Tema 7.- Representaciones de grupos finitos. Introducción a los anillos no conmutativos

7.1 Nociones básicas

En lo que sigue, k denotará un cuerpo arbitrario y los espacios vectoriales lo serán sobre k. Si V es un espacio vectorial, $\mathrm{GL}(V)$ denotará su grupo de automorfismos. Dado un entero $d \geq 0$, denotaremos por $\mathrm{GL}(d, k)$ el grupo (multiplicativo) de las matrices inversibles $d \times d$ de elementos de k.

Si V es de dimensión d, entonces la elección de una base de V determina un isomorfismo de grupos $\mathrm{GL}(V) \simeq \mathrm{GL}(d, k)$. Por ejemplo, en $V = k^d$ la elección de la base canónica nos da un isomorfismo $\mathrm{GL}(k^d) \simeq \mathrm{GL}(d, k)$.

Definición 7.1.1.– Sea G un grupo (no necesariamente finito). Una *representación (lineal)* de G (sobre k) es un par (V, ρ), donde V es un espacio vectorial y ρ es un homomorfismo de grupos

$$\rho \colon G \to \mathrm{GL}(V).$$

En tal caso también diremos que ρ es una representación (lineal) de G en V.

Para simplificar la notación, y si no hay peligro de confusión, dada una representación (V, ρ) de G, para cada $g \in G$ y cada $v \in V$ notaremos $gv := \rho(g)(v)$, de manera que se tienen las reglas $1v = v$, $g(hv) = (gh)v$, $g, h \in G$, $v \in V$.

Nota 7.1.2.– De manera análoga, podemos definir una *representación matricial* de G de orden d (sobre k) como un homomorfismo de grupos $\rho \colon G \to \mathrm{GL}(d, k)$. Toda representación matricial de G de orden d determina una representación (lineal) en el espacio vectorial k^d.

Ejemplo 7.1.3.–

1. Para cada espacio vectorial V, el homomorfismo trivial constante $\rho \colon G \to \mathrm{GL}(V)$, $\rho(g) = \mathrm{Id}_V$ para todo $g \in G$, determina una representación de G que llamaremos *representación trivial* en V. Cuando $V = k$ la denominaremos *representación unidad*.

2. Consideremos el grupo simétrico S_3 y sea $\rho \colon S_3 \to \mathrm{GL}(3, k)$ la aplicación que a cada permutación σ le asocia la matriz que se obtiene al permutar las filas de la matriz identidad según σ^{-1}. La aplicación ρ es un homomorfismo de grupos.

3. El ejemplo anterior nos proporciona una representación (lineal) de S_3 en k^3 que viene dada por:

   $$\sigma(x_1, x_2, x_3) = (x_{\sigma^{-1}(1)}, x_{\sigma^{-1}(2)}, x_{\sigma^{-1}(3)})$$

   para cada $\sigma \in S_3$ y cada $(x_1, x_2, x_3) \in k^3$. De manera análoga podemos definir una representación de S_n en k^n.

4. La representación *signo*, dada por

$$\sigma \in S_n \mapsto \text{signatura}(\sigma) \in \{1, -1\} \subset k^* = \mathrm{GL}(k).$$

5. Supongamos que G es un grupo finito[1] y sea $V = k^G$ el espacio vectorial de todas las funciones definidas en G con valores en k. La aplicación $\rho : G \to \mathrm{GL}(V)$ dada por

$$[\rho(g)(\varphi)](h) = \varphi(g^{-1}h)$$

es un homomorfismo de grupos que determina la llamada *representación regular* de G.

Definición 7.1.4.– Sean (V, ρ) y (W, λ) dos representaciones de G sobre k.

1. Un *subsespacio invariante* o *subrepresentación* de V es un subespacio vectorial $W \subset V$ verificando $gw \in W$ para todos $g \in G$ y $w \in W$. Nótese que si W es un subespacio invariante de (V, ρ), entonces

$$g \in G \mapsto \rho(g)|_W \in \mathrm{GL}(W)$$

es de nuevo una representación de G.

2. Un *homomorfismo de representaciones*, o un G-homomorfismo, es un homomorfismo lineal $T\colon V \to W$ compatible con ρ y λ, i.e. $T(gv) = gT(v)$ para todos $g \in G$ y $v \in V$.

Naturalmente, si $T : V \to W$ es un G-homomorfismo, $\ker T$ e $\operatorname{Im} T$ son subrepresentaciones de V y W respectivamente.

Está claro que la identidad es un G-homomorfismo y que la composición de G-homomorfismos es un G-homomorfismo. Asimismo, el inverso de un G-homomorfismo biyectivo es también un G-homomorfismo. En tal caso diremos que es un *G-isomorfismo* y que las representaciones correspondientes son G-isomorfas.

3. La aplicación $\rho \oplus \lambda : G \to \mathrm{GL}(V \bigoplus W)$ dada por $(\rho \oplus \lambda)(g)(v, w) = (\rho(g)(v), \rho(g)(w))$ es un homomorfismo de grupos que determina la llamada *suma directa* de (V, ρ) y (W, λ).

4. El espacio de las aplicaciones lineales $\mathrm{Hom}_k(V, W)$ es una representación de G de la siguiente forma: dados $g \in G$ y $\phi \in \mathrm{Hom}_k(V, W)$, definimos $(g\phi)(v) := g\phi(g^{-1}v)$ para cada $v \in V$. En particular, si $W = k$ es la representación unidad obtenemos la representación *dual* de V, $V^* = \mathrm{Hom}_k(V, k)$, dada por

$$(g\vartheta)(v) := \vartheta(g^{-1}v), \quad \vartheta \in V^*, v \in V, g \in G.$$

[1] En el caso infinito existen construcciones similares bajo ciertas circunstancias. Por ejemplo, si G es un *grupo topológico* compacto y k es el cuerpo de los números reales o de los números complejos, en lugar de considerar el espacio de todas las funciones definidas en G con valores en k, podemos considerar el espacio V de las funciones continuas de G en k, o el de las funciones de *cuadrado integrable* respecto de una *medida de Haar* en G.

5. El producto tensorial $V \otimes_k W$ es una representación de G de la siguiente forma: para todo $g \in G$ y $v \in V, w \in W$, definimos $g(v \otimes w) := (gv) \otimes (gw)$.

7.2 Álgebras de grupo

La k-álgebra de G se define como $k[G] = \bigoplus_{\sigma \in G} k \cdot \sigma$, con la multiplicación dada por

$$\left(\sum_{\sigma \in G} a_\sigma \cdot \sigma \right) \left(\sum_{\sigma \in G} b_\sigma \cdot \sigma \right) = \sum_{\tau \in G} \left(\sum_{\sigma \cdot \sigma' = \tau} a_\sigma b_{\sigma'} \right) \tau.$$

Los elementos de $k[G]$ pueden interpretarse como las funciones de G en k que se anulan en *casi todos* (todos salvo un número finito) los elementos de G. Así, el elemento $\sum_{\sigma \in G} a_\sigma \sigma$ se identifica con la función $f \colon G \to k$ dada por $f(\sigma) = a_\sigma$. La multiplicación anterior admite entonces la descripción mediante la *convolución*

$$(f * g)(\tau) = \sum_{\sigma \in G} f(\sigma) g(\sigma^{-1} \tau).$$

Es fácil probar que la multiplicación así definida en el k-espacio vectorial $k[G]$ es asociativa, tiene elemento unidad ($f(\sigma) = 1$ si $\sigma = 1_G$, $f(\sigma) = 0$ si $\sigma \neq 1_G$), es distributiva respecto de la suma y $f \cdot (cg) = (cf) \cdot g = c(f \cdot g)$ para $f, g \in k[G]$ y $c \in k$.

Se trata pues de un anillo que no es conmutativo a menos que G lo sea.

Nota 7.2.1.– Las representaciones de G se pueden considerar como $k[G]$-módulos a la izquierda: toda representación V de G tiene estructura de $k[G]$-módulo a la izquierda con la multiplicación externa definida de la siguiente manera:

$$\left(\sum_{\sigma \in G} a_\sigma \sigma \right) \cdot v := \sum a_\sigma (\sigma v).$$

De este modo, la noción de subrepresentación corresponde a la de sub-$k[G]$-módulo, la de G-homomorfismo a la de homomorfismo de $k[G]$-módulos, la de núcleo (o imagen) de un G-homomorfismo a la de núcleo (o imagen) de un homomorfismo de $k[G]$-módulos y la de suma directa de representaciones a la de suma directa de $k[G]$-módulos.

7.3 Descomposición en representaciones irreducibles

Definición 7.3.1.– Una representación se dice *irreducible* si no tiene ninguna subrepresentación no trivial (distinta de 0 y de sí misma). En el lenguaje de los módulos esto corresponde a la noción de $k[G]$-módulo *simple*.

Ejemplo 7.3.2.– Un ejemplo (trivial) de representación irreducible es la representación unidad k. Más generalmente, toda representación de dimensión 1 es irreducible.

Toda representación irreducible de un grupo abeliano sobre un cuerpo algebraicamente cerrado es de dimensión 1.

DEFINICIÓN 7.3.3.– Una representación V se dice *completamente reducible* si es suma directa de representaciones irreducibles.

EJEMPLO 7.3.4.– Sea $V = \mathbb{C}^2$ y consideremos $G = \mathbb{Z}$ como el grupo aditivo de los enteros. Sea $\rho\colon \mathbb{Z} \to \mathrm{GL}(V)$ dada por $\rho(n) = A^n$, donde

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Esta representación no es irreducible, porque $W = \langle (0,1) \rangle \subset V$ es una subrepresentación no trivial. De hecho W es la única subrepresentación no trivial, y por tanto V no es completamente reducible.

TEOREMA 7.3.5.– *(Reducibilidad completa de los grupos finitos)* Toda representación de un grupo finito compleja, o más generalmente, sobre un cuerpo de característica 0, de dimensión finita es completamente reducible.

Recordemos que un espacio vectorial hermítico es un espacio vectorial complejo V dotado de una forma hermítica, es decir, una forma $\langle -, - \rangle\colon V \times V \to \mathbb{C}$ bilineal para la suma y que además verifica

- $\langle \alpha v, w \rangle = \bar{\alpha} \langle v, w \rangle$.
- $\langle v, \alpha w \rangle = \alpha \langle v, w \rangle$.
- Para todo $v \neq 0$, es $\langle v, v \rangle \in \mathbb{R}$ y $\langle v, v \rangle > 0$.

DEFINICIÓN 7.3.6.– Una representación unitaria es una representación (V, ρ), tal que V es hermítico y la forma hermítica $\langle -, - \rangle$ es compatible con la estructura de $k[G]$-módulo, es decir,

$$\langle \sigma \cdot v, \sigma \cdot w \rangle = \langle v, w \rangle, \qquad \text{para todo } \sigma \in G \text{ y todos } v,\, w \in V\ .$$

PRUEBA: Hay dos formas de demostrar el Teorema: usando, bien representaciones unitarias, bien proyectores.

- Supongamos que V es una representación unitaria. Demostraremos el resultado por inducción sobre la dimensión de V. Si la dimensión es 1 o si V es irreducible, no hay nada que decir. Si la dimensión es mayor y V no es irreducible, sea $W \subset V$ una subrepresentación no trivial (naturalmente, también es unitaria). Entonces, $W^\perp$ también es invariante. En efecto, si $v \in W^\perp$ y $\sigma \in G$ es $\sigma \cdot v \in W^\perp$, pues $\langle \sigma \cdot v, w \rangle = \langle v, \sigma^{-1} \cdot w \rangle = 0$, porque $\sigma^{-1} \cdot w \in W$.

  Así, $V = W \oplus W^\perp$. Como las dimensiones de W y $W^\perp$ son menores que la dimensión de V, por la hipótesis de inducción, son sumas directas de subespacios invariantes. Por tanto, también lo es V.

Supongamos ahora que (V, ρ) no es una representación unitaria, y sea $W \subset V$ una subrepresentación. Sea $\langle -, - \rangle$ una forma hermítica cualquiera en V, y definamos la siguiente forma hermítica:

$$\langle v, w \rangle' = \sum_{\sigma \in G} \langle \sigma \cdot v, \sigma \cdot w \rangle.$$

Esta nueva forma promediada verifica que

$$\langle \tau v, \tau w \rangle' = \langle v, w \rangle, \quad \tau \in G, v, w \in V,$$

luego V es una representación unitaria para $\langle -, - \rangle'$.

- En este caso, sólo haremos uso de que k es un cuerpo de característica cero (para dividir por $|G|$). Sea $W \subset V$ invariante, y sea $p \colon V \to W$ un proyector (i.e., $p^2 = p$) de imagen W . Consideremos

$$p'(v) = \frac{1}{|G|} \sum_{\sigma \in G} \sigma \cdot p(\sigma^{-1} \cdot v).$$

Entonces $p' \colon V \to W$ también es un proyector. Aún más, $\ker p'$ es invariante. En efecto, si $v \in \ker p'$, es $p'(v) = 0$. Tenemos que probar que $p'(\tau v) = 0$ para todo $\tau \in G$. Pero se tiene la igualdad

$$p'(\tau \cdot v) = \frac{1}{|G|} \sum_{\sigma \in G} \sigma \cdot p(\sigma^{-1} \tau \cdot v).$$

Renombrando $\lambda^{-1} = \sigma^{-1}\tau$, se puede escribir

$$p'(\tau v) = \frac{1}{|G|} \sum_{\lambda \in G} \tau \lambda p(\lambda^{-1} v) = \frac{1}{|G|} \tau p'(v) = 0.$$

Finalmente, como p' es un proyector, se tiene $V = \operatorname{Im} p' \oplus \ker p' = W \oplus \ker p'$. Aplicando la hipótesis de inducción se tiene el resultado.

$\square$

NOTA 7.3.7.– La ventaja de la primera demostración es que se puede generalizar a representaciones continuas de grupos topológicos compactos en un espacio de Hilbert. La de la segunda es que es puramente algebraica y funciona sobre un cuerpo k arbitrario de característica cero.

El objeto principal de la teoría de representaciones de los grupos finitos es describir todas sus representaciones (complejas, por ejemplo) irreducibles, así como la manera efectiva en que cualquier representación de dimensión finita se descompone en suma directa de representaciones irreducibles. Un resultado importante afirma que cada grupo finito G tiene un número finito de representaciones irreducibles no isomorfas.

Ejercicio 1.– Describir todas las representaciones irreducibles, salvo isomorfismo, del grupo aditivo de los enteros $\mathbb{Z}$.

Denotemos por $\hat{G}$ al conjunto (finito) de las clases de isomorfía de representaciones irreducibles de un grupo finito G. Uno de los resultados centrales de la teoría es la igualdad

$$|G| = \sum_{V \in \hat{G}} (\dim V)^2 \,,$$

cuya prueba requiere el estudio de los *caracteres* de G (ver la bibliografía).

7.4 Caso del grupo simétrico S_3

Consideremos $G = S_3$ el grupo simétrico. Hay dos representaciones irreducibles evidentes (son de dimensión 1) no isomorfas:

1 La representación *unidad*, dada por $\rho\colon S_3 \to \mathbb{C}^* = \mathrm{GL}(\mathbb{C})$ tal que $\rho(g) = 1$ para todo $g \in G$.

2 La representación *signo*, dada por $\rho\colon S_3 \to \{1, -1\} \subset \mathbb{C}^* = \mathrm{GL}(\mathbb{C})$, tal que $\rho(g) = \mathrm{signatura}(g)$.

Hay también una tercera representación menos evidente que describimos a continuación:

3 Sea $V = \{(v_1, v_2, v_3) \in \mathbb{C}^3 \;\mid\; v_1 + v_2 + v_3 = 0\}$, y $\rho\colon G \to \mathrm{GL}(V)$ dada por

$$\rho(g)(v_1, v_2, v_3) = (v_{g^{-1}(1)}, v_{g^{-1}(2)}, v_{g^{-1}(3)}).$$

Esta representación también es irreducible. Lo demostraremos restringiendo ρ a dos subgrupos de G. Sea pues $\tau = (1, 2, 3)$, y $H = \langle \tau \rangle \subset S_3$. Llamaremos $T = \rho(\tau)$, y tenemos $T\colon V \to V$. Como $\mathrm{ord}(\tau) = 3$, es $T^3 = \mathrm{Id}_V$, luego T es diagonalizable y tiene sus autovalores en el conjunto $\{w, w^2, w^3 = 1\}$, con $w = e^{2\pi i/3}$. Consideraremos entonces la suma directa $V = V_1 \oplus V_w \oplus V_{w^2}$, donde $V_{w^i} = \ker(w^i \mathrm{Id} - T)$.

Como se comprueba fácilmente, si $T(v) = v$, entonces $v = 0$. Sin embargo, $v_{w^2} := (1, w, w^2)$ es un autovector para el autovalor w^2, de forma que $\langle v_{w^2} \rangle \subset V$ es estable para T.

Sea ahora $\sigma = (1, 2)$. Es evidente que $\tau\sigma = \sigma\tau^2$, luego debe verificarse que

$$\begin{aligned} T(\sigma v) = \tau(\sigma v) = (\tau\sigma)v = (\sigma\tau^2)v = \sigma(\tau^2 v) = \\ = \sigma T^2(v) = \sigma((w^2)^2 v) = \sigma(wv) = w(\sigma v), \end{aligned}$$

para todo $v \in V_{w^2}$. Así, si v es un autovector para T de autovalor w^2, entonces σv es autovector de autovalor w, luego $\sigma V_{w^2} \subset V_w$.

De manera análoga se prueba que $\sigma V_w \subset V_{w^2}$, y por tanto $\sigma V_{w^2} = V_w$ y $V_w, V_{w^2} \neq 0$.

Como hemos visto antes, $V_1 = 0$, luego $V = V_w \oplus V_{w^2}$. Como V es de dimensión 2, cada uno de los sumandos es de dimensión 1. Ahora bien, esta suma directa no es una suma directa de subrepresentaciones, puesto que $\sigma V_{w^2} \subset V_w$. Como V_w y V_{w^2} son los únicos subespacios propios estables por la acción de τ (o de T), deducimos que V no tiene subrepresentaciones no triviales y por tanto V es irreducible. Además, como V es de dimensión 2, no es isomorfa ni a la representación *unidad* ni a la representación *signo*.

Tenemos pues tres representaciones irreducibles, y sabemos que $|G|$ es igual a la suma de los cuadrados de las dimensiones de las representaciones irreducibles, luego éstas tres son todas las representaciones irreducibles de S_3.

`Estudio del álgebra de` S_3`,` $\mathbb{C}[S_3]$`...`