Teoría de Representaciones

Cándido Martín González

Noviembre de 2021

---

1 Prolegómenos sobre representaciones de anillos y álgebras

En esta sección vamos a describir los anillos artinianos simples así como los artinianos semisimples. Aunque algunas veces lo especificaremos, si no se dice lo contrario, la palabra "anillo" significará "anillo con unidad".

Lema 1 (Lema de Brauer). *Sea R un anillo (con unidad) que posee un ideal por la izquierda minimal K de modo que $K^2 \neq 0$. Entonces existe un idempotente $e \in K$ tal que $K = Re$ siendo además eRe un anillo de division.*

Proof. Como $K^2 \neq 0$ existe $u \in K$ tal que $Ku \neq 0$. Por minimalidad de K se tiene $K = Ku$ luego existe $e \in K$ no nulo tal que $eu = u$. Luego $reu - ru = 0$ y por lo tanto (tomando $r \in K$) se llega a que $re - r \in \mathrm{Lann}_K(u) := \{x \in K : xu = 0\}$. Pero $\mathrm{Lann}_K(u)$ es un ideal por la izquierda de R contenido en K lo que implica que $\mathrm{Lann}_K(u) = 0$ o $\mathrm{Lann}_K(u) = K$. Esto último es incompatible con que $K^2 \neq 0$. Por lo tanto $\mathrm{Lann}_K(u) = 0$ y consecuentemente $re - e = 0$ para cada $r \in K$. Eso quiere decir que e es un idempotente (no nulo) de K. Esto implica que $K = Re$. Sea ahora $\Delta := eRe$ y veamos que es un anillo de división. Tomemos $0 \neq b \in \Delta$. Entonces $0 \neq Rb = K = Re$ por lo tanto $e = rb$ para algún $r \in R$. Además $e = erb = ereb$ ya que $b \in eRe$. Así pues tenemos $e = b'b$ siendo $b' = ere$. Esto demuestra que Δ es un anillo de división teniendo en cuenta la observación que hay después de esta demostración. □

Nota 1 Si R es un anillo con unidad en el que cada elemento no nulo tiene un inverso por la izquierda, entonces R es un anillo de división. En efecto: cada elemento no nulo $r \in R$ es simplificable a izquierda, es decir, la igualdad $rx = ry$ implica $x = y$. Entonces si tomamos un $a \in R \setminus \{0\}$ sabemos que $\exists a' \in R \setminus \{0\}$ tal que $a'a = 1$. Podemos escribir $a'aa' = a'1$ y como $a' \neq 0$ simplificando obtenemos $aa' = 1$.

Nota 2 Un módulo sobre un anillo R se dice artiniano si toda sucesión

$$N_1 \supset N_2 \supset \cdots \supset N_m \supset \cdots$$

es estacionaria, es decir, existe un k tal que $N_k = N_{k+1} = \cdots$. Esto es equivalente a que cada familia de submódulos de M tiene un elemento minimal. En efecto, si M es artiniano y $\mathbf{F}$ una familia de submódulos de M que no tiene un elemento minimal, entonces seleccionamos arbitrariamente un $N_1 \in \mathbf{F}$. Como N_1 no es minimal existe $N_2 \in \mathbf{F}$ tal que N_1 contiene estrictamente a N_2. Así podemos construir una sucesión infinita escritamente decreciente de submódulos de M.

Nota 3 Todo submódulo de un módulo artiniano es artiniano. Esto se debe a que todo submódulo de un submódulo de un módulo M es un submódulo de M.

Un anillo R se dice artiniano a izquierda si ${}_RR$ es un R-módulo artiniano. Equivalentemente cada sucesión

$$I_1 \supset I_2 \supset \cdots \supset I_m \supset \cdots$$

de ideales por la izquierda es estancionaria. Esto también equivale a que cada familia de ideales por la izquierda tiene un elemento minimal. Normalmente hablaremos de anillo artiniano a secas, sin especificar que lo queremos decir es "artiniano a izquierda". Dicho de otro modo, de ahora en adelante el término "anillo artiniano" querrá decir "anillo artiniano por la izquierda".

Un anillo R se dice semiprimo si para cada ideal I de R se tiene que $I^2 = 0$ implica $I = 0$. Si R es semiprimo entonces para cada ideal por la izquierda I de R se tiene también $I^2 = 0$ implica $I = 0$. Recordemos que todo anillo simple es un anillo primo. En particular en un anillo simple si un ideal por la izquierda K tiene cuadrado nulo, $K^2 = 0$, entonces necesariamente $K = 0$.

Teorema 1 (Wedderburn-Artin) *Sea R un anillo artiniano simple, entonces existe una anillo de división Δ y un natural $n \geq 1$ tal que $R \cong M_n(\Delta)$.*

Proof. Como R es artiniano posee ideales por la izquierda minimales. Sea K uno de ellos. Por la observación hecha en el párrafo anterior a este teorema, se tiene que $K^2 \neq 0$ luego el lema de Brauer nos dice que $K = Re$ siendo e un idempotente tal que $\Delta := eRe$ es un anillo de división. Podemos definir en K una estructura de espacio vectorial por la derecha para el producto $K \times \Delta \to K$ tal que $re \cdot er'e := rer'e$. Consideremos entonces el anillo $\mathrm{End}_\Delta(K)$ de todas las aplicaciones Δ-lineales de K en K (donde el producto es la composición de endomorfismos). Por otra parte la aplicación $L\colon R \to \mathrm{End}_\Delta(K)$ tal que $a \mapsto L_a$ (donde $L_a\colon K \to K$ es el operador de multiplicación a izquierda $L_a(x) = ax$). Es rutinario comprobar que L es un homomorfismo de anillos. Ahora $\ker(L) = \mathrm{Lann}_R(K)$ y como $\ker(L) \lhd R$, al ser R simple se tiene que $\ker(L) = 0$ o $\ker(L) = R$. Pero esto último implicaría que $RK = 0$ luego $K^2 = 0$ una contradicción. Por lo tanto $\ker(L) = 0$ lo que nos permite concluir que L es un monomorfismo de R en $\mathrm{End}_\Delta(K)$. Para ver que

es un epimorfismo tengamos en cuenta que $ReR = R$ por tanto $1 = \sum_i r_i e s_i$ para ciertos $r_i, s_i \in R$. Sea ahora $T \in \mathrm{End}_\Delta(K)$ un elemento arbitrario y definamos $a = \sum_i T(r_i e) e s_i$. Se comprueba entonces que $T = L_a$ y ya tenemos que L es un isomorfismo de anillos de R en $\mathrm{End}_\Delta(K)$. $\square$

Vamos ahora a estudiar los anillos semisimples artinianos. Un módulo $M \neq 0$ sobre un anillo R se dice semisimple si cada submódulo N de M es un sumando directo de M. Dicho de otro modo: para cada submódulo N de M existe un submódulo N' de M tal que $M = N \oplus N'$. Una propiedad fácil de demostrar para módulos es que todo submódulo y todo módulo cociente de un módulo semisimple, es un módulo semisimple. Un anillo (con unidad) R se dice semisimple por la izquierda si ${}_RR$ es un R-módulo semisimple. Como vamos a trabajar siempre considerando a R un módulo sobre si mismo por la izquierda, diremos simplemente que R es semisimple y nos olvidaremos de mencionar "a izquierda". Equivalentemente, decir que R es semisimple es lo mismo que decir que para cada ideal a izquierda I de R existe otro ideal (por la izquierda) J tal que $R = I \oplus J$.

Lema 2 *Sea R semisimple y $I \lhd R$ tal que $I^2 = 0$. Entonces $I = 0$. En otras palabras, un anillo semisimple es semiprimo.*

Proof. Se tiene $R = I \oplus J$ donde J es ideal a izq. de R. Ahora $IJ \subset I \cap J = 0$. Escribamos entonces $1 = i + j$ con $i \in I$, $j \in J$. Entonces multiplicando por i a izquiera y a derecha se tiene $i = i^2 + ij = i^2 + ji$ de donde $ij = ji = 0$. Así pues $1 = i^2 + j^2 = i + j$ luego $i^2 = i$, $j^2 = j$. Como $I^2 = 0$ se tiene $i = 0$ de modo que $1 = j$ por tanto $J = R$ y $I = 0$. $\square$

Corolario 1 *Para R semisimple se tiene que $\forall I \lhd R$ con $I \neq 0$*

$$\mathrm{Ann}_I(I) = 0.$$

Proof. Empecemos recordando que $\mathrm{Ann}_I(I) := \{x \in I : xI = Ix = 0\}$. Entonces $\mathrm{Ann}_I(I)^2 = 0$ luego como R es semiprimo por el Lemma 2, concluimos que $\mathrm{Ann}_I(I) = 0$. $\square$

Lema 3 *Todo anillo artiniano semisimple R tiene ideales minimales no nulos.*

Proof. Sea $\mathbf{F}$ la familia de los ideales no nulos de R. Como R es artiniano $\mathbf{F}$ posee un elemento minimal. $\square$

Teorema 2 *Sea R un anillo semisimple artiniano. Entonces R es la suma directa de sus ideales minimales. Cada uno de ellos es un anillo artiniano simple.*

Proof. Sea $\mathbf{F}$ la familia de los ideales minimales de R. Si $I, J \in \mathbf{F}$ son distintos, entonces $I \cap J = 0$ ya que de lo contrario $I \cap J = I = J$. Por lo tanto $IJ = 0$. Sea $S := \sum_{I \in \mathbf{F}} I$ y veamos que dicha suma es directa: sea $I \in F$ y $z \in I \cap \sum_{J \in F \setminus \{I\}} J$. Entonces $zI = Iz = 0$. Luego $z \in \mathrm{Ann}_I(I) = 0$ por el Corolario 1. Así la suma S es directa. Ahora queremos

ver que $R = S$. Pero como R es semisimple se tiene $R = S \oplus H$ para un cierto ideal por la izquierda H de R. Obsérvese que $SH \subset S \cap H = 0$ por lo tanto $H \subset \mathrm{Rann}_R(S) \lhd R$ (téngase en cuenta que $\mathrm{Rann}_R(S) = \{x \in R : xS = 0\}$). Pero $S \cap \mathrm{Rann}_R(S) = 0$ porque $(S \cap \mathrm{Rann}_R(S))^2 = 0$ y R es semiprimo. Entonces también se tiene $R = S \oplus \mathrm{Rann}_R(S)$ pero $\mathrm{Rann}_R(S) \lhd R$ hereda las condiciones de ser semisimple y artiniano. El Lema 3 implica que $\mathrm{Rann}_R(S)$ posee un ideal minimal no nulo L. Pero entonces ese ideal L es un ideal minimal no nulo de R luego pertenece a $\mathbf{F}$ y en consecuencia está contenido en S. Es decir $L \subset S \cap \mathrm{Rann}_R(S) = 0$. Por tanto $R = S$. $\square$

1.1 Álgebras vs. anillos

Sabemos que la categoría de anillos es isomorfa a la de $\mathbb{Z}$-álgebras. Más formalmente hay un functor $\mathcal{F}$ de la categoría de anillos **Rng** a la de $\mathbb{Z}$-álgebras $\mathbb{Z}$-álg y otro functor $\mathcal{G}$ de $\mathbb{Z}$-álgebras en anillos tal que $\mathcal{F} \circ \mathcal{G} \cong 1_{\mathbb{Z}-\text{álg}}$ y $\mathcal{G} \circ \mathcal{F} \cong 1_{\mathbf{Rng}}$ (donde $\cong$ significa isomorfismo natural). Recordemos que una inmersión de una categoría $\mathfrak{A}$ en una categoría $\mathfrak{B}$ es un functor $\mathcal{F} : \mathfrak{A} \to \mathfrak{B}$ que inyectivo en objetos y fiel. La fidelidad de $\mathcal{F}$ quiere decir que para cualquier par de objetos $X, Y \in \mathfrak{A}$ la aplicación $\hom_{\mathfrak{A}}(X, Y) \to \hom_{\mathfrak{B}}(\mathcal{F}(X), \mathcal{F}(Y))$ dada por $f \mapsto \mathcal{F}(f)$ es inyectiva.

Recordemos que dado un anillo R, un R-módulo (a izquierda) M es un grupo abeliano $(M, +)$ provisto de una aplicación $R \times M \to M$ que cumple (i) $r(m + m') = rm + rm'$, (ii) $r(m + m') = rm + rm'$, (iii) $(rr')m = r(r'm)$ y (iv) $1m = m$; para cualesquiera $r, r' \in R$, $m, m' \in M$. Ahora bien dada una K-álgebra sobre el cuerpo K, un A-módulo (a izquierda) sobre el álgebra A es un módulo sobre el anillo subyacente a A provisto de una estructura de espacio vectorial sobre el cuerpo K.

Si K es un anillo, hay una inmersión de la categoría de K-álgebras en la de anillos dada por el functor de olvido. También hay una inmersión de la categoría de A-módulos en la de módulos sobre el anillo subyacente a A. Tanto el Lema de Brauer como el Teorema de Wedderburn-Artin y el Teorema 2 admite versiones para álgebras sobre cuerpos: Si K es un cuerpo y A es un álgebra semisimple de dimensión finita, entonces es suma directa de su familia de ideales minimales los cuales son álgebras simples y finito-dimenionales en sí mismos. Más aún cada álgebra simple de dimensión finita es isomorfa a $M_n(\Delta)$ donde $n \geq 1$ es un natural y Δ es una K-álgebra de división y dimensión finita.

1.2 Complementos de módulos semisimples.

Sea R un anillo y $M \neq 0$ un R-módulo semisimple. Sea $m \in M$ no nulo, entonces $0 \neq Rm \leq M$ y tenemos un epimorfismo $f : R \to Rm$ dado por $f(r) = rm$. Luego existe un ideal por la izquierda I de R tal que $\bar{f} : R/I \cong Rm$ es un isomorfismo tal que $\bar{f}(r + I) = rm$. Obsérvese que R/I es un R-módulo semisimple (por ser isomorfo a Rm que es semisimple por ser submódulo de un módulo semisimple). Aplicando el Lema de Zorn vemos que existe un ideal por la izquiera maximal M que contiene a I. Por tanto

$M/I \leq R/I$ y tenemos $R/I = M/I \oplus W$ donde $W \leq R/I$. En consecuencia

$$W \cong \frac{R/I}{M/I} \cong R/M$$

por lo tanto W es un R-módulo simple ya que R/M lo es por ser M ideal a izquierda maximal. Como W es un R- simple, su imagen por $\bar{f}$ es un R-módulo simple contenido en Rm luego es un R-módulo simple de M. Bueno, en definitiva vemos que cada módulo semisimple tiene módulos simples. Vamos a demostrar a continuación que si M es semisimple, existe una colección $\{S_i\}_{i\in\Omega}$ de R-submódulos simples tal que $M = \oplus_{i\in\Omega} S_i$.

Teorema 3 *Todo R-módulo semisimple es suma directa de módulos simples.*

Dem. Una familia $\mathbf{F}$ de R-módulos simples se dice que es directa si para cada $N \in \mathbf{F}$ se tiene

$$N \cap \sum_{L\in\mathbf{F}\setminus\{N\}} L = 0.$$

Como M tiene algún submódulo simple (sea N uno de ellos) la familia cuyo ´unico elemento es N, es una familia directa. Definamos ahora un conjunto $\mathcal{G}$ dado por:

$$\mathcal{G} = \{\mathbf{F}\colon \mathbf{F} \text{ es una familia directa de submódulos simples de } M\}.$$

Consideramos la relación de inclusión en $\mathcal{G}$. Como $(\mathcal{G}, \subset)$ es un conjunto inductivo, aplicando el Lema de Zorn $\mathcal{G}$ tiene un elemento maximal. Sea $\mathbf{F} \in \mathcal{G}$ un elemento maximal. Veremos que $M = \oplus_{L\in\mathbf{F}} L$. En caso contrario $M = Z \oplus (\oplus_{L\in\mathbf{F}} L)$ para un $Z \neq 0$. Entonces Z es semisimple luego posee un submódulo simple $Z' \leq Z$. Pero en ese caso la nueva familia $\mathbf{F}' := \mathbf{F} \cup \{Z'\}$ es directa y contiene estrictamente a $\mathbf{F}$ lo que contradice que $\mathbf{F}$ era maximal. Por tanto $Z = 0$ y $M = \oplus_{L\in\mathbf{F}} L$. $\square$

El recíproco del teorema anterior es también cierto: si M es una suma directa de R-módulos simples entonces M es semisimple. La idea de la demostración consiste en considerar el conjunto (ordenado por inclusión) $\mathcal{G}$ cuyos elementos son las familias directas $\mathbf{F}$ de submódulos simples tales que

$$N \cap \left(\sum_{X\in\mathbf{F}} X \right) = 0.$$

Aplicando el Lema de Zorn se demuestra que existe un elemento maximal $\mathbf{F} \in \mathcal{G}$. A partir de ahí se llega a que $N \oplus (\oplus_{X\in\mathbf{F}} X) = M$ por tanto se demuestra que cada submódulo es sumando directo, por tanto M es semisimple.

Finalmente me gustaría comentar que estos resultado para anillos se trasladan sin problema al caso de módulos sobre K-álgebras A (siendo K un cuerpo). Una módulo M sobre el álgebra A se dice semisimple si todo A-submódulo N de M es un sumando directo, es decir, $M = N \oplus N'$ para cierto A-submódulo N'. Se tiene entonces que M es semisimple si y sólo si es suma directa de A-submódulos simples.

2 Representaciones de grupos finitos

Sesiones 1-2

Empecemos recordando algunas nociones que aunque ya han sido introducidas conviene explicitar. Sea R un anillo conmutativo y unitario con unidad. Un R-módulo A se dice que es una R-álgebra si esta dotada de una aplicación

$$A \times A \to A$$

que es R-lineal en cada variable. Dicha operación (llamada producto en lo sucesivo) se denotará usualmente por la simple yuxtaposición o por un punto $\cdot$. Si dicha operación es asociativa diremos que A es una R-álgebra asociativa. En esta parte de la asignatura, todas las álgebras que consideremos serán asociativas.

Si una R-álgebra A tiene elemento neutro para el producto, diremos que es un álgebra con unidad. Las álgebras que consideraremos en este capítulo serán siempre álgebras con unidad. Un álgebra (asociativa) y con unidad $1 \in A$ diremos que es un álgebra de división si

$$\forall x \in A \setminus \{0\}, \exists y \in A \colon xy = yx = 1.$$

3 Álgebras reales de división

Cuando el anillo base R sea un cuerpo, $R = K$, toda K-álgebra es un espacio vectorial por tanto tiene sentido hablar de su dimensión (como espacio vectorial).

Como ejemplos de álgebras reales (es decir $\mathbb{R}$-álgebras), podemos citar $\mathbb{R}$, $\mathbb{C}$ y $\mathbb{H}$. El álgebra $\mathbb{H}$ de los cuaterniones de Hamilton consiste en un espacio vectorial de dimensión cuatro con una base $\{1, i, j, k\}$ cuya tabla de multiplicar se resume en

$$i^2 = j^2 = k^2 = ijk = -1.$$

La tabla de multiplicar completa de $\mathbb{H}$ es

$\cdot$	1	i	j	k
1	1	i	j	k
i	i	-1	k	$-j$
j	j	$-k$	-1	i
k	k	j	$-i$	-1

Por ejemplo, para deducir que $ij = k$ hacemos

$$ijk = -1 \Rightarrow ijk^2 = -k \Rightarrow ij = k.$$

Por lo tanto $\mathbb{H} = \{\lambda_0 1 + \lambda_1 i + \lambda_2 j + \lambda_3 k \colon \lambda_i \in \mathbb{R}\}$. La aplicación lineal $\mathbb{H} \to \mathbb{H}$ dada por $x \mapsto \overline{x}$ donde

$$\overline{\lambda_0 1 + \lambda_1 i + \lambda_2 j + \lambda_3 k} := \lambda_0 1 - \lambda_1 i - \lambda_2 j - \lambda_3 k$$

satisface las propiedades

$$\overline{xy} = \overline{y}\ \overline{x}, \qquad \overline{\overline{x}} = x$$

para todos $x, y \in \mathbb{H}$. Esta aplicación se llama conjugación cuaterniónica.

Teorema 4 *Para cada $x \in \mathbb{H}$ se tiene $x\overline{x} = \|x\|^2$ donde la norma viene dada por $\|x\|^2 = \lambda_0^2 + \lambda_1^2 + \lambda_2^2 + \lambda_3^2$ siendo $x = \lambda_0 1 + \lambda_1 i + \lambda_2 j + \lambda_3 k$.*

Corolario 2 *$\mathbb{H}$ es un álgebra de división*

Dem. Si $x \neq 0$ se tiene $\|x\| \neq 0$ luego $x^{-1} = \|x\|^{-2}\bar{x}$. $\square$

En un álgebra A de dimensión finita, sobre un cuerpo K, todo elemento $x \in A$ es raíz de un polinomio mónico mínimal

$$m(x) = 0.$$

La minimalidad quiere decir que si otro polinomio f verifica que $f(x) = 0$, entonces f es un múltiplo de m. Veamos que cada $x \in A$ es raíz de un polinomio mónico: consideremos las potencias de x:

$$1 = x^0, x, x^2, \ldots, x^n, \ldots$$

Como A es de dimensión finita dicho conjunto no puede ser linealmente independiente para todo n. Luego existe un n tal que $1 = x^0, x, x^2, \ldots, x^n$ es linealmente dependiente. Dicho n se puede tomar mínimo. Por tanto existen escalares $\lambda_i \in K$ con $\lambda_n \neq 0$ tales que $\lambda_0 + \lambda_1 x + \cdots + \lambda_n x^n = 0$. Dividiendo entre λ_n vemos que x es raíz de un polinomio mónico de grado n mínimo. Ahora consideramos el anillo de ideales $K[T]$ en la indeterminada T. Este es un dominio de ideales principales y el conjunto

$$I := \{p \in K[T] \colon p(x) = 0\}$$

es un ideal de $K[T]$. Por tanto dicho ideal es principal. Luego existe un polinomio mónico $m \in K[T]$ tal que $I = (m)$. Esto demuestra la minimalidad de m.

Teorema 5 *Sea A un álgebra de dimensión finita sobre un cuerpo K algebraicamente cerrado. Si A es de división, entonces $A \cong K$.*

Dem. Sea $x \in A$ y m su polinomio minimal. Dicho polinomio se descompone en producto de polinomios de primer grado:

$$m = m_1 \cdots m_k$$

con $m_i \in K[T]$ cada uno de ellos de primer grado. Entonces

$$0 = m(x) = m_1(x) \cdots m_k(x)$$

y como A es de división, alguno de los factores es nulo. Por tanto $m_i(x) = 0$ para algún i. Como m_i es de primer grado, $m_i = aT + b$ con $a, b \in K$ y $a \neq 0$. Luego $ax + b1 = 0$ y por tanto $x = -a^{-1}b1$. Hemos demostrado que todo elemento es múltiplo escalar de 1.

$$A = K1 \cong K. \quad \square$$

Corolario 3 *Toda álgebra compleja de división y de dimensión finita es isomorfa a* $\mathbb{C}$.

¿Y qué se puede decir de las álgebras reales de división y dimensión finita?

Proposición 1 *Sea* A *una* $\mathbb{R}$*-álgebra de división de dimensión finita (unital). Entonces todo el polinomio minimal de cada elemento de* A *es de grado* ≤ 2.

Dem. Sea $x \in A$, si $x = \lambda 1 \in \mathbb{R}1$ entonces x satisface el polinomio $T - \lambda$. Supongamos que x no es escalar. Sea m su polinomio minimal. Sabemos que $m = \prod_i m_i$ donde cada m_i es un polinomio irreducible de $\mathbb{R}[T]$ (por lo tanto cada m_i es de grado uno o dos). Como $0 = m(x) = \prod_i m_i(x)$, al ser A un álgebra de división, concluimos que para algún i se tienen $m_i(x) = 0$. Por tanto x es raíz de un polinomio de grado dos (al no ser escalar x, no puede ser raíz de un polinomio de grado uno). $\square$

Hemos demostrado que en un álgebra real de división y de dimensión finita A, los elementos no escalares son raíz de polinomios de segundo grado:

$$\forall x \in A \setminus \mathbb{R}1, \exists p, q \in \mathbb{R} : x^2 = px + q.$$

(esto es lo que se llama un álgebra cuadrática).

Recordemos de la teoría de extensiones de cuerpos:

Teorema 6 *Si* F *es un cuerpo extensión de* $\mathbb{R}$ *con* $dim_{\mathbb{R}}(F)$ *finita, entonces* $F \cong \mathbb{R}$ *o* $F \cong \mathbb{C}$.

Sketch de la demo.

$$F \cong \mathbb{R}[T]/(p)$$

donde p es un polinomio irreducible de $\mathbb{R}[T]$. Luego p es de grado 1 o 2. Como $\dim_{\mathbb{R}}(F) = \dim_{\mathbb{R}}\mathbb{R}[T]/(p) = \text{grado}(p)$ concluimos que F es de dimensión 1 o 2 como $\mathbb{R}$-espacio.

Si $\dim_{\mathbb{R}}(F) = 1$ se tiene $F \cong \mathbb{R}$.

Si $\dim_{\mathbb{R}}(F) = 2$ y tomamos $x \in F \setminus \mathbb{R}1$ existen $p, q \in \mathbb{R}$ tales que $x^2 = px + q$. Entonces $y := x - p/2$ verifica

$$y^2 = x^2 - px + p^2/4 = q + p^2/4 \in \mathbb{R}1.$$

Tenemos entonces $y \in F \setminus \mathbb{R}1$ cuyo cuadrado es un escalar k. Veamos que dicho k es negativo:

$$y^2 = k$$

Si $k \geq 0$ tenemos

$$0 = y^2 - k1 = (y - \sqrt{k}1)(y + \sqrt{k}1)$$

luego $y = \sqrt{k}1$ o $y = -\sqrt{k}1$ contradicción. Luego $y^2 = k1$ con $k < 0$. Definamos entonces

$$i := y/\sqrt{-k}.$$

Es fácil ver que $i^2 = -1$ y que $\{1, i\}$ es linealmente independiente con lo que $F = \mathbb{R} \oplus \mathbb{R}i \cong \mathbb{C}$. $\square$

Lema 4 *Si A es un álgebra real de división de dimensión finita mayor que 1, siempre existe un elemento cuyo cuadrado es -1.*

Teorema 7 (Frobenius) *Toda álgebra real de división y de dimensión finita es isomorfa a $\mathbb{R}$, $\mathbb{C}$ o $\mathbb{H}$.*

Como corolario, las álgebras reales de división y dimensión finita solo pueden tener dimensión 1, 2 o 4.

Dem. del T. de Frobenius.

Sea D una $\mathbb{R}$-álgebra de división de dim. finita. Sea F un subespacio conmutativo de D de dimensión máxima. Definamos el centralizador de F en D como el subespacio

$$C_D(F) := \{x \in D \colon xy = yx,\ \forall y \in F\}.$$

Se tiene $F \subset C_D(F)$. Veamos que $F = C_D(F)$: tomemos $x \in C_D(F)$, entonces $F \subset F + \mathbb{R}x$ y por maximalidad de F se tiene $F = F + \mathbb{R}x$ lo que implica $x \in F$.

$$F = C_D(F).$$

Por un lado se tiene que F es cerrado para el producto: si $x, y \in F$ entonces para cada $f \in F$ se tiene $xyf = xfy = fxy$ luego $xy \in C_D(F) = F$. Por otra parte F es cerrado para la inversion: si $x \in F$ entonces $xf = fx$ para todo $f \in F$. Luego $f = x^{-1}fx$ luego $fx^{-1} = x^{-1}f$ por tanto $x^{-1} \in C_D(F) = F$. Esto no permite concluir que F es un cuerpo, y por lo tanto $F \cong \mathbb{R}$ o $F \cong \mathbb{C}$ como vimos antes. Ahora, si $\dim(D) = 1$ tenemos $D = \mathbb{R}$ y en este caso hemos terminado. Suponemos pues $\dim(D) > 1$. Por el Lema previo existe un elemento i de cuadrado -1.

Estamos en el caso $\dim(D) > 1$ y $\exists i \in D$ tal que $i^2 = -1$. Entonces F no puede ser $F = \mathbb{R}1$ porque $\mathbb{R}1 \oplus \mathbb{R}i$ es un subespacio conmutativo de dimensión 2 lo que contradice la maximalidad de F. Por lo tanto podemos tomar $F = \mathbb{R}1 \oplus \mathbb{R}i \cong \mathbb{C}$. D es un F-espacio vectorial por la izquierda Definamos

$$S \colon D \to D,\ \text{tal que } S(x) = xi$$

para cada x. Esta aplicación es F-lineal y como $S^2 = -1_D$, es diagonalizable.

Como S es raíz del polinomio $T^2 + 1 = 0$ los únicos posibles autovalores son $\pm i$. Sea $D_+ := \{x \in D \colon xi = ix\}$ es espacio propio de autovalor i,

$D_- := \{x \in D \colon xi = -ix\}$ es espacio propio de autovalor $-i$. Se tiene $D_+ \cap D_- = 0$ y $D = D_+ + D_-$. Esto último obedece a la igualdad

$$x = \frac{1}{2}(x - ixi) + \frac{1}{2}(x + ixi)$$

donde $x - ixi \in D_+$, $x + ixi \in D_-$.

$$D = D_+ \oplus D_-$$

$$D_+D_+ \subset D_+,\ D_-D_- \subset D_+,\ D_+D_- \subset D_-,\ D_-D_+ \subset D_-.$$

Por otra parte $D_+ \subset C_D(F) = F \subset D$ luego $D_+ = \mathbb{R}1 \oplus \mathbb{R}i$. Si $D_- = 0$ hemos demotrado que $D = D_+ \cong \mathbb{C}$. Supongamos $D_- \neq 0$.

Si fijamos $z \in D_- \setminus \{0\}$, la aplicación $D_+ \to D_-$ tal que $x \mapsto zx$ es un isomorfismo de espacios vectoriales (su inversa en $x \mapsto z^{-1}x$). Por lo tanto $\dim(D_+) = \dim(D_-)$ y $\dim(D) = 2\dim(D_+)$.

Sea $z \in D_-$ no nulo. Como z satisface una ecuación de segundo grado $z^2 = pz+q$ donde $p, q \in \mathbb{R}$. Por otra parte $z \in D_-$ luego $zi = -iz$ y $z^2i = iz^2$ lo que implica $pzi+qi = piz+qi$, es decir, $pzi = piz$ por tanto $p = 0$ y $z^2 \in \mathbb{R}1$.

$$z^2 = k1, \quad k \in \mathbb{R}$$

Si $k \geq 0$, tenemos

$$0 = z^2 - k1 = (z - \sqrt{k}1)(z + \sqrt{k}1)$$

luego $z = \pm\sqrt{k} \in \mathbb{R}$ una contradicción.

Así $k < 0$ y definiendo $j = z/\sqrt{-k}$ tenemos $j \in D_-$ tal que $j^2 = -1$. Definamos ahora $k = ij$.

$$k^2 = ijij = -i^2j^2 = j^2 = -1$$

$$ijk = kk = -1$$

por lo tanto

Además $1, i, j, k$ son linealmente idempendientes y $D = \mathbb{R}1 \oplus \mathbb{R}i \oplus \mathbb{R}j \oplus \mathbb{R}k$ satisfaciéndose

$$i^2 = j^2 = k^2 = ijk = -1.$$

En resumen

$$D \cong \mathbb{H}.$$

Demostración alternativa. Si $\dim(D) = 1$ tenemos $D \cong \mathbb{R}$. Si $\dim(D) = 2$ entonces A es un álgebra commutativa (y de división) luego es un cuerpo y por el Teorema 6 se tiene $D \cong \mathbb{C}$. Supongamos pues que $\dim(D) > 2$. Por el Lema 4 existe $i \in D$ tal que $i^2 = -1$. Sea $S\colon D \to D$ la aplicación dada por $S(x) = ixi^{-1}$. Como $S^2 = 1_D$ tenemos $D = D_1 \oplus D_{-1}$ donde $D_i = \{x \in D\colon S(x) = ix\}$ for $i = \pm 1$. Veamos que $D_1 = \mathbb{R}1 \oplus \mathbb{R}i$. Está claro que $\mathbb{R}1 \oplus \mathbb{R}i \subset D_1$. Si ahora tomamos $z \in D_1$, como z conmuta con i, la subálgebra de D generada por $1, i$ y z es conmutativa y de división. Esto implica que es 2-dimensional luego z es combinación lineal de 1 e i. Así $D_1 = \mathbb{R}1 \oplus \mathbb{R}i$. Tomemos $j \in D_{-1}$ tal que $j^2 = -1$ (analícese por qué esta elección es posible). Como $j \in D_{-1}$ se tiene $ij = -ji$. Definamos $k := ij$. Entonces $iki^{-1} = i(ij)i^{-1} = -j(-i) = ji = -k$ luego $k \in D_{-1}$. Además $\dim(D_1) = \dim(D_{-1})$ por lo que $D_{-1} = \mathbb{R}j \oplus \mathbb{R}k$. $\square$

4 Semisimplicidad

Un álgebra A se dice que es simple si $A^2 \neq 0$ y sus únicos ideales son 0 y A.

Si un álgebra A tiene unidad son equivalentes:

(1) A es simple.

(2) Los únicos ideales de A son 0 y A.

Como consecuencia de la teoría de Wedderburn-Artin, si A es un álgebra simple y de dimensión finita sobre un cuerpo K, se tiene que A es isomorfa a un álgebra $M_n(D)$ (matrices $n \times n$ con coeficientes en D) donde D es una K-álgebra de división y dimensión finita.

Corolario 4 *Si A es un álgebra compleja, simple y finito-dimensional,*

$$A \cong M_n(\mathbb{C})$$

para un cierto natural n.

En natural n del corolario anterior es único: si $M_n(\mathbb{C}) \cong M_k(\mathbb{C})$ entonces $n = k$.

Corolario 5 *Si A es un álgebra real, simple y finito-dimensional, A es isomorfa a $M_n(\mathbb{R})$, a $M_n(\mathbb{C})$ o a $M_n(\mathbb{H})$ para algún n.*

Al igual que antes, si $M_n(D) \cong M_k(D)$ entonces $n = k$ (válido para $D = \mathbb{R}, \mathbb{C}$ o $\mathbb{H}$). Además, $\forall n, k$ se tiene $M_n(\mathbb{R}) \ncong M_k(\mathbb{C})$, $M_n(\mathbb{R}) \ncong M_k(\mathbb{H})$, $M_n(\mathbb{C}) \ncong M_k(\mathbb{H})$.

Un álgebra A se dice *semisimple* si es suma directa de álgebras simples. Esto es equivalente a que A sea semisimple como módulo sobre si mismo a izquierda: ${}_AA$ es un A-módulo semisimple. Otra caracterización de la semisimplicidad de A es que todo A-submódulo de ${}_AA$ sea un sumando directo.

Teorema 8 *A es un álgebra semisimple (de dimensión finita) sobre un cuerpo K algebraicamente cerrado si y solo si A es isomorfa a*

$$M_{n_1}(K) \oplus \cdots \oplus M_{n_q}(K)$$

donde $n_i \in \mathbb{N}^*$. Los naturales n_i están determinados de forma única.

Teorema 9 *A es un álgebra semisimple (de dimensión finita) sobre $\mathbb{R}$ si y solo si A es isomorfa a*

$$M_{n_1}(D_1) \oplus \cdots \oplus M_{n_q}(D_q)$$

donde $n_i \in \mathbb{N}^*$ y cada D_i es $\mathbb{R}$, $\mathbb{C}$ o $\mathbb{H}$. Los naturales n_i y las álgebras D_i están determinados de forma única.

Problema 1 *¿Salvo isomorfismo, cuántas álgebras complejas semisimples de dimensión ≤ 4 hay?*

Solución:
Dimensión 1: $\mathbb{C}$
Dimensión 2: $\mathbb{C}^2$
Dimensión 3: $\mathbb{C}^3$
Dimensión 4: $\mathbb{C}^4$, $M_2(\mathbb{C})$.

Problema 2 *¿Salvo isomorfismo, cuántas álgebras reales semisimples de dimensión* ≤ 4 *hay?*

Solución:
Dimensión 1: $\mathbb{R}$
Dimensión 2: $\mathbb{R}^2$, $\mathbb{C}$
Dimensión 3: $\mathbb{R}^3$, $\mathbb{R} \oplus \mathbb{C}$
Dimensión 4: $\mathbb{R}^4$, $\mathbb{R}^2 \oplus \mathbb{C}$, $\mathbb{C}^2$, $\mathbb{H}$, $M_2(\mathbb{R})$.

5 Descomposición de Peirce

Sea A una R-álgebra (con unidad). R es un anillo no necesariamente un cuerpo. Supongamos que

$$\{e_1, \ldots, e_n\}$$

es un sistema de idempotentes ortogonales (i.e. $e_i e_j = \delta_{ij} e_i$) tales que $\sum_1^n e_i = 1$. Sea $A_{ij} := e_i A e_j = \{e_i x e_j : x \in A\}$ para $i, j = 1, \ldots, n$. Entonces

$$A = \bigoplus_{i,j=1}^{n} A_{ij}$$

Dem. Sea $x \in A$,

$$x = 1x1 = (\sum_i e_i)x(\sum_i e_j) = \sum_{ij} e_i x e_j \in \sum_{ij} A_{ij}.$$

Esto prueba que $A = \sum_{ij} A_{ij}$. Se deja al lector demostrar que la suma es directa.

Si A es conmutativa y $i \neq j$ se tiene $A_{ij} = e_i A e_j = A e_i e_j = 0$. Además $A_{ii} = e_i A e_i = A e_i = e_i A$. Luego en el caso conmutativo la descomposición de Peirce es

$$A = \oplus_1^n A e_i.$$

6 El álgebra grupo

Sea R un anillo conmutativo y unitario. Sea X un conjunto, definimos el R-módulo libre generado por X como el R-módulo RX de todas las aplicaciones $f : X \to R$ de soporte finito. Recordemos que

$$\mathrm{Sop}(f) := \{x \in X : f(x) \neq 0\}.$$

$$RX = \{f: X \to R| \text{ Sop}(f) \text{ es finito } \}$$

La aplicación $X \to RX$ tal que $x \mapsto f_x$, donde $f_x: X \to R$ viene dada por $f_x(y) = \delta_{xy}$ es una inyección por lo que identificamos X con su imagen en RX. Además todo elemento de RX es combinación lineal de ciertos f_x:

$$\forall f \in R(X), f = \sum_{x \in \text{Sop}(f)} f(x) f_x$$

Como el conjunto $\{f_x: x \in X\}$ es R-linealmente independiente es una base de RX, i.e. el R-módulo RX es libre. Cuando R es un cuerpo se obtiene el espacio vectorial libre generado por X. Como X se ha identificado con $\{f_x: x \in X\}$, podemos abusar un poco de la notación y escribir

$$RX = \{\sum_x \lambda_x x: \lambda_x \in R\}.$$

En caso de que $R = K$ un cuerpo, el K-espacio vectorial libre generado por un conjunto X es el conjunto de combinaciones lineales formales

$$\sum_x \lambda_x x$$

donde $x \in X$ y los escalares $\lambda_x \in K$ son nulos salvo un número finito.

Obviamente las operaciones que dan a RX estructura de R-módulo vienen dadas por

$$\sum_x \lambda_x x + \sum_x \mu_x x := \sum_x (\lambda_x + \mu_x) x,$$

$$\alpha \sum_x \lambda_x x := \sum_x \alpha \lambda_x x.$$

Si $X = G$ un grupo, entonces el R-módulo RG admite una estructura de R-álgebra

$$(\sum_g \lambda_g g)(\sum_h \mu_h h) := \sum_{g,h} \lambda_g \mu_h (gh).$$

Este álgebra RG es lo que se llama el "*álgebra grupo*"de G con coeficientes en R.

Ejemplo: $\mathbb{R}\mathbb{Z}_2$

$\mathbb{Z}_2 = \{1, u\}$ con $u^2 = 1$.

$$\mathbb{R}\mathbb{Z}_2 = \{\alpha 1 + \beta u: \alpha, \beta \in \mathbb{R}\}.$$

Busquemos los idempotentes de este álgebra $e = \alpha 1 + \beta u$,

$$e^2 = \alpha^2 1 + \beta^2 1 + 2\alpha\beta u = \alpha 1 + \beta u$$

$$\begin{cases} \alpha^2 + \beta^2 = \alpha \\ 2\alpha\beta = \beta. \end{cases}$$

Si $\beta \neq 0$ tenemos $\alpha = 1/2 \Rightarrow \beta = \pm 1/2$.
Si $\beta = 0$, tenemos $\alpha = 0, 1$.

Por lo tanto los idempotentes de $\mathbb{R}\mathbb{Z}_2$ son $0, 1, \frac{1}{2}(1+u), \frac{1}{2}(1-u)$. Definamos $e_1 := \frac{1}{2}(1+u)$, $e_2 := \frac{1}{2}(1-u)$. Estos dos idempotentes son ortogonales

$$e_1 e_2 = \frac{1}{4}(1+u)(1-u) = \frac{1}{4}(1^2 - u^2) = 0$$

y su suma es 1. Por lo tanto la descomposición de Peirce nos da

$$\mathbb{R}\mathbb{Z}_2 = \mathbb{R}e_1 \oplus \mathbb{R}e_2 \cong \mathbb{R} \oplus \mathbb{R}$$

ya que $\mathbb{R}e_1 \cong \mathbb{R}$ y $\mathbb{R}e_2 \cong \mathbb{R}$.

En realidad en la demostración anterior solo hemos utilizado que $1/2 \in \mathbb{R}$ por lo tanto el resultado es cierto para todo cuerpo de característica distinta de dos:

Teorema 10 *Si $car(K) \neq 2$ se tiene $K\mathbb{Z}_2 \cong K \oplus K$.*

7 Teorema de Maschke

Teorema 11 (Maschke) *Sea G un grupo finito y K un cuerpo cuya característica no divida al orden de G. Entonces el álgebra grupo KG es semisimple.*

Dem. Sea $A := KG$ y V un A-submódulo de A. Tenemos que demostrar que V es un sumando directo de A. Para ello tomamos un subespacio vectorial W complementario de V, es decir, $A = V \oplus W$ como espacios vectoriales. Sea $p\colon A \to A$ tal que $p(v) = v$ para cada $v \in V$ y $p(W) = 0$. La imagen de p está contenida en V y p es una aplicación lineal pero no es necesariamente un homomorfismo de A-módulos . Definamos $q\colon A \to A$ mediante la fórmula

$$q(x) = \frac{1}{|G|} \sum_{g \in G} gp(g^{-1}x).$$

Como $\mathrm{car}(K)$ no divide a $|G|$ el escalar $\frac{1}{|G|}$ pertenece a K lo que le da sentido a la fórmula de arriba. Por otra parte como la imagen de p es V cada elemento $gp(x) \in V$ para cada x. Luego la imagen de q está contenida en V. Es fácil demostrar que $q(x+y) = q(x) + q(y)$ para cualesquiera $x, y \in A$. Veamos que $q(hx) = hq(x)$ para cada $h \in G$ y $x \in A$.

$$q(hx) = \frac{1}{|G|} \sum_{g \in G} gp(g^{-1}hx) =$$

$$\frac{1}{|G|} \sum_{g \in G} hh^{-1}gp(g^{-1}hx) = h\frac{1}{|G|} \sum_{g \in G} h^{-1}gp(g^{-1}hx) =$$

$$h\frac{1}{|G|} \sum_{k \in G} kp(k^{-1}x) = hq(x).$$

Por lo tanto q es un homomorfismo de A-módulos $q\colon A \to A$. Además si $x \in V$ se tiene $g^{-1}x \in V$ luego $p(g^{-1}x) = g^{-1}x$ y $q(x) = x$. Veamos que $q^2 = q$. Como $q(x) \in V$, $q(q(x)) = q(x)$. Tenemos pues $q^2 = q$. Como q es un homomorfismo de A-módulos , $\ker(q)$ e $\mathrm{im}(q)$ son A-submódulos. Veamos que

$$A = \ker(q) \oplus \mathrm{im}(q).$$

Si $x \in \ker(q) \cap \mathrm{im}(q)$ tenemos $x = q(y)$ y además $0 = q(x) = q(q(y)) = q(y) = x$. Por tanto $\ker(q) \cap \mathrm{im}(q) = 0$.

Por otra parte para cada $a \in A$ se tiene $a = q(a) + a - q(a)$ donde $q(a) \in \mathrm{im}(q)$ y $a - q(a) \in \ker(q)$. Como $V = \mathrm{im}(q)$ concluimos

$$A = \ker(q) \oplus V. \ \square$$

Sesiones 2-3

8 Representaciones

Sea K un cuerpo, V un K-espacio vectorial y A una K-álgebra. Consideremos la K-álgebra $\mathrm{End}_K(V)$ de las aplicaciones lineales $V \to V$ (con la suma de aplicaciones, la composición y el producto por escalares habitual). Si $r\colon A \to \mathrm{End}_K(V)$ es un homomorfismo de K-álgebras, diremos que r es una representación de A en el espacio V. La dimensión de V se llamará *grado* de la representación (también *dimensión* de la representación).

Fijada un álgebra A, podemos definir la categoría $\mathrm{Rep}(A)$ cuyos objectos son todas las posibles representaciones $r\colon A \to \mathrm{End}_K(V)$ y cuyos morfismos definimos a continuación.

Definición 1 *Dadas dos representaciones $r_i\colon A \to End_K(V_i)$ $(i = 1, 2)$ una aplicación lineal $f\colon V_1 \to V_2$ diremos que es un homomorfismo de r_1 a r_2 si para cada $a \in A$, conmuta el diagrama*

$$\begin{array}{ccc} V_2 & \xrightarrow{r_2(a)} & V_2 \\ {\scriptstyle f}\uparrow & & \uparrow{\scriptstyle f} \\ V_1 & \xrightarrow[r_1(a)]{} & V_1 \end{array}$$

equivalentemente $f\ r_1(a) = r_2(a)\ f$ para cada $a \in A$.

Una representación r se dice fiel si r es un monomorfismo.

Definición 2 *Sea S un subespacio vectorial de un K-espacio V e $i\colon S \to V$ la inclusión. Sean $r'\colon A \to End_K(S)$ y $r\colon A \to End_K(V)$ dos representaciones. Diremos que r' es una subrepresentación de r si la inclusión es un homomorfismo de r' a r en la categoría $Rep(A)$. Equivalentemente: el subespacio S es r-invariante, lo que quiere decir que $r(a)(S) \subset S$ para cada $a \in A$. Dada una representación $r\colon A \to End_K(V)$, con $V \neq 0$, diremos que es irreducible cuando los únicos subespacios r-invariantes de V son el propio V y 0. Esto es equivalente a afirmar que las únicas subrepresentaciones de r son ella misma y la trivial.*

Definición 3 *Sea A una K-álgebra (recordemos que $1 \in A$) y V un K-espacio vectorial. Diremos que V es un A-módulo (de forma más precisa un A-módulo a izquierda) si existe una aplicación $A \times V \to V$ tal que $(a, v) \mapsto av$ sujeta a:*

1. *La aplicación es bilineal.*
2. *$\forall a_1, a_2 \in A, \forall v \in V,\ a_1(a_2 v) = (a_1 a_2)v$.*

3. $\forall v \in V,\ 1v = v$.

Denotemos por A-mod la categoría cuyos objetos son los A-módulos y cuyos morfismos son los homomorfismos de A-módulos . Recordemos que si M y N son A-módulos una aplicación lineal $f\colon M \to N$ se dice que es un homomorfismo de A-módulos cuando

$$\forall a \in A, \forall m \in M, \quad f(am) = af(m).$$

Teorema 12 *Existe un functor $F\colon Rep(A) \to A-mod$ tal que si $r \in Rep(A)$ viene dada por $r\colon A \to End_K(V)$, entonces $F(r) = V$ dotado de estructura de A-módulo con la operación $A \times V \to V$ dada por*

$$am = r(a)(m)$$

para cada $a \in A$ y $m \in M$.

Teorema 13 *Existe otro functor $G\colon A - mod \to Rep(A)$ tal que si M es un A-módulo entonces*

$$G(M) = r\colon A \to End_K(M)$$

viene dada por

$$r(a)(m) = am$$

para cada $a \in A$ y $m \in M$. Este G es el functor inverso de F en el sentido de que

$$GF = 1_{Rep(A)}, \quad FG = 1_{A-mod}.$$

Recordemos que si M y N son A-módulos con $M \subset N$, diremos que M es un submódulo de N cuando la aplicación de inclusión $i\colon M \to N$ es un homomorfismo de A-módulos . Un A-módulo $M \neq 0$ se dice simple si sus únicos A-submódulos son 0 y M.

En los functores

$$F\colon \mathrm{Rep}(A) \to A - \mathrm{mod}, \quad G\colon A - \mathrm{mod} \to \mathrm{Rep}(A)$$

se cumple

1. $r \in \mathrm{Rep}(A)$ es irreducible $\Leftrightarrow V = F(r)$ es una A-módulo simple.

2. M es un A-módulo simple $\Leftrightarrow G(M) = r$ es una representación irreducible.

Definición 4 (Representación regular) *Dada una K-álgebra A, llamamos representación regular de A (por la izquierda) al homomorfismo de álgebras $L\colon A \to End_K(A)$ tal que $a \mapsto L_a$ siendo $L_a\colon A \to A$ el operador de multiplicación por a a izquierda, es decir, $L_a(x) = xa$ para todo $x \in A$. El hecho de que L es un homomorfismo de K-álgebras obedece a que*

$$L_{ab} = L_a L_b$$

para cualesquiera $a, b \in A$.

Si calculamos el núcleo de la representación regular $\ker(L) = \{a \in A : L_a = 0\}$ resulta que si $L_a = 0$ entonces $0 = L_a(1) = a$ luego L es un monomorfismo de álgebras.

Proposición 2 *Toda álgebra asociativa (unital) se puede indentificar con una subálgebra de $End_K(A)$. Si además $dim(A) = n$ es finita, A se puede identificar con una subálgebra de $M_n(K)$.*

Proposición 3 *Toda álgebra asociativa (unital) se puede indentificar con una subálgebra de $End_K(A)$. Si además $dim(A) = n$ es finita, A se puede identificar con una subálgebra de $M_n(K)$.*

Para la segunda parte téngase en cuenta que

$$\mathrm{End}_K(A) \cong M_n(K)$$

siendo un isomorfismo el que asocia a cada aplicación lineal $T: A \to A$, su matriz relativa a una base fijada de antemano.

Por lo tanto toda álgebra asociativa unital de dimensión finita es (isomorfa a) una subálgebra del álgebra de matrices. Este es uno de los aspectos de la teoría de representaciones: el poder ver las álgebras como álgebras matriciales.

9 Representación regular de los cuaterniones

Vamos a explicitar la representación regular (a izq.) del álgebra $\mathbb{H}$. Para ello fijaremos la base $\{1, i, j, k\}$ de $\mathbb{H}$ tal que

$$i^2 = j^2 = k^2 = ijk = -1.$$

Sea $L: \mathbb{H} \to \mathrm{End}_{\mathbb{R}}(\mathbb{H})$ entonces $L_1 = 1$ y su matriz es la identidad 4×4.

$$L_i: \mathbb{H} \to \mathbb{H} \begin{cases} L_i(1) = i & (0,1,0,0) \\ L_i(i) = -1 & (-1,0,0,0) \\ L_i(j) = ij = k & (0,0,0,1) \\ L_i(k) = ik = -j & (0,0,-1,0) \end{cases}$$

$$L_j: \mathbb{H} \to \mathbb{H} \begin{cases} L_j(1) = j & (0,0,1,0) \\ L_j(i) = ji = -k & (0,0,0,-1) \\ L_j(j) = jj = -1 & (-1,0,0,0) \\ L_j(k) = jk = i & (0,1,0,0) \end{cases}$$

$$L_k: \mathbb{H} \to \mathbb{H} \begin{cases} L_k(1) = k & (0,0,0,1) \\ L_k(i) = ki = j & (0,0,1,0) \\ L_k(j) = kj = -i & (0,-1,0,0) \\ L_k(k) = kk = -1 & (-1,0,0,0) \end{cases}$$

Por lo tanto si llamamos $\theta\colon \mathrm{End}_{\mathbb{R}}(\mathbb{H}) \to M_4(\mathbb{R})$ al isomorfismo que envía cada aplicación lineal a su matriz en la base $\{1, i, j, k\}$, la composición $r := \theta L\colon \mathbb{H} \to M_4(\mathbb{R})$ actúa en la forma:

$$1 \mapsto I_4, \qquad i \mapsto \begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

$$j \mapsto \begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix}, \quad k \mapsto \begin{pmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

Y así a un quaternión genérico $q = a_0 + a_1 i + a_2 j + a_3 k$ (con $a_n \in \mathbb{R}$) le corresponde

$$r(q) = \begin{pmatrix} a_0 & -a_1 & -a_2 & -a_3 \\ a_1 & a_0 & -a_3 & a_2 \\ a_2 & a_3 & a_0 & -a_1 \\ a_3 & -a_2 & a_1 & a_0 \end{pmatrix}$$

El determinante de esta matriz es $(a_0^2 + a_1^2 + a_2^2 + a_3^2)^2$ por lo tanto si la matriz no es nula, es necesariamente inversible (otra forma de ver que $\mathbb{H}$ e un álgebra de división).

10 Representación regular del cuerpo $\mathbf{F}_4$

Para todo primo p y todo natural $n > 0$ existe un cuerpo (que es único salvo isomorfismo) de cardinal p^n. Dicho cuerpo que denotaremos por $\mathbf{F}_{p^n}$ es el cuerpo de descomposición del polinomio $x^{p^n} - x$ sobre $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$. El cuerpo $\mathbf{F}_4$ es el cuerpo de descomposición de $x^4 - x$ sobre $\mathbb{Z}_2$. Como $x^4 - x = x(x-1)(x^2+x+1) = x(x-1)(x-a)(x-b)$ tenemos $a + b = 1$, $ab = 1$ por la fórmula de Cardano-Vieta. De ahí se deduce $a^2 + 1 = a$ de donde $a^2 = b$ y análogamente $b^2 = a$. Por lo tanto $\mathbf{F}_4 = \{0, 1, a, b\}$ con tablas de sumar y multiplicar:

$+$	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

$\cdot$	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

El cuerpo $\mathbf{F}_4$ es un álgebra sobre $\mathbb{Z}_2$ con base $\{1, a\}$, es decir, $\mathbf{F}_4 = \mathbb{Z}_2 1 \oplus \mathbb{Z}_2 a$. En efecto hay solo cuatro $\mathbb{Z}_2$-combinaciones lineales de 1 y a que son: 0, 1, a, $1 + a = b$. Por lo tanto $\dim(\mathbf{F}_4) = 2$ como e.v. sobre $\mathbb{Z}_2$. La representación regular sera entonces $\rho\colon \mathbf{F}_4 \to M_2(\mathbb{Z}_2)$ y a cada elemento de $\mathbf{F}_4$ le hacemos corresponder la matriz del operador $L_x\colon \mathbf{F}_4 \to \mathbf{F}_4$. Por lo tanto $\rho(0) = 0$ y $\rho(1) = 1_2$ (matriz identidad 2×2). Además $\rho(a)$ es la matriz de L_a (por columnas). Como $L_a(1) = a$, $L_a(a) = a^2 = b = 1 + a$ tenemos

$$\rho(a) = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \qquad \rho(b) = 1 - \rho(a) = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}.$$

Luego $\mathbf{F}_4$ es isomorfo a la subálgebra de $M_2(\mathbb{Z}_2)$ generada por 1 y $\rho(a)$. Identificando $\mathbf{F}_4$ con esta subálgebra tenemos que un elemento genérico de $\mathbf{F}_4$ es

$$x\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} + y\begin{pmatrix}0 & 1\\ 1 & 1\end{pmatrix} = \begin{pmatrix}x & y\\ y & x+y\end{pmatrix},$$

donde $x, y \in \mathbb{Z}_2$. Por lo tanto podríamos haber definido

$$\mathbf{F}_4 = \{\begin{pmatrix}x & y\\ y & x+y\end{pmatrix} : x, y \in \mathbb{Z}_2\}.$$

11 Representaciones de grupos

Una representación de A es un homomorfismo de K-álgebras $r\colon A \to \mathrm{End}_K(A)$ pero si A es de dimensión finita n, fijando una base, tenemos un isomorfismo $\mathrm{End}_K(A) \cong M_n(K)$. Componiendo r con este isomorfismo obtenemos un homomorfismo de K-álgebras $r'\colon A \to M_n(K)$. Esto justifica que podemos definir una representación (matricial) de la K-álgebra A como un homomorfismo $r'\colon A \to M_n(K)$.

Sea V un K-espacio vectorial y denotemos por $\mathrm{GL}(V)$ el grupo de todas las aplicaciones lineales inversibles $T\colon V \to V$. Cuando V es de dimensión finita n, tenemos un isomorfimo $\theta\colon \mathrm{GL}(V) \cong \mathrm{GL}_n(K)$ siendo este último el grupo de matrices inversibles $n \times n$ con coeficientes en K. Fijada una base de V, el isomorfismo actúa asociando a cada T su matriz en la base fijada.

Definición 5 *Una representación de un grupo G en el espacio V no es más que un homomorfismo de grupos $\rho\colon G \to GL(V)$. La dimensión de V se llama el grado de la representación y V se dice que es el espacio de la representación. Si V es de dimensión finita, también podemos decir que una representación de G es el homomorfismo de grupos $\rho'\colon G \to GL_n(K)$ donde $\rho' = \theta\rho$.*

Fijado un grupo G, podemos considerar la categoría $\mathrm{Rep}_K(G)$ cuyos objetos son todas las representaciones de G en un K-espacio vectorial. Por otra parte dadas dos representaciones de $\rho_i\colon G \to \mathrm{GL}(V_i)$, $(i = 1, 2)$, diremos que $f\colon V_1 \to V_2$ es un morfismo de ρ_1 a ρ_2 cuando para todo $g \in G$, commute el diagrama:

$$\begin{array}{ccc} V_2 & \xrightarrow{\rho_2(g)} & V_2 \\ {\scriptstyle f}\uparrow & & \uparrow{\scriptstyle f} \\ V_1 & \xrightarrow[\rho_1(g)]{} & V_1 \end{array}$$

equivalentemente $f\ \rho_1(g) = \rho_2(g)\ f$.

Si S es un K-subespacio de V y tenemos dos representaciones $\rho\colon G \to \mathrm{GL}(V)$ y $\rho'\colon G \to \mathrm{GL}(S)$, diremos que ρ' es una subrepresentación de ρ cuando la inclusión $i\colon S \to V$ sea un

morfismo de ρ' a ρ. Esto equivale a afirmar que S es ρ-invariante (i.e. $\rho(g)(S) \subset S$ para todo $g \in G$). Una representación $\rho\colon G \to \mathrm{GL}(V)$ con $V \neq 0$ se dice irreducible si las unicas subrepresentaciones de ρ son la trivial y la propia ρ .

Sea G un grupo y M un K-espacio vectorial. Diremos que M es un G-módulo si existe una aplicación

$$G \times M \to M, \quad (g, m) \mapsto gm,$$

verificando:

1. $g(m_1 + m_2) = gm_1 + gm_2$,
2. $g(\lambda m) = \lambda gm$,
3. $g_1(g_2 m) = (g_1 g_2)m$,
4. $1m = m$,

con $g, g_1, g_2 \in G$, $m, m_1, m_2 \in M$, $\lambda \in K$.

Si M y N son espacios vectoriales sobre el mismo cuerpo K y además son G-módulos , una aplicación $f\colon M \to N$ se dice que es un homomorfismo de G-módulos si es K-lineal y cumple

$$f(gm) = gf(m)$$

para cada $m \in M$, $g \in G$. Ahora, fijado un cuerpo base K, podemos definir la categoría $G\text{-mod}_K$ cuyos objetos son todos los G-módulos (que son K-espacios vectoriales) y cuyos morfismos son los homomorfismos de G-módulos .

Si M y N son objetos de $G\text{-mod}_K$ y $M \subset N$, diremos que M es un G-submódulo de N si la inclusión de M en N es un homomorfismo de G-módulos . Un G-módulo no nulo M diremos que es simple si sus únicos submódulos son el trivial y él mismo. Por otra parte si M_1 y M_2 son elementos de $G\text{-mod}_K$ se define su suma directa como el K-espacio vectorial $M_1 \oplus M_2$ con estructura de G-módulo :

$$g(m_1 + m_2) := gm_1 + gm_2$$

para $g \in G$, $m_i \in M_i$, $(i = 1, 2)$.

Teorema 14 *Existe un functor $F\colon Rep_K(G) \to G - mod_K$ tal que dada $\rho\colon G \to GL(V)$ se tiene $F(\rho) = V$ dotado de estructura de G-módulo con la aplicación $G \times V \to V$ tal que $gv = \rho(g)(v)$. Existe un functor $H\colon G - mod_K \to Rep_K(G)$ tal que a cada G-módulo M le corresponde la representación $\rho\colon G \to GL(M)$ tal que $\rho(g)(m) = gm$. Además*

$$FH = 1_{G-mod_K}, HF = 1_{Rep_K(G)}.$$

En el anterior isomorfismo de categorías, las representaciones irreducibles se corresponden con los G-módulos simples. Dadas dos representaciones de $\mathrm{Rep}_K(G)$:

$$\rho_i\colon G \to \mathrm{GL}(V_i), (i = 1, 2),$$

podemos definir su suma directa

$$\rho_1 \oplus \rho_2 \colon G \to \mathrm{GL}(V_1 \oplus V_2)$$

como la representación tal que $(\rho_1 \oplus \rho_2)(g)(v_1 + v_2) := \rho_1(g)(v_1) + \rho_2(g)v_2$ para cada $g \in G$, $v_i \in V_i$, $i = 1, 2$.

Sean $\rho_i \colon G \to \mathrm{GL}(V_i)$, con $i = 1, 2$ dos representaciones de $\mathrm{Rep}_K(G)$.El functor $F \colon \mathrm{Rep}_K(G) \to G - \mathrm{mod}_K$ verifica

$$F(\rho_1 \oplus \rho_2) = V_1 \oplus V_2$$

es decir, transforma suma directa de representaciones en suma directa de G-módulos . El functor H inverso de F actúatransformando sumas directas de G-módulos en sumas directas de representaciones.

12 Recordatorio de algunas consecuencias de la teoría de Wedderburn-Artin

(1) Si D es una K-álgebra de división de dimensión finita y $A = M_n(D)$, el único A-módulo simple (salvo isomorfismos) es D^n y la estructura de A-módulo es la canónica $A \times D^n \to D^n$, $(M, v) \mapsto Mv$ donde $\forall M \in A$, $\forall v \in D^n$ (representado como vector columna), Mv es la multiplicación matricial considerando a v como una matriz $n \times 1$.
(2) Si $A = M_{n_1}(D_1) \oplus \cdots \oplus M_{n_q}(D_q)$, donde las D_i son K-álgebras de división finito-dimensionales, entonces salvo isomorfismo, los únicos A-módulos simples son los correspondientes $D_i^{n_i}$y dos cualesquiera de ellos son no isomorfos como A-módulos . Además en caso de que $D_i = K$ para cada i se tiene:

$$\dim(A) = n_1^2 + \cdots + n_q^2.$$

Por lo tanto las representaciones irreducibles de un álgebra semisimple A, son las asociadas a los A-módulos simples (todo salvo isomorfismo). Esto quiere decir que todas ellas aparecen en la descomposición de A como suma de álgebras simples.

Recordemos que un conjunto completo de representaciones irreducibles S de un álgebra A, se define como un conjunto de representaciones irreducibles no isomorfas dos a dos y tales que cualquier representación irreducible de A es isomorfa a alguna de S. Si seleccionamos un conjunto completo de representaciones irreducibles de un álgebra semisimple finito-dimensional A, la dimensión de A coincide con la suma de los cuadrados de los grados de dichas representaciones irreducibles.

Sesiones 3-4

Recordemos que dada una categoría $\mathcal{C}$ y dos objectos X, Y de $\mathcal{C}$, un isomorfimo de X a Y es una flecha $f\colon X \to Y$ de $\mathcal{C}$ tal que existe otra flecha $g\colon Y \to X$ de $\mathcal{C}$ de modo que $fg = 1_Y$, $gf = 1_X$. En la categoría $\mathrm{Rep}_K(G)$, dado un objecto $\rho\colon G \to \mathrm{GL}(V)$, la identidad $1\colon \rho \to \rho$ es la aplicación identidad $1\colon V \to V$.

Dos representaciones $\rho_i\colon G \to \mathrm{GL}(V_i)$ son isomorfas si existen aplicaciones K-lineales $t\colon V_1 \to V_2$ y $s\colon V_2 \to V_1$ tales que $ts = 1_{V_2}$, $st = 1_{V_1}$ y

$$\begin{cases} \rho_2(g)t = t\rho_1(g) \\ \rho_1(g)s = s\rho_2(g) \end{cases}$$

para cada $g \in G$.

Definición 6 *Una representación de grado uno es $\rho\colon G \to GL(V)$ con $dim(V) = 1$. Por tanto $V \cong K$ y $GL(V) \cong K^\times := K \setminus \{0\}$. La representación se identifica con un homomorfismo de grupos $\rho\colon G \to K^\times$.*

Si $\rho_i\colon G \to K^\times$ son dos representaciones de grado uno isomorfas, la condición de isomorfa

$$\begin{cases} \rho_2(g)t = t\rho_1(g) \\ \rho_1(g)s = s\rho_2(g) \end{cases}$$

se convierte en $\rho_2(g) = \rho_1(g)$ para cada g. Por tanto $\rho_1 = \rho_2$.

Nota 4 *Dos representaciones de grado uno de un mismo grupo son isomorfas si y solo si son iguales.*

Problema 3 *Determinar las representaciones irreducibles complejas del grupo Δ_3.*

$$\Delta_3 = \{1, g, g^2, s, sg, sg^2\}.$$
$$\Delta_3 = \langle s, g\colon s^2 = g^3 = 1, sg = g^2 s\rangle.$$

El álgebra grupo $\mathbb{C}\Delta_3$ tiene dimensión 6 y es semisimple. Solo hay dos posibilidades:

$$\mathbb{C}^6, \quad M_2(\mathbb{C}) \oplus \mathbb{C}^2$$

Como el grupo Δ_3 no es abeliano llegamos a que $\mathbb{C}\Delta_3 \cong M_2(\mathbb{C}) \oplus \mathbb{C}^2$. Por lo tanto Δ_3 solo tiene tres representaciones irreducibles: las asociadas a los módulos simples: $\mathbb{C}^2$, $\mathbb{C}$ y $\mathbb{C}$ del álgebra grupo. Vamos a intentar determinar dichas representaciones.

Supongamos una representación compleja $\rho\colon G \to \mathrm{GL}(V)$ con $\dim(V) = 1$. En ese caso $V \cong \mathbb{C}$ y $\mathrm{GL}(V) \cong \mathbb{C}^* := \mathbb{C} \setminus \{0\}$. Por tanto podemos identificar la representación con un

homomorfismo de grupos $\rho\colon G \to \mathbb{C}^*$. En el caso del grupo dihédrico Δ_3 sea $\rho\colon \Delta_3 \to \mathbb{C}^*$ y escribamos $s' = \rho(s)$, $g' = \rho(g)$. Se debe tener entonces

$$s'^2 = 1 = g'^3, s'g' = g'^2 s'$$

lo que implica $g' = 1$ y $s' = \pm 1$. Estas son entonces dos representaciones irreducibles distintas

$$\begin{array}{cc} \Delta_3 \to \mathbb{C}^* & \Delta_3 \to \mathbb{C}^* \\ s \mapsto 1 & s \mapsto -1 \\ g \mapsto 1 & g \mapsto 1 \end{array}$$

Vamos a describir la representación irreducible de grado 2.

$$\Delta_3 \to \mathrm{GL}_2(\mathbb{C}), \quad s \mapsto s', g \mapsto g'$$

$s'^2 = 1 = g'^3$ luego las dos matrices son diagonalizables. Si ponemos $s' = \pm 1$ entonces $s'g' = g'^2 s'$ implica $g' = 1$ y esta representación no es irreducible. Por tanto s' es de orden dos $s' \neq \pm 1$. Como es diagonalizable podemos tomar

$$s' = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Si ahora escribimos

$$g' = \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix}$$

e imponemos la condiciones $g'^3 = 1$, $s'g' = g'^3 s'$ encontramos las soluciones:

$$x_4 = -\frac{1}{2}, \quad x_3 \neq 0, \quad x_2 = -\frac{3}{4x_3}, \quad x_1 = -\frac{1}{2}$$

$$g' = \begin{pmatrix} -\frac{1}{2} & \frac{\sqrt{3}}{2} \\ -\frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix}$$

En definitiva tenemos la representación $\Delta_3 \to \mathrm{GL}_2(\mathbb{C})$ tal que

$$s \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \text{simetría respecto al eje } X \ ,$$

$$g \mapsto \begin{pmatrix} -\frac{1}{2} & \frac{\sqrt{3}}{2} \\ -\frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix}, \text{giro de } \tfrac{2\pi}{3} \text{ rad. entorno al origen.}$$

Problema 4 *¿Cuál es el álgebra grupo del grupo A_4 (permutaciones pares del grupo simétrico S_4)?*

Sol. El grupo simétrico S_n siempre admite como subgrupo a A_n que es el formado por todas las permutaciones pares. El orden de A_n es $\frac{n!}{2}$. Por tanto $|A_4| = 12$. El álgebra grupo $\mathbb{C}A_4$ es de dimensión 12, semisimple y no conmutativa. Ademas 12 se expresa como suma de cuadrados en las siguientes formas:

Descomp.	$\mathbb{C}A_4$	IRREPS
$12 = 2^2 + 1^2 + \cdots_{(8)} \cdots + 1^2$	$M_2(\mathbb{C}) \oplus \mathbb{C}^8$	9
$12 = 2^2 + 2^2 + 1^2 + \cdots_{(4)} \cdots + 1^2$	$M_2(\mathbb{C})^2 \oplus \mathbb{C}^4$	6
$12 = 2^2 + 2^2 + 2^2$	$M_2(\mathbb{C})^3$	3
$12 = 3^2 + 1^2 + 1^2 + 1^2$	$M_3(\mathbb{C}) \oplus \mathbb{C}^3$	4

donde IRREPS= no. de repr. irred. complejas

Calculamos las clases de conjugación del grupo A_4.

$$A_4 = \{1, (12)(34), (13)(24), (14)(23), (234), (243), (134), (143), (124), (142), (123), (132)\}$$

Clases de conjugación

$[1] = 1$
$[(12)(34)] = \{(12)(34), (13)(24), (14)(23)\}$
$[(123)] = \{(123), (142), (134), (243)\}$
$[(132)] = \{(132), (143), (124), (234)\}$
Hay cuatro clases de conjugación.

$$\mathbb{C}A_4 \cong M_3(\mathbb{C}) \oplus \mathbb{C}^3$$

El grupo A_4 tiene (salvo isomorfismo) una representación irreducible de grado 3 y tres representaciones irreducibles de grado 1. Demostraremos este resultado más tarde: el número de representaciones irreducibles complejas de un grupo finito coincide con el número de sus clases de conjugación.

13 Reducibilidad completa

Recordemos que fijado un cuerpo K, la categoría $\mathrm{Rep}_K(G)$ de representaciones del grupo G es isomorfa a la categoría de G-módulos . Esta, a su vez, es isomorfa a la categoría de KG-módulos . Si asumimos las hipótesis habituales de que G es un grupo finito y la característica de K no divide a $|G|$, sabemos que KG es semisimple.

Si A es un álgebra semisimple, todo A-módulo es semisimple. En particular todo KG-módulo es semisimple por tanto es suma directa de módulos simples. Usando el isomorfismo $\mathrm{Rep}_K(G) \cong KG - \mathrm{mod}$ resulta que toda representación de G es suma directa de representaciones irreducibles.

Explicitemos un poco esta afirmación: como la suma directa de KG-módulos es un concepto claro, podemos usar el isomorfismo de categorías para explicitar el concepto de suma directa de representaciones: tomemos dos representaciones de G en sendos K-espacios V_1 y V_2:

Entonces $\rho_1 \colon G \to \mathrm{GL}(V_1)$ y $\rho_2 \colon G \to \mathrm{GL}(V_2)$. La suma $\sigma := \rho_1 \oplus \rho_2$ es la nueva representación

$$\sigma \colon G \to \mathrm{GL}(V_1 \oplus V_2), \quad \sigma(g) \colon V_1 \oplus V_2 \to V_1 \oplus V_2$$

tal que $\sigma(g)(v_1+v_2) = \rho_1(g)(v_1)+\rho_2(g)(v_2)$. En terminos matriciales, si $\rho_1\colon G \to \mathrm{GL}_{n_1}(K)$, $\rho_2\colon G \to \mathrm{GL}_{n_2}(K)$, entonces $\sigma = \rho_1 \oplus \rho_2$ es la representación $\sigma\colon G \to \mathrm{GL}_{n_1+n_2}(K)$ tal que

$$\sigma(g) = \begin{pmatrix} \rho_1(g) & 0 \\ 0 & \rho_2(g) \end{pmatrix}.$$

Teorema 15 *Para toda representación $\tau\colon G \to GL_n(K)$ existe una descomposición $n = n_1 + \ldots + n_q$ y q representaciones irredudibles $\rho_i\colon G \to GL_{n_i}(K)$ tal que τ es isomorfa a la representación*

$$\begin{array}{c} G \to GL_n(K) \\ g \mapsto \begin{pmatrix} \rho_1(g) & \cdots & 0 \\ \vdots & & \vdots \\ 0 & \cdots & \rho_q(q) \end{pmatrix}. \end{array}$$

Teorema 16 *Si G es un grupo finito y K un cuerpo cuya característica no divida al orden de G, toda representación de G es suma directa de representaciones irreducibles.*

Teorema 17 *Si A es una K-álgebra de dimensión finita, cada A-módulo simple es de dimensión finita:*

Dem. Sea M un A-módulo simple. Como $M \neq 0$ (por definición) tomemos $0 \neq m \in M$. Por simplicidad $M = Am$ y la aplicación $\varphi\colon A \to Am = M$ tal que $a \mapsto am$ es un epimorfismo lo que implica que $M \cong A/\ker(\varphi)$ en particular $\dim(M)$ es finita. □

Corolario 6 *Si G es un grupo finito, cada representación irreducible de G es de grado finito (la dimensión del espacio de la representación es finita).*

14 Producto tensorial de representaciones

Si V y W son espacios vectoriales sobre el cuerpo K, podemos definir su producto tensorial como el K-espacio vectorial libre generado por el producto cartesiano $V \times W$ módulo el subespacio S generado por los elementos

$$(\alpha v_1 + \beta v_2, w) - \alpha(v_1, w) - \beta(v_2, w),$$

$$(v, \alpha w_1 + \beta w_2) - \alpha(v, w_1) - \beta(v, w_2),$$

para $\alpha, \beta \in K$, $v, v_1, v_2 \in V$, $w, w_1, w_2 \in W$.

Por lo tanto

$$V \otimes W := K(V \times W)/S.$$

Normalmente la clase de equivalencia de un elemento $(v, w) \in V \times W$ en el cociente $K(V \times W)/S$ se denota por $v \otimes w$. Siendo así, tenemos las igualdades

$$(\alpha v_1 + \beta v_2) \otimes w = \alpha(v_1 \otimes w) + \beta(v_2 \otimes w),$$

$$v \otimes (\alpha w_1 + \beta w_2) = \alpha(v \otimes w_1) + \beta(v \otimes w_2),$$

para $\alpha, \beta \in K$, $v, v_1, v_2 \in V$, $w, w_1, w_2 \in W$.

Es bien sabido que si $\{v_i\}_{i\in I}$ es una base de V y $\{w_j\}_{j\in J}$ una base de W, entonces $\{v_i \otimes w_j\}_{(i,j)\in I\times J}$ es una base de $V \otimes W$. Como corolario, si $v \otimes w = 0$ se tiene $v = 0$ o $w = 0$.

Definición 7 *Sea G un grupo, K un cuerpo fijo y V, W dos K-espacios vectoriales. Supongamos dadas sendas representaciones $\rho_i\colon G \to GL(V_i)$, $(i = 1, 2)$. Entonces el producto de dichas representaciones es la nueva representación*

$$\pi := \rho_1 \otimes \rho_2\colon G \to GL(V_1 \otimes V_2)$$

tal que $\pi(g)(v_1 \otimes v_2) := \rho_1(v_1) \otimes \rho_2(v_2)$, para cualesquiera $v_i \in V_i$.

15 Producto tensorial de matrices

Sean $A = (a_{ij}) \in M_n(K)$, $B \in M_q(K)$. Definimos $A \otimes B \in M_{nq}(K)$ como

$$A \otimes B = \begin{pmatrix} a_{11}B & \cdots & a_{1n}B \\ \vdots & & \vdots \\ a_{n1}B & \cdots & a_{nn}B \end{pmatrix}$$

Ejemplo. $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$, $B = \begin{pmatrix} b_{11} & b_{12} & b_{13} \\ b_{21} & b_{22} & b_{23} \\ b_{31} & b_{32} & b_{33} \end{pmatrix}$. Entonces $A \otimes B$ es

$$\left(\begin{array}{ccc|ccc} a_{11}b_{11} & a_{11}b_{12} & a_{11}b_{13} & a_{12}b_{11} & a_{12}b_{12} & a_{12}b_{13} \\ a_{11}b_{21} & a_{11}b_{22} & a_{11}b_{23} & a_{12}b_{21} & a_{12}b_{22} & a_{12}b_{23} \\ a_{11}b_{31} & a_{11}b_{32} & a_{11}b_{33} & a_{12}b_{31} & a_{12}b_{32} & a_{12}b_{33} \\ \hline a_{21}b_{11} & a_{21}b_{12} & a_{21}b_{13} & a_{22}b_{11} & a_{22}b_{12} & a_{22}b_{13} \\ a_{21}b_{21} & a_{21}b_{22} & a_{21}b_{23} & a_{22}b_{21} & a_{22}b_{22} & a_{22}b_{23} \\ a_{21}b_{31} & a_{21}b_{32} & a_{21}b_{33} & a_{22}b_{31} & a_{22}b_{32} & a_{22}b_{33} \end{array}\right)$$

Esto permite definir el producto tensorial de representaciones en términos matriciales: Si $\rho_i\colon G \to \mathrm{GL}_{n_i}(K)$ son representaciones de G, entonces podemos definir el producto tensorial $\pi = \rho_1 \otimes \rho_2\colon G \to \mathrm{GL}_{n_1 n_2}(K)$ de modo que

$$\pi(g) = \rho_1(g) \otimes \rho_2(g).$$

Con anterioridad, hemos definido la suma de representaciones de un grupo. Ahora acabamos de definir un producto de representaciones. Esto sugiere la posibilidad de definir una estructura de anillo en el conjunto de las representaciones de un grupo. Para formalizar esta idea consideremos fijado un cuerpo K y un grupo G finito. En el conjunto de todas

las clases de isomorfía de representaciones finito-dimensionales de G (lo que incluye las irreducibles), definiremos una estructura de anillo.

Si $A = KG$ y M, un A-módulo . representaremos por $[M]$ la clase de isomorfía de M:

$$[M] := \{N \in \mathrm{Obj}(A - \mathrm{mod}) \colon N \cong M \text{ en } A\text{-mod}\}.$$

Dados dos A-módulos M y N podemos definir una suma

$$[M] + [N] := [M \oplus N].$$

Esta operación está bien definida tiene neutro $[0]$ y es asociativa y conmutativa. El conjunto de clases de isomorfía de A-módulos (f.d.) es un monoide conmutativo.

Ahora dado un monoide conmutativo M existe una forma canónica de sumergirlo en un grupo (el grupo de Grothendieck de M). Dicho grupo es

$$\mathcal{G} := (M \times M)/\equiv$$

donde $(x, y) \equiv (s, t)$ si y solo si existe $k \in M$ tal que

$$x + t + k = y + s + k.$$

Sea $\overline{(m, n)}$ la clase de equivalencia del elemento (m, n). La operación que da estructura de grupo a $\mathcal{G}$ es

$$\overline{(m, n)} + \overline{(s, t)} := \overline{(m + s, n + t)}.$$

Podemos representar las clases de equivalencia de (m, n) de la forma $m-n$. Si el monoide M es cancelativo hay un monomorfismo de monoides $M \to G$ tal que $m \mapsto [(m, 0)] = m-0$.

Tomemos pues el grupo de Grothendieck $\mathcal{G}$ del monoide de las clases de isomorfía de todos los KG-módulos de dimensión finita.

El lector de estas notas puede demostrar que el conjunto de clases de isomorfía de $A = KG$-módulos simples (equivalentemente, representaciones irreducibles de G) es una base como $\mathbb{Z}$-módulo de $\mathcal{G}$: dicho de otro modo $\mathcal{G}$ es un $\mathbb{Z}$-módulo libre con base las clases de isomorfía de representaciones irreducibles del grupo G.

16 El anillo de representaciones de un grupo

Dado un grupo G finito, el $\mathbb{Z}$-módulo libre $\mathcal{G}$ que tiene como base las clases de isomorfía de representaciones irreducibles se puede dotar de estructura de anillo. Para ello basta definir el producto de elementos de la base. Si $[\rho_1]$ y $[\rho_2]$ son dos clases siendo ρ_1 y ρ_2 irreducibles definimos

$$[\rho_1] \cdot [\rho_2] := [\rho_1 \otimes \rho_2].$$

Como $\rho_1 \otimes \rho_2$ es de grado finito, es suma directa (finita) de representaciones irreducibles.

El resto de comprobaciones de que $\mathcal{G}$ con este producto es un anillo (conmutativo) son consecuencia de las propiedades del producto tensorial.

Problema 5 *Determinar el anillo de representaciones del grupo* Δ_3.

Recordemos que las tres clases de isomorfía de representaciones irreducibles complejas son:

$$\begin{array}{cc} 1\colon \Delta_3 \to \mathbb{C}^* & u\colon \Delta_3 \to \mathbb{C}^* \\ s \mapsto 1 & s \mapsto -1 \\ g \mapsto 1 & g \mapsto 1 \end{array}$$

$$d\colon \Delta_3 \to \mathrm{GL}_2(\mathbb{C})$$
$$s \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$
$$g \mapsto \begin{pmatrix} -\frac{1}{2} & \frac{\sqrt{3}}{2} \\ -\frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix}.$$

$$\begin{array}{cc} 1 \otimes 1 = 1 & 1 \otimes u = u \\ u \otimes u = 1 & 1 \otimes d = d \end{array}$$

Calculamos $u \otimes d$.

$$(u \otimes d)(s) = -1 \otimes \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$$
$$(u \otimes d)(g) = 1 \otimes \begin{pmatrix} -\frac{1}{2} & \frac{\sqrt{3}}{2} \\ -\frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix} = \begin{pmatrix} -\frac{1}{2} & \frac{\sqrt{3}}{2} \\ -\frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix}$$

$$u \otimes d\colon \Delta_3 \to \mathrm{GL}_2(\mathbb{C})$$
$$s \mapsto \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$$
$$g \mapsto \begin{pmatrix} -\frac{1}{2} & \frac{\sqrt{3}}{2} \\ -\frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix}$$

Esta representación es isomorfa a d: la matriz $M = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ cumple

$$M \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} M^{-1} = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$$
$$M \begin{pmatrix} -\frac{1}{2} & \frac{\sqrt{3}}{2} \\ -\frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix} M^{-1} = \begin{pmatrix} -\frac{1}{2} & \frac{\sqrt{3}}{2} \\ -\frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix}$$

Concluimos que:

$$u \otimes d \cong d$$

Finalmente calculamos $d \otimes d$:

$$(d \otimes d)(s) = d(s) \otimes d(s) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} =$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$(d \otimes d)(g) = d(g) \otimes d(g) = \begin{pmatrix} -\frac{1}{2} & \frac{\sqrt{3}}{2} \\ -\frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix} \otimes \begin{pmatrix} -\frac{1}{2} & \frac{\sqrt{3}}{2} \\ -\frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix} =$$

$$\begin{pmatrix} \frac{1}{4} & -\frac{\sqrt{3}}{4} & -\frac{\sqrt{3}}{4} & \frac{3}{4} \\ \frac{\sqrt{3}}{4} & \frac{1}{4} & -\frac{3}{4} & -\frac{\sqrt{3}}{4} \\ \frac{\sqrt{3}}{4} & -\frac{3}{4} & \frac{1}{4} & -\frac{\sqrt{3}}{4} \\ \frac{3}{4} & \frac{\sqrt{3}}{4} & \frac{\sqrt{3}}{4} & \frac{1}{4} \end{pmatrix}$$

Luego $d \otimes d$ viene dada por

$$s \mapsto \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} := S$$

$$g \mapsto \begin{pmatrix} \frac{1}{4} & -\frac{\sqrt{3}}{4} & -\frac{\sqrt{3}}{4} & \frac{3}{4} \\ \frac{\sqrt{3}}{4} & \frac{1}{4} & -\frac{3}{4} & -\frac{\sqrt{3}}{4} \\ \frac{\sqrt{3}}{4} & -\frac{3}{4} & \frac{1}{4} & -\frac{\sqrt{3}}{4} \\ \frac{3}{4} & \frac{\sqrt{3}}{4} & \frac{\sqrt{3}}{4} & \frac{1}{4} \end{pmatrix} =: G$$

Vamos a demostrar que

$$d \otimes d \cong 1 \oplus u \oplus d.$$

Definamos

$$v_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix},\ v_2 = \begin{pmatrix} 0 \\ -1 \\ 1 \\ 0 \end{pmatrix},\ v_3 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ -1 \end{pmatrix},\ v_4 = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}.$$

a) Se tiene que $Sv_1 = v_1, Gv_1 = v_1$, luego $\mathbb{C}v_1$ es $d \otimes d$-invariante. La restricción $d \otimes d\colon \Delta_3 \to \mathrm{GL}(\mathbb{C}v_1)$ es una irrep. isomorfa a 1.

b) Como $Sv_2 = -v_2, Gv_2 = v_2$, tenemos que $\mathbb{C}v_2$ es $d \otimes d$-invariante. La restricción $d \otimes d\colon \Delta_3 \to \mathrm{GL}(\mathbb{C}v_2)$ es una irrep. isomorfa a u.

c) Las igualdades

$$Sv_3 = v_3, \quad Gv_3 = -\frac{1}{2}v_3 + \frac{\sqrt{3}}{2}v_4$$

$$Sv_4 = -v_4, \quad Gv_4 = -\frac{\sqrt{3}}{2}v_3 - \frac{1}{2}v_4,$$

implican que el subespacio $\mathbb{C}v_3 \oplus \mathbb{C}v_4$ es $d \otimes d$-invariante. La restricción $d \otimes d \colon \Delta_3 \to \mathrm{GL}(\mathbb{C}v_3 \oplus \mathbb{C}v_4)$ es isomorfa a d. Por lo tanto $d \otimes d \cong 1 \oplus u \oplus d$. En resumen, la tabla de multiplicar del anillo de representaciones de Δ_3 es

$\otimes$	$[1]$	$[u]$	$[d]$
$[1]$	$[1]$	$[u]$	$[d]$
$[u]$	$[u]$	$[1]$	$[d]$
$[d]$	$[d]$	$[d]$	$[1] + [u] + [d]$

Este anillo es isomorfo al subanillo de $\mathbb{Z}^3$ dado por

$$\mathbb{Z}(1,1,1) \oplus \mathbb{Z}(-1,1,1) \oplus \mathbb{Z}(0,-1,2).$$

El isomorfismo es el inducido por

$$\begin{aligned} [1] &\mapsto (1,1,1) \\ [u] &\mapsto (-1,1,1) \\ [d] &\mapsto (0,-1,2). \end{aligned}$$

Sesiones 4-5

Empezaremos esta sección con un resultado clásico en teoría de representaciones.

Teorema 18 *Sea G un grupo finito. El número de clases de isomorfía de representaciones irreducibles complejas coincide con el número de clases de conjugación de G*

Dem. $KG = M_{n_1}(\mathbb{C}) \oplus \cdots \oplus M_{n_q}(\mathbb{C})$ y el número de representaciones irreducibles complejas es q.

$$Z(KG) = \mathbb{C} \oplus \cdots \oplus \mathbb{C} \quad \text{(hay } q\text{-sumandos)} ,$$

por lo tanto $\dim(Z(KG)) = q$. Veamos que hay tantas clases de conjugación como $\dim(Z(KG))$: Sea $z \in Z(KG)$ y pongamos $z = \sum_{g\in G} \lambda_g g$. Para todo $h \in G$ se tiene

$$z = hzh^{-1} = \sum_g \lambda_g hgh^{-1} = \sum_{g'} \lambda_{h^{-1}g'h} g' =$$

$$\sum_g \lambda_{h^{-1}gh} g.$$

por tanto $\lambda_g = \lambda_{h^{-1}gh}$ para todo h. Todos los conjugados de g tienen el mismo escalar en la expresión $z = \sum_{g\in G} \lambda_g g$. Luego si denotamos por g^* la suma de todos los conjugados de g, tenemos un g^* por cada clase de conjugación. Además

$$z = \sum \lambda_g g^*$$

lo que quiere decir que el conjunto de los diferentes g^* es un sistema de generadores de $Z(KG)$. Además son L.I. porque si $\sum \lambda_g g^* = 0$ como las clases de conjugación forman una partición del grupo, se tiene $\lambda_g = 0$. Por tanto $\{g^*\}$ es una base de $Z(KG)$ y $q = \dim(Z(KG))$ = número de clases de conjugación de G. $\square$.

17 Teoría de caracteres.

Recordermos que la traza de una matriz cuadrada es la suma de los elementos de su diagonal. Si denotamos por tr la traza de una matriz, se trata de una aplicación lineal

$$\text{tr: } M_n(K) \to K$$

dada por $\text{tr}(a_{ij}) = \sum_i a_{ii}$. Esta aplicación lineal cumple que

$$\forall A, B \in M_n(K),\ \text{tr}(AB) = \text{tr}(BA).$$

Por lo tanto si P es cualquier matriz inversible

$$\mathrm{tr}(PAP^{-1}) = \mathrm{tr}(A)$$

para toda $A \in M_n(K)$. Esta propiedad permite definir el concepto de traza de una aplicación lineal $f: V \to V$ siendo V un e.v. de dim. finita. En efecto: fijemos una base B de V y definamos

$$\mathrm{tr}(f) := \mathrm{tr}(M_B(f))$$

siendo $M_B(f)$ la matriz de f relativa a la base B. La definición no depende de la base elegida porque si B' es otra base, existe una matriz inversible tal que $M_{B'}(f) = PM_B(f)P^{-1}$ y entonces $\mathrm{tr}(M_{B'}(f)) = \mathrm{tr}(M_B(f))$.

Por lo tanto tenemos una aplicación lineal

$$\mathrm{tr}: \mathrm{End}_K(V) \to K$$

tal que $\forall f, g \in \mathrm{End}_K(V)$, se cumple

$$\mathrm{tr}(fg) = \mathrm{tr}(gf).$$

Definición 8 *Carácter de una representación. Dada una representacion de grado finito $\rho: G \to GL(V)$ de un grupo G en el espacio V, definimos el carácter de ρ (denotado χ_ρ) como la aplicación*

$$\chi_\rho: G \to K$$

tal que $\forall g \in G$, se tiene $\chi_\rho(g) := \mathrm{tr}(\rho(g))$.

Problema 6 *Calcular el carácter de la representación de Δ_3 dada por $d: \Delta_3 \to GL_2(\mathbb{C})$ siendo*

$$d(s) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad d(g) = \begin{pmatrix} -1/2 & \sqrt{3}/2 \\ -\sqrt{3}/2 & -1/2 \end{pmatrix}.$$

Sol.: Tenemos

$$d(g^2) = \begin{pmatrix} -\frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix}, d(sg) = \begin{pmatrix} -\frac{1}{2} & \frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & \frac{1}{2} \end{pmatrix},$$

$$d(sg^2) = \begin{pmatrix} -\frac{1}{2} & -\frac{\sqrt{3}}{2} \\ -\frac{\sqrt{3}}{2} & \frac{1}{2} \end{pmatrix}.$$

Por tanto el carácter χ_d de la representación es:

	1	g	g^2	s	sg	sg^2
χ_d	2	-1	-1	0	0	0

Problema 7 *Determinar la tabla de caracteres de Δ_3.*

Aparte de la representación de grado dos, cuyo carácter hemos calculado en el problema anterior, teníamos dos representaciones irreducibles de grado uno no isomorfas

$$\begin{array}{cc} 1\colon \Delta_3 \to \mathbb{C}^\times & u\colon \Delta_3 \to \mathbb{C}^\times \\ s \mapsto 1 & s \mapsto -1 \\ g \mapsto 1 & g \mapsto 1 \end{array}$$

La table completa de caracteres de Δ_3 es:

	1	g	g^2	s	sg	sg^2
χ_1	1	1	1	1	1	1
χ_u	1	1	1	-1	-1	-1
χ_d	2	-1	-1	0	0	0

Nota 5 *A partir de aquí, el cuerpo base será* $\mathbb{C}$.

Algunas consecuencias de las definiciones:

1. Para toda representación $\rho\colon G \to \mathrm{GL}(V)$, $\chi_\rho(1) = \dim(V)$.
2. Si $\dim(V) = 1$, se tiene $\chi_\rho = \rho$.
3. Si ρ_1 y ρ_2 son representaciones isomorfas de G,

$$\chi_{\rho_1} = \chi_{\rho_2}.$$

Dem. La condición de isomorfía implica la existencia de un isomorfismo lineal $f\colon V_1 \to V_2$ tal que $\forall g \in G$, $\rho_2(g)f = f\rho_1(g)$. Entonces $\rho_2(g) = f\rho_1(g)f^{-1}$ luego $\chi_{\rho_2}(g) = \chi_{\rho_1}(g)$ por tanto $\chi_{\rho_1} = \chi_{\rho_2}$.

4. Si $\rho\colon G \to \mathrm{GL}(V)$ es una representación compleja, $\forall g \in G$ se tienen $\chi_\rho(g^{-1}) = \overline{\chi_\rho(g)}$.
   Dem. Como $\rho(g)$ es diagonalizable su traza es la suma de sus autovalores.

$$\rho(g) = p\ \mathrm{diag}(\lambda_1, \ldots, \lambda_q)p^{-1}$$

$$\rho(g^{-1}) = p\ \mathrm{diag}(\lambda_1^{-1}, \ldots, \lambda_q^{-1})p^{-1}$$

Pero cada λ_i es de norma unidad ya que $\rho(g)$ es de orden finito (todo endomorfismo de orden finito tiene autovalores que son raíces n-ésimas de la unidad). Así

$$\overline{\chi_\rho(g)} = \sum_i \overline{\lambda_i} = \sum_i \lambda_i^{-1} = \mathrm{tr}(\rho(g^{-1})) = \chi_\rho(g^{-1}).$$

Teorema 19 *Si A es un álgebra de dimensión finita sobre un cuerpo K algebraicamente cerrado y M es un A-módulo simple, entonces $\forall f \in End_A(M)$ no nulo, existe $\lambda \in K^\times (= K \setminus \{0\})$ tal que $f = \lambda 1_M$.*

Dem. $ker(f)$ es una A-submódulo de M luego $\ker(f) = 0$ (no puede ser $\ker(f) = M$ porque $f \neq 0$). Análogamente $\mathrm{Im}(f) = M$. Luego f es un automorfismo. Por lo tanto todo elemento no nulo del álgebra $\mathrm{End}_A(M)$ es inversible lo que quiere decir que $\mathrm{End}_A(M)$ es un álgebra de división (y de dimensión finita por serlo M). Como K es algebraicamente cerrado, $\mathrm{End}_A(M) \cong K$ luego todo elemento es múltiplo escalar de la identidad. $\square$

Sean $\rho_1 \colon G \to \mathrm{GL}(V)$ y $\rho_2 \colon G \to \mathrm{GL}(W)$ dos representaciones de G. Suponemos que V y W son K-espacios vectoriales. Definamos por $\hom(V, W)$ el K espacio de todas las aplicaciones lineales $V \to W$. Si V y W son finito-dimensionales $\hom(V, W)$ cumple

$$\dim(\hom(V, W)) = \dim(V)\dim(W).$$

Denotemos por $\hom_G(V, W)$ el subespacio de $\hom(V, W)$ de todas las $f \colon V \to W$ tales que $f(gv) = gf(v)$ para cada $g \in G$, $v \in V$.

Teorema 20 (Teorema dimensional) *Supongamos que $\rho_1 \colon G \to GL(V)$ y $\rho_2 \colon G \to GL(W)$ son irreps de G.*

1. *Si $\rho_1 \ncong \rho_2$ se tiene $hom_G(V, W) = 0$.*
2. *Sea K algebraicamente cerrado. Si $\rho_1 \cong \rho_2$ se tiene $dim(hom_G(V, W)) = 1$.*

Dem Sea $f \in \hom_G(V, W)$. V y W son G-módulos simples luego $\ker(f)$ es 0 o V. Análogamente $\mathrm{Im}(f) = 0$ o W. Como las representaciones no son isomorfas, V no es isomorfo a W como G-módulo . Por tanto $\ker(f) = V$, $\mathrm{Im}(f) = 0$. En este caso $\hom_G(V, W) = 0$. Supogamos ahora que $\rho_1 \cong \rho_2$ y K algebraicamente cerrado. Existe un isomorfismo de G-módulos $f \colon V \to W$. Para cualquier otro $g \in \hom_G(V, W)$ se tiene $f^{-1}g \in \mathrm{End}_G(V) \cong K$ por tanto $f^{-1}g = \lambda 1$ 'para algún $\lambda \in K^\times$, luego $g = \lambda f$ y $\dim(\hom_G(V, W)) = 1$. $\square$

Definición 9 *Sea $\rho \colon G \to GL(V)$ una representación en el K-espacio vectorial V. Sea $V^* := hom_K(V, K)$ el dual de V. Definimos la representación dual $\rho^* \colon G \to GL(V^*)$ mediante*

$$\rho^*(g)(f) = f\rho(g^{-1})$$

para cada $g \in G$, $f \colon V \to K$ elemento de V^*.

Problema 8 *Demostrar que $\forall g \in G$, $\chi_{\rho^*}(g) = \overline{\chi_\rho(g)}$.*

Recordemos que si V y W son K-espacios vectoriales de dimensión finita, hay un isomorfismo

$$\theta \colon V^* \otimes W \cong \hom(V, W)$$

tal que $f \otimes w \mapsto f(\ )w$ siendo esta, la aplicación $V \to W$ tal que $v \mapsto f(v)w$:

$$[f(\ )w](v) := f(v)w$$

para cada $f \in V^*$, $w \in W$, $v \in V$. Para convencerse de dicho isomorfismo, es fácil ver que θ es un monomorfismo y como ambos espacios tienen la misma dimensión, θ es un isomorfismo.

Proposición 4 *Si $A \in M_n(K)$, $B \in M_q(K)$ entonces* $\mathrm{tr}(A \otimes B) = \mathrm{tr}(A)\mathrm{tr}(B)$.

Dem. Si $A = (a_{ij})$ entonces

$$\mathrm{tr}(A \otimes B) = \mathrm{tr} \begin{pmatrix} a_{11}B & \cdots & a_{1n}B \\ \vdots & & \vdots \\ a_{n1}B & \cdots & a_{nn}B \end{pmatrix} =$$

$$a_{11}\mathrm{tr}(B) + \cdots + a_{nn}\mathrm{tr}(B) = \mathrm{tr}(A)\mathrm{tr}(B).$$

□

Corolario 7 *Si $\rho_i \colon G \to GL(V_i)$ para $i = 1, 2$ son representaciones de G en los K-espacios V_1 y V_2, entonces $\chi_{\rho_1 \otimes \rho_2}(g) = \chi_{\rho_1}(g)\chi_{\rho_2}(g)$ para cada $g \in G$.*

Dem.

$$\chi_{\rho_1 \otimes \rho_2}(g) = \mathrm{tr}(\rho_1(g) \otimes \rho_2(g)) =$$
$$\mathrm{tr}(\rho_1(g))\mathrm{tr}(\rho_2(g)) = \chi_{\rho_1}(g)\chi_{\rho_2}(g).$$

□

Si $\rho_1 \colon G \to \mathrm{GL}(V)$ y $\rho_2 \colon G \to \mathrm{GL}(W)$ son representaciones de G en los K-espacios V yW, podemos definir la representación

$$\rho_1 \vdash \rho_2 \colon G \to \mathrm{GL}(\hom(V, W))$$

tal que $(\rho_1 \vdash \rho_2)(g) \colon \hom(V, W) \to \hom(V, W)$ viene dada por

$$T \mapsto \rho_2(g) T \rho_1(g^{-1}).$$

El isomorfismo $\theta \colon V^* \otimes W \to \hom(V, W)$ descrito anteriormente, induce un isomorfismo de representaciones

$$\rho_1 \vdash \rho_2 \cong \rho_1^* \otimes \rho_2.$$

Compruebe el lector que para cada $g \in G$ se tienen cuadrados conmutativos

$$\begin{array}{ccc} V^* \otimes W & \xrightarrow{(\rho_1^* \otimes \rho_2)(g)} & V^* \otimes W \\ \downarrow{\scriptstyle \theta} & & \downarrow{\scriptstyle \theta} \\ \hom(V, W) & \xrightarrow[(\rho_1 \vdash \rho_2)(g)]{} & \hom(V, W) \end{array}$$

Corolario 8

$$\chi_{\rho_1 \vdash \rho_2} = \chi_{\rho_1^* \otimes \rho_2}$$

En particular, para representaciones complejas, $\forall g \in G$ se tiene

$$\chi_{\rho_1 \vdash \rho_2}(g) = \chi_{\rho_1^*}(g)\chi_{\rho_2}(g) = \overline{\chi_{\rho_1}(g)}\chi_{\rho_2}(g). \tag{1}$$

Recordemos que si S es un subespacio de un K-espacio vectorial V, y fijamos una descomposición $V = S \oplus S'$, una aplicación $p\colon V \to V$ tal que $p(x) = x$ para cada $x \in S$ y $p(S') = 0$ se llamará una proyección en S. En este caso si V es de dimensión finita,

$$\mathrm{tr}(p) = \dim(S).$$

En efecto, en una base conveniente de V, la matriz de p es

$$\begin{pmatrix} I_n & 0 \\ 0 & 0 \end{pmatrix}, \quad n = \dim(S).$$

Lema 5 *Para que una aplicación $f\colon V \to V$ sea una proyección en un subespacio S de V es suficiente que*

1. *$f^2 = f$, y*
2. *$f(x) = x$ si y solo si $x \in S$.*

Dem. Si p es una proyección en S, el núcleo de p es S' y su imagen S. Por lo tanto $V = \ker(p) \oplus \mathrm{Im}(f)$. Además como $p(x) \in S$ se tiene $p(p(x)) = x$ para todo x. Recíprocamente, si se cumplen las dos condiciones, es fácil comprobar que $\ker(f) \cap \mathrm{Im}(f) = 0$ (porque si $z \in \ker(f) \cap \mathrm{Im}(f)$ se tiene $z = f(q)$ luego $0 = f(z) = f(f(q)) = f(q) = z$). Además $\forall x \in V$, $x = f(x) + (x - f(x))$ y $x - f(x) \in \ker(f)$. Por tanto

$$V = \mathrm{Im}(f) \oplus \ker(f).$$

Además, si $x \in S$, tenemos $x = f(x) \in \mathrm{Im}(f)$. Por otra parte si $x \in \mathrm{Im}(f)$ tenemos $x = f(y)$ luego $f(x) = f(f(y)) = f(y) = x$ lo que implica $x \in S$. Concluimos que

$$S = \mathrm{Im}(f).$$

y f es una proyección en S. □

Sea G un grupo finito, $\rho_1\colon G \to \mathrm{GL}(V)$ y $\rho_2\colon G \to \mathrm{GL}(W)$ representaciones complejas de G. Definamos $F\colon \hom(V,W) \to \hom(V,W)$ por

$$F(T) = \frac{1}{|G|} \sum_{g \in G} \rho_2(g) T \rho_1(g^{-1}).$$

Lema 6 *La imagen de F es $hom_G(V,W)$.*

Lo primero que vamos a demostrar es que siendo $S := F(T)$, se tiene $S \in \hom_G(V, W)$. Para ello sea $v \in V$, $h \in G$:

$$S(hv) = S(\rho_1(h)(v)) =$$

$$\frac{1}{|G|}\sum_{g\in G}\rho_2(g)\{T[\rho_1(g^{-1})(\rho_1(h)(v))]\} =$$

$$\frac{1}{|G|}\sum_{g\in G}\rho_2(g)\{T[\rho_1(g^{-1}h)(v))]\} =$$

$$\frac{1}{|G|}\rho_2(h)\sum_{g\in G}\rho_2(h^{-1}g)\{T[\rho_1(g^{-1}h)(v))]\} =$$

$$\frac{1}{|G|}\rho_2(h)\sum_{g\in G}\rho_2(h^{-1}g)\{T[\rho_1(g^{-1}h)(v))]\} =$$

$$\rho_2(h)\frac{1}{|G|}\sum_{k\in G}\rho_2(k)T\rho_1(k^{-1})(v) =$$

$$\rho_2(h)(S(v)) = hS(v).$$

Esto prueba que $\mathrm{Im}(F) \subset \hom_G(V, W)$.

Veamos ahora $\hom_G(V, W) \subset \mathrm{Im}(F)$. Sea $T \in \hom_G(V, W)$. Entonces $\forall g \in G$ se tiene $\rho_2(g)T = T\rho_1(g)$ por tanto

$$F(T) = \frac{1}{|G|}\sum_{g\in G}\rho_2(g)T\rho_1(g^{-1}) =$$

$$\frac{1}{|G|}\sum_{g\in G}T\rho_1(g)\rho_1(g^{-1}) = \frac{1}{|G|}\sum_{g\in G}T = T,$$

luego $T \in \mathrm{Im}(F)$. Como corolario $F^2 = F$ y en consecuencia

$$\mathrm{tr}(F) = \dim(\hom_G(V, W)).$$

□

Corolario 9 *Si las irreps $\rho_1 : G \to GL(V)$ y $\rho_2 : G \to GL(W)$ son isomorfas, entonces* $\mathrm{tr}(F) = 1$*, en caso contrario* $\mathrm{tr}(F) = 0$.

Véase el Teorema 20

Definición 10 *Si $\rho_1 : G \to GL(V)$ y $\rho_2 : G \to GL(W)$ son representaciones complejas de grado finito de un grupo finito G, definimos el producto escalar de sus caracteres:*

$$\langle \chi_{\rho_1}, \chi_{\rho_2} \rangle := \frac{1}{|G|}\sum_{g\in G}\chi_{\rho_1}(g)\overline{\chi_{\rho_2}(g)}$$

Esta aplicación es lineal en la variable de la izquierda y conjugado-lineal en la variable de la derecha:

$$\langle \chi_1 + \chi_2, \chi_3 \rangle = \langle \chi_1, \chi_3 \rangle + \langle \chi_2, \chi_3 \rangle,$$
$$\langle \chi_1, \chi_2 + \chi_3 \rangle = \langle \chi_1, \chi_2 \rangle + \langle \chi_1, \chi_3 \rangle,$$
$$\langle k\chi_1, \chi_2 \rangle = k\langle \chi_1, \chi_2 \rangle,$$
$$\langle \chi_1, k\chi_2 \rangle = \bar{k}\langle \chi_1, \chi_2 \rangle,$$

Para cualquier $k \in \mathbb{C}$ y caracteres χ_i, $i = 1, \ldots, 4$.

Además

$$\langle \chi_1, \chi_2 \rangle = \overline{\langle \chi_2, \chi_1 \rangle}$$

y

$$\forall \chi,\ \langle \chi, \chi \rangle \geq 0.$$
$$\forall \chi (\langle \chi, \chi \rangle = 0 \text{ si y solo si } \chi = 0).$$

Teorema 21 *Si $\rho_1 \colon G \to GL(V)$ y $\rho_2 \colon G \to GL(W)$ son irreps complejas del grupo finito G cuyos caracteres son respectivamente χ_1 y χ_2, entonces*

$$\langle \chi_1, \chi_2 \rangle = \begin{cases} 1 & si\ \rho_1 \cong \rho_2 \\ 0 & si\ \rho_1 \ncong \rho_2 \end{cases}$$

Dem. Recordemos que $F \colon \hom(V, W) \to \hom(V, W)$ dada por

$$F(T) = \frac{1}{|G|} \sum_{g \in G} \rho_2(g) T \rho_1(g^{-1}).$$

tiene $\mathrm{tr}(F) = 1$ si $\rho_1 \cong \rho_2$ y $\mathrm{tr}(F) = 0$ en caso contrario (véase Corolario 9). Además:

$$(\rho_1 \vdash \rho_2)(g)(T) = \rho_2(g) T \rho_1(g^{-1}) \Rightarrow$$

$$F = \frac{1}{|G|} \sum_g (\rho_1 \vdash \rho_2)(g)$$

$$F = \frac{1}{|G|} \sum_g (\rho_1 \vdash \rho_2)(g)$$

$$\mathrm{tr}(F) = \frac{1}{|G|} \sum_g \mathrm{tr}(\rho_1 \vdash \rho_2)(g)) = \frac{1}{|G|} \sum_g \chi_{\rho_1 \vdash \rho_2}(g)) =$$

$$\frac{1}{|G|} \sum_g \overline{\chi_{\rho_1}(g)} \chi_{\rho_2}(g) = \langle \chi_{\rho_2}, \chi_{\rho_1} \rangle = \overline{\langle \chi_{\rho_1}, \chi_{\rho_2} \rangle}.$$

Luego $\langle \chi_{\rho_1}, \chi_{\rho_2} \rangle$ es nulo si $\rho_1 \ncong \rho_2$ y 1 si $\rho_1 \cong \rho_2$. $\square$

Teorema 22 *Sea G un grupo finito y $\rho: G \to GL(V)$ una representación compleja de grado finito. Descompongamos ρ como suma directa de irreps de G:*

$$\rho \cong \sum_i n_i \rho_i$$

con $n_i \in \mathbb{Z} \setminus \{0\}$ y cada ρ_i es una irrep. ($\rho_i \ncong \rho_j$ si $i \neq j$). Sea $\tau: G \to GL(W)$ una irrep. compleja cualquiera de G. Entonces $\langle \chi_\rho, \chi_\tau \rangle = n_i$ siendo $\rho_i \cong \tau$.

Dem. Se tiene que

$$\langle \chi_\rho, \chi_\tau \rangle = \sum_i n_i \langle \chi_{\rho_i}, \chi_\tau \rangle,$$

y el único sumando no nulo es aquel en que $\tau \cong \rho_i$. Por tanto

$$\langle \chi_\rho, \chi_\tau \rangle = n_i$$

donde $\tau \cong \rho_i$.

Teorema 23 *Sea G un grupo finito. Una representación compleja $\rho: G \to GL(V)$ de grado finito es irreducible si y solo si su carácter χ cumple $\langle \chi, \chi \rangle = 1$.*

Dem. Ya hemos visto que si ρ es irreducible $\langle \chi, \chi \rangle = 1$. Veamos el recíproco. Sabemos $\langle \chi, \chi \rangle = 1$, descompongamos ρ como suma de irreps

$$\rho = \sum_i n_i \rho_i$$

con $n_i \geq 0$ (enteros) y las ρ_i no isomorfas dos a dos.

Entonces $\chi = \sum_i n_i \chi_i$ siendo $\chi_i := \chi_{\rho_i}$.

$$1 = \langle \chi, \chi \rangle = \langle \sum_i n_i \chi_i, \sum_j n_j \chi_j \rangle = \sum_{i,j} n_i n_j \langle \chi_i, \chi_j \rangle =$$

$$\sum_i n_i^2$$

Por lo tanto solo puede haber un n_i y vale 1. Luego ρ es irreducible.

18 Irreps de $\mathbb{Z}_n$

Todas las irreps complejas de un grupo abeliano finito son de grado 1: sea $\rho: G \to \mathrm{GL}(V)$ con $\dim(V)$ finita y G abeliano finito. El conjunto $\{\rho(g)\}_{g \in G} \subset \mathrm{GL}(V)$ es un conjunto de aplicaciones diagonalizables y que conmutan dos a dos. Es sabido que existe una base de V tal que todas las $\rho(g)$ diagonalizan en dicha base. Si tomamos un elemento v de dicha

base, el subespacio generado por v es por lo tanto ρ-invariante. Como ρ es irreducible, V es el subespacio generado por v luego $\dim(V) = 1$.

Por lo tanto todas las irreps complejas de $\mathbb{Z}_n$ son de grado uno, es decir, homomorfismos de grupos $\mathbb{Z}_n \to \mathbb{C}^\times$. Sabemos que hay tantas irreps complejas como clases de conjugación del grupo. Como el grupo es abeliano, hay tantas clases de conjugación como elementos en el grupo. Por lo tanto, salvo isomorfismo, solo hay n irreps de $\mathbb{Z}_n$.

Vamos a calcularlas. Si ponemos $\mathbb{Z}_n = \langle \pi : \pi^n = 1 \rangle$ todo homomorfismo $\rho : \mathbb{Z}_n \to \mathbb{C}^\times$ queda determinado por $\rho(\pi)$ que es una raíz n-ésima de la unidad. Escribiendo $\omega = \exp(\frac{2\pi}{n} i)$ tenemos las representaciones $\rho_0, \rho_1, \ldots, \rho_{n-1}$ definidas por

$$\rho_k(\pi) = \omega^k.$$

Como son todas distintas, son todas ellas no isomorfas.

Algunos ejemplos

$\mathbb{Z}_2$	1	π
ρ_0	1	1
ρ_1	1	-1

$\mathbb{Z}_3$	1	π	π^2
ρ_0	1	1	1
ρ_1	1	ω	ω^2
ρ_2	1	ω^2	ω

$\omega = \exp 2\pi i/3$

$\mathbb{Z}_4$	1	π	π^2	π^3
ρ_0	1	1	1	1
ρ_1	1	i	-1	$-i$
ρ_2	1	-1	1	-1
ρ_3	1	$-i$	-1	i

Teorema 24 *En un el grupo $G = \mathbb{Z}_n$, por cada irrep ρ de G tenemos un idempotente*

$$e_\rho := \frac{1}{|G|} \sum_{g \in G} \rho(g) g$$

en el álgebra grupo $\mathbb{C}G$. Si ρ y τ son irreps no isomorfas $e_\rho e_\tau = 0$. Además

$$\sum_\rho e_\rho = 1.$$

Dem.

$$e_\rho e_\tau = \frac{1}{|G|^2} \sum_{g,h} \chi_\rho(g) \chi_\tau(h) gh =$$

$$\frac{1}{|G|^2} \sum_{g,h} \chi_\rho(g) \chi_\tau(g^{-1}gh) gh =$$

$$\frac{1}{|G|^2}\sum_{g,h}\chi_\rho(g)\chi_\tau(g^{-1})\chi_\tau(gh)gh =$$

$$\frac{1}{|G|}\sum_{g}\chi_\rho(g)\chi_\tau(g^{-1})\frac{1}{|G|}\sum_{h}\chi_\tau(gh)gh =$$

$$\frac{1}{|G|}\sum_{g}\chi_\rho(g)\chi_\tau(g^{-1})\frac{1}{|G|}\sum_{h}\chi_\tau(gh)gh = \langle\chi_\rho,\chi_\tau\rangle e_\tau$$

$$e_\rho e_\tau = \langle\chi_\rho,\chi_\tau\rangle e_\tau$$

luego

$$e_\rho^2 = e_\rho, \qquad e_\rho e_\tau = 0, \text{ si } \rho \neq \tau.$$

Veamos que $\sum_\rho e_\rho = 1$.

Para demostrar

$$\sum_\rho e_\rho = 1$$

tengamos en cuenta que las representaciones son $\rho_0, \ldots, \rho_{n-1}$ y que $\rho_k(\pi) = \omega^k$.

$$e_{\rho_k} = \frac{1}{n}\sum_{j=0}^{n-1}\rho_k(\pi^j)\pi^j = \frac{1}{n}\sum_{j=0}^{n-1}\omega^{jk}\pi^j$$

$$\sum_\rho e_\rho = \frac{1}{n}\sum_{k=0}^{n-1}\sum_{j=0}^{n-1}\omega^{jk}\pi^j = \frac{1}{n}\sum_{j=0}^{n-1}(\sum_{k=0}^{n-1}\omega^{jk})\pi^j$$

Por lo tanto

$$\sum_\rho e_\rho = \frac{1}{n}\sum_{j=0}^{n-1}(\sum_{k=0}^{n-1}\omega^{jk})\pi^j.$$

$$\text{Para } j \neq 0, \quad \sum_{k=0}^{n-1}\omega^{jk} = \frac{1-\omega^{jn}}{1-\omega^j} = 0 \text{ pues } \omega^n = 1$$

$$\text{Para } j = 0, \quad \sum_{k=0}^{n-1}\omega^{jk} = n$$

$$\sum_\rho e_\rho = 1.$$

Así, el álgebra grupo compleja de $\mathbb{Z}_n$ se descompone como

$$\mathbb{C}\mathbb{Z}_n = \bigoplus_\rho \mathbb{C}e_\rho$$

donce ρ varía en el conjunto de representaciones irreducibles (dos a dos no isomorfas) de $\mathbb{Z}_n$. Sabemos además que hay exactamente n de tales representaciones.

Ejemplos

$\mathbb{Z}_2$	1	π
ρ_0	1	1
ρ_1	1	-1

$$e_{\rho_0} = \tfrac{1}{2}(1+\pi),\quad e_{\rho_1} = \tfrac{1}{2}(1-\pi)$$

$$\mathbb{C}\mathbb{Z}_2 = \mathbb{C}e_0 \oplus \mathbb{C}e_1$$

donde $e_i := e_{\rho_i}$, $i = 0, 1$.

Siendo $\omega = \exp 2\pi i/3$,

$\mathbb{Z}_3$	1	π	π^2
ρ_0	1	1	1
ρ_1	1	ω	ω^2
ρ_2	1	ω^2	ω

$$\begin{aligned} e_{\rho_0} &= \tfrac{1}{3}(1+\pi+\pi^2) \\ e_{\rho_1} &= \tfrac{1}{3}(1+\omega\pi+\omega^2\pi^2) \\ e_{\rho_2} &= \tfrac{1}{3}(1+\omega^2\pi+\omega\pi^2) \end{aligned}$$

$$\mathbb{C}\mathbb{Z}_3 = \mathbb{C}e_0 \oplus \mathbb{C}e_1 \oplus \mathbb{C}e_2,$$

$$e_i := e_{\rho_i}, i = 1, 2, 3.$$

19 La ecuación de tercer grado

Sobre el cuerpo de funciones racionales $F = \mathbb{C}(x_1, x_2, x_3)$ tomemos el polinomio

$$(x - x_1)(x - x_2)(x - x_3) \in F[x].$$

Consideremos los polinomios simétricos en las indeterminadas x_i, $i = 1, 2, 3$:

$$\sigma_1 := x_1 + x_2 + x_3, \quad \sigma_2 := x_1x_2 + x_1x_3 + x_2x_3, \quad \sigma_3 := x_1x_2x_3.$$

Definamos $A := \frac{1}{3}(x_1 + \omega x_2 + \omega^2 x_2)$, $B := \frac{1}{3}(x_1 + \omega^2 x_2 + \omega x_3)$, donde $\omega := e^{2\pi i/3}$. Entonces $\sum_i x_i^2 = \sigma_1^2 - 2\sigma_2$. Por otra parte para expresar $\sum_i x_i^3$ en función de los polinomios simétricos tenemos que hacer lo siguiente:

$$\sigma_1(\sigma_1^2 - 2\sigma_2) = \sum_i x_i \sum_i x_i^2 = \sum_i x_i^3 + \sum_{i \neq j} x_i^2 x_j.$$

También

$$\sigma_1^3 = (\sum_i x_i)^3 = \sum_i x_i^3 + 3\sum_{i \neq j} x_i^2 x_j + 6x_1x_2x_3 \Rightarrow \sigma_1^3 - 6\sigma_3 = \sum_i x_i^3 + 3\sum_{i \neq j} x_i^2 x_j,$$

por lo tanto tenemos el sistema:

$$\begin{cases} \sum x_i^3 + \sum_{i \neq j} x_i^2 x_j = \sigma_1(\sigma_1^2 - 2\sigma_2) \\ \sum x_i^3 + 3\sum_{i \neq j} x_i^2 x_j = \sigma_1^3 - 6\sigma_3 \end{cases}$$

de donde

$$\sum x_i^3 = \frac{1}{2}\begin{vmatrix} \sigma_1(\sigma_1^2 - 2\sigma_2) & 1 \\ \sigma_1^3 - 6\sigma_3 & 3 \end{vmatrix} = \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3$$

$$\sum_{i\neq j} x_i^2 x_j = \frac{1}{2}\begin{vmatrix} 1 & \sigma_1(\sigma_1^2 - 2\sigma_2) \\ 1 & \sigma_1^3 - 6\sigma_3 \end{vmatrix} = \sigma_1\sigma_2 - 3\sigma_3.$$

A continuación vamos a expresar

$$A := \frac{1}{3}(x_1 + \omega x_2 + \omega^2 x_3), \quad B := \frac{1}{3}(x_1 + \omega^2 x_2 + \omega x_3)$$

como polinomios en σ_1, σ_2 y s_3. Trabajando un poco el asunto se llega a:

$$\begin{cases} A^3 + B^3 = \frac{2}{27}\sigma_1^3 - \frac{1}{3}\sigma_1\sigma_2 + \sigma_3 \\ AB = \frac{1}{9}\sigma_1^2 - \frac{1}{3}\sigma_2 \end{cases}$$

de donde podemos expresar A y B como funciones (con radicales) dependientes de los polinomios simétricos.

Ahora consideremos la ecuación cúbica $x^3+px+q = 0$ con $p, q \in \mathbb{C}$. Entonces las fórmulas de Cardano-Vieta nos dicen que $\sigma_1 = x_1 + x_2 + x_3 = 0$, $\sigma_2 = x_1x_2 + x_1x_3 + x_2x_3 = p$, $\sigma_3 = x_1x_2x_3 = -q$. Consideremos el subespacio vectorial $\mathcal{R}$ de $\mathbb{C}(x_1, x_2, x_3)$ generado por x_1, x_2 y x_3 y el grupo cíclico de tres elementos: $\mathbb{Z}_3 = \{1, \pi, \pi^2\}$ (notación multiplicativa). El álgebra grupo $\mathbb{C}\mathbb{Z}_3$ admite una representación en $\mathcal{R}$ inducida por la acción $\mathbb{Z}_3 \times \mathcal{R} \to \mathcal{R}$ tal que $\pi x_1 = x_2$, $\pi x_2 = x_3$ y $\pi x_3 = x_1$. Las representaciones irreducibles complejas de $\mathbb{Z}_3$ son:

$\mathbb{Z}_3$	1	π	π^2
ρ_0	1	1	1
ρ_1	1	ω	ω^2
ρ_2	1	ω^2	ω

por lo tanto los elementos $e_1, e_2, e_3 \in \mathbb{C}\mathbb{Z}_3$ definimos por

$$e_1 := \frac{1}{3}(1 + \pi + \pi^2), \quad e_2 := \frac{1}{3}(1 + \omega\pi + \omega^2\pi^2), \quad e_3 := \frac{1}{3}(1 + \omega^2\pi + \omega\pi^2),$$

son un sistema de idempotentes ortogonales tales que $1 = e_1 + e_2 + e_3$. Esto nos permite determinar x_1, x_2 y x_3 mediante:

$$x_1 = 1x_1 = (e_1+e_2+e_3)x_1 = \frac{1}{3}(x_1+x_2+x_3)+\frac{1}{3}(x_1+\omega x_2+\omega^2 x_3)+\frac{1}{3}(x_1+\omega^2 x_2+\omega x_3) =$$

$$= \frac{1}{3}\sigma_1 + A + B$$

donde $\sigma_1 = x_1 + x_2 + x_3 = 0$ y

$$A = \frac{1}{3}(x_1 + \omega x_2 + \omega^2 x_3), \quad B = \frac{1}{3}(x_1 + \omega^2 x_2 + \omega x_3).$$

Por lo tanto para determinar $x_1 = A + B$ solo necesitamos expresar A y B en función de los polinomios simétricos elementales. Ahora bien

$$\begin{cases} A^3 + B^3 = \sigma_3 \\ AB = -\frac{1}{3}\sigma_2 \end{cases}$$

de donde

$$A^3 - \frac{\sigma_2^3}{27A^3} = \sigma_3 \;\Rightarrow\; 27A^6 - 27\sigma_3 A^3 - \sigma_2^3 = 0$$

lo que nos da

$$A^3 = \frac{\sigma_3}{2} \pm \sqrt{\frac{\sigma_3^2}{4} + \frac{\sigma_2^3}{27}} = -\frac{q}{2} \pm \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$$

$$A = \sqrt[3]{-\frac{q}{2} \pm \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}, \qquad B = \frac{-p}{3\sqrt[3]{-\frac{q}{2} \pm \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}}$$

$$x_1 = \sqrt[3]{-\frac{q}{2} \pm \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} - \frac{p}{3\sqrt[3]{-\frac{q}{2} \pm \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}}$$