-módulo semisimple.

De nuevo $A$ es suma directa de un número finito de módulos simples, $A = N_1^{n_1} \oplus \overset{r}{\ldots} \oplus N_r^{n_r}$, con $N_i \not\simeq N_j$, $i \neq j$. De nuevo, todo módulo es suma directa de los simples $N_i$, y todo módulo simple es isomorfo a alguno de estos $N_i$.

**10. Teorema :** *Un anillo es semisimple si y sólo si es producto de anillos de matrices sobre cuerpos no conmutativos.*

*Demostración.* Si $A$ es semisimple entonces $A = S_1^{n_1} \oplus \ldots \oplus S_r^{n_r}$, $S_i \not\simeq S_j$, $i \neq j$, simples. $A^0 = \operatorname{End}_A(A) = \operatorname{End}_A S_1^{n_1} \oplus \ldots \oplus \operatorname{End}_A S_r^{n_r}$.

□

**11. Definición :** Un anillo se dice que es artiniano si toda cadena descendente de ideales estabiliza. Un ideal $I \subseteq A$ se dice que es nilpotente si existe un $n > 0$ de modo que $I^n = 0$.

**12. Corolario :** *$A$ es semisimple si y sólo si es artiniano sin ideales nilpotentes.*

*Demostración.* Si $A$ es semisimple entonces es $A = M_{n_1}(K_1) \times \ldots \times M_{n_r}(K_r)$. Todo ideal $I \subseteq A$ es $I = I_1 \times \ldots \times I_r$. Las álgebras $M_{n_i}(K_i)$ son artinianas. Los ideales mínimos son idempotentes, $I \cdot I = I \cdot A \cdot I = A \cdot I = I$, luego no hay ideales nilpotentes. Se concluye.

Supongamos que $A$ es artiniano sin ideales nilpotentes. Sea $I$ un ideal mínimo de $A$, que existe por ser $A$ artiniano. Se cumple que $I^2 = I$, porque $0 \neq I^2 \subseteq I$. Existe un $a \in I$ de modo que $I \cdot a = I$. En particular, existe $b \in I$ tal que $b \cdot a = a$, luego $b^2 \cdot a = b \cdot a$. Como multiplicar por $a$ es un isomorfismo en $I$, $b^2 = b$. Así pues, $A = A \cdot b \oplus A(1-b) = I \oplus I'$. Consideremos un ideal mínimo $J$ incluido en $I'$, sea $c \in J$ tal que $c^2 = c$ (y $J = Ac = Jc$). Tenemos que $A = Ac \oplus A(1-c)$, por tanto, $I' = I'c \oplus I'(1-c) = J \oplus J'$. En conclusión, $A = I \oplus J \oplus J'$. Por recurrencia y artiniedad obtendremos que $A = I_1 \oplus \ldots \oplus I_n$, $I_i$ simples. En conclusión, $A$ es semisimple.

□

## 1.3 Automorfismos de un anillo simple

Sea $K$ un cuerpo no conmutativo y $E, E'$ dos $K$-espacio vectoriales.

**1. Definición :** Se dice que una aplicación $f\colon E \to E'$ es semilineal cuando existe un automorfismo $\sigma$ de $K$ de modo que

$$f(e+e') = f(e) + f(e')$$
$$f(\lambda e) = \sigma(\lambda) f(e)$$

para todo $e, e' \in E$ y $\lambda \in K$.

**2. Proposición :** *Supongamos que* $\dim_K E \geq 2$. *Una biyección* $f\colon E \to E$ *es semilineal si aplica biyectivamente rectas en rectas y* $f(e+e') = f(e) + f(e')$, *para todo* $e, e' \in E$.

*Demostración.* Dado $e \in E$, tenemos que $f(\lambda \cdot e) = \sigma_e(\lambda) f(e)$, para cierta aplicación $\sigma_e\colon K \to K$. Veamos que $\sigma e'(\lambda) = \sigma_e(\lambda)$: Supongamos que $e$ y $e'$ son linealmente independientes. Se tiene que $f(e)$ y $f(e')$ son linealmente independientes. Pues si hubiese una relación entre ellos, $f^{-1}$ de esta relación es una relación lineal de $e$ y $e'$. Ahora tenemos

$$\sigma_{e+e'}(\lambda)(e+e') = f(\lambda(e+e') = f(\lambda e + \lambda e') = \sigma_e(\lambda) f(e) + \sigma_{e'}(\lambda) f(e')$$

Por tanto, $\sigma_e(\lambda) = \sigma_{e+e'}(\lambda) = \sigma_{e'}(\lambda)$. De igual modo $\sigma_{\mu e}(\lambda) = \sigma_{e'}(\lambda) = \sigma_e(\lambda)$.

Escribamos, pues, $\sigma_e = \sigma$. Dejamos al lector que pruebe que $\sigma$ es un automorfismo de cuerpos.

□

El conjunto de los automorfismos semilineales de un $K$-espacio vectorial $E$ forman un grupo con la composición, que denotaremos $Sem_K(E)$. Cada automorfismo semilineal $f\colon E \to E$ induce un automorfismo de álgebra en $\mathrm{End}_K(E)$, a saber, la conjugación por $f$, es decir, $\tau_f(g) = f \circ g \circ f^{-1}$. Se cumple que $\tau_f = \mathrm{Id}$ si y sólo si $f$ es una homotecia por elementos de $Z(K^*)$ (arguméntese como en la demostración de que $Z(\mathrm{End}_B(B^n)) = Z(B) \cdot \mathrm{Id}$). Así pues, el núcleo del morfismo

$$Sem_K(E) \to \mathrm{Aut}(\mathrm{End}_K(E)),\ f \mapsto \tau_f$$

es $Z(K^*)$. El grupo $Sem_K(E)/Z(K^*)$ es el denominado grupo de Staudt, y el teorema fundamental de la Geometría Proyectiva afirma que coincide con el grupo de las colineaciones del espacio proyectivo $\mathbb{P}_K(E)$. Se trata ahora de probar que todo automorfismo de $\mathrm{End}_K(E)$ es el inducido por una transformación semilineal.

**3. Teorema de Skolem-Noether:** *Sean $K$ un cuerpo no conmutativo, $E$ un $K$-espacio vectorial de dimensión finita y $A = \mathrm{End}_K(E)$. La sucesión,*

$$1 \to Z(K^*) \to Sem_K(E) \to \mathrm{Aut}(A) \to 1$$

*es exacta.*

*Demostración.* Sea $\tau$ un automorfismo de anillos de $A = \mathrm{End}_K(E)$. Éste induce en $E$ otra estructura de $A$-módulo: $a*e = \tau(a)\cdot e$, para cada $a \in A$ y $e \in E$. Por ser $A$ un anillo simple todos los $A$-módulos simples son isomorfos, luego existe una biyección aditiva $f\colon E \to E$ de modo que $f(a*e) = a \cdot f(e)$. Es decir, se cumple la fórmula $f(\tau(a)\cdot e) = a \cdot f(e)$. La conjugación por $f$ en $A$ es $\tau$, luego hemos concluido si comprobamos que $f$ es semilineal.

Si $I \subset A$ es el ideal de todos los endomorfismos de $E$ que se anulan en un subespacio $E'$, entonces $f \cdot I \cdot f^{-1}$ es el ideal de endomorfismos de $E$ que se anulan en $f(E')$, luego $f(E')$ es un subespacio vectorial de $E$. Si $I$ es maximal, $E'$ tiene dimensión 1, y $f \cdot I \cdot f^{-1}$ es maximal. Por tanto, $f(E')$ es de dimensión 1. En conclusión, $f$ aplica rectas en rectas y es semilineal.

□

**4. Corolario:** *Consideremos la inclusión de $K$-álgebras $K \hookrightarrow M_n(K), \lambda \mapsto \lambda\,\mathrm{Id}$. La sucesión*

$$1 \to Z(K^*) \to M_n(K) \xrightarrow{\tau} \mathrm{Aut}_{K-alg}(M_n(K)) \to 1$$

*es exacta, con $n > 1$ y $\tau$ asigna a cada matriz el automorfismo conjugar por ella. En particular, si $K$ es conmutativo,* $\mathrm{Aut}_K(M_n(K)) = \mathrm{PGl}_K(n)$.

*Demostración.* Sabemos que la sucesión

$$1 \to Z(K^*) \to Sem_K(K^n) \to \mathrm{Aut}(M_n(K)) \to 1$$

es exacta. Basta ver que dada una aplicación semilineal $f$, tal que $f(\lambda e) = \sigma(\lambda)f(e)$, entonces la conjugación por $f$ en $M_n(K)$ al restringirse a $K$ es el automorfismo $\sigma$. Es decir, $f \circ \lambda\,\mathrm{Id} = \sigma(\lambda)\,\mathrm{Id} \circ f$, lo cual es obvio.

□

## 1.4 Álgebras de Azumaya

Sea $k$ un cuerpo conmutativo. Siempre que digamos $k$-álgebra entendemos que $k$ está incluida en el centro de dicha álgebra.

Las $k$-álgebras simples no son necesariamente simples por cambio de base. En esta sección vamos a estudiar las álgebras simples para todo cambio de base.

**1. Definición:** Diremos que una $k$-álgebra finita $A$ es de Azumaya si es simple y $Z(A) = k$ (es decir, es central).

$M_n(k)$ es una $k$-álgebra de Azumaya. Dada un $k$-álgebra finita simple $A$, si $Z(A)$ es un cuerpo entonces $A$ es una $Z(A)$-álgebra de Azumaya. Si $K$ es una $k$-extensión finita de cuerpos no conmutativa ($k \subseteq Z(K)$) entonces $K$ es una $Z(K)$-álgebra de Azumaya.

Toda $k$-álgebra $A$ es de modo natural un $A \otimes_k A^o$-módulo: $(a \otimes b) * c = acb$, o equivalentemente, tenemos el morfismo de $k$-álgebras

$$A \otimes_k A^o \xrightarrow{f_A} \mathrm{End}_k(A),\ f_A(a \otimes b)(c) = acb$$

**2. Teorema de caracterización:** *La condición necesaria y suficiente para que una $k$-álgebra finita $A$ sea de Azumaya es que el morfismo $f_A$ sea isomorfismo.*

*Demostración.* Observemos que los ideales biláteros de $A$ son precisamente los $A \otimes_k A^o$-submódulos de $A$ y que $Z(A) = \mathrm{End}_{A\otimes_k A^o}(A) \subseteq \mathrm{End}_A(A) = A^o$.

Veamos la suficiencia. $A$ es simple cuando lo es como $A \otimes A^o$-módulo. Como $A \otimes_k A^o = \mathrm{End}_k(A)$ y $A$ es un $\mathrm{End}_k(A)$-módulo simple, concluimos, que $A$ es un anillo simple. Además, $Z(A) = \mathrm{End}_{A\otimes_k A^o}(A) = \mathrm{End}_{\mathrm{End}_k(A)}(A) = Z(\mathrm{End}_k(A)) = k$.

Veamos la necesidad. Sea $B = \mathrm{Im}\, f_A$, entonces $A$ es un $B$-módulo simple, pues $A$ no tiene ideales biláteros, y de la inclusión $B \hookrightarrow \mathrm{End}_k(A) = A \oplus \cdots \oplus A$, se deduce que $B$ es simple. Por tanto, por el teorema de Wedderburn, $B = \mathrm{End}_D A$, donde $D = \mathrm{End}_B(A) = \mathrm{End}_{A\otimes_k A^o}(A) = Z(A) = k$. Luego $f_A$ es epiyectivo y por dimensiones es un isomorfismo. □

**3. Corolario:** *Sea $k \hookrightarrow K$ una extensión de cuerpos (conmutativos): $A$ es una $k$-álgebra de Azumaya si y sólo si $A_K = A \otimes_k K$ es una $K$-álgebra de Azumaya.*

**4. Corolario:** *$A$ y $B$ son $k$-álgebras de Azumaya si y sólo si $A \otimes_k B$ es una $k$-álgebra de Azumaya.*

*Demostración.* $f_A \otimes_k f_B = f_{A\otimes_k B}$. □

**5. Corolario:** *La condición necesaria y suficiente para que una $k$-álgebra $A$ sea de Azumaya es que $A \otimes_k \bar{k} = M_n(\bar{k})$, siendo $\bar{k}$ el cierre algebraico de $k$.*

**6. Corolario:** *La dimensión de una $k$-álgebra de Azumaya es un cuadrado perfecto.*

**7. Proposición:** *Una $k$-álgebra de Azumaya $A$, de grado $n^2$ es de matrices si y sólo si contiene una $k$-subálgebra trivial $K = k \times \overset{n}{\ldots} \times k$ de grado $n$.*

*Demostración.* Si $A = M_n(k)$ entonces contiene la $k$-subálgebra trivial formada por las matrices diagonales

$$\begin{pmatrix} \lambda_1 & 0 & \ldots & 0 \\ 0 & \lambda_2 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & \lambda_n \end{pmatrix}$$

Recíprocamente, supongamos que $A$ contiene una $k$-subálgebra trivial $K = k \times \overset{n}{\ldots} \times k$. Tenemos que $A = A \otimes_K K = A \otimes_K (k \times \overset{n}{\ldots} \times k) = I_1 \times \ldots \times I_n$, donde algún ideal $I_i$ ha de ser de dimensión menor o igual que $n$. El morfismo $A \to \mathrm{End}_k(I_i)$ es un isomorfismo, porque el núcleo es un ideal bilátero y por dimensiones.

□

**8. Proposición:** *Toda $k$-álgebra de Azumaya $A$ de dimensión $n^2$ contiene una $k$-subálgebra conmutativa separable de dimensión $n$.*

*Demostración.* Para cada $a \in A$ consideremos la subálgebra que genera, $k[a]$, que es una $k$-subálgebra conmutativa separable de dimensión $n$ precisamente cuando el polinomio anulador de $a$ sea un polinomio separable de grado $n$. Recordemos que $A \otimes_k \bar{k} = M_n(\bar{k})$. El polinomio anulador de $a$ es el mismo que el de $a \otimes 1$. El discriminante del polinomio característico de $a \otimes 1$ es una función polinómica sobre el $k$-espacio vectorial $A$, y este polinomio no es nulo porque no es nulo en $A \otimes_k \bar{k} = M_n(\bar{k})$. Si $k$ tiene infinitos elementos, podemos concluir que este polinomio no se anula en algún elemento $a \in A$, de modo que el polinomio característico de $a$ no tiene raíces dobles y coincide con el anulador.

Si $k$ tiene un número finito de elementos, procedamos como sigue. $A = M_r(K)$, donde $K$ es un cuerpo no conmutativo y $k = Z(M_r(K)) = Z(K)$. Es decir, $K$ es un álgebra de Azumaya. Fácilmente reducimos la proposición al caso $A = K$. Sea ahora, $K_1$ una $k$-subálgebra conmutativa de dimensión máxima de $K$. Denotemos $C_{K_1}(K) = \{a \in K \colon a \cdot b = b \cdot a \text{ para todo } b \in K_1\}$. Por ser máxima, se cumple que $C_{K_1}(K) = K_1$. Veamos que esto implica que $\dim_k K_1 = n$ (donde $\dim_k K = n^2$). Si $b_1, \cdots, b_s$ es una $k$-base de $K_1$, $C_{K_1}(K)$ es el núcleo del morfismo $K \to K \oplus \overset{s}{\ldots} \oplus K$, $a \mapsto (ab_1 - b_1a, \ldots, ab_s - b_sa)$. Ahora es sencillo probar que $C_{K_1}(K) \otimes_k \bar{k} = C_{K_1 \otimes_k \bar{k}}(K \otimes_k \bar{k})$. Por ser $k$ finito, toda extensión finita es separable, luego $K_1 \otimes_k \bar{k} = \bar{k} \times \overset{m}{\ldots} \times \bar{k}$. En conclusión, vamos a suponer que $k$ es algebraicamente cerrado, $K_1 = k \times \overset{m}{\ldots} \times k$ y $K = M_n(k) = \mathrm{End}_k(E)$. Entonces, $E = E \otimes_{K_1} K_1 = E_1 \oplus \ldots \oplus E_m$ y $K_1$ opera sobre cada $E_i$ por homotecias por elementos de $k$. Ahora es fácil comprobar, que si $C_{K_1}(K) = K_1$, entonces $\dim_k E_i = 1$ y $m = n$.

□

**9. Teorema :** *Si $A$ es una álgebra de Azumaya, existe una extensión finita de Galois $k \hookrightarrow K$, de modo que $A_K = M_n(K)$.*

*Demostración.* Sea $K_1 \subset A$ una $k$-subálgebra conmutativa de dimensión $n$ y $K$ la envolvente de Galois de $K_1$. $A \otimes_k K$ es una $K$-álgebra de Azumaya de grado $n^2$, que contiene una $K$-álgebra trivial, $K_1 \otimes_k K = K \times \overset{n}{\ldots} \times K$, luego por la proposición 1.4.8, $A_K = M_n(K)$.

□

**10. Definición :** Si $A \otimes_k K = M_n(K)$ diremos que $K$ neutraliza a $A$.

Sea $k \hookrightarrow K$ una extensión de Galois de grupo de Galois $G$. Ahora vamos a exponer un método para construir las $k$-álgebras de Azumaya $A$ tales que $A_K = M_n(K)$.

**11. Definición :** Sea $E$ un $K$-espacio vectorial. Dar una operación de $G$ en $E$ es dar un morfismo de grupos $\rho \colon G \to \mathrm{Aut}_k(E)$, de modo que $\rho(g)(\lambda e) = g(\lambda)\rho(g)(e)$.

Diremos que dos operaciones $\rho, \rho'$ de $G$ en sendos espacios vectoriales son equivalentes si existe un isomorfismo $K$-lineal, $T$, de modo que $T(\rho(g))(e) = \rho'(g)(T(e))$. Cuando no cause confusión, escribiremos $\rho(g)(e) = ge$.

Si los morfismos $k$-lineales y $K$-lineales se sustituyen por morfismos de $k$-álgebras y $K$-álgebras, se obtiene la definición de operación de $G$ en una $K$-álgebra y de equivalencia de tales operaciones.

Sea $K[G] = \bigoplus_{g \in G} K \cdot g$, donde el producto está definido por la linealización de los productos $(\lambda \cdot g) \cdot (\lambda' \cdot g') = \lambda g(\lambda') \cdot gg'$. Cada operación $\rho$ de $G$ en un $K$-espacio vectorial $E$, define en $E$ una estructura de $K[G]$-módulo

$$(\sum_i \lambda_i \cdot g_i)e = \sum_i \lambda_i \rho(g_i)(e)$$

Recíprocamente, cada estructura de $K[G]$-módulo en $E$ define una operación de $G$ en $E$

$$\rho(g)(e) = ge$$

**12. Lema :** *$K[G] = \mathrm{End}_k(K)$ y, por tanto, es una $k$-álgebra simple.*

*Demostración.* La operación natural de $G$ en $K$ define un morfismo de $K$-álgebras $K[G] \to \mathrm{End}_k(K)$. Este morfismo es inyectivo, porque los elementos de $G = \mathrm{Aut}_{k-\text{álg}}(K) = \mathrm{Hom}_{K-\text{álg}}(K \otimes_k K, K) = \mathrm{Hom}_{K-\text{álg}}(\prod^G K, K)$ son $K$-linealmente independientes. Como ambos espacios vectoriales tienen la misma dimensión, el morfismo es un isomorfismo. □

**13. Corolario:** *Si $G$ opera en un $K$-espacio vectorial $E$, el morfismo natural $E^G \otimes_k K \to E$ es un isomorfismo.*

*Demostración.* $K$ es un $K[G]$-módulo simple, luego $E$ es como $K[G]$-módulo suma directa de unas cuantas $K$. El corolario se reduce al caso $E = K$, que es trivial, por el teorema de Artin.

□

**14. Teorema:** *El conjunto de las $k$-álgebras de Azumaya de grado $n^2$ neutralizadas por $K$, módulo isomorfismos, es biyectivo con el conjunto de las operaciones de $G$ en la $K$-álgebra $M_n(K)$, módulo automorfismos internos.*

*Demostración.* Si $A$ es una $k$-álgebra de Azumaya de grado $n^2$, neutralizada por $K$, entonces $A \otimes_k K \simeq M_n(K)$ y la operación natural de $G$ en $A \otimes_k K$ induce una operación de $G$ en $M_n(K)$, unívocamente definida salvo automorfismo internos de $M_n(K)$.

Recíprocamente, dada una operación de $G$ en $M_n(K)$, entonces $M_n(K)^G$ es una $k$-álgebra de Azumaya de grado $n^2$ neutralizada por $K$, porque $M_n(K)^G \otimes_k K = M_n(K)$, por el corolario anterior.

Estas asignaciones son inversas entre sí.

□

**15. Ejemplo:** Construyamos todos las extensiones finitas de cuerpos no conmutativos de $\mathbb{R}$: Sea $K$ una tal extensión. $K$ es un álgebra simple, luego es una $Z(K)$-álgebra de Azumaya. $Z(K)$ es una extensión de cuerpos conmutativos finita de $\mathbb{R}$, luego es $\mathbb{R}$ o $\mathbb{C}$.

Si $Z(K) = \mathbb{C}$, entonces una $\mathbb{C}$-subálgebra conmutativa (que será cuerpo) máxima de $K$ sólo puede ser $\mathbb{C}$, luego por dimensiones $K = \mathbb{C}$.

Si $Z(K) = \mathbb{R}$, entonces una $\mathbb{R}$-subálgebra conmutativa (que será cuerpo) maximal de $K$, sólo puede ser $\mathbb{R}$ o $\mathbb{C}$. Si es $\mathbb{R}$, por dimensiones $K = \mathbb{R}$. Si es $\mathbb{C}$, entonces por dimensiones $K \otimes_{\mathbb{R}} \mathbb{C} = M_2(\mathbb{C})$.

Calculemos, pues, las $\mathbb{R}$-álgebras de Azumaya de grado 4 neutralizadas por $\mathbb{C}$. Por el teorema, equivale a definir un morfismo de grupos, salvo automorfismos internos de $M_2(\mathbb{C})$, $\phi\colon \mathbb{Z}/2\mathbb{Z} = \langle\sigma\rangle \to \mathrm{Aut}_{\mathbb{R}-\mathrm{álg}}(M_2(\mathbb{C}))$, de modo que $\phi(\sigma)(\lambda A) = \sigma(\lambda)\phi(\sigma)(A)$. Observemos que $\phi$ queda determinado por $\phi(\sigma)$, que ha de cumplir que $\phi(\sigma)^2 = \mathrm{Id}$ y $\phi(\sigma)(\lambda A) = \sigma(\lambda)\phi(\sigma)(A)$. Por el teorema de Skolem-Noether, salvo un factor multiplicativo, $\phi(\sigma)$ es conjugar por una aplicación semilineal $\tau\colon \mathbb{C}^2 \to \mathbb{C}^2$, de modo que $\tau^2 = \mu$ y $\tau(\lambda e) = \sigma(\lambda)\tau(e)$. Observemos que $\mu\tau = \tau^3 = \tau\mu = \sigma(\mu)\tau$, luego $\mu \in \mathbb{R}$. Dar $\tau$, equivale a dotar a $\mathbb{C}^2$, de estructura de $\mathbb{C}_\mu[\mathbb{Z}/2\mathbb{Z}]$-módulo, donde $\mathbb{C}_\mu[\mathbb{Z}/2\mathbb{Z}] = \mathbb{C} \oplus \mathbb{C}\sigma$, con $\sigma^2 = \mu$ y $\sigma \cdot \lambda = \sigma(\lambda)\sigma$. Ahora bien, $\mathbb{C}_\mu[\mathbb{Z}/2\mathbb{Z}]$ es una $\mathbb{R}$-álgebra de Azumaya, porque $\mathbb{C}_\mu[\mathbb{Z}/2\mathbb{Z}] \otimes_{\mathbb{R}} \mathbb{C} = \mathbb{C}[\mathbb{Z}/2\mathbb{Z}] \otimes_{\mathbb{R}} \mathbb{C}$, $\sigma \otimes 1 \mapsto \sigma \otimes \sqrt[2]{\mu}$. Por tanto, $\mathbb{C}^2$ tiene una única estructura de $\mathbb{C}_\mu[\mathbb{Z}/2\mathbb{Z}]$-módulo. Si en vez de $\tau$ consideramos $\lambda\tau$, entonces $(\lambda\tau)^2 = N(\lambda)\mu$, como $\mathbb{C}/N(\mathbb{C}) = \pm 1$, podemos suponer que $\tau^2 = \pm 1$. En conclusión, sólo pueden existir, dos $\mathbb{R}$-álgebras de Azumaya de dimensión 4. Explícitamente, $\mathbb{C}[\mathbb{Z}/2\mathbb{Z}] = \mathrm{End}_{\mathbb{R}}(\mathbb{C}) = M_2(\mathbb{R})$ y $\mathbb{C}_{-1}[\mathbb{Z}/2\mathbb{Z}] = \mathbb{C} \oplus \mathbb{C}\sigma = \mathbb{R} \oplus \mathbb{R}i \oplus \mathbb{R}j \oplus \mathbb{R}k$, donde $j = \sigma$ y $k = i\sigma$, que cumplen $i^2 = j^2 = k^2 = -1$, $ij = k$ y $ij = -ji$. A $\mathbb{C}_{-1}[\mathbb{Z}/2\mathbb{Z}]$ se le denomina el álgebra de los cuaterniones de Hamilton, que es un cuerpo no conmutativo. Como $\mathbb{R}$-subálgebra de $M_2(\mathbb{C})$ tenemos que una base de $\mathbb{C}_{-1}[\mathbb{Z}/2ZZ]$ es

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad i = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad j = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \quad k = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

Recordemos que si $A = M_n(K)$, siendo $K$ un cuerpo no conmutativo entonces $K = \mathrm{End}_A(I)$, siendo $I$ un $A$-módulo simple. Luego, $K$ está determinado, salvo isomorfismos, por $A$.

**16. Definición:** Diremos que dos $k$-álgebras de Azumaya son equivalentes si son álgebras de matrices sobre cuerpos no conmutativos isomorfos. Denotaremos por $\mathrm{Br}(K/k)$ al conjunto de las clases de equivalencia de las $k$-álgebras de Azumaya neutralizadas por $K$, que se identifica con el conjunto de las clases de isomorfía de los cuerpos no conmutativos neutralizados por $K$. El producto tensorial en $Br(K/k)$, $[A]\otimes_k[B]=[A\otimes_k B]$, dota a $\mathrm{Br}(K/k)$ de estructura de grupo, denominado grupo de Brauer (de las $k$-álgebras de Azumaya neutralizadas por $K$). El inverso de $[A]$ es $[A^o]$.

**17. Teorema:** *Sea $k\hookrightarrow K$ una extensión de Galois de grupo $\mathbb{Z}/n\mathbb{Z}$. Existe una identificación natural $\mathrm{Br}(K/k)=k^*/N(K^*)$, donde $N\colon K\to k$ es la norma.*

*Demostración.* Escribamos $\mathbb{Z}/n\mathbb{Z}=\langle\sigma\rangle$. Dado $\mu\in k^*$ denotaremos $K_\mu[\mathbb{Z}/n\mathbb{Z}]=K\oplus K\sigma\oplus\cdots K\sigma^{n-1}$, la $k$-álgebra obvia tal que $\sigma\cdot\mu=\sigma(\mu)\sigma$ y $\sigma^n=\mu$. Se cumple que $K_\mu[\mathbb{Z}/n\mathbb{Z}]$ es una $k$-álgebra de Azumaya, porque el morfismo $K_\mu[\mathbb{Z}/n\mathbb{Z}]\otimes_k k[\sqrt[n]{\mu}]\to K[\mathbb{Z}/n\mathbb{Z}]\otimes_k k[\sqrt[n]{\mu}]$, $\sigma\otimes_k 1\mapsto\sigma\otimes\sqrt[n]{\mu}$ es un isomorfismo de $k[\sqrt[n]{\mu}]$-álgebras y $K[\mathbb{Z}/n\mathbb{Z}]$ es una $k$-álgebra de Azumaya.

Vamos a probar que

$$\mathrm{Br}(K/k)=\{K_\mu[\mathbb{Z}/n\mathbb{Z}]\}_{[\mu]\in k^*/N(K^*)}$$

Las $k$-álgebras de Azumaya $A$ neutralizadas por $K$, salvo isomorfismos, se corresponden con los morfismos de grupos, $\phi\colon\mathbb{Z}/n\mathbb{Z}\to\mathrm{Aut}_{k-\mathrm{àlg}}(M_r(K))$, salvo automorfismos internos de $M_r(K)$, de modo que $\phi(\sigma)(\lambda b)=\sigma(\lambda)\phi(\sigma)(b)$. El morfismo $\phi$ está determinado por $\phi(\sigma)$ que habrá de cumplir $\phi(\sigma)^n=\mathrm{Id}$ y $\phi(\sigma)(\lambda b)=\sigma(\lambda)\phi(\sigma)(b)$. Por el teorema de Skolem-Noether, $\phi(\sigma)$ es conjugar por una aplicación semilineal, $\tau$, de $K^r$, única salvo un factor $\lambda\in K^*$, que habrá de verificar que $\tau^n=\mu$ y $\tau(\lambda e)=\sigma(\lambda)\tau(e)$. Observemos que $\mu\cdot\tau=\tau^{n+1}=\tau\mu=\sigma(\mu)\tau$, luego $\mu\in k^*$. Dar $\tau$ equivale a dotar a $K^r$ de estructura de $K_\mu[\mathbb{Z}/n\mathbb{Z}]$-módulo. Ahora bien, $K_\mu[\mathbb{Z}/n\mathbb{Z}]$ es un anillo simple, luego $K^r$ tiene una única de estructura de $K_\mu[\mathbb{Z}/n\mathbb{Z}]$-módulo, salvo isomorfismos. Además, si consideramos $\lambda\tau$ en vez de $\tau$, tenemos que $(\lambda\tau)^n=N(\lambda)\mu$. Asignemos a cada $A$ el elemento $[\mu]\in k^*/N(K^*)$, que denotaremos $\mathrm{inv}(A)$. Si $A=M_s(k)\otimes_k B$, es fácil comprobar que $\mathrm{inv}(A)=\mathrm{inv}(B)$. En conclusión, tenemos una inclusión

$$\mathrm{Br}(K/k)\hookrightarrow k^*/N(K^*),\quad [A]\mapsto\mathrm{inv}(A)$$

Para la epiyección, sólo nos falta comprobar que $\mathrm{inv}(K_\mu[\mathbb{Z}/n\mathbb{Z}])=\mu$: Consideremos la aplicación semilineal $\tau\colon K^n\to K^n$, $\tau(\lambda_1,\ldots,\lambda_n)=(\mu\sigma(\lambda_n),\sigma(\lambda_1),\ldots,\sigma(\lambda_{n-1}))$ (es decir, $\tau$ es la aplicación semilineal de automorfismo $\sigma$, tal que $\tau^n=\mu$ y existe un vector $e$ tal que $e$, $\{e,\tau(e),\ldots,\tau^{n-1}(e)\}$ es una base, sobre la que hemos escrito la matriz de $\tau$). Se cumple que $\tau^n=\mu\,\mathrm{Id}$. Sea $F\colon M_n(K)\to M_n(K)$ la conjugación por $\tau$. Se cumple que $F^n=\mathrm{Id}$ y $\langle F\rangle=\mathbb{Z}/n\mathbb{Z}$. Consideremos el morfismo inyectivo $K_\mu[\mathbb{Z}/n\mathbb{Z}]\hookrightarrow M_n(K)$, $\sigma$ en $M_n(K)$, es la aplicación $\sigma(\lambda_1,\ldots,\lambda_n)=(\mu\lambda_n,\lambda_1,\ldots,\lambda_{n-1})$. Se cumple que $M_n(K)^{\mathbb{Z}/n\mathbb{Z}}=K_\mu[\mathbb{Z}/n\mathbb{Z}]$. Por tanto, $\mathrm{inv}(K_\mu[\mathbb{Z}/n\mathbb{Z}])=\mu$.

□

Si $k$ es un cuerpo finito, toda extensión finita de Galois $k\hookrightarrow K$ es cíclica, así que el Teorema 90 de Hilbert afirma la exactitud de la siguiente sucesión de morfismos de grupos

$$1\to k^*\to K^*\xrightarrow{f}K^*\xrightarrow{N}k^*$$

donde $f(\lambda)=\frac{\lambda}{\sigma(\lambda)}$ y $\sigma$ es un generador del grupo de Galois. Por órdenes, se obtiene que la norma $N$ es epiyectiva. Es decir, $k^*/N(K^*)=1$ y podemos concluir que toda $k$-álgebra de Azumaya es un álgebra de matrices sobre $k$. En particular, toda cuerpo no conmutativo con un número finito de elementos es conmutativo (Teorema de Wedderburn).

## 1.5 Álgebras finitas

Sea $A$ una $k$-álgebra finita (no necesariamente conmutativa). Sean $\{E_i\}$ el conjunto de todos los módulos simples desisomorfos de $A$. Consideremos el morfismo $A \to \prod_i \mathrm{End}_k(E_i)$ y sea $\bar{A}$ la imagen del morfismo. $\bar{A}$ es una $k$-álgebra finita luego se inyecta en un producto directo finito $\bar{A} \hookrightarrow \mathrm{End}_k(E_1) \times \overset{n}{\cdots} \times \mathrm{End}_k(E_n)$. Ahora bien, $E_1, \ldots, E_n$ son $\bar{A}$-módulos simples y $\mathrm{End}_k(E_i) = \oplus E_i$, luego $\bar{A}$ es semisimple. Por tanto, $\bar{A} = \mathrm{End}_{K_1}(E_1) \times \cdots \times \mathrm{End}_{K_n}(E_n)$ y los $\bar{A}$-módulos simples son $E_1, \ldots, E_n$, que son todos los $A$-módulos simples.

**1. Definición:** Se denomina radical de $A$ al núcleo del morfismo $A \to \bar{A}$.

Sea $E$ un $A$-módulo finito generado. Sea $E_1$ el $A$-submódulo semisimple maximal de $E$. Observemos que $E_1 = 0$ si y sólo si $E = 0$. Sea $E_2 \subset E$, que contenga a $E_1$ y $E_2/E_1$ sea el $A$-submódulo semisimple maximal de $E/E_1$. Así sucesivamente, terminamos obteniendo una cadena

$$0 \subset E_1 \subset E_2 \subset E_n \subset E$$

Tenemos que $E_i/E_{i_1}$ son $A$-módulo semisimple, luego $\bar{A}$-módulos, luego $R \cdot E_i \subseteq E_{i-1}$. En particular, $R \cdot E \subset E_n$.

**2. Proposición:** *Sea $E$ un $A$-módulo finito generado y $R$ el radical de $A$. Se cumple que $R \cdot E = E$ si y sólo si $E = 0$.*

**3. Corolario:** *Existe $n$ tal que $R^n = 0$.*

*Demostración.* Existe $n$ tal que $R^n = R^{n+1}$, luego $R^n = 0$. □

Se dice que una $k$-álgebra es reducida si no existen ideales biláteros nilpotentes.

**4. Proposición:** *Una $k$-álgebra finita es semisimple si y sólo si es reducida.*

*Demostración.* Si es reducida entonces el radical es nulo y el álgebra es semisimple. Si es semisimple es producto de simples, que son reducidas (pues no contienen ideales biláteros propios), luego el álgebra es reducida. □

**5. Definición:** Diremos que una $k$-álgebra finita $A$ es separable si es universalmente reducida, es decir, $A \otimes_k K$ es reducida para toda extensión de cuerpos $k \hookrightarrow K$.

**6. Teorema:** *Sea $A$ una $k$-álgebra finita. Las siguientes condiciones son equivalentes,*

1. *$A$ es separable.*
2. *$A$ es universalmente semisimple.*
3. *$A \otimes_k \bar{k}$ es producto directo de álgebras de matrices, donde $\bar{k}$ es un cuerpo algebraicamente cerrado.*
4. *$A$ es semisimple y su centro es un álgebra conmutativa separable.*
5. *$A \otimes_k A^o$ es semisimple (o reducida).*

*Demostración.* Las tres primeras son obviamente equivalentes.

1.,3. $\Rightarrow$) 4. $Z(A) \otimes_k \bar{k} = Z(A \otimes_k \bar{k}) = \prod \bar{k}$ luego $Z(A)$ es separable. Obviamente $A$ es semisimple.

4. $\Rightarrow$) 3. $A$ es producto directo de álgebras simples. Como el centro de un producto directo es el producto directo de los centros, podemos reducirnos al caso de que $A$ sea simple. En este caso $Z(A)$

es un cuerpo, pues $A = \mathrm{End}_K(E)$ y $Z(A) = Z(K)$. Por tanto, $A$ es una $Z(A)$-álgebra de Azumaya y $A \otimes_k \bar{k} = A \otimes_{Z(A)} Z(A) \otimes_k \bar{k} = A \otimes_{Z(A)} \prod \bar{k}$ que es producto directo de álgebras de matrices.

3. $\Rightarrow$) 5. Basta ver que por cambio de base al cierre algebraico de $k$, $A \otimes_k A^o$ es reducida. Ahora bien, el producto tensorial de álgebras de matrices es un álgebra de matrices., que son reducidas.

5. $\Rightarrow$) 4. Por ser $Z(A \otimes A^o) = Z(A) \otimes Z(A)$ y ser $A \otimes A^o$ reducida se concluye que $Z(A) \otimes Z(A)$ es un álgebra conmutativa reducida y, por tanto, separable. Además, el radical de $A \subset A \otimes A^o$, contiene a $R \otimes A + A \otimes R$ siendo $R$ el radical de $A$, luego $A$ es reducida.

□

Dada la $k$-álgebra $A$ el epimorfismo $A \otimes_k A^o \to A$, $a \otimes b \mapsto ab$ es un morfismo de $A \otimes A^o$-módulos. Denotemos por $\Delta$ el núcleo, que es un ideal por la izquierda de $A \otimes A^o$.

Como sabemos, llamamos $\Omega_{A/k} = \Delta/\Delta^2$ el módulo de las diferenciales de Kahler de $A$.

**7. Proposición:** *Si $A$ es una $k$-álgebra finita separable entonces $\Omega_{A/k} = 0$.*

*Demostración.* Por ser $A$ separable entonces $A \otimes A^o$ es semisimple. Por tanto, $A \otimes A^o$ es producto directo de álgebras de matrices, que cumplen que todo ideal por la izquierda es idempotente. Luego $\Delta = \Delta^2$ y $\Omega_{A/k} = 0$. □

Sea $M$ un $A \otimes A^o$-módulo, (sigamos la notación $(a \otimes b) \cdot m = amb$). Definimos por $\mathrm{Der}_k(A, M)$, al conjunto de las aplicaciones $k$-lineales $D$ tales que $D(ab) = (Da)b + aDb$.

**8. Teorema:** $\mathrm{Der}_k(A, M) = \mathrm{Hom}_{A \otimes A^o}(\Delta, M)$.

*Demostración.* Sea $d\colon A \to \Delta$ definido por $da := a \otimes 1 - 1 \otimes a$. Se verifica que $d(ab) = a \otimes 1 \cdot db + da \cdot (1 \otimes b) = adb + (da)b$, es una derivación de $A$ en $\Delta$.

Dada $F \in \mathrm{Hom}_{A \otimes A^o}(\Delta, M)$, sea $D_F := F \circ d$. Se cumple que $D_F \in \mathrm{Der}_k(A, M)$.

Recíprocamente, dada $D \in \mathrm{Der}_k(A, M)$ sea $F_D \in \mathrm{Hom}_{A \otimes A^o}(\Delta, M)$, definido por $F_D(\sum_i a_i \otimes b_i) = \sum_i (Da_i)b_i$, para $\sum_i a_i \otimes b_i \in \Delta$. Se cumple que $F_D(adb) = aDb$ y $F_D((da)b) = (Da)b$, lo que muestra que $F_D$ es un morfismo de $A \otimes A^o$-módulos.

□

Supongamos ahora que la estructura de $A$-módulo de $M$ por la derecha es la misma que por la izquierda, es decir, $am = ma$, para todo $a \in A$ y $m \in M$. Luego, $M$ es un $A$-módulo tal que $(ab - ba)m = 0$, para todo $a, b \in A$ y todo $m \in M$, porque $abm = m(ab) = (ma)b = amb = bam$. Recíprocamente, si $M$ es un $A$-módulo tal que $(ab - ba)m = 0$, para todo $a, b \in A$ y todo $m \in M$, entonces podemos dotarlo de estructura de $A \otimes A^o$-módulo: $ma := am$. En este caso, $D \in \mathrm{Der}_k(A, M)$ si y sólo si $D$ es $k$-lineal y $D(ab) = aDb + bDa$. Observemos que $\Omega_{A/k}$ es uno de estos módulos.

**9. Teorema:** *Sea $M$ un $A$-módulo tal que $(ab - ba)m = 0$, para todo $a, b \in A$ y $m \in M$. Entonces*

$$\mathrm{Der}_k(A, M) = \mathrm{Hom}_A(\Omega_{A/k}, M)$$

Si $A \to B$ es un epimorfismo de $k$-álgebras tal que el núcleo $R$ cumple que $R^2 = 0$, entonces $R$ es un $B$-módulo por la derecha e izquierda y diremos que $A$ es la extensión de $B$, por $R$. Dado un $B$-módulo por la derecha e izquierda $M$, diremos que $A = B \oplus M$, con la multiplicación definida por

$$(a, m) \cdot (a', m') = (aa', am' + ma')$$

es la extensión trivial de $B$ por $M$.

Diremos que un morfismo de $k$-álgebras $\phi\colon A \to A'$ es un morfismo de extensiones si se tiene un diagrama conmutativo

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M & \longrightarrow & A & \longrightarrow & B & \longrightarrow & 0 \\ & & \| & & \phi & & \| & & \\ 0 & \longrightarrow & M & \longrightarrow & A' & \longrightarrow & B & \longrightarrow & 0 \end{array}$$

Diremos que dos extensiones son equivalentes si existe un isomorfismo de extensiones entre ellas. Denotemos por $Extalg(B, M)$ el conjunto de la extensiones de álgebras de $B$ por $M$, módulo equivalentes.

Toda extensión de álgebras $A$, de $B$ por $M$, es como $k$-espacio vectorial $B \oplus M$, ahora bien, el producto será $(b, m) \cdot (b', m') = (bb', \phi(b, b') + bm' + mb')$, donde $\phi$ es una aplicación $k$-bilineal, por la bilinealidad del producto en $A$, y para que el producto sea asociativo habrá de cumplirse

$$\phi(b_1, b_2) \cdot b_3 + \phi(b_1 b_2, b_3) - b_1 \phi(b_2, b_3) - \phi(b_1, b_2 b_3) = 0$$

Así podemos definir en $B \oplus M$ tantos productos como elementos $\phi \in \mathrm{Hom}_k(B \otimes_k B, M)$ tales que $\phi(b_1 \otimes b_2) \cdot b_3 + \phi(b_1 b_2 \otimes b_3) - b_1 \phi(b_2 \otimes b_3) - \phi(b_1 \otimes b_2 b_3) = 0$

Dada un extensión de álgebras $A = B \oplus M$ de $B$ por $M$, dar un automorfismo de extensiones $A = B \oplus M \to B \oplus M = A$, $(b, m) \mapsto (b, \varphi(b) + m)$, equivale a dar $\varphi \in \mathrm{Der}_k(A, M)$, es decir, $\varphi \in \mathrm{Hom}_k(B, M)$ ha de verificar $\varphi(bb') = b\varphi(b') + \varphi(b)b'$. Si en $A = B \oplus M$ consideramos un producto, es decir un $\phi \in \mathrm{Hom}_k(B \otimes_k B, M)$ tal que $\phi(b_1 \otimes b_2) \cdot b_3 + \phi(b_1 b_2 \otimes b_3) - b_1 \phi(b_2 \otimes b_3) - \phi(b_1 \otimes b_2 b_3) = 0$, entonces vía un automorfismo, es decir, $\varphi \in \mathrm{Hom}_k(B, M)$ que verifica $\varphi(bb') = b\varphi(b') + \varphi(b)b'$, obtenemos un nuevo producto que es $\phi + \varphi \circ \mu$, donde $\mu\colon B \otimes B \to B$, $\mu(b \otimes b') = bb'$. En conclusión,

$$Extalg(B, M) = \left\{ \begin{array}{l} \phi \in \mathrm{Hom}_k(B \otimes_k B, M)\colon \\ \phi(b_1 \otimes b_2) \cdot b_3 + \phi(b_1 b_2 \otimes b_3) \\ -b_1 \phi(b_2 \otimes b_3) - \phi(b_1 \otimes b_2 b_3) = 0 \end{array} \right\} \Big/ \left\{ \begin{array}{l} \varphi \in \mathrm{Hom}_k(B, M)\colon \\ \varphi(bb') - b\varphi(b') \\ -\varphi(b)b' = 0 \end{array} \right\}$$

**10. Teorema:** $\mathrm{Ext}^2_{B \otimes_k B^o}(B, M) = Extalg(B, M)$.

*Demostración.* Consideremos la sucesión de $B \otimes B^o$-módulos

$$\cdots B \otimes \overset{n}{\cdots} \otimes B \overset{d_{n-2}}{\to} B \otimes \overset{n-1}{\cdots} \otimes B \overset{d_{n-3}}{\to} \cdots \overset{d_1}{\to} B \otimes B \overset{d_0}{\to} B \to 0$$

donde $d_{n-2}(b_1 \otimes \cdots \otimes b_n) := \sum_{i=1}^{n-1} (-1)^{i-1} (b_1 \otimes \overset{i}{\cdots} \otimes b_i b_{i+1} \otimes \cdots \otimes b_n)$ y consideramos que $B \otimes \overset{n}{\cdots} \otimes B$ es $B \otimes B^o$-módulos operando $B$ por la izquierda en el primer factor y $B^o$ por la derecha en el último factor. Además esta sucesión es exacta, porque $d_i \circ d_{i-1} = 0$ (como se comprueba), luego $\mathrm{Im}\, d_{i-1} \subset \mathrm{Ker}\, d_i$, y si consideramos los morfismos $s_{n_2}\colon B \otimes \overset{n-1}{\cdots} \otimes B \to B \otimes \overset{n}{\cdots} \otimes B$, $s_{n_2}(a_1 \otimes \cdots \otimes a_{n-1}) = 1 \otimes a_1 \otimes \cdots \otimes a_{n-1}$, tenemos que $\mathrm{Id} = d_{n-2} \circ s_{n-2} + s_{n-3} \circ d_{n-3}$, luego $\mathrm{Ker}\, d_{n-3} \subset \mathrm{Im}\, d_{n-2}$.

Así pues, si denotamos $d_i^*$ al morfismo inducido por $d_i$ al tomar $\mathrm{Hom}_{B \otimes B^o}(-, M)$, tenemos por definición

$$\mathrm{Ext}^2_{B \otimes_k B^o}(B, M) = \mathrm{Ker}\, d_3^* / \mathrm{Im}\, d_2^*$$

Ahora bien, $\mathrm{Hom}_{B \otimes B^o}(B \otimes \overset{n}{\cdot} \otimes B, M) = \mathrm{Hom}_k(1 \otimes B \overset{n-2}{\cdots} \otimes B \otimes 1, M)$, $d_3^*\colon \mathrm{Hom}_k(B \otimes B, M) \to \mathrm{Hom}_k(B \otimes B \otimes B, M)$, es explícitamente $d_3^* \phi(b_1 \otimes b_2 \otimes b_3) = \phi(b_1 \otimes b_2) \cdot b_3 + \phi(b_1 b_2 \otimes b_3) - b_1 \phi(b_2 \otimes$

$b_3) - \phi(b_1 \otimes b_2 b_3)$ y $d_2^*$: $\mathrm{Hom}_k(B, M) \to \mathrm{Hom}_k(B \otimes_k B, M)$ es explícitamente $d_2^*\varphi(b_1 \otimes b_2) = b_1\varphi(b_2) - \varphi(b_1 b_2) - \varphi(b_1)b_2$. En conclusión,

$$\mathrm{Ext}^2_{B \otimes_k B^o}(B, M) = Extalg(B, M)$$

□

## 1.6 Semisimplicidad del álgebra conmutadora

Esta sección será necesaria para probar más adelante que el grupo lineal es semisimple.

Sea $K$ un cuerpo no conmutativo y $E$ un $K$-espacio vectorial. $E^* = \mathrm{Hom}_K(E, K)$ es un $K^o$-espacio vectorial ($(\lambda w)(e) := w(e) \cdot \lambda$).

**1. Proposición :** *Supongamos que $E$ es un $K$-espacio vectorial de dimensión finita. Se verifica el isomorfismo de álgebras*

$$\mathrm{End}_K(E)^o = \mathrm{End}_{K^o}(E^*)$$

**2. Teorema:** *Si $A$ es una $k$-álgebra finita y $M$ es un $A$-módulo semisimple finito, entonces* $\mathrm{End}_A(M)$ *es un anillo semisimple.*

*Demostración.* Considerando el álgebra imagen por el morfismo $A \to \mathrm{End}_k(M) = M \oplus \cdots \oplus M$ se puede suponer que $A$ es semisimple. Además, si $M = M_1 \oplus \cdots \oplus M_n$ es la descomposición de $M$ en $A$-módulos homogéneos, se tiene que $\mathrm{End}_A(M) = \prod_i \mathrm{End}_A(M_i)$, luego podemos suponer que $M$ es homogéneo y $A$ anillo simple. Sea $I$ un $A$-módulo simple, $K = \mathrm{End}_A(I)$ y $E = \mathrm{Hom}_A(M, I)$. Por el teorema de Wedderburn,

$$\mathrm{End}_A(M) = \mathrm{End}_K(E)^o = \mathrm{End}_{K^o}(E^*)$$

que es simple. □

**3. Corolario :** *Sea $E$ un $k$-espacio vectorial de dimensión finita. Sea $A \subseteq \mathrm{End}_k(E)$ una $k$-subálgebra semisimple y denotemos por $C(A)$ a la subálgebra conmutadora de $A$, es decir, $C(A) = \{\phi \in \mathrm{End}_k(E) \colon a \circ \phi = \phi \circ a$, para todo $a \in A\}$. Se cumple que $C(A)$ es semisimple.*

*Demostración.* $C(A) = \mathrm{End}_A(E)$ y se aplica el teorema anterior. □

# Capítulo 2

# Representaciones lineales de grupos finitos

## 2.1 Representaciones lineales. Teorema de Maschke

Sea $G$ un grupo y $E$ un $k$-espacio vectorial.

**1. Definición:** Una representación lineal de $G$ en $E$ es un morfismo de grupos $\rho\colon G \to \mathrm{Aut}_k(E)$. Diremos que $E$ es un $G$-espacio vectorial. Se dice que el $\dim_k E$ es el grado de la representación lineal $\rho$.

Sea $k[G] = \bigoplus_{g\in G} k \cdot g$ la $k$-álgebra no conmutativa, de operaciones

$$(\sum_{g\in G}\lambda_g g) + (\sum_{g\in G}\lambda'_g g) := \sum_{g\in G}(\lambda_g + \lambda'_g)g$$

$$(\sum_{g\in G}\lambda_g g)\cdot(\sum_{g\in G}\lambda'_g g) := \sum_{g\in G}(\sum_{g'\cdot g''=g}\lambda_{g'}\lambda'_{g''})g$$

La $k$-álgebra $k[G]$ es conmutativa si y sólo si $G$ es un grupo abeliano.

Dada una representación lineal $\rho\colon G \to \mathrm{Aut}_k(E)$, podemos dotar a $E$ de estructura de $k[G]$-módulo:

$$(\sum_{g\in G}\lambda_g g)\cdot e := \sum_{g\in G}\lambda_g \rho(g)(e)$$

Recíprocamente, si $E$ tiene estructura de $k[G]$-módulo podemos definir la representación lineal $\rho\colon G \to \mathrm{Aut}_k(E)$, $\rho(g)(e) := g \cdot e$.

Se dice que dos representaciones lineales $\rho\colon G \to \mathrm{End}_k(E)$, $\rho'\colon G \to \mathrm{End}_k(E')$ son equivalentes si existe un isomorfismo lineal $T\colon E \to E'$ de modo que $T(\rho(g)(e)) = \rho'(g)(T(e))$, es decir, si y sólo si $E$ y $E'$ son $k[G]$-módulos isomorfos.

**2. Definición:** Se dice que la representación lineal $\rho\colon G \to \mathrm{Aut}_k(E)$ es irreducible, si no existe un subespacio vectorial propio de $E$ estable por $G$.

Es fácil probar que la representación lineal $\rho\colon G \to \mathrm{Aut}_k(E)$ es irreducible si y sólo si $E$ es un $k[G]$-módulo simple.

Si $\rho\colon G \to \mathrm{Aut}_k(E)$ y $\rho'\colon G \to \mathrm{Aut}_k(E')$ son dos representaciones lineales de $G$, podemos definir una representación lineal natural $\rho + \rho'$ de $G$ en $E \oplus E'$: $(\rho + \rho')(g)((e, e')) = (\rho(g)(e), \rho'(g)(e'))$. De otro modo, la suma directa de $k[G]$-módulos es $k[G]$-módulo de modo natural.

**3. Teorema Maschke:** *Sea $G$ un grupo finito. Toda representación $k$-lineal de $G$ es suma directa de representaciones irreducibles si y sólo si $\#G$ y $\operatorname{car} k$ son primos entre sí.*

*Demostración.* Tenemos que ver cuándo todo $k[G]$-módulo es suma directa de $k[G]$-módulos simples, es decir, cuándo $k[G]$ es semisimple.

Supongamos que $\#G$ y $\operatorname{car} k$ son primos entre sí. Dado un $k[G]$-módulo $E$ y un $k[G]$-submódulo $E'$, consideremos la sucesión exacta

$$0 \to E' \to E \xrightarrow{\pi} E/E' \to 0$$

Sea $s\colon E/E' \to E$ una sección de $k$-espacios vectoriales de $\pi$. El morfismo $s'\colon E/E' \to E$ definido por $s' = \frac{1}{\#G} \sum_{g \in G} g \cdot s \cdot g^{-1}$ es un morfismo de $k[G]$-módulos y es sección de $\pi$. Por tanto, $E = E' \oplus E/E'$ y por 1.1.5 $E$ es semisimple y $k[G]$ es semisimple.

Supongamos que $\#G$ es múltiplo de $\operatorname{car} k$. Si toda representación $k$-lineal de $G$ es suma directa de representaciones irreducibles, $k[G]$ sería semisimple y por Wedderburn $k[G] = M_{n_1}(K_1) \times \ldots \times M_{n_r}(K_r)$. Consideremos $s = \sum_{g \in G} g$, que es no nulo y pertenece al $Z(k[G]) = Z(K_1) \times \ldots \times Z(K_r)$. Se cumple que $s^2 = \#G \cdot s = 0$, que es imposible.

□

A partir de ahora supondremos que $\operatorname{car} k$ no divide a $\#G$ y supongamos que $k$ es algebraicamente cerrado.

Por el teorema de Wedderburn, $k[G] = M_{n_1}(k) \times \ldots \times M_{n_r}(k)$. Como sabemos $\mathrm{End}_k(E)$ es un anillo simple y $E$ es el único $\mathrm{End}_k(E)$-módulo simple (pues sólo hay uno y este lo es). Si escribimos, $k[G] = \mathrm{End}_k(E_1) \times \ldots \times \mathrm{End}_k(E_r)$, entonces la composición de los morfismos naturales $G \hookrightarrow k[G] \to \mathrm{End}_k(E_i)$ son todas las representaciones irreducibles de $G$, desisomorfas entre sí. Además, $\mathrm{End}_k(E_i) = E_i \oplus \overset{n_i}{\ldots} \oplus E_i$, así pues, la descomposición $k[G] = M_{n_1}(k) \times \ldots \times M_{n_r}(k)$ es la descomposición de $k[G]$ en suma de homogéneos. En ésta descomposición, aparece la representación trivial $G \to M_1(k)$, $g \mapsto \mathrm{Id}$ y por tanto los elementos invariantes por $G$ de $k[G]$ es $k[G]^G = M_1(k) = k$, explícitamente $k[G]^G = \langle \sum_{g \in G} g \rangle$.

**4. Ejemplo :** Si $G$ es un grupo cíclico el número de representaciones irreducibles es el orden de $G$ y todas son de grado 1:

Tenemos el isomorfismo de $k$-álgebras $k[x]/(x^n - 1) = k[\mathbb{Z}/n\mathbb{Z}], x^i \mapsto [i]$. Además, si $\xi_n$ es una raíz $n$-ésima primitiva de la unidad $k[x]/(x^n - 1) = \prod_{i=1}^{n} k[x]/(x - \xi_n^i) = k^n = M_1(k) \times \overset{n}{\ldots} \times M_1(k)$. En conclusión, $k[\mathbb{Z}/n\mathbb{Z}] = M_1(k) \times \overset{n}{\ldots} \times M_1(k)$ y explícitamente $[1] \mapsto ((\xi_n^1), \ldots, (\xi_n^n))$. Luego, los morfismos $\rho_i\colon \mathbb{Z}/n\mathbb{Z} \to M_1(k), [1] \mapsto (\xi_n^i)$ son todas las representaciones lineales irreducibles de $\mathbb{Z}/n\mathbb{Z}$.

**5. Ejercicio :** Sea $G = G_1 \times G_2$, probar que $k[G_1 \times G_2] = k[G_1] \otimes k[G_2]$. Probar que las representaciones irreducibles de $G_1 \times G_2$ son justamente el producto tensorial de las representaciones irreducibles de $G_1$, por las de $G_2$.

**6. Ejercicio:** Sea $G = \mathbb{Z}/n_1\mathbb{Z} \times \ldots \times \mathbb{Z}/n_s\mathbb{Z}$. Denotemos por $\xi_n$ una raíz $n$-ésima primitiva de la unidad. Probar que los morfismos

$$\begin{array}{rccc} \rho_{i_1,\ldots,i_s}\colon & \mathbb{Z}/n_1\mathbb{Z} \times \ldots \times \mathbb{Z}/n_s\mathbb{Z} & \to & M_1(k) \\ & (0,\ldots,\underset{r}{[1]},\ldots,0) & \mapsto & \xi_{n_r}^{i_r} \end{array}$$

son todas las representaciones lineales de $G = \mathbb{Z}/n_1\mathbb{Z} \times \ldots \times \mathbb{Z}/n_s\mathbb{Z}$

Obviamente $k[G]$ es un $k[G]$-módulo, luego tenemos una representación $G \to \mathrm{Aut}_k(k[G])$, representación que se denomina representación regular.

**7. Teorema:** *Sean $\#G$ y $\operatorname{car} k$ primos entre sí y supongamos que $k$ es algebraicamente cerrado. Sea $n = \#G$ y $n_i$ el grado de las representaciones irreducibles. Se cumple que*

1. $\sum_i n_i^2 = n$.
2. *Toda representación irreducible está contenida en la representación regular tantas veces como su grado.*
3. *El número de las representaciones irreducibles de $G$ desisomorfas coincide con el número de las clases de conjugación de $G$ y coincide con la dimensión del centro de $k[G]$.*

*Demostración.* 1. $n = \#G = \dim_k k[G] = \sum_i \dim_k \mathrm{End}_k(E_i) = \sum_i n_i^2$.

2. Dada una base $\{e_1,\ldots,e_n\}$ de un espacio vectorial $E$, tenemos el isomorfismo de $\mathrm{End}_k(E)$-módulos $\mathrm{End}_k(E) \simeq E \oplus \overset{n}{\ldots} \oplus E, T \mapsto (T(e_1),\ldots,T(e_n))$. Por tanto, $k[G] = (E_1 \oplus \overset{n_1}{\ldots} \oplus E_1) \oplus \ldots \oplus (E_r \oplus \overset{n_r}{\ldots} \oplus E_r)$ y se concluye.

3. Es fácil comprobar que $Z(\mathrm{End}_k(E)) = k \cdot \mathrm{Id}$. Por tanto,

$$Z(\mathrm{End}_k(E_1) \times \ldots \times \mathrm{End}_k(E_r)) = k \times \overset{r}{\ldots} \times k$$

y $\dim_k Z(k[G]) = r$. Por otra parte,

$$\begin{aligned} Z(k[G]) &= \{\sum_g \lambda_g g\colon g' \cdot (\sum_g \lambda_g g) \cdot {g'}^{-1},\ \text{para todo } g' \in G\} \\ &= \{\sum_g \lambda_g g\colon \lambda_g = \lambda_{g'gg'^{-1}},\ \text{para todo } g, g' \in G\} \\ &= \bigoplus_{\bar{h} \in G/\sim} k \cdot (\sum_{\bar{g}=\bar{h}} g) \end{aligned}$$

donde $G/\sim$ es el conjunto de clases de conjugación. Por tanto, $\dim_k k[G] = \#G/\sim$.

□

## 2.2 Representaciones irreducibles del grupo simétrico de $n$-letras

El cálculo de las representaciones irreducibles del grupo simétrico de $n$-letras fue resuelto por primera vez por Fröbenius y Young (1901-1903). La exposición que seguimos es debida a von Neumann y Van der Waerden. Supondremos el cuerpo algebraicamente cerrado de característica mayor que $n$.

Sea $S_n$ el grupo simétrico de $n$-letras. Toda permutación $s \in S_n$ es producto de ciclos disjuntos $s = s_1 \cdots s_r$ (incluyamos los ciclos de orden 1). Sea $n_i = \mathrm{ord}(s_i)$ y digamos que $n_1 \geq n_2 \geq \cdots \geq n_r$. Otra permutación, $s' \in S_n$, $s' = s'_1 \cdots s'_{r'}$, $n'_i = \mathrm{ord}(s'_i)$ y $n'_1 \geq n'_2 \geq \cdots \geq n'_{r'}$ es conjugada de $s$ si y sólo si $r = r'$ y $n_i = n'_i$, para todo $i$. Así pues, hay tantas clases de conjugación en $S_n$, como sucesiones de números naturales positivos $n_1 \geq n_2 \geq \cdots \geq n_r$, con $\sum_i n_i = n$; que es el número de representaciones irreducibles de $S_n$.

Los ideales minimales de $\mathrm{End}_k(E)$ están generados por por un endomorfismo que se anula en un hiperplano. Si $\{e_1, \ldots, e_n\}$ es una base de $E$ y $T(e_1) \neq 0$ y $T(e_i) = 0$ para todo $i > 1$, tendremos que $\mathrm{End}_k(E) \cdot T$ es un ideal mínimo y $T \cdot \mathrm{End}_k(E) \cdot T = kT$. Además, $T$ se anula en un hiperplano y el endomorfismo no es nulo si y sólo si $T \neq 0$ y $T \cdot \mathrm{End}_k(E) \cdot T = kT$.

Dejamos que el lector pruebe la siguiente proposición.

**1. Proposición:** *Un ideal $I \subseteq k[G]$ es minimal si y sólo si existe un generador $c \in I$, de modo que $c \cdot k[G] \cdot c = k \cdot c$.*

Sea $\alpha = (n_1, \ldots, n_h)$, con $n_1 \geq n_2 \geq \cdots \geq n_h$ y $\sum_i n_i = n$. Consideremos el diagrama (de Young)

$$\begin{array}{cccc}
1 & n_1 + 1 & \cdots & \sum_{i=1}^{h-1} n_i + 1 \\
\vdots & \vdots & \cdots & \vdots \\
\vdots & \vdots & \cdots & n \\
\vdots & \vdots & \cdots & \\
n_2 & n_1 + n_2 & & \\
\vdots & & & \\
n_1 & & &
\end{array}$$

Sea $P_\alpha = \{p \in S_n : p \text{ permuta los elementos de las filas del diagrama}\}$ y $Q_\alpha = \{q \in S_n : q \text{ permuta los elementos de la columna del diagrama}\}$.

**2. Lema:** *Dado $s \in S_n$ se cumple*

1. *o bien existen $p \in P_\alpha$ y $q \in Q_\alpha$ de modo que $s = p \cdot q$,*

2. *o bien, existen dos trasposiciones $u \in P_\alpha$ y $v \in Q_\alpha$ de modo que $u \cdot s \cdot v = s$.*

*Demostración.* Consideremos los dos diagramas "$\alpha$" y "$s(\alpha)$"

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| $1$ | $n_1+1$ | $\cdots$ | $\sum_{i=1}^{h-1} n_i+1$ | $s(1)$ | $s(n_1+1)$ | $\cdots$ | $s(\sum_{i=1}^{h-1} n_i+1)$ |
| $\vdots$ | $\vdots$ | $\cdots$ | $\vdots$ | $\vdots$ | $\vdots$ | $\cdots$ | $\vdots$ |
| $\vdots$ | $\vdots$ | $\cdots$ | $n$ | $\vdots$ | $\vdots$ | $\cdots$ | $s(n)$ |
| $\vdots$ | $\vdots$ | $\cdots$ | | $\vdots$ | $\vdots$ | $\cdots$ | |
| $n_2$ | $n_1+n_2$ | | | $s(n_2)$ | $s(n_1+n_2)$ | | |
| $\vdots$ | | | | $\vdots$ | | | |
| $n_1$ | | | | $s(n_1)$ | | | |

Supongamos que todo par de números $r, r'$ que estén en una misma fila del diagrama $\alpha$ yacen en distintas columnas del diagrama $s(\alpha)$. Sea $p \in P_\alpha$, la permutación tal que $\alpha$ y $p(s(\alpha))$ tengan los mismos números (salvo órdenes) en las filas. Sea $q \in Q_\alpha$, de modo que $\alpha = q(p(s(\alpha)))$. Por construcción, $s = p^{-1}q^{-1}$ y obtenemos 1.

Supongamos que existen $r, r'$ que estén en una misma fila del diagrama $\alpha$ y en una misma columna del diagrama $s(\alpha)$. Tenemos pues, que $r = s(t)$, $r' = s(t')$, donde $t$ y $t'$ yacen en una misma columna del diagrama $\alpha$. Sea $u \in P_\alpha$ la transposición que permuta $r$ y $r'$. Entonces $s^{-1}us = v$ es la transposición que permuta $t$ y $t'$, luego pertenece a $Q_\alpha$, $usv^{-1} = s$ y obtenemos 2.

□

Para cada $\alpha = (n_1, \ldots, n_r)$, sea $p_\alpha = \sum_{p \in P_\alpha} p \in k[S_n]$, $q_\alpha = \sum_{q \in Q_\alpha} \operatorname{sgn}(q) q \in k[S_n]$ y $c_\alpha = p_\alpha \cdot q_\alpha$. El elemento $c_\alpha$ es distinto de cero ya que $pq = p'q'$ ($p.p' \in P_\alpha$ y $q, q' \in Q_\alpha$) si y sólo si $p^{-1}p' = q{q'}^{-1}$ si y sólo si $p = p'$ y $q = q'$.

**3. Teorema :** *Toda representación irreducible de $S_n$ es isomorfa a alguno de los ideales $k[S_n] \cdot c_\alpha$, los cuales son desisomorfos entre sí.*

*Demostración.* En primer lugar veamos que $k[S_n] \cdot c_\alpha$ es un ideal mínimo. Para ellos basta ver que $c_\alpha \cdot k[S_n] \cdot c_\alpha = kc_\alpha$. Obviamente $c_\alpha \cdot k[S_n] \cdot c_\alpha \subseteq p_\alpha \cdot k[S_n] \cdot q_\alpha$. Dado $s \in S_n$, si $s = pq$, con $p \in P_\alpha$ y $q \in Q_\alpha$, tenemos que $p_\alpha \cdot pq \cdot q_\alpha = \operatorname{sgn}(q) p_\alpha \cdot q_\alpha = \operatorname{sgn}(q) \cdot c_\alpha$; si existen transposiciones $u \in P_\alpha$, $v \in Q_\alpha$, tales que $usv = s$, entonces que $p_\alpha \cdot s \cdot q_\alpha = p_\alpha \cdot usv \cdot q_\alpha = -p_\alpha \cdot s \cdot q_\alpha$ y $p_\alpha \cdot s \cdot q_\alpha = 0$. Con todo, $p_\alpha \cdot k[S_n] \cdot q_\alpha = kc_\alpha$ y concluimos.

Veamos que si $\alpha = (n_1, \ldots, n_r) \neq \alpha' = (n'_1, \ldots, n'_{r'})$ entonces $k[S_n] \cdot c_\alpha$ no es isomorfo a $k[S_n] \cdot c_{\alpha'}$. Basta demostrar que $k[S_n] \cdot c_\alpha \cdot k[S_n] \cdot c_{\alpha'} = 0$, que equivale a que $c_\alpha \cdot k[S_n] \cdot c_{\alpha'} = 0$. Así pues, tenemos que probar que $c_\alpha \cdot s \cdot c_{\alpha'} = 0$, para toda $s \in S_n$. Basta ver que $c_\alpha \cdot (sc_{\alpha'}s^{-1}) = 0$, para toda $s \in S_n$. Ahora bien, $(sc_{\alpha'}s^{-1})$ se obtiene del mismo modo que $c_{\alpha'}$, considerando en vez de $\{1, \ldots, n\}$ el conjunto $\{s(1), \ldots, s(n)\}$. Denotaremos por razones obvias $sc_{\alpha'}s^{-1} = c_{s(\alpha')}$.

Sea $n_i$ el primer número distinto de $n'_i$; podemos suponer que $n_i > n'_i$. En alguna columna $j \leq i$, correspondiente al diagrama asociado a $\alpha$ existen dos números naturales $r, r'$, que yacen en una misma fila del diagrama correspondiente a $s(\alpha')$: Si todos los elementos de la primera columna del diagrama de $\alpha$ yacen en distintas filas del diagrama de $s(\alpha')$, reordenando los elementos de las filas de este

último, podemos suponer que yacen todos en la primera columna. Argumentando del mismo modo con las sucesivas columnas de $\alpha$ este argumento no podrá ser mantenido hasta la columna $i$ incluida.

Sea $u$ la transposición que permuta $r$ y $r'$. Tenemos que $c_\alpha \cdot c_{s(\alpha')} = (-c_\alpha \cdot u) \cdot c_{s(\alpha')} = -c_\alpha \cdot (u \cdot c_{s(\alpha')}) = -c_\alpha \cdot c_{s(\alpha')}$, luego $c_\alpha \cdot (s c_{\alpha'} s^{-1}) = 0$.

Por último, como hay tantas representaciones irreducibles como $\alpha$ distintos, toda representación irreducible de $S_n$ es isomorfa a alguno de los ideales $k[S_n] \cdot c_\alpha$.

□

## 2.3 Carácter asociado a una representación lineal

Supongamos por sencillez que $k$ es algebraicamente cerrado.

**1. Definición:** Se llama caracter de una representación $\rho\colon G \to \mathrm{End}_k(E)$, a la función, $\chi_E\colon G \to k$, definida por

$$\chi_E(g) = \mathrm{tr}(\rho(g))$$

Observemos que la composición de los morfismos

$$G \hookrightarrow k[G] = \mathrm{End}_k(E_1) \times \ldots \times \mathrm{End}_k(E_r) \xrightarrow{\pi_i} \mathrm{End}_k(E_i) \xrightarrow{\mathrm{tr}_i} k$$

es justamente el carácter $\chi_{E_i}$, donde hemos denotado $\mathrm{tr}_i$ la aplicación que asigna a cada matriz su traza.

**2. Proposición:** *Los caracteres asociados a las representaciones irreducibles son linealmente independientes.*

*Demostración.* Todo carácter $\chi_E$ extiende de modo único por linealidad a una forma lineal sobre $k[G]$. Los caracteres asociados a las representaciones irreducibles son linealmente independientes si y sólo si lo son sus extensiones lineales sobre $k[G]$.

Consideremos la descomposición $k[G] = \mathrm{End}_k(E_1) \times \ldots \times \mathrm{End}_k(E_r)$ y las proyecciones $\pi_i\colon k[G] \to \mathrm{End}_k(E_i)$. Tenemos que $\chi_{E_i} = \mathrm{tr}_i \circ \pi_i$, que claramente son linealmente independientes, pues

$$(\chi_{E_i})_{|\,\mathrm{End}_k(E_j)} = \delta_{ij} \cdot \mathrm{tr}_i$$

□

Observemos que $\chi_E + \chi_{E'} = \chi_{E \oplus E'}$ y $\chi_E \cdot \chi_{E'} = \chi_{E \otimes_k E'}$.

**3. Proposición:** *Dos representaciones lineales son equivalentes si y sólo si los caracteres son iguales (*$\mathrm{car}\, k = 0$*).*

*Demostración.* Sea una representación lineal de $G$ en $\mathrm{End}_k(E)$. Sea la descomposición $E = E_1^{m_1} \oplus \ldots \oplus E_r^{m_r}$. Tenemos que $\chi_E = m_1 \cdot \chi_{E_1} + \cdots + m_r \chi_{E_r}$. Los números $m_i$ están unívocamente determinados por $\chi_E$ por la proposición anterior y clasifican a $E$.

□

**4. Ejercicio:**

1. Calcular la traza del endomorfismo $L_g\colon k[G] \to k[G]$, $L_g(h) = gh$.
2. Dada una matriz $g \in M_n(k)$, podemos considerar el endomorfismo $L_g\colon M_n \to M_n$, $L_g(h) = gh$. Probar que $\mathrm{tr}(L_g) = n\,\mathrm{tr}(g)$.

3. Sean $E_1, \ldots, E_n$ todas las representaciones lineales (desisomorfas) irreducibles de $G$ y $n_i = \dim_k E_i$. Probar que si $g \neq 1$, entonces

$$\sum_i n_i \chi_{E_i}(g) = 0$$

**5. Ejercicio:** Sea $E$ un $G$-espacio vectorial y supongamos que $E^G = 0$. Probar que $\sum_{g\in G} \chi_E(g) = 0$.

## 2.4 Producto de convolución

Dada una $k$-álgebra finita $A$, se define la traza $\mathrm{Tr}\colon A \to k$, como la aplicación que asigna a cada $a \in A$, la traza de la homotecia de razón $a$, en $A$. La traza, a su vez, define una métrica simétrica en $A$, $T_2(a,b) = \mathrm{Tr}(a \cdot b)$, denominada métrica de la traza. $A^*$ es un $A$-módulo por la izquierda $((a \cdot w)(b) := w(ba))$ y por la derecha $((w \cdot a)(b) := w(ab))$. La métrica de la traza define la polaridad $T_2\colon A \to A^*$, $a \mapsto T_2(a,-) = T_2(-,a)$, que resulta ser un morfismo de $A$-módulos por la derecha y la izquierda. Por tanto, $\mathrm{Im}\, T_2 = A \cdot T_2(1,-) = A \cdot Tr$.

En $k[G]$ podemos definir la métrica de la traza. Observemos que

$$T_2(g,g') = \begin{cases} 0 & \text{si } g \neq g'^{-1} \\ \#G & \text{si } g = g'^{-1} \end{cases}$$

Lo que muestra que $T_2$ es no singular.

Denotemos $C(G) = Aplic(G,k)$. Se cumple que $Aplic(G,k) = \mathrm{Hom}_k(k[G],k) = k[G]^*$.

**1. Proposición:** *La polaridad $T_2\colon k[G] \to C(G)$ es un isomorfismo de $G$-módulos por la derecha e izquierda.*

Observemos que la descomposición $k[G] = M_{n_1}(k) \times \cdots \times M_{n_r}(k)$ es ortogonal para $T_2$ y los elementos $\frac{\mathrm{Id}_i}{n_i} \in M_{n_i}(k)$ son ortonormales entre sí. Además, $T_2(\frac{\mathrm{Id}_i}{n_i}, g) = \mathrm{Tr}(\frac{\mathrm{Id}_i}{n_i} \cdot g) = \mathrm{tr}_i(g) = \chi_{E_i}(g)$. En conclusión, por la polaridad definida por $T_2$, tenemos

$$\begin{array}{ccc} C(G) & \overset{T^2}{\simeq} & k[G] \\ \chi_{E_i} & \mapsto & \frac{\mathrm{Id}_i}{n_i} \end{array}$$

Por tanto, con la métrica $T^2$ de $C(G)$, definida por $T_2$, los $\chi_{E_i}$ son ortonormales. Así pues,

$$\chi_E = T^2(\chi_E, \chi_{E_1})\chi_{E_1} + \ldots + T^2(\chi_E, \chi_{E_r})\chi_{E_r}$$

**2. Proposición:** *$E$ es un $G$-espacio vectorial irreducible $\iff T^2(\chi_E, \chi_E) = 1$ ($cark = 0$).*

Explicitemos $T^2$: Observemos que $T_2(g) = \#G \cdot \delta_{g^{-1}}$, donde $\delta_g(g') = 0$ si $g \neq g'$ y $\delta_g(g) = 1$, luego

$$T^2(f,h) = T^2(\sum_{g\in G} f(g)\delta_g, \sum_{g\in G} h(g)\delta_g) = (\frac{1}{\#G}\sum_{g\in G} f(g)g^{-1})(\sum_{g\in G} h(g)\delta_g) = \frac{1}{\#G}\sum_{g\in G} f(g)h(g^{-1})$$

En $C(G)^* = k[G]$ existe un único elemento $G$-invariante, que sobre $1 \in C(G)$ vale 1, que es $\frac{1}{\#G}\sum_{g\in G} g$. Se cumple que $T^2(f,h) = (\frac{1}{\#G}\sum_{g\in G} g)(f(x^{-1})h(x))$. Si denotamos $\frac{1}{\#G}\sum_{g\in G} g = \int_G dg$, denotaremos $T^2(f,h) = \int_G f(g)h(g^{-1})dg$.

En el anillo $C(G)$ podemos definir, también, la traza $\mathrm{Tr}'$, que pertenece a $C(G)^* = k[G]$, y resulta $\mathrm{Tr}' = \sum_{g\in G} g$. $\mathrm{Tr}'$ define una métrica simétrica $T'^2$ en $C(G)$, que explícitamente es $T'^2(f,h) = \sum_{g\in G} f(g)h(g)$. La polaridad asociada cumple $T'^2(\delta_g, -) = g$. Si $*\colon k[G] \to k[G]$ es el morfismo $k$-lineal que aplica $g$ en $g^{-1}$, tenemos el diagrama conmutativo:

$$\begin{array}{ccc} k[G] & \overset{T_2}{=\!=} & C(G) \\ \| & \diagup\!\diagup_{\#G\cdot T_2'} & \\ k[G] & & \end{array} \qquad (*)$$

Existe un único producto en $C(G)$ de modo que la polaridad $T^2\colon C(G) \to C(G)^* = k[G]$ sea un morfismo de anillos, producto que denotaremos por $*$ y llamaremos producto de convolución. Explícitamente,

$$\begin{aligned} f * h &= (\sum_g f(g)\delta_g) * (\sum_g h(g)\delta_g) = T_2((\frac{1}{\#G}\sum_g f(g)g^{-1}) \cdot (\frac{1}{\#G}\sum_g h(g)g^{-1})) \\ &= T_2(\frac{1}{\#G}\sum_{x\in G}(\frac{1}{\#G}\sum_{g^{-1}g'^{-1}=x} f(g)h(g')\cdot x)) = T_2(\frac{1}{\#G}\sum_{x\in G}(\frac{1}{\#G}\sum_{g^{-1}g'^{-1}=x^{-1}} f(g)h(g')\cdot x^{-1})) \\ &= T_2(\frac{1}{\#G}\sum_{x\in G}(\frac{1}{\#G}\sum_{g\in G} f(g)h(xg^{-1})x^{-1})) = T_2(T^2(\sum_{x\in G}\frac{1}{\#G}\sum_{g\in G} f(g)h(xg^{-1})\delta_x)) \\ &= \sum_{x\in G}\frac{1}{\#G}\sum_{g\in G} f(g)h(xg^{-1})\delta_x \end{aligned}$$

luego, $(f*h)(x) = \int_G f(g)h(xg^{-1})dg$.

Por otra parte $C(G)$ es un anillo conmutativo, y por tanto $T_2$ definirá en $k[G]$ un producto conmutativo. Resulta que es el "tonto": $(\sum \lambda_g g) * (\sum \mu_g g) = \sum \lambda_g\mu_g g$.

Por último, reformulemos el morfismo definido por la traza tr. Tenemos que $\mathrm{End}_k(E)^* = (E^* \otimes_k E)^* = E \otimes_k E^* = E^* \otimes_k E = \mathrm{End}_k(E)$. $T_2\colon k[G] = \mathrm{End}_k(E_1) \times \ldots \times \mathrm{End}_k(E_r) \simeq k[G]^* = \mathrm{End}_k(E_1) \times \ldots \times \mathrm{End}_k(E_r)$, es explícitamente $T_2(T_1,\ldots,T_r) = (n_1\cdot T_1, \ldots, n_r \cdot T_r)$, $(n_i = \dim_k E_i)$. El producto de convolución es explícitamente

$$(T_1,\ldots,T_r) * (T_1',\ldots,T_r') = (\frac{T_1\cdot T_1'}{n_1},\ldots,\frac{T_r\cdot T_r'}{n_r})$$

**3. Teorema de Burnside:** *Sea $k$ un cuerpo algebraicamente cerrado de característica cero. El grado de una representación irreducible de un grupo divide al orden del grupo.*

*Demostración.* Sea $G \to \mathrm{End}_k E_i$ una representación irreducible, $n = \#G$ y $n_i = \dim_k E_i$. Siguiendo las notaciones anteriores hemos probado que $T^2(\chi_{E_i}) = \frac{\mathrm{Id}_i}{n_i}$. Además, $\chi_{E_i} = \sum_g \chi_{E_i}(g)\delta_g$ y $T^2(\delta_g) = \frac{1}{n}g^{-1}$. Por tanto,

$$\frac{\mathrm{Id}_i}{n_i} = \frac{1}{n}\sum_g \chi_{E_i}(g)g^{-1}$$

En conclusión, $\frac{n\,\mathrm{Id}_i}{n_i} = \sum_g \chi_{E_i}(g)g^{-1}$. Tenemos que $g^n = \mathrm{Id}$, luego sus valores propios son raíces $n$-ésimas de la unidad y $\chi_{E_i}(g)$ es una combinación con coeficientes naturales de raíces $n$-ésimas de la unidad. Por tanto, $\frac{n\,\mathrm{Id}_i}{n_i} \in \mathbb{Z}[\xi][G]$, siendo $\xi \in k$ una raíz n-ésima primitiva de la unidad. $\mathbb{Z}[\xi][G]$ es un $\mathbb{Z}$-módulo libre, y el polinomio característico de la homotecia de razón $\frac{n\,\mathrm{Id}_i}{n_i}$, es un polinomio con coeficientes en $\mathbb{Z}$. Ahora bien, el polinomio anulador de $\frac{n\,\mathrm{Id}_i}{n_i}$ (con coeficientes en $\mathbb{Q}$) es $(x - \frac{n}{n_i}) \cdot x$ (si sólo existe una única representación irreducible es $x - \frac{n}{n_i}$). Por tanto, $\frac{n}{n_i}$ es una raíz del polinomio característico, que es mónico luego $\frac{n}{n_i} \in \mathbb{Z}$.

□

Puede refinarse este teorema.

**4. Teorema :** *Sea $k$ un cuerpo algebraicamente cerrado de característica cero. El grado de una representación irreducible de un grupo $G$ divide al orden del grupo cociente de $G$ por su centro.*

*Demostración.* Sea $Z$ el centro de $G$. Tenemos que $\chi_1 \times \ldots \times \chi_r \colon k[Z] = k \times \ldots \times k$, donde $\chi_i$ son los $r$ caracteres irreducibles de $Z$.

Tenemos $k[G] = k[G] \otimes_{k[Z]} k[Z] = k[G] \otimes_{k[Z]} (k \times \ldots \times k) = k[G]_1 \times \overset{r}{\ldots} \times k[G]_r$ que es la descomposición de $k[G]$ en submódulos, que son $Z$-módulos homogéneos de tipo distinto. Si $G/Z = \{\bar{g}_1, \ldots, \bar{g}_s\}$ entonces $\{g_1, \ldots, g_s\}$ es una base del $k[Z]$-módulo libre $k[G]$ y sus clases son una base del $k$-espacio vectorial $k[G]_i$.

Si $E$ es un $k[G]$-módulo irreducible de grado $n_i$, sobre él $Z$ opera por un carácter, digamos $\chi_i$.

Como decíamos en la demostración anterior,

$$\frac{\mathrm{Id}_i}{n_i} = \frac{1}{\#G}\sum_g \chi_E(g)g^{-1}$$

Ahora bien, $\chi_E(gz) = \chi_E(g) \cdot \chi_i(z)$ y $z$ operando sobre $k[G]_i$ es la homotecia de razón $\chi_i(z)$. Por tanto, tenemos que

$$\frac{\mathrm{Id}_i}{n_i} = \frac{\#Z}{\#G}\sum_i \chi_E(g_i^{-1})g_i$$

en $k[G]_i$. y por tanto, $\frac{\#G}{\#Z}\frac{\mathrm{Id}_i}{n_i} \in \mathbb{Z}[\xi]g_1 \oplus \ldots \oplus \mathbb{Z}[\xi]g_s \subset k[G]_i$. Ahora ya como en la demostración anterior concluimos que $\frac{\#G}{\#Z n_i} \in \mathbb{Z}$.

□

## 2.5 Representación lineal inducida

Sea $H \subseteq G$ un subgrupo y $E$ un $k[H]$-módulo. Diremos que $k[G] \otimes_{k[H]} E$ ($gh \otimes e = g \otimes he$) es la representación $G$-lineal inducida por el subgrupo $H$ ($g(g' \otimes e) = gg' \otimes e$). Ésta verifica la propiedad universal

$$Hom_{k[G]}(k[G] \otimes_{k[H]} E, E') = Hom_{k[H]}(E, E')$$

para todo $k[G]$-módulo $E'$.

Dado un $k[G]$-módulo $E$, podemos considerarlo como $k[H]$-módulo.

Observemos que $k[G] \otimes_{k[H]} E = (\underset{\bar{g} \in G/H}{\oplus} gk[H]) \otimes_{k[H]} E = \underset{\bar{g} \in G/H}{\oplus} g \cdot E$ (formalmente) y $\dim_k k[G] \otimes_{k[H]} E = \dim_k E \cdot \#(G/H)$.

**1. Proposición :** *Sea $N$ un subgrupo normal de $G$ y $E$ un $G$-espacio vectorial irreducible. Entonces existe un subgrupo $N \subseteq H \subseteq G$ y un $H$-espacio vectorial irreducible $E'$, $N$-homogéneo, de modo que $E = k[G] \otimes_{k[H]} E'$.*

*Demostración.* $E = E_1 \oplus \ldots \oplus E_n$ la descomposición de $E$ en suma directa de $k[N]$-módulos homogéneos. Cada $g \in G$ permuta los sumandos de la descomposición, porque si $V$ es un $k[N]$-submódulo de $E$ entonces $gV$ lo es también, pues $N$ es normal, y si $V$ es un $k[N]$-módulo isomorfo a $V'$ entonces $gV$ es isomorfo a $gV'$. Tenemos que $E = \bigoplus_{\bar{g} \in G/H} g \cdot E_1 = k[G] \otimes_{k[H]} E_1$, donde $H$ es el subgrupo de $G$ que estabiliza a $E_1$.

□

**2. Corolario :** *Si $N$ es un subgrupo normal conmutativo de $G$, el grado de toda representación irreducible de $G$ divide a $\#G/N$.*

*Demostración.* Siguiendo las notaciones de la proposición anterior escribamos $E = k[G] \otimes_{k[H]} E'$. Si $H \subsetneq G$ entonces por inducción sobre el orden del grupo, tendremos que la dimensión de $E'$ divide a $\#H/N$, luego la dimensión de $E$ divide a $\#G/N$. Si $H = G$, entonces $E$ es un $k[N]$-módulo homogéneo. Como $N$ es conmutativo actúa en $E$ por homotecias. Si denotamos por $G'$ y $N'$ las imágenes de $G$ y $N$ en su representación en $\mathrm{End}_k E$, tendremos que $N'$ está incluido en el centro de $G'$. Por 2.4.4, la dimensión de $E$ divide a $\#G'/N'$. Como $G'/N'$ es un cociente de $G/N$ hemos terminado.

□

**3. Definición :** Diremos que un grupo $G$ es superresoluble si existe una cadena de subgrupos normales en $G$, $0 = G_0 \subset G_1 \subset \cdots \subset G_n = G$ de modo que $G_i/G_{i-1}$ sean grupos cíclicos.

**4. Lema :** *Sea $G$ un grupo no abeliano superresoluble. Entonces existe un subgrupo normal abeliano no incluido en el centro de $G$.*

*Demostración.* Sea $Z$ el centro de $G$. El cociente $G/Z$ es superresoluble, luego contiene un subgrupo cíclico normal, $H$. La imagen inversa de $H$ en $G$, es el subgrupo normal abeliano buscado.

□

**5. Teorema :** *Sea $G$ un grupo superresoluble. Toda representación irreducible de $G$ está inducida por una representación de grado 1 de un subgrupo de $G$.*

*Demostración.* Vamos a probar el teorema por inducción sobre el orden de $G$. Si $\rho\colon G \to \mathrm{End}_k(E)$ es la representación irreducible, considerando en vez de $G$ su imagen por $\rho$ podemos suponer que $\rho$ es inyectivo (es decir, que la representación es fiel).

Si $G$ es abeliano el teorema es obvio. Si $G$ no es abeliano por el lema existe un subgrupo normal abeliano $N$ no incluido en el centro de $G$. Siguiendo las notaciones de 2.5.1, tenemos que $E = k[G] \otimes_{k[H]} E'$ y basta demostrar el teorema para $H$, con lo que hemos concluido si $H \neq G$. Ahora bien, si $H = G$, entonces $E = E'$ y $N$ que actúa en $E'$ por homotecias estaría incluido en el centro de $G$, lo que es contradictorio.

□

Sea $N \subset G$ un subgrupo normal y supongamos que existe un subgrupo $H \subset G$ suplementario de $N$ en $G$, es decir, la aplicación $N \times H \to G, (n, h) \mapsto nh$ es biyectiva. Suele escribirse $G = N \ltimes H$, y observemos que la operación de $G$ se escribe en $N \ltimes H$: $(n, h) \cdot (n', h') = (n \cdot hn'h^{-1}, hh')$.

Supongamos, además, que $N$ es abeliano. $G$ actúa de modo natural sobre el conjunto de los caracteres de $N$: dado $\chi\colon N \to k^*$, definimos $g(\chi) = \chi \circ \tau_g$, donde $\tau_g$ es la conjugación por $g \in G$ en $N$. Dado un $G$-espacio vectorial irreducible $E$, sabemos que $E = k[G] \otimes_{k[H_i']} E'$, donde $N$ actúa en $E'$ por homotecias ($n \cdot e' = \chi_i(n) \cdot e'$, $\chi_i\colon N \to k^*$ es un carácter, que es un morfismo de grupos) y $H_i'$ es el subgrupo de $G$ que deja fijo a $\chi_i$. Además $E'$ coincide con el subespacio vectorial de $E$ sobre el que $N$ actúa por el carácter $\chi_i$ y $H_i'$ el subgrupo de $G$ que deja estable $E'$. Obviamente $E'$ es $H_i'$-irreducible. Recíprocamente si $E'$ es $H_i'$-irreducible entonces $k[G] \otimes_{k[H_i']} E'$ es $G$-irreducible.

Tendremos que $H_i' = N \ltimes H_i$. Si $E$ es $G$-irreducible, entonces $E'$ es $H_i'$-irreducible, luego $H_i$-irreducible. Denotemos estas representaciones lineales $\rho\colon G \to \mathrm{End}_k(E)$, $\rho_i'\colon H_i' \to \mathrm{End}_k(E')$ y $\rho_i\colon H_i \to \mathrm{End}_k(E')$. Se cumple que $\rho$ es la representación inducida por $\rho_i'$ y

$$\rho_i'(n, h_i)(e) = \chi_i(n) \cdot \rho_i(h_i)(e)$$

Notaremos $\rho_i' = \chi_i \otimes \rho_i$. Hemos obtenido,

**6. Teorema:** *Sea $N$ un subgrupo normal abeliano de $G$ y supongamos que $G = N \ltimes H$. Para cada carácter $\chi_i\colon N \to k^*$, sea $H_i$ el subgrupo de $H$ que lo deja fijo. Toda representación lineal irreducible de $G$ está inducida por una representación lineal $\chi_i \otimes \rho_i$, de $N \ltimes H_i$ donde $\rho_i$ es una representación lineal irreducible de $H_i$. Además, las representaciones lineales inducidas por $\chi_i \otimes \rho_i$ y $\chi_j \otimes \rho_j$ son equivalentes, si y sólo si existe $g \in G$ tal que $\chi_i = \chi_j \circ \tau_g$ y $\rho_i$ es equivalente a $\rho_j \circ \tau_g$.*

**7. Ejemplo:** Sea $D_n = (\mathbb{Z}/n\mathbb{Z}) \ltimes \mathbb{Z}/2\mathbb{Z} = \langle \sigma, \tau \rangle$, donde el orden de $\sigma$ es $n > 2$, el de $\tau$ es 2 y $\tau\sigma\tau^{-1} = \sigma^{-1}$, el grupo diédrico del polígono regular de $n$ lados. Por 2.5.2, como $\mathbb{Z}/n\mathbb{Z}$ es un subgrupo abeliano normal de índice 2, el grado de toda representación irreducible de $D_n$ es 2 o 1.

Sea $\xi$ una raíz primitiva $n$-ésima de la unidad. Sea $\chi_i\colon \mathbb{Z}/n\mathbb{Z} = \langle \sigma \rangle \to k^*$, el carácter definido por $\chi_i(\sigma) = \xi^i$. Se cumple que $\tau(\chi_i) = \chi_{-i}$.

Por tanto, $H_i = \mathrm{Id}$ para $i \neq 0$ e $i \neq \frac{n}{2}$. En estos casos la representación irreducible es $E = k[D_n] \otimes_{k[\mathbb{Z}/n\mathbb{Z}]} k = 1 \cdot k \oplus \tau \cdot k$, de modo que $\sigma(1) = 1 \cdot \xi^i$, $\sigma(\tau) = \tau \cdot \xi^{-i}$ y $\tau(1) = \tau$ y $\tau(\tau) = 1$. Matricialmente

$$\sigma = \begin{pmatrix} \xi^i & 0 \\ 0 & \xi^{-i} \end{pmatrix} \qquad \tau = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Por último, $H_i = \langle \tau \rangle$, para $i = 0$ o $i = \frac{n}{2}$ ($n$ par). En estos casos, $E = \langle e \rangle$, $\sigma(e) = e$ ó $\sigma(e) = -e$ y $\tau(e) = \pm e$.

## 2.6 Teorema de Artin

**1. Lema:** *Sean $E_1, E_2$ dos $G$-espacios vectoriales. Se cumple que*

$$T^2(\chi_{E_1}, \chi_{E_2}) = \dim_k \mathrm{Hom}_{k[G]}(E_1, E_2) = \dim_k (E_1^* \otimes E_2)^G$$

*Demostración.* Escribamos $E_1 = V_1^{n_1} \oplus \ldots \oplus V_r^{n_r}$, y $E_2 = V_1^{m_1} \oplus \ldots \oplus V_r^{m_r}$ como suma directa de $G$-espacios vectoriales irreducibles ($n_i, m_i \geq 0$). Por el lema de Schur, tenemos

$$\begin{aligned} T^2(\chi_{E_1}, \chi_{E_2}) &= T^2\Big(\sum_i n_i \chi_{V_i}, \sum_j m_j \chi_{V_j}\Big) = \sum_i n_i m_i \\ &= \sum_i \dim_k \mathrm{Hom}_{k[G]}(V_i^{n_i}, V_i^{m_i}) = \dim_k \mathrm{Hom}_{k[G]}(E_1, E_2) \end{aligned}$$

□

**2. Fórmula de reciprocidad de Fröbenius:** *Sea $H \subset G$ un subgrupo, $E$ un $G$-espacio vectorial y $E'$ un $H$-espacio vectorial y $T^2, T'^2$ las métricas definidas en $\mathcal{C}(G)$ y $\mathcal{C}(H)$ respectivamente. Se cumple la igualdad*

$$T^2(\chi_{k[G]\otimes_{k[H]}E'}, \chi_E) = T'^2(\chi_{E'}, Rest(\chi_E))$$

*donde $Rest(\chi_E)$ es la función $\chi_E$ restringida a $H$.*

*Demostración.* Por el lema anterior,

$$T^2(\chi_{k[G]\otimes_{k[H]}E'}, \chi_E) = \dim_k \operatorname{Hom}_{k[G]}(k[G]\otimes_{k[H]} E', E) = \dim_k \operatorname{Hom}_{k[H]}(E', E) = T'^2(\chi_{E'}, \chi_E)$$

□

Denotemos por $Cl(G)$ como la subálgebra de $C(G)$ formada por las aplicaciones que son constantes sobre cada clase de conjugación de $G$. Los caracteres $\chi_E$ son constantes sobre las clases de conjugación. Por dimensiones, una base de $Cl(G)$ la forman los $\chi_{E_i}$, $E_i$ irreducibles. Dado un subgrupo $H \subset G$ tenemos el morfismo natural de restricción $Rest : Cl(G) \to Cl(H)$, escribiremos $\chi_E \mapsto \chi_E$. Sea $Ind_H^G$ la aplicación que hace conmutativo el diagrama

$$\begin{array}{ccc} Cl(H) & \xrightarrow{Ind_H^G} & Cl(G) \\ \| T'^2 & & \| T^2 \\ Cl(H)^* & \xrightarrow{Rest^*} & Cl(G)^* \end{array}$$

El teorema de reciprocidad de Fröbenius dice que $Ind_H^G(\chi_E) = \chi_{k[G]\otimes_{k[H]}E}$.

Si $E'$ es un $G$-espacio vectorial entonces $Ind_H^G$ es un morfismo de $Cl(G)$-módulos, es decir, $Ind_H^G(\chi_E \cdot \chi_{E'}) = Ind_H^G(\chi_E) \cdot \chi_{E'}$, porque el morfismo

$$k[G] \otimes_{k[H]} (E \otimes_k E') = (k[G] \otimes_{k[H]} E) \otimes_k E',\ g \otimes (e \otimes e') \mapsto (g \otimes e) \otimes ge'$$

es un isomorfismo. Por tanto, $Cl(H)$ a través de $Ind_H^G$ es un ideal de $Cl(G)$.

**3. Teorema Artin:** *Sea $X$ una familia de subgrupos de $G$. La unión de los subgrupos conjugados pertenecientes a $X$ es igual a $G$ si y sólo si todo carácter es combinación lineal con coeficientes racionales de caracteres inducidos por subgrupos de $X$ ($\operatorname{car} k = 0$).*

*Demostración.* La unión de los subgrupos conjugados pertenecientes a $X$ es igual a $G$ si y sólo si la aplicación natural $Rest\colon Cl(G) \to \bigoplus_{H\in X} Cl(H)$ es inyectiva, que equivale a decir que $Rest^*\colon \bigoplus_{H\in X} Cl(H)^* \to Cl(G)^*$ es epiyectiva, que por el teorema de reciprocidad de Fröbenius equivale a que $\bigoplus_{H\in X} Ind_H^G\colon \bigoplus_{H\in X} Cl(H) \to Cl(G)$ sea epiyectiva.

Evidentemente, si todo carácter es combinación lineal con coeficientes racionales de caracteres inducidos por subgrupos de $X$, $\bigoplus_{H\in X} Ind_H^G\colon \bigoplus_{H\in X} Cl(H) \to Cl(G)$ es epiyectiva. Recíprocamente, supongamos que esta aplicación es epiyectiva y sea $\{Ind_H^G(\chi_V)\}$ una base. Sean $E_i$ los $G$-espacios vectoriales irreducibles. Tenemos que $k[G] \otimes_{k[H]} V = \bigoplus_i E_i^{m_i}$ y $Ind_H^G(\chi_V) = \sum_i m_i \chi_{E_i}$. Por tanto, $\chi_{E_i}$ es una combinación lineal con coeficientes racionales de los $Ind_H^G(\chi_V)$.

□

**4. Corolario :** *Cada carácter de $G$ es combinación lineal con coeficientes racionales de caracteres inducidos por caracteres de subgrupos cíclicos de $G$*

Sea $E$ un $H$-espacio vectorial. Consideremos la representación $G$-lineal inducida por $H$, $k[G]\otimes_{k[H]} E = \bigoplus_{\bar{g}\in G/H} g\cdot E$. Consideremos ésta como $H$-espacio vectorial. Tenemos que $H$ por traslaciones por la izquierda permuta los $g\cdot E$. Se cumple que $H_g = (gHg^{-1})\cap H$ es el grupo de isotropía de $gE$. Por tanto, tendremos

$$k[G]\otimes_{k[H]} E = \bigoplus_{\bar{g}\in G/H} g\cdot E = \bigoplus_{\bar{g}\in H\backslash G/H}\ \bigoplus_{\bar{h}\in H/H_g} hg\cdot E = \bigoplus_{\bar{g}\in H\backslash G/H} k[H]\otimes_{k[H_g]} gE$$

donde $H\backslash G/H$ es el conjunto de clases $HgH$ de $G$. La representación de $H_g$ como endomorfismos de $gE$ es como sigue: $h\cdot ge = g(g^{-1}hg)e$. A través del isomorfismo obvio $gE = E$, la representación lineal de $H_g$ como endomorfismos de $E$, $\rho_g$, es la conjugada por $g$, de la restricción de la representación lineal $\rho$ de $G$ a $H_g$.

**5. Criterio de irreducibilidad de Mackey:** *Sigamos las notaciones previas. La representación $G$-lineal $Ind_H^G(\rho)$, inducida por la representación $H$-lineal $\rho$, es irreducible $\iff$ $\rho$ es irreducible y para todo $g\in G-H$, $\rho_g$ es disjunta con la restricción de $\rho$ a $H_g$.*

*Demostración.* Un $G$-espacio vectorial $V$ es irreducible si y sólo si $\dim_k \mathrm{Hom}_{k[G]}(V,V) = 1$.

$$\begin{aligned}\mathrm{Hom}_{k[G]}(k[G]\otimes_{k[H]} E, k[G]\otimes_{k[H]} E) &= \mathrm{Hom}_{k[H]}(E, k[G]\otimes_{k[H]} E)\\ &= \mathrm{Hom}_{k[H]}(E, \sum_{g\in H\backslash G/H} k[H]\otimes_{k[H_g]} gE) = \sum_{g\in H\backslash G/H}\mathrm{Hom}_{k[H_g]}(E, gE)\end{aligned}$$

Por tanto, $k[G]\otimes_{k[H]} E$ es irreducible si y sólo si $E$ es $H$-irreducible y es disjunto con todo $gE$ para $g\in G-H$.

□

Reescribamos la fórmula de reciprocidad de Frobenius y el teorema de Artin.

Sea $K$ el $\mathbb{Z}$-módulo libre de base las representaciones $k$-lineales de $G$, $F$ el submódulo generado por $E-E_1-E_2$, donde $0\to E_1\to E\to E_2\to 0$ es una sucesión exacta de $G$-espacios vectoriales. Diremos que $R(G) := K/F$ es el anillo de representaciones $k$-lineales de $G$. $R(G)$ es un $\mathbb{Z}$-módulo libre de base las representaciones lineales irreducibles de $G$. $R(G)$ es un anillo, con la suma directa y el producto tensorial de representaciones lineales. En $R(G)$ podemos definir la métrica

$$\langle E_1, E_2\rangle := \dim_k \mathrm{Hom}_{k[G]}(E_1,E_2) = \dim_k (E_1^*\otimes E_2)^G$$

que es no singular porque las representaciones irreducibles forman una base ortogonal. Dado un morfismo de grupos $\phi\colon G\to G'$, sean $\phi_*\colon R(G)\to R(G')$, $E\mapsto k[G']\otimes_{k[G]} E$ y $\phi^*\colon R(G')\to R(G)$, $E\mapsto E$, que es un morfismo de anillos. Se cumple que $(\phi\circ\phi')_* = \phi_*\circ\phi'_*$ y $(\phi\circ\phi')^* = \phi'^*\circ\phi^*$. Se cumple la fórmula de proyección

$$\phi_*(E\otimes\phi^*E') = \phi_*E\otimes E'$$

porque $k[G']\otimes_{k[G]}(E\otimes E') = (k[G']\otimes_{k[G]} E)\otimes E'$, $g'\otimes(e\otimes e')\mapsto (g'\otimes e)\otimes g'e'$. Por tanto, $\phi_*$ es un morfismo de $R(G')$-módulos. Si consideramos el morfismo $\phi\colon 1\to G$, entonces $\phi^*\colon R(G)\to R(1)=\mathbb{Z}$, $E\mapsto \dim_k E$. Si consideramos el morfismo $\pi\colon G\to 1$, entonces $\pi_*\colon R(G)\to R(1)$, $E\mapsto E^G$, (porque $k\otimes_{k[G]} E = E^G$, pues $\mathrm{Hom}_k(E^G,E') = \mathrm{Hom}_G(E,E')$, donde $G$ opera en $E'$ trivialmente). Así pues,

si aplicamos $\pi_*$ a la fórmula de proyección $\phi_*(E \otimes \phi^* E'^*) = \phi_* E \otimes E'^*$, obtenemos la fórmula de reciprocidad de Frobenius

$$\langle E, \phi^* E' \rangle = \langle \phi_* E, E' \rangle$$

que por otra parte es de demostración inmediata.

Recordemos que en $C(G)$ tenemos definida la métrica: $\langle f, h \rangle := \frac{1}{n} \int f(g) h(g^{-1}) dg$.

**6. Proposición:** *La aplicación,*

$$R(G) \otimes_{\mathbb{Z}} k \to Cl(G),\ E \mapsto \chi_E$$

*define una isometría de $R(G) \otimes_{\mathbb{Z}} k$ con su imagen. Ésta aplicación es epiyectiva, si las raíces $n$-ésimas de la unidad pertenecen a $k$.*

Dado un subgrupo $\phi\colon H \hookrightarrow G$, el morfismo de restricción en $Cl(G) \to Cl(H)$ define en $R(G)$, $\phi^*$.

**7. Artin:** *Sea $\{H_i\}$ una familia de subgrupos de $G$. Si $G$ es igual a la unión de todos los conjugados de todos los $H_i$ de la familia, entonces la aplicación*

$$\oplus \phi_{i*}\colon \bigoplus_i R(H_i) \otimes_{\mathbb{Z}} \mathbb{Q} \to R(G) \otimes_{\mathbb{Z}} \mathbb{Q}$$

*es epiyectiva, donde los $\phi_i\colon H_i \hookrightarrow G$ son las inclusiones naturales.*

## 2.7 Teorema de Brauer

En esta sección queremos probar el teorema de Brauer, que dice que todo carácter es combinación $\mathbb{Z}$-lineal de caracteres inducidos por caracteres de representaciones lineales de grado 1. Seguiremos literalmente a Serre, en Linear Representations of Finite Groups.

**1. Proposición:** $Ind_H^G(\chi_E)(x) = \chi_{k[G] \otimes_{k[H]} E}(x) = \sum_{\substack{\bar{g} \in G/H \\ g^{-1} x g \in H}} \chi_E(g^{-1} x g)$.

*Demostración.* $k[G] \otimes_{k[H]} E = \sum_{\bar{g} \in G/H} gE$. El endomorfismo multiplicar por $x$ sólo tendrá traza no nula sobre los sumandos $gE$ tales que $x(gE) = gE$. Por tanto, habrá de ser $\overline{xg} = \bar{g}$ en $G/H$. Es decir, $g^{-1} x g \in H$. Además, $x(ge) = g(g^{-1} x g e)$, es decir, el endomorfismo multiplicar por $x$ en $gE$, es el endomorfismo multiplicar por $g^{-1} x g$ en $E$. Ahora es sencillo concluir.

□

Sea $C \subset G$ un grupo cíclico de orden $n$. Sea $\theta_C\colon C \to \mathbb{Z}$ la aplicación definida por

$$\theta_C(g) = \begin{cases} 0 & \text{si } g \text{ no genera } C \\ n & \text{si } g \text{ genera } C \end{cases}$$

**2. Proposición:** *Sea $X$ el conjunto de los subgrupos cíclicos de $G$. Se cumple que*

$$\#G = \sum_{C \in X} Ind_C^G(\theta_C)$$

*Demostración.* $Ind_C^G(\theta_C)(g) = \#\{h \in G\colon hgh^{-1} \text{ genera } C\}$. Como para cada $h \in G$, $hgh^{-1}$ genera un único grupo cíclico, tenemos que

$$\sum_{C \in X} Ind_C^G(\theta_C)(g) = \#G$$

□

**3. Proposición:** *$\theta_C$ es combinación lineal con coeficientes enteros de caracteres de $C$.*

*Demostración.* Procedamos por inducción sobre el orden de $C$. Si el orden de $C$ es uno la proposición es obvia. En general, sea $X$ el conjunto de los subgrupos cíclicos de $C$. Por la proposición anterior

$$\#C = \sum_{C' \in X} Ind_{C'}^C(\theta_{C'})$$

y $\theta_C = \#C - \sum_{\substack{C' \subseteq C \\ \neq}} Ind_{C'}^C(\theta_{C'})$. Hemos concluido por inducción. □

**Notación:** Denotaremos $Cl_A(G)$ a las aplicaciones $f\colon G \to A$ constantes sobre cada clase de conjugación de $G$.

**4. Proposición:** *Si $f \in Cl_{\mathbb{Z}}(G)$ y es divisible por $n = \#G$, entonces es una combinación $\mathbb{Z}[\xi_n]$-lineal de caracteres inducidos por subgrupos cíclicos de $G$.*

*Demostración.* Sabemos que $n = \sum_C Ind_C^G(\theta_C)$. Por tanto,

$$f = n\chi = (\sum_C Ind_C^G(\theta_C)) \cdot \chi = \sum_C Ind_C^G(\theta_C \cdot \chi)$$

Como $\theta' = \theta_C \cdot \chi\colon C \to \mathbb{Z}$ es divisible por el orden de $C$, tenemos que $T^2(\theta', \chi_E) \in \mathbb{Z}[\xi_n]$, para todo carácter $\chi_E$, luego $\theta'$ es combinación $\mathbb{Z}[\xi_n]$-lineal de caracteres de $C$ y hemos concluido.

□

Dado $g \in G$, sea $p^n \cdot m$, $p$ primo y $(m,p) = (1)$, el orden de $g$. El grupo $\langle g \rangle$ es el producto directo de un grupo cíclico de orden $p^n$ por un grupo cíclico de orden $m$, de modo único. Tendremos una descomposición única $g = g_{p'} \cdot g_p$, de modo que $g_{p'} \cdot g_p = g_p \cdot g_{p'}$, $\text{ord}(g_{p'}) = m$ y $\text{ord}(g_p) = p^n$.

**5. Lema:** *Sea $\chi \in Cl_{\mathbb{Z}}(G)$ que sea combinación $\mathbb{Z}[\xi_n]$-lineal de caracteres de $G$. Se cumple que*

$$\chi(g) \equiv \chi(g_{p'}) \mod p$$

*Demostración.* Restringiéndonos al grupo generado por $g$, podemos suponer que $G$ es cíclico. Escribamos $\chi = \sum a_i\chi_i$, con $a_i \in \mathbb{Z}[\xi_n]$ y $\chi_i$ caracteres irreducibles (de grado 1). Para $q = p^n >> 0$, tenemos que $g^q = g_{p'}^q$ y por tanto que $\chi_i(g)^q = \chi_i(g_{p'})^q$. Luego

$$\begin{aligned}\chi(g)^q = (\sum a_i\chi_i(g))^q &\equiv \sum a_i^q\chi_i(g)^q \equiv \sum a_i^q\chi_i(g_{p'})^q \\ &\equiv \chi(g_{p'})^q \mod p\mathbb{Z}[\xi_n]\end{aligned}$$

Como $p\mathbb{Z}[\xi_n] \cap \mathbb{Z} = p\mathbb{Z}$ entonces $\chi(g)^q \equiv \chi(g_{p'})^q \mod p$. Por tanto, $\chi(g) \equiv \chi(g_{p'}) \mod p$, ya que elevar a $p$ es la identidad en $\mathbb{Z}/p\mathbb{Z}$. □

Si $g$ es un elemento de orden $m$, con $(m,p)=1$, diremos que es un $p'$-elemento. Denotemos $Z(g)=\{g'\in G\colon g'g=gg'\}$. Sea $Z(g)_p$ un p-grupo de Sylow de $Z(g)$ y $H=\langle g\rangle\times Z(g)_p$, grupo que se denomina grupo $p$-elemental asociado a $g$, y es único salvo conjugaciones en $Z(g)$.

**6. Lema:** *Sea $g\in G$ un $p'$-elemento y $H$ un grupo $p$-elemental asociado a $g$. Existe una $f\in Cl_{\mathbb{Z}}(H)$ que es combinación $\mathbb{Z}[\xi_n]$-lineal de caracteres de $G$, tal que $Ind_H^G(f)=f'$ cumple*

1. *$f'(g)\not\equiv 0 \mod p$.*
2. *$f'(g')=0$ para cada $p'$-elemento que no sea conjugado de $g$.*

*Demostración.* Sea $m=\mathrm{ord}(g)$ y $C=\langle g\rangle$. La función $m\cdot\delta_g\colon C\to\mathbb{Z}$, es constante sobre cada clase de conjugación y $T_2(m\delta_g,\chi_E)=\chi_E(g^{-1})$, para cada carácter de $C$. Por tanto, $m\cdot\delta_g$ es combinación $\mathbb{Z}[\xi_n]$-lineal de caracteres de $C$.

La función $f\colon H=C\times P\to\mathbb{Z}$, definida por $f(c,p)=m\cdot\delta_g(c)$, es combinación $\mathbb{Z}[\xi_n]$-lineal de caracteres de $H$. Veamos que verifica las condiciones del lema:

Si $g'$ es un $p'$-elemento que no es conjugado de $g$, entonces no es conjugado de ningún elemento de $g\times P$ y $f'(g')=Ind_H^G(f)(g')=0$. Igualmente,

$$f'(g)=\sum_{\substack{\bar{s}\in G/H\\ s^{-1}gs=g}} f(g)=\sum_{\bar{s}\in Z(g)/H} f(g)=\#(Z(g)/P)$$

que es primo con $p$, pues $P$ es un $p$-subgrupo de Sylow de $Z(g)$.

□

**7. Lema :** *Existe una $f\in Cl_{\mathbb{Z}}(G)$ que es combinación $\mathbb{Z}[\xi_n]$-lineal de caracteres inducidos por $p$-grupos elementales, tal que $f(g)\neq 0 \mod p$, para toda $g\in G$.*

*Demostración.* Sea $\{g_i\}$ un sistema de representantes de las clases de conjugación de $p'$-elementos. Por el lema anterior existen $f_i'\in Cl_{\mathbb{Z}}(G)$, que es combinación $\mathbb{Z}[\xi_n]$-lineal de caracteres, de modo que $f_i'(g_j)=\delta_{ij} \mod p$. Sea $\phi=\sum_i f_i$, que pertenece a $Cl_{\mathbb{Z}}(G)$ y es combinación $\mathbb{Z}[\xi_n]$-lineal de caracteres de $G$. Dado $g\in G$, escribamos $g=g_pg_{p'}$ y sea $g_i$ el conjugado de $g_{p'}$. Por el lema 2.7.5

$$\phi(g)\equiv\phi(g_{p'})\equiv\phi(g_i)\not\equiv 0 \mod p$$

□

**8. Teorema Brauer:** *Todo carácter es combinación lineal con coeficientes enteros de caracteres inducidos por caracteres de grado* 1.

*Demostración.* Basta probar que son combinación lineal con coeficientes enteros de caracteres inducidos por caracteres de grupos $p$-elementales, pues los grupos $p$-elementales son superresolubles y todo carácter de estos grupos es inducido por una combinación lineal de caracteres de grado 1, por 2.5.5.

Sea $\chi\in Cl_{\mathbb{Z}}(G)$, que sea combinación $\mathbb{Z}[\xi_n]$-lineal de caracteres inducidos por $p$-grupos elementales, tal que $\chi(g)\neq 0 \mod p$, para toda $g\in G$. Si $p^n\cdot m=\#G$, $(m,p)=1$, sea $N=\#(\mathbb{Z}/p^n\mathbb{Z})$. Entonces, $\chi^N(g)=1 \mod p$, para todo $g\in G$. Se cumple que $m\cdot(\chi^N-1)$ es múltiplo de $\#G$. Por la proposición 2.7.4, $m\cdot(\chi^N-1)$ es combinación $\mathbb{Z}[\xi_n]$-lineal de caracteres inducidos por caracteres de grupos cíclicos. Luego $m$ es combinación $\mathbb{Z}[\xi_n]$-lineal de caracteres inducidos por caracteres de grupos $p$-elementales. Variando $p$ si es necesario, obtenemos que 1 es combinación $\mathbb{Z}[\xi_n]$-lineal de caracteres inducidos por

caracteres de grupos $p$-elementales. Ahora bien, 1 es el carácter definido por la representación lineal trivial, por tanto 1 es combinación $\mathbb{Z}[\xi_n] \cap \mathbb{Q} = \mathbb{Z}$-lineal de caracteres inducidos por caracteres de grupos $p$-elementales.

Los caracteres inducidos por las caracteres de un subgrupo, forman un ideal dentro del conjunto de todos los caracteres. Como el 1 es combinación $\mathbb{Z}$-lineal de caracteres inducidos por caracteres de grupos $p$-elementales, tendremos que todo carácter de $G$ es combinación $\mathbb{Z}$-lineal de caracteres inducidos por caracteres de grupos $p$-elementales.

□

## 2.8 Representaciones lineales sobre cuerpos no algebraicamente cerrados

En esta sección supondremos que el cuerpo es de característica cero, aunque no necesariamente algebraicamente cerrado.

Sabemos que $k[G]$ es semisimple, y por el teorema de Wedderburn $k[G] = \mathrm{End}_{K_1}(E_1) \times \cdots \times \mathrm{End}_{K_r}(E_r)$. Los $E_i$ son todas las representaciones irreducibles de $G$ desisomorfas entre sí. La representación de $G$ como endomorfismos $k$-lineales de $E$ es la composición de los morfismos naturales $G \to \mathrm{End}_{K_i}(E_i) \subset \mathrm{End}_k(E_i)$. Sea $\mathrm{tr}_{K_i} \colon K_i \to k$ la traza, se cumple que

$$\chi_{E_i}(g) = \mathrm{tr}_{K_i}(\mathrm{tr}(g_{rs})) = \sum_r \mathrm{tr}_{K_i}(g_{rr})$$

donde $(g_{ij})$ es la matriz de $g$ como endomorfismo $K_i$-lineal de $E_i$.

Igualmente, la métrica $T_2$ de $k[G]$ cumple que $T^2(\chi_{E_i}) = \frac{\mathrm{Id}_i}{n_i}$ (con $n_i = \dim_{K_i} E_i$) y tendremos que $T^2(\chi_{E_i}, \chi_{E_j}) = \dim_k K_i \cdot \delta_{ij}$.

**1. Definición:** Sea $k \hookrightarrow K$ una extensión de cuerpos. Diremos que una representación $K$-lineal $G \to \mathrm{End}_K(E)$ es realizable sobre $k$, si existe un $k$-espacio vectorial $E'$ y una representación $k$-lineal de $G$ en los endomorfismos de $E'$, de modo que $E = E' \otimes_k K$ como $G$-espacios vectoriales.

**2. Ejercicio:** Probar que todas las representaciones $\mathbb{C}$-lineales del grupo diédrico son $\mathbb{R}$-realizables.

Denotemos por $R_K(G)$ la $\mathbb{Z}$-álgebra generada por los caracteres asociados a las representaciones $K$-lineales. Diremos que $R_K(G)$ es el anillo de las representaciones $K$-lineales de $G$. Dada una extensión de cuerpos $k \to K$, el morfismo $R_k(G) \to R_K(G)$, $\chi_E \mapsto \chi_{E \otimes_k K}$ es un morfismo inyectivo de anillos, porque

$$T^2(\chi_E, \chi_{E'}) = T^2(\chi_{E \otimes_k K}, \chi_{E' \otimes_k K})$$

Además, es isomorfismo si y sólo si toda representación $K$-lineal es realizable sobre $k$: Si es isomorfismo entonces dado un carácter sobre $K$, $\chi_E$ tendremos que $\chi_E = \sum_i n_i \chi_{E_i \otimes_k K}$, con $n_i \in \mathbb{Z}$, ahora bien, $0 \leq T^2(\chi_E, \chi_{E_j \otimes_k K}) = n_j \dim_k K_j$, luego $n_j > 0$ y $E = (\oplus_i E_i^{n_i}) \otimes_k K$.

**3. Teorema:** *Toda representación lineal de un grupo $G$ de orden $n$ sobre un cuerpo algebraicamente cerrado, de característica $p$ que no divide a $n$, es realizable sobre $\mathbb{Q}[\xi_n]$, si $p = 0$ o $\mathbb{Z}/p\mathbb{Z}[\xi_n]$ si $p \neq 0$.*

*Demostración.* El anillo de las representaciones $k[\xi_n]$-lineales de $G$ es un subanillo del anillo de las representaciones $\bar{k}$-lineales de $G$. Ahora bien, toda representación $\bar{k}$-lineal de $G$, inducida por una representación $\bar{k}$-lineal de $G$ de grado uno es realizable sobre $k[\xi_n]$, y éstas generan el anillo de las

representaciones $\bar{k}$-lineales de $G$. En conclusión, el anillo de las representaciones $\bar{k}$-lineales de $G$ coincide con el anillo de las representaciones $k[\xi_n]$-lineales de $G$ y hemos concluido.

Demos otra demostración que no dependa del teorema de Brauer. Sea $k = \mathbb{Z}/p\mathbb{Z}[\xi_n]$, $\operatorname{car} k = p > 0$. Sabemos que $k[G] = \operatorname{End}_{K_1}(E_1) \times \ldots \times \operatorname{End}_{K_n}(E_n)$, donde los $K_i$ son cuerpos conmutativos. Tenemos que demostrar que $K_i = k$.

Consideremos el morfismo traza obvio $\operatorname{tr}\colon \operatorname{End}_{K_1}(E_1) \to K_1$. Componiendo este morfismo con la proyección $k[G] \to \operatorname{End}_{K_1}(E_1)$ tenemos el epimorfismo $\operatorname{tr}\colon k[G] \to K_1$. Dado $g \in G$, tenemos que $E_1$ descompone en suma directa de $K_1$-espacios vectoriales sobre los $g$ es la homotecia por una raíz $n$-ésima de la unidad. Sobre esta base, es claro que $\operatorname{tr}(g) \in k$. Por tanto, $\operatorname{tr}(k[G]) = k$ y $K_1 = k$.

MAL:Sea ahora $k = \mathbb{Q}[\xi_n]$ y $\bar{k}$ su cierre algebraico. Sabemos que $\bar{k}[G] = \operatorname{End}_{\bar{k}}(E_1) \times \ldots \times \operatorname{End}_{\bar{k}}(E_n)$ y los caracteres $\chi_{E_i}\colon G \to \bar{k}$ valoran en $k$, luego podemos decir que $\chi_{E_i} \in k[G]^*$. Éstos descomponen $k[G]$ en producto de $n$-álgebras (la unidad de cada álgebra es $T^2(n_i\chi_{E_i}) = \mathrm{Id}_i$, y esta álgebra coincide con el incidente $(\sum_{i\neq j} k[G]\cdot\chi_{E_i})^0$). Tenemos pues, $k[G] = \operatorname{End}_{K_1}(E_1') \times \ldots \times \operatorname{End}_{K_n}(E_n')$, donde cada $K_i$ es un cuerpo no conmutativo que es álgebra de Azumaya, digamos de dimensión $m_i^2$. Sea $D_i$ una subextensión conmutativa de $K_i$ de dimensión $m_i$. Los $E_i'$ son $D_i$-espacios vectoriales, podemos definir los morfismos traza $\operatorname{tr}\colon \operatorname{End}_{K_i}(E_i) \to D_i$ y de nuevo tenemos que $\operatorname{tr}(k[G]) = k$, luego $D_i = k$ y $K_i = k$.

□

Sea $Gal \subseteq (\mathbb{Z}/n\mathbb{Z})^*$ el grupo de Galois de la extensión $k \hookrightarrow k[\xi_n]$. Consideremos la siguiente acción de $Gal$ en $G$: $m \cdot g = g^m$, para $m \in Gal \subseteq (\mathbb{Z}/n\mathbb{Z})^*$ y $g \in G$. Además, la acción de $G$ en $G$ por conjugación conmuta con la acción de $Gal$, por tanto, tenemos una acción natural de $G \times Gal$ en $G$.

**4. Proposición:** *Sean $\chi \in R_{\bar{k}}(G)$ y $t \in Gal$. Se cumple*

$$t(\chi(g)) = \chi(t \cdot g)$$

*para todo $g \in G$.*

*Demostración.* Podemos suponer que $\chi = \chi_E$. Tenemos que $\chi_E(g) = \sum_i w_i$, donde las $w_i$ son los valores propios del endomorfismo de $E$ definido por $g$, que son raíces $n$-ésimas de la unidad. Entonces, $t(\chi(g)) = \sum_i w_i^t = \chi(g^t) = \chi(t \cdot g)$.

□

**5. Corolario:** *$\chi \in R_{\bar{k}}(G)$ toma valores en $k \iff \chi(t \cdot g) = \chi(g)$, para todo $g \in G$ y $t \in Gal$.*

Dada una extensión finita $k \hookrightarrow K$ consideremos el morfismo de la traza $\operatorname{tr}\colon K \to k$. Sea $E$ un $K$-espacio vectorial y $\rho\colon G \to \operatorname{End}_K(E)$ una representación lineal. Denotemos $\chi_E^K$ el carácter asociado. Podemos considerar $E$ como $k$-espacio vectorial y $\rho$ como una $k$-representación lineal de $G$, sea $\chi_E^k$ el carácter asociado. Se cumple que $\operatorname{tr} \circ \chi_E^K = \chi_E^k$. Tenemos pues los dos morfismos naturales $i\colon R_k(G) \to R_K(G)$, $\chi_E \mapsto \chi_{E\otimes_k K}$ y $j\colon R_K(G) \to R_k(G)$, $\chi_E^K \mapsto \chi_E^k$. Se cumple que $j \circ i = n\cdot$ $(n = \dim_k K)$ y $i \circ j = \operatorname{tr}$.

**6. Teorema:** *$R_k(G) \otimes_{\mathbb{Z}} k$ es igual al espacio vectorial de las funciones sobre $G$ constantes sobre las clases en $G$ por la acción de $G \times Gal$.*

*Demostración.* Sea $K = k[\xi_n]$. El diagrama

$$R_k(G) \otimes_{\mathbb{Z}} K \overset{i\otimes 1}{\hookrightarrow} R_K(G) \otimes_{\mathbb{Z}} K \overset{j\otimes 1}{\to} R_k(G) \otimes_{\mathbb{Z}} K \overset{i\otimes 1}{\hookrightarrow} R_K(G) \otimes_{\mathbb{Z}} K$$

nos permite pensar identificar $R_k(G)\otimes_{\mathbb{Z}} K$ (vía $i\otimes 1$) con $tr(R_K(G)\otimes_{\mathbb{Z}} K)$. Ahora bien, $R_K(G)\otimes_{\mathbb{Z}} K$ coincide con las funciones de $G$ sobre $K$, constantes sobre las clases por la acción por conjugación de $G$ y $R_k(G)\otimes_{\mathbb{Z}} K = tr(R_K(G)\otimes_{\mathbb{Z}} K)$ con las funciones de $G$ en $K$ constantes sobre las clases en $G$ por la acción de $G\times Gal$.

Así pues, $R_k(G)\otimes_{\mathbb{Z}} k$ es igual al espacio vectorial de las funciones sobre $G$ constantes sobre las clases en $G$ por la acción de $G\times Gal$. □

**7. Corolario :** *El número de representaciones irreducibles de $G$ sobre $k$ es igual al número de $G\times Gal$-clases de $G$.*

**8. Corolario :** *Todos los caracteres de las representaciones $\bar{k}$-lineales de $G$ toman valores sobre $k$ si y sólo las clases de conjugación sobre $G$ coinciden con las $G\times Gal$-clases.*

**9. Corolario :** *El número de representaciones irreducibles de $G$ sobre $\mathbb{Q}$ es igual al número de clases de conjugación de subgrupos cíclicos de $G$.*

**10. Lema :** *Si $\theta\in R_{\mathbb{Q}}(G)$ cumple que $\sum_{g\in C}\theta(g)=0$, para todo subgrupo cíclico $C$ de $G$, entonces $\theta=0$.*

*Demostración.* Procedamos por inducción sobre el orden de $G$. Podemos suponer que $G$ es cíclico, porque si no lo es, por inducción $\theta=0$ al restringirla a todo subgrupo cíclico, luego es nula. Escribamos $G=\langle g\rangle$. Si $g'\in G$, no genera $G$, la restricción de $\theta$ al subgrupo generado por $g'$ es nula, luego $\theta(g')=0$. Si $g'$ genera $G$ entonces pertenece a la misma $G\times Gal$-clase que $g$ luego $\theta(g)=\theta(g')$. Por tanto,

$$0=\sum_{g'\in\langle g\rangle}\theta(g')=n\theta(g)$$

Luego $\theta(g)=0$ y $\theta=0$. □

**11. Proposición :** *Todo $\chi\in R_{\mathbb{Q}}(G)$ es combinación lineal con coeficientes en $\mathbb{Q}$ de caracteres $Ind_C^G(1_C)$, donde $C$ es un subgrupo cíclico de $G$ y $1_C$ es su carácter unidad.*

*Demostración.* Si $T^2(\theta, Ind_C^G(1_C)) = T^2(\theta_{|C}, 1_C) = \frac{1}{\#C}\sum_{g\in C}\theta(g)$ es nula para todo subgrupo cíclico $C$ de $G$, entonces $\theta=0$. Por tanto, $\theta$ es combinación lineal con coeficientes en $\mathbb{Q}$ de los caracteres $Ind_C^G(1_C)$. □

**12. Proposición :** *Sean $E$ y $E'$ dos $\mathbb{Q}$-espacios vectoriales sobre los que opera $G$. Se cumple que $E$ es isomorfo a $E'$ como $G$-espacios vectoriales $\iff \dim_{\mathbb{Q}} E^C = \dim_{\mathbb{Q}} {E'}^C$, para todo grupo cíclico $C$.*

*Demostración.* $T^2(\chi_E, Ind_C^G(1_C)) = T^2((\chi_E)_{|C}, 1_C) = \dim_{\mathbb{Q}} E^C$. $E$ es isomorfo a $E'$ si y sólo si $\chi_E=\chi_{E'}$, $\chi_E=\chi_{E'}$ si y sólo si $T_2(\chi_E,-)=T_2(\chi_{E'},-)$ y se tiene esta igualdad si y sólo si $\dim_{\mathbb{Q}} E^C = \dim_{\mathbb{Q}} {E'}^C$. □

**13. Ejercicio :** Si toda representación lineal de $G$ es $\mathbb{R}$-realizable, probar que

$$\sum_i n_i = \#\{g\in G \mid g^2=1\}$$

donde los $n_i$ son los grados de las representaciones lineales irreducibles. (Cálculese la signatura de la métrica de la traza de $\mathbb{R}[G]$).

## 2.9 Teoría de invariantes

**1. Definición:** Diremos que un grupo $G$ (finito o no) es linealmente semisimple si todo $G$-espacio vectorial es semisimple.

**2. Teorema:** *$G$ es linealmente semisimple si y sólo si el funtor "tomar invariantes" es exacto.*

*Demostración.* Si $G$ es semisimple, toda sucesión exacta de $G$-módulos rompe, y es claro que la toma de invariantes es exacta. Recíprocamente, supongamos que la toma de invariantes es exacta. Dado un morfismo epiyectivo de $G$-módulos $\pi\colon M \to M'$, consideremos el epimorfismo inducido

$$\pi_*\colon \operatorname{Hom}_k(M', M) \to \operatorname{Hom}_k(M', M')$$

donde $G$ opera por conjugación, es decir, $g * f(m) = g \cdot (f(g^{-1}m))$. Tomando invariantes, se obtienen exactamente los morfismos de $G$-módulos y, por tanto, la identidad tiene alguna antiimagen, que es morfismos de $G$-módulos. En conclusión, $\pi$ tiene sección, y toda sucesión exacta de $G$-módulos rompe y $G$ es semisimple.

□

Si $G$ es semisimple y $E$ es un $G$-espacio vectorial, entonces $E = E^G \oplus E^M$, donde $E^G$ son los invariantes de $E$ por $G$ y $E^M$ es la suma de todos los submódulos simples no invariantes, es decir, es el máximo submódulo de $E$ que no contiene vectores no nulos invariantes. Además, dado un morfismo $f\colon E \to E'$ de $G$-espacios vectoriales, entonces $f(E^G) \subseteq {E'}^G$ y $f(E^M) \subset {E'}^M$. La proyección natural $E \to E/E^M = E^G$ suele llamarse operador de Reynolds.

**3. Estabilidad de los invariantes:** *Sea $G$ un grupo linealmente semisimple que opera por automorfismos en un anillo $A$ y sea $A^G$ el subanillo de $A$ de invariantes por $G$. Sea $A^G \to B$ un morfismo de anillos. Se cumple que $(A \otimes_{A^G} B)^G = B$.*

*Demostración.* $A^M$ es un $A^G$-submódulo de $A$, pues dado $a \in A^G$, el morfismo $A \xrightarrow{a\cdot} A$ aplica $A^M$ en $A^M$. Los subespacios $A^M \otimes b \subseteq A^M \otimes_{A^G} B$, que son cocientes de $A^M$, no pueden contener vectores no nulos invariantes, luego $(A^M \otimes_{A^G} B)^G = 0$. En conclusión, $(A \otimes_{A^G} B)^G = (A^G \otimes_{A^G} B \oplus A^M \otimes_{A^G} B)^G = B$.

□

**4. Teorema:** *Sea $G$ un grupo linealmente semisimple, que opera por automorfismos en un anillo $A$. Sea $I \subseteq A^G$ un ideal. Se cumple que $(I \cdot A) \cap A^G = I$.*

*Demostración.* Consideremos en la proposición anterior $B = A^G/I$. Entonces, $(A/IA)^G = (A \otimes_{A^G} A^G/I)^G = A^G/I$, lo que implica que $(IA) \cap A^G = I$.

□

**5. Corolario:** *Sea $G$ un grupo linealmente semisimple, que opera por automorfismos en un anillo $A$. Sea $I \subseteq A^G$ un ideal. Se cumple que $(G_{IA}A)^G = G_I A^G$.*

**6. Corolario:** *Sea $G$ un grupo linealmente semisimple, que opera por automorfismos en un anillo $A$. Si $A$ es un anillo noetheriano entonces $A^G$ es noetheriano.*

**7. Corolario:** *Sea $G$ un grupo linealmente semisimple, que opera por automorfismos en una $k$-álgebra de tipo finito $A$. Supongamos que todo subespacio vectorial de dimensión finita, de cualquier $G$-espacio vectorial, está incluido en un $G$-subespacio vectorial de dimensión finita. Entonces, $A^G$ es una $k$-álgebra de tipo finito.*

*Demostración.* Si $B = \underset{n\in\mathbb{N}}{\oplus} B_n$, con $B_0 = k$ es una $k$-álgebra graduada de tipo finito, donde $G$ opera por automorfismos graduados, entonces $B^G$ también es de tipo finito: Una $k$-álgebra graduada $C = \underset{n\in\mathbb{N}}{\oplus} C_n$, con $C_0 = k$ es de tipo finito si y sólo si el ideal irrelevante es un $C$-módulo finito generado. Por tanto, una $k$-álgebra graduada $C = \underset{n\in\mathbb{N}}{\oplus} C_n$, con $C_0 = k$ es de tipo finito si y sólo si es un anillo noetheriano. Por tanto, como $B^G = \underset{n}{\oplus} B_n^G$, es noetheriana, por el corolario anterior y $B_0^G = k$, concluimos que $B^G$ es de tipo finito.

Escribamos $A = k[\xi_1, \ldots, \xi_n]$ y sea $E$ un $G$-subespacio vectorial de dimensión finita de $A$ que contenga a todos los $\xi_i$. La inclusión $E \hookrightarrow A$ de $G$-espacios vectoriales extiende a un morfismo de $k$-álgebras $B = S_k^{\cdot} E \to A$, de $G$-espacios vectoriales y epiyectivo. Tomando invariantes $A^G$ es un cociente de $B^G$, que por el párrafo anterior, es una $k$-álgebra de tipo finito. En conclusión, $A^G$ es una $k$-álgebra de tipo finito.

□

**8. Corolario :** *Sea $G$ un grupo linealmente semisimple, que opera por automorfismos en un anillo $A$. El morfismo*

$$\operatorname{Spec} A \to \operatorname{Spec} A^G$$

*es cociente topológico.*

*Demostración.* Denotemos $\pi\colon \operatorname{Spec} A \to \operatorname{Spec} A^G$. Dado $x \in \operatorname{Spec} A^G$, tenemos que $\pi^{-1}(x) = \operatorname{Spec} A_x/\mathfrak{p}_x A_x$. Por la estabilidad de los invariantes, tenemos que $A_x^G = (A_x)^G$ y por el teorema $\mathfrak{p}_x A_x \neq A_x$, pues $\mathfrak{p}_x A_x \cap A_x^G = \mathfrak{p}_x A_x^G$. En conclusión, $\pi^{-1}(x) \neq \emptyset$ y $\pi$ es epiyectivo.

Sea $D \subseteq \operatorname{Spec} A^G$ un subconjunto tal que $\pi^{-1}(D) = C$ sea un cerrado. Sea $I \subseteq A$ el ideal de todas las funciones que se anulan en todo $C$. Obviamente, $C$ es $G$-estable e $I$ es un $G$-módulo. Por la exactitud de la toma de invariantes, el morfismo $A^G \to (A/I)^G$ es epiyectivo, luego $(A/I)^G = A^G/I'$. Por el párrafo anterior, $D = \pi(C) = (I')_0$. En conclusión, $D$ es cerrado y $\pi$ es cociente topológico.

□

**9. Corolario :** *Sea $G$ un grupo linealmente semisimple, que opera por automorfismos en un anillo $A$. Si las órbitas de los puntos cerrados de* $\operatorname{Spec}_{max} A$ *son cerradas en* $\operatorname{Spec}_{max} A$ *entonces*

$$\operatorname{Spec}_{max} A^G = (\operatorname{Spec}_{max} A)/G.$$

*Demostración.* Dado un punto cerrado $x \in \operatorname{Spec} A^G$ tenemos que ver que $\pi^{-1}(x)$ es una órbita, donde $\pi\colon \operatorname{Spec} A \to \operatorname{Spec} A^G$ es el morfismo natural.

Por la estabilidad de los invariantes y la fórmula de la fibra $\pi^{-1}(x) = \operatorname{Spec} A_x/\mathfrak{p}_x A_x$, podemos suponer que $A^G = k$.

Si hubiera dos órbitas $C_1 = (\mathfrak{p}_1)_0$, $C_2 = (\mathfrak{p}_2)_0$, entonces $\mathfrak{p}_1 + \mathfrak{p}_2 = A$ y $0 + 0 = \mathfrak{p}_1^G + \mathfrak{p}_2^G = A^G = k$, lo que es contradictorio.

□

# Capítulo 3

# Grupos algebraicos y representaciones lineales

## 3.1 Funtor de puntos y grupos algebraicos

Una $k$-variedad algebraica (afín) es una pareja $(\operatorname{Spec} A, A)$ donde $A$ es una $k$-álgebra de tipo finito. Un morfismo entre variedades algebraicas $(\operatorname{Spec} A, A)$, $(\operatorname{Spec} A', A')$ es una pareja de morfismos $f\colon \operatorname{Spec} A \to \operatorname{Spec} A'$, $\phi\colon A' \to A$, de modo que $\phi$ sea un morfismo de $k$-álgebras y $f$ sea el morfismo inducido en los espectros por $\phi$. Por sencillez de escritura, dada una variedad algebraica $(\operatorname{Spec} A, A)$ escribiremos simplemente $\operatorname{Spec} A$, y un morfismo entre dos variedades algebraicas $X = \operatorname{Spec} A$, $X' = \operatorname{Spec} A'$ lo notaremos $X \to X'$. El conjunto de morfismos entre dos variedades algebraicas $X = \operatorname{Spec} A$, $X' = \operatorname{Spec} A'$, lo denotaremos $\operatorname{Hom}_{\text{var}}(X, X')$, que con rigor es el conjunto $\operatorname{Hom}_{k-\text{álg}}(A', A)$.

Por ejemplo, $\operatorname{Hom}_{\text{var}}(\operatorname{Spec} A, \mathbb{A}_1) = \operatorname{Hom}_{k-\text{álg}}(k[x], A) = A$.

Sea $X = \operatorname{Spec} A$ una $k$-variedad algebraica. El funtor $X^{\cdot}$ de la categoría de $k$-álgebras en la categoría de conjuntos definido por

$$X^{\cdot}(B) \underset{\text{def}}{=} \operatorname{Hom}_{k-\text{álg}}(A, B)$$

se le denomina funtor de puntos de $X$.

Si $X = \operatorname{Spec} k[x_1, \ldots, x_n]/(p_1(x_1, \ldots, x_n), \ldots, p_r(x_1, \ldots, x_n))$ entonces

$$\begin{aligned} X^{\cdot}(B) &= \operatorname{Hom}_{k-\text{álg}}(k[x_1, \ldots, x_n]/(p_1(x_1, \ldots, x_n), \ldots, p_r(x_1, \ldots, x_n)), B) \\ &= \left\{ \begin{array}{l} \text{Soluciones del sistema de ecuaciones} \\ p_1(x_1, \ldots, x_n) = 0, \ldots, p_r(x_1, \ldots, x_n) = 0 \\ \text{con valores en } B \end{array} \right. \end{aligned}$$

**1. Ejemplo:** Si en el plano afín, $\mathbb{A}_2 = \operatorname{Spec} k[x, y]$, consideramos las subvariedades $X = \operatorname{Spec} k[x, y]/(y) \equiv \{y = 0\}$ e $\operatorname{Spec} k[x, y]/(y^2) \equiv \{y^2 = 0\}$ tendremos que

$$X^{\cdot}(B) = \{(b_1, 0), b_1 \in B\} \text{ y } Y^{\cdot}(B) = \{(b_1, b_2)\colon b_2^2 = 0,\ b_1, b_2 \in B\}$$

Si $F$ un funtor sobre la categoría de $k$-álgebras y $B$ es una $k$-álgebra denotaremos $F(B) = F(\operatorname{Spec} B)$.

**2. Lema:** *Sea $F$ un funtor sobre la categoría de $k$-álgebras, $X = \operatorname{Spec} A$ una variedad algebraica y $X^{\cdot}$ el funtor de puntos de $X$. Se cumple*

$$\operatorname{Hom}_{funt}(X^{\cdot}, F) = F(X)$$

*Demostración.* Dado un morfismo $\theta\colon X^{\cdot} \to F$, está determinado por $\theta_X(\mathrm{Id}) \in F(X)$: Sea $Y = \operatorname{Spec} B$ y $f \in X^{\cdot}(Y) = \operatorname{Hom}_{\mathrm{var}}(Y, X) = \operatorname{Hom}_{k-\mathrm{álg}}(A, B)$. Si consideramos los diagramas

$$\begin{array}{ccc} X^{\cdot}(Y) & \xrightarrow{\theta_Y} & F(Y) \\ {\scriptstyle f_*}\uparrow & & \uparrow{\scriptstyle f_*} \\ X^{\cdot}(X) & \xrightarrow{\theta_X} & F(X) \end{array} \qquad \begin{array}{ccc} f & \dashrightarrow & \theta_Y(f) = f_*(\theta_X(\mathrm{Id})) \\ \uparrow & & \uparrow \\ \mathrm{Id} & \longrightarrow & \theta_X(\mathrm{Id}) \end{array}$$

concluimos. Recíprocamente, dado $s \in F(X)$, existe un único morfismo $\theta\colon X^{\cdot} \to F$ de modo que $\theta_X(\mathrm{Id}) = s$.

□

Como corolario inmediato obtenemos

**3. Lema de Yoneda:** $\operatorname{Hom}_{funt}(X^{\cdot}, Y^{\cdot}) = Y^{\cdot}(X) = \operatorname{Hom}_{var}(X, Y)$.

Así pues, dos variedades algebraicas son isomorfas si y sólo si tienen el mismo funtor de puntos. Este lema nos permite tratar a las variedades algebraicas como meros conjuntos de puntos.

**4. Ejercicio:** Sea $X = \operatorname{Spec} k[x_1, \ldots, x_n]/(p_1(x_1, \ldots, x_n), \ldots, p_r(x_1, \ldots, x_n))$ e $Y = \operatorname{Spec} B$. Probar que

$$\operatorname{Hom}_{\mathrm{var}}(X, Y) = \{(b_1, \ldots, b_n)\colon p_i(b_1, \ldots, b_n) = 0, \text{ para todo } i, \text{ con } b_j \in B, \text{ para todo } j\}$$

**5. Definición:** Si $X = \operatorname{Spec} A$ e $Y = \operatorname{Spec} B$ son dos $k$-variedades algebraicas, se define $X \times_k Y$ como la variedad algebraica que cumple que

$$(X \times_k Y)^{\cdot} = X^{\cdot} \times Y^{\cdot}$$

Se cumple que $X \times_k Y = \operatorname{Spec}(A \otimes_k B)$:

$$\begin{aligned} \operatorname{Hom}_{\mathrm{var}}(Z = \operatorname{Spec} C, X \times_k Y) &= \operatorname{Hom}_{\mathrm{var}}(Z, X) \times \operatorname{Hom}_{\mathrm{var}}(Z, Y) \\ &= \operatorname{Hom}_{k-\mathrm{álg}}(A, C) \times \operatorname{Hom}_{k-\mathrm{álg}}(B, C) = \operatorname{Hom}_{k-\mathrm{álg}}(A \otimes_k B, C) \\ &= \operatorname{Hom}_{\mathrm{var}}(Z, \operatorname{Spec}(A \otimes_k B)) \end{aligned}$$

**6. Definición:** Una variedad algebraica $G$ se dice que es un grupo algebraico si el funtor $G^{\cdot}$ valora en la categoría de grupos.

**7. Proposición:** *$G$ es un grupo algebraico si existen tres morfismos $\mu\colon G \times_k G \to G$, $\mathrm{inv}\colon G \to G$, $e\colon \operatorname{Spec} k \to G$, de modo que cumplen*

1. *La propiedad asociativa: $\mu \circ (\mu \times \mathrm{Id}) = \mu \circ (\mathrm{Id} \times \mu)$.*
2. *Elemento neutro: $\mu \circ (e \times \mathrm{Id}) = \mathrm{Id}$.*
3. *Elementos inversos: $\mu \circ (\mathrm{inv} \times \mathrm{Id}) = e \circ \pi$, donde $\pi\colon G \to \operatorname{Spec} k$ es la proyección estructural.*

*Demostración.* $G$ es un grupo algebraico si y sólo si $G^{\cdot}(T)$ es un grupo para todo $T = \operatorname{Spec} B$. Es decir, si para todo $T$, tenemos aplicaciones (funtoriales) $\mu_T \colon G^{\cdot}(T) \times G^{\cdot}(T) \to G^{\cdot}(T)$, $e_T \colon (\operatorname{Spec} k)^{\cdot}(T) \to G^{(}T)$, $\operatorname{inv}_T \colon G^{\cdot}(T) \to G^{\cdot}(T)$, cumpliendo las propiedades obvias. Por el lema de Yoneda concluimos que dar estas aplicaciones $\mu_T, e_T, \operatorname{inv}_T$, con las propiedades "obvias", equivale a definir $\mu, e, \operatorname{inv}$ cumpliendo las propiedades exigidas en la proposición. □

**8. Ejemplo:** 1. Sea $G_a$ el funtor definido por $G_a(B) = B$, que es un grupo con la operación + de $B$. Como $G_a = (\operatorname{Spec} k[x])^{\cdot}$, es un grupo algebraico, denominado grupo aditivo. Explícitamente,

$$\mu \colon G_a \times_k G_a \longrightarrow G_a$$

Con los puntos $\qquad (\alpha, \beta) \longrightarrow \alpha + \beta$

En los anillos $\qquad k[x] \otimes_k k[y] = k[x, y] \longleftarrow k[z]$

$$x + y \longleftarrow z$$

2. Sea $Gl_n$ el funtor definido por $Gl_n(B) = M_n(B)^*$, las matrices invertibles con coeficientes en $B$. $Gl_n(B)$ es un grupo con el producto de matrices. Como $Gl_n = (\operatorname{Spec} k[x_{ij}, \frac{1}{\det(x_{ij})}])^{\cdot}$, es un grupo algebraico, denominado grupo lineal. Explícitamente,

$$\mu \colon Gl_n \times_k Gl_n \longrightarrow Gl_n$$

Con los puntos $\qquad ((a_{ij}), (b_{ij})) \longrightarrow (a_{ij}) \cdot (b_{ij})$

En los anillos $\qquad k[x_{ij}, \frac{1}{\det(x_{ij})}] \otimes_k k[y_{ij}, \frac{1}{\det(y_{ij})}] = k[x_{ij}, y_{ij}, \frac{1}{\det(x_{ij})}, \frac{1}{\det(y_{ij})}] \longleftarrow k[z_{ij}, \frac{1}{\det(z_{ij})}]$

$$\sum_l x_{il} y_{lj} \longleftarrow z_{ij}$$

3. Sea $G$ un grupo finito y consideremos el funtor $G(B) = G$ para todo $B$. Sea $A = \operatorname{Aplic}(G, k)$, que es una $k$-álgebra finita trivial de grado $\#G$, con la suma y multiplicación de funciones. Se cumple que $G = (\operatorname{Spec} A)^{\cdot}$:

$$(\operatorname{Spec} A)^{\cdot}(B) = \operatorname{Hom}_{k-\text{álg}}(\operatorname{Aplic}(G, k), B) \overset{\phi}{=} G$$

donde $\phi^{-1}(g)(f) = f(g)$, para cada $g \in G$ y $f \in \operatorname{Aplic}(G, k)$. Así pues, $G$ es un grupo algebraico.

**9. Definición:** Diremos que una $k$-variedad algebraica $E$ es un $k$-espacio vectorial algebraico de dimensión $n$, si $E^{\cdot}(B)$ es un $B$-módulo libre de rango $n$ (y dado un morfismo de $k$-álgebras $B \to B'$ el morfismo funtorial $E^{\cdot}(B) \to E^{\cdot}(B')$ es de $B$-módulos).

Si $E$ es un $k$-espacio vectorial de dimensión $n$, entonces $\operatorname{Spec} S_k^{\cdot} E^*$ es un $k$-espacio vectorial algebraico de dimensión $n$, pues

$$(\operatorname{Spec} S_k^{\cdot} E^*)^{\cdot}(B) = \operatorname{Hom}_{k-\text{àlg}}(S_k^{\cdot} E^*, B) = \operatorname{Hom}_k(E^*, B) = E \otimes_k B$$

que es un $B$-módulo libre de rango $n$.

**10. Proposición:** *$E$ es un espacio vectorial algebraico entonces $E = \operatorname{Spec} S_k^{\cdot}(E^{\cdot}(k)^*)$.*

*Demostración.* Los morfismos naturales $E^{\cdot}(k) \to E^{\cdot}(B)$ definen los morfismos $E^{\cdot}(k) \otimes_k B \to E^{\cdot}(B)$, que definen un morfismo $(\operatorname{Spec} S_k^{\cdot} E^{\cdot}(k)^*)^{\cdot} \to E^{\cdot}$, que por último, induce por Yoneda, un morfismo entre las correspondientes variedades algebraicas. Para demostrar que es un isomorfismo, podemos suponer, por cambio de base, que $k$ es algebraicamente cerrado. Cuando tomemos los funtores de puntos, podemos restringirnos a las $k$-álgebras $B$ de tipo finito. Para demostrar que $E^{\cdot}(k) \otimes_k B \to E^{\cdot}(B)$ es un isomorfismo de $B$-módulos (libres), basta verlo tensorializando por $\otimes_B B/\mathfrak{m}$, para todo ideal maximal $\mathfrak{m}$. Por dimensiones, por el diagrama conmutativo

$$\begin{array}{ccc} E^{\cdot}(k) & \longrightarrow & E^{\cdot}(B) \otimes_B B/\mathfrak{m} \\ & \searrow & \downarrow \\ & & E^{\cdot}(B/\mathfrak{m}) \end{array}$$

concluimos. □

**11. Definición:** Sea $G$ un funtor de grupos, $E$ un $k$-espacio vectorial y denotemos también por $E$ el funtor $E(B) = E \otimes_k B$. Diremos que $E$ es un funtor de $G$-espacio vectoriales, si $E(B)$ es (funtorialmente) un $G$-espacio vectorial.

Sea $E$ es un espacio vectorial, y $Aut_k(E)$ el funtor definido por $Aut_k(E)(B) = \operatorname{Aut}_B(E \otimes_k B)$. Todo morfismo $G \to \operatorname{Aut}_k(E)$ de funtores de grupos induce en $E$ una estructura de $G$-espacio vectorial y viceversa.

**12. Definición:** Sea $G$ un grupo algebraico y $E$ un espacio vectorial algebraico. Diremos que $E$ es un $G$-espacio vectorial algebraico, si es un funtor de $G^{\cdot}$-espacios vectoriales.

**13. Ejercicio:** $E$ es un $G$-espacio vectorial algebraico si y sólo si existe un morfismo de variedades algebraicas $G \times E \to E$ (escribamos con los puntos $(g, e) \mapsto ge$), de modo que $g(e + e') = ge + ge'$, $g(\lambda e) = \lambda ge$ y $(gg')e = g(g'e)$.

Si $E$ es un espacio vectorial de dimensión $n$, entonces $Aut_k(E)$ es isomorfo a $Gl_n$. Por tanto, es el funtor de puntos de un grupo algebraico.

**14. Ejercicio:** Probar que las estructuras de $E$ como $G$-espacio vectorial algebraico se corresponden con los morfismos de grupos algebraicos $G \to Aut_k(E)$.

## 3.2 Completa reducibilidad del grupo lineal

Sea $G$ un grupo algebraico y $E$ un $G$-espacio vectorial, diremos que $E$ es un $G$-espacio vectorial simple si no contiene $G$-subespacios vectoriales propios. Diremos que $E$ es semisimple si es suma directa de simples.

Diremos que $G = \operatorname{Spec} A$ es un grupo algebraico linealmente semisimple, si todo $G$-espacio vectorial es semisimple.

**1. Proposición:** *El grupo multiplicativo es semisimple. Los espacios vectoriales irreducibles son de dimensión* 1*, sobre los que opera el grupo multiplicativo por un carácter.*

*Demostración.* Sea una representación lineal del grupo multiplicativo, $G_m \to \mathrm{End}_k(E)$. Sea $t \in G_m(k[t]_t)$ un punto general de $G_m$ y un vector $e \in E$. Escribamos $t \cdot e = \sum_i t^i e_i$. Entonces

$$\sum_i (t't)^i e_i = (t't) \cdot e = t' \cdot (\sum_i t^i e_i) = \sum_i t^i (t' \cdot e_i)$$

Luego $t' \cdot e_i = (t')^i e_i$, además $e = \sum_i e_i$. En consecuencia, los subespacios de $E$ sobre los que opera $G_m$ por caracteres distintos, que están en suma directa, generan $E$. □

**2. Teorema:** *El grupo lineal es un grupo semisimple (característica del cuerpo base cero).*

*Demostración.* Sea $G = \mathrm{Aut}_k(E)$ el grupo lineal y $\phi\colon G \to \mathrm{End}_k(V)$, $g \mapsto (f_{ij}(g))$ una representación lineal.

1. Salvo un factor $\det(g)^n$, $n \in \mathbb{Z}$ podemos suponer que los $f_{ij}(g)$ son polinomios en las variables $g$, es decir $\phi$ extiende a $\mathrm{End}_k(E)$.

2. Podemos suponer que todos los polinomios $f_{ij}(g)$ son homogéneos de grado $r$: El grupo multiplicativo $G_m$, centro de $G$, descompone $V$ en suma directa de subespacios sobre los que actúa por caracteres distintos. Por conmutar que con su centro ha de dejar estos subespacios estables. En conclusión podemos suponer que dado un punto general $t$ de $G_m$, entonces $t \cdot v = t^r v$, para todo $v \in V$. Por tanto,

$$\begin{aligned}(g \cdot t) \cdot v = g \cdot (t^r v) &= t^r (f_{ij}(g))(v) \\ &= (f_{ij}(tg))(v)\end{aligned}$$

Por tanto, $f_{ij}(tg) = t^r f_{ij}(g)$ y los $f_{ij}(g)$ son polinomios homogéneos de grado $r$.

3. Así pues, $\phi$ factoriza (de modo único) a través del morfismo $\mathrm{End}_k(E) \to S^r \mathrm{End}_k(E)$, $g \mapsto g \cdot .\overset{r}{.}. \cdot g$. Ahora bien,

$$S^r \mathrm{End}_k(E) = (\mathrm{End}_k(E) \otimes .\overset{r}{.}. \otimes \mathrm{End}_k(E))^{S_r} = \mathrm{End}_k(E \otimes .\overset{r}{.}. \otimes E)^{S_r} = C_{k[S_r]}(\mathrm{End}_k(E \otimes .\overset{r}{.}. \otimes E))$$

que es una álgebra simple por 1.6.3. Además los $G$-subespacios vectoriales de $V$ coinciden con los $S^r \mathrm{End}_k(E)$-módulos. Por tanto, $V$ descompone en suma directa de $G$-submódulos simples.

□

# Índice de Materias