UNIVERSIDAD
COMPLUTENSE
MADRID

FACULTAD DE CIENCIAS MATEMÁTICAS

DEPARTAMENTO DE ÁLGEBRA, GEOMETRíA Y TOPOLOGíA

Trabajo de Fin de Grado:

REPRESENTACIÓN DE GRUPOS FINITOS

Por: Patricia Quintanilla Peinado

Tutor: Enrique Arrondo Esteban

INDICE

Abstract.

In this work we study representations of finite groups. As one can see, the title is general, but throughout this text we will focus on linear representations of finite groups and mainly on how to find all irreducible representations of a finite group.
To do that, we will see six sections which I sum up below.
First two sections, introduction and goals, represent a global view of the subject and what we want to achieve. A representation of a group is a homomorphism which allows us to simplify the study of the group itself, one of the most important is the linear representation. A representation of a group is linear if it is a homomorphism between the group and a general linear group. Most of the texts about this subject has a common factor, character theory. The character of a representation is a function that associates to each element of the group the trace of the matrix given by the representation. Our aim is to separate both theories.
In section 3 we show some concepts and results about vector spaces and representations of groups which will be useful later in this text. One important result that we will see in this section is *Any representation is a direct sum of irreducible representations and this descomposition is unique.* Most of the results come from 'Representation Theory: A First Course' even some of them have an alternative proof and others are our own since the book has a different approach to representation theory.
In section 4 we prove a series of well-known results about representation theory but in a different way from other texts and we explain how to compute primitive idempotents elements which will replace the characters. First we describe the center of the regular representation as a finite affine scheme of length equal to the number of conjugacy classes of the group. Based on the points of this scheme, we form a map which allows us to compute the primitive idempotents that we were looking for. Then, we see how to associate to each idempotent an irreducible representation, and vice versa, which concludes with the proof of Artin-Wedderburn theorem: *If the characteristic of K does not divide the order of G, the regular representation can descompose as $K(G) = \oplus_i End(V_i)$ where V_i are all irreducible representations of G. Besides, there is the same number of irreducible representations as cojugacy classes of G.*
In section 5 we go through some examples which will show us how to get the primitive idempotents elements of some known finite groups.
Finally, in section 6, we compare characters and primitive idempotents to show that both notions can be related and, more over, that the idempotents

are easier to find and impose less restrictive hypothesis on the results.
The last conlusion is that the aim of this paper is achievable, we can replace characters and use primitive idempotents instead to prove the known results about representation theory.

Key Words:
- Character(of a group),
- Conjugacy class,
- Primitive idempotent,
- Irreducible representation,
- Regular representation.

Resumen.

En este trabajo vamos a hablar sobre representaciones de grupos finitos. Como puede verse, el titulo es algo general, pero a lo largo del texto vamos a ir concretando hasta centrarnos en representación lineal de grupos finitos y sobre todo en cómo hallar todas las representaciones irreducibles de un grupo finito.
Para ello, vamos a desarrollar seis secciones que resumo a continuación.
Las dos primeras, introducción y objetivos, son una visión global del trabajo y de lo que queremos conseguir con este. Una representación de un grupo es un homomorfismo que nos va a permitir simplificar el estudio del mismo, entre las más importantes están las representaciones lineales que consisten en homomorfismos del grupo con un grupo general lineal de un espacio vectorial. La mayoría de los textos sobre este tema tienen un factor común que es la teoría de caracteres, donde los caracteres de una representación vienen dados por la función que a cada elemento del grupo le da la traza de la matriz que le corresponde por la representación. Nuestro objetivo es desvincular estas dos teorías.
En la sección 3 exponemos una serie de conceptos y resultados sobre espacios vectoriales y representaciones de grupos que serán útiles a lo largo del resto de secciones. Uno de los resultados más importantes de la sección es que *toda representación sobre un cuerpo cuya característica no divide al orden del grupo es suma directa de representaciones irreducibles de forma única*. La mayoría están extraidos del libro 'Representation Theory: A First Course', aunque algunos resultados están demostrados de manera alternativa y otros son propios, ya que nuestro enfoque de la teoría de representaciones es distinta a la de dicho libro.
En la sección 4 demostramos una serie de resultados ya conocidos sobre representación de grupos de una manera distinta a la de otros textos y explicamos cómo hallar los elementos idempotentes primitivos que serán sustitutos de los caracteres. Primero, describimos el centro de la representación regular como un esquema afín de puntos. De aquí surge de forma natural una aplicación que nos permite calcular los elementos idempotentes primitivos que buscábamos. Luego, vemos cómo asociar a cada representación irreducible uno de estos idempotentes primitivos, y viceversa, lo cual concluye con la demostración del Teorema de Artin-Wedderburn: *Si la característica de K no divide al orden de G, la representación regular se puede descomponer como $K(G) = \oplus_i End(V_i)$ donde V_i son todas las representaciones irreducibles de G. Además, hay el mismo número de representaciones irreducibles que clases de conjugación*

de G.
En la 5, exponemos una serie de ejemplos que muestran cómo hallar los elementos idempotentes primitivos de grupos finitos conocidos.
Finalmente, en la sección 6 mostramos la comparación con los caracteres para que se vea que pueden relacionarse ambos conceptos y que los elementos idempotentes usados son, en efecto, algo más fácil e incluso menos restrictivo en cuanto a las hipótesis que hay que pedir en los resultados.
La conlusión final es que nuestro objetivo era posible, se pueden sustituir los caracteres por estos idempotentes primitivos y, con ellos, demostrar los resultados que ya conocemos de teoría de representación de grupos sin ayuda de los caracteres.

Palabras clave:
- Caracter(de un grupo),
- Clase de conjugación,
- Idempotentes primitivos,
- Representación irreducible,
- Representación regular.

1 Introducción y Antecedentes.

Introducción.
En matemáticas una representación es una estructura que conserva una serie de propiedades, en el caso de grupos una representación es un homomorfismo de grupos, es decir, preserva la operación binaria. La representación de un grupo intenta simplificar el estudio del mismo, transformándolo en algo más sencillo. Aunque también puede verse como el estudio de cómo un grupo dado puede actuar sobre espacios vectoriales. Estos dos son los principales enfoques de la teoría y son los que vamos a usar en este texto.
La teoría de representación de grupos se divide a su vez en otras según el grupo que se quiera representar. En este caso, nos centraremos en **representación de grupos finitos**, pero cabe destacar otras representaciones como las de:
- **Grupos topológicos compactos:** se usan resultados de grupos finitos pasando a grupos infinitos mediante integrales que solo se pueden definir en los grupos compactos o localmente compactos.
- **Grupos de Lie:** crucial para la representación de grupos en el estudio de campos.

Como hemos dicho antes, el objetivo de esta teoría es simplificar el estudio de los grupos. Una de las formas más comunes, que es la que nosotros veremos a lo largo del trabajo, es la **representación lineal** de un grupo. Una representación es lineal cuando el objeto que asociamos al grupo a través del homomorfismo es un grupo general lineal sobre un espacio vectorial. De modo que los resultados que queremos ver sobre los grupos, podrán verse a través de matrices de automorfismos del espacio vectorial.
Debemos también notar la diferencia entre representación de grupos sobre un cuerpo de característica 0, **representación ordinaria**, y sobre uno de característica prima, **representación modular**. En el caso de la representación ordinaria, que es lo mismo que la modular si la característica del cuerpo no divide al orden del grupo, una representación queda determinada por sus **caracteres**, donde los caracteres de una representación vienen dados por la función que a cada elemento del grupo le da la traza de la matriz que le corresponde por la representación, ya que la traza es invariante por semejanza.
Hemos observado que hay varias formas de interpretar la teoría de representación de grupos, sin embargo un factor común es la teoría de caracteres. A pesar de ello, los caracteres parecen algo artificial y, en muchos casos, difíciles de calcular. Por ello, nuestra labor ahora es separar

la teoría de representación de grupos de la teoría de caracteres.

Antecedentes.
Como se podrá ver a lo largo del texto, este trabajo trata de encontrar un punto de vista nuevo de la teoría de representación de grupos finitos, por tanto ni los antecedentes ni la bibliografía son muy extensos. Precisamente hemos querido que el trabajo sea innovador y no usamos muchos resultados de otros libros o publicaciones.
En primer lugar, este trabajo parte de la investigación previa de mi tutor, Enrique Arrondo Esteban, que empieza con el objetivo de descomponer cualquier función en sus partes simétricas, siguiendo el esquema que tenemos para funciones de dos variables que descomponemos como suma de su parte simétrica y su parte alternada. Al realizar dicha descomposición para funciones de 3 y 4 variables, encuentra un truco que hace sencillo el trabajo, pero quiere extenderlo a cualquier función. Es aquí donde se topa con la teoría de Representación de Grupos y con los caracteres. Estos aparecen como algo difícil de conseguir a partir del grupo de partida. Por este motivo, surge la idea de desarrollar esta teoría sin la necesidad de usar los caracteres.
El propósito de nuestro trabajo posterior es aproximarnos a la teoría de representación de grupos finitos desde un nuevo punto de vista, basado en geometría algebraica. Este permitirá recuperar resultados sobre representaciones de grupos sin la necesidad del uso de los caracteres. Usando, en su lugar, unos elementos idempotentes primitivos que vamos a definir y aprender a calcular en este trabajo.
Cabe también hablar en esta sección del libro **'Representation Theory: A First Course'** de William Fulton y Joe Harris, ya que la teoría de representaciones es algo que no se estudia durante el grado y, por ello, me he basado en este libro para poder aprender aquellos conceptos que necesitaba. De este libro también he sacado todo lo referente a caracteres para entender cómo se calculan y cómo se usan, y así poder compararlos con el nuevo enfoque.
Por último, mencionar también el libro **'Algebraic Geometry: A First Course'** de Joe Harris que me ha servido para extraer conceptos de geometría algebraica que necesitábamos para algunas pruebas y que, sobre todo, he utilizado en el apéndice para aclarar al lector qué resultados se utilizan de este tema y por qué son necesarios.

2 Objetivos.

El objetivo principal de este trabajo es presentar resultados sobre representaciones lineales de grupos finitos, que puedan aplicarse para obtener propiedades o demostrar teoremas sobre los grupos mismos, prescindiendo de los caracteres. La culminación de todos los resultados será la demostración del **Teorema de Artin-Wedderburn** que nos da el resultado clásico sobre la descomposición de la representación regular, del cual extraemos que hay el mismo número de representaciones irreducibles que clases de conjugación tiene el grupo.
Otros objetivos que desarrollamos a lo largo del texto son, por ejemplo, conseguir que el lector aprenda a calcular los elementos idempotentes primitivos y comparar estos elementos con los caracteres, para llegar a la conclusió final que exponemos en el resumen.

3 Preliminares.

Comenzamos este trabajo introduciendo algunas nociones de teoría de representación de grupos que vamos a necesitar a lo largo de este. En todo el texto vamos a suponer que G es grupo finito a no ser que se indique lo contrario. Todas las definiciones de esta sección están sacadas de [1, Páginas 3-11].

Definición 3.1. Dado G un grupo y V un espacio vectorial que suponemos finito sobre K, una *representación* de G en V es un homomorfismo de G en el grupo de automorfismos de V, $\rho : G \to GL(V)$. A veces, se llama V a la representación en lugar de al homomorfismo ρ. En este caso, se define la siguiente acción de G sobre V: $g \cdot v = \rho(g)(v)$.

Definición 3.2. Una *subrepresentación* de V es un subespacio vectorial W de V tal que es invariante por la acción de G.

Definición 3.3. Una representación de un grupo G se dice *irreducible* si ningún subespacio de V es invariante bajo G excepto el $\{0\}$ y V.

Veamos ahora un lema que nos muestra que si la característica del cuerpo no divide al orden del grupo, entonces la noción de irreducible coincide lo que uno podría imaginar, a saber, que no puede descomponerse como suma directa de dos representaciones.

Lema 3.1 *Sea W una subrepresentación de V donde V espacio vectorial sobre un cuerpo K cuya característica no divide al orden de G, entonces existe W' subespacio vectorial de V invariante bajo la acción de G tal que $V = W \oplus W'$.*

Demostración.
Vamos a seguir la demostración de [1, Proposition 1.5].
Sea U un subespacio vectorial cualquiera de V que cumple $V = W \oplus U$, es decir, un complementario de W en V. Sea $\pi : V \to W$ la proyección dada por la descomposición de V en suma directa de W y U. Y sea $\pi_0 : V \to V$ la aplicación dada por:

$$\pi_0(v) = \Sigma_{g \epsilon G}(g \cdot \pi(g^{-1} \cdot v))$$

Si $w \epsilon W$, entonces $g \cdot \pi(g^{-1} \cdot w) = g \cdot (g^{-1} \cdot w) = w$ luego $\pi_0(w) = |G|w$.

Entonces, $W' = ker(\pi_0)$ satisface $V = W \oplus W'$, porque la característica de K no divide al orden de G lo cual implica que $\mathrm{Im}(\pi_0) = W$, y es invariante bajo la acción de G:
Si tomamos $g' \epsilon G$ y $v \epsilon V$, entonces $g' \cdot \pi_0(g'^{-1} \cdot v) = \Sigma_{g \epsilon G}(g' \cdot g \cdot \pi(g^{-1} \cdot v \cdot g'^{-1})) = \pi_0(v)$. Si $\pi_0(v) = 0$, es decir si $v \epsilon W'$, entonces $g' \cdot \pi_0(g'^{-1} \cdot v) = 0$, se tiene que $\pi_0(g'^{-1} \cdot v) = 0$.
Luego, existe el complementario de W tal que es invariante bajo la acción de G. $\square$

Teorema 3.2 *Toda representación sobre un cuerpo cuya característica no divide al orden de G es suma directa de representaciones irreducibles.*

Demostración.
Procedemos por inducción completa sobre la dimensión del espacio V.
-Si $\dim(V) = 1$, es trivial porque V no tiene subespacios no triviales.
-Si $\dim(V) \geq 2$, si V es irreducible no hay nada que probar. Si, en cambio, V no es irreducible existe algún $W \subset V$ subespacio vectorial tal que W es invariante por la acción de G. Y, por el Lema 3.1, existe un subespacio invariante $W' \subset V$ tal que $V = W \oplus W'$. Y como $\dim(V) > \dim(W), \dim(W')$, hemos acabado. Ya que, por hipótesis de inducción W y W' son, o bien representaciones irreducibles de G, o bien suma directa de irreducibles. $\square$

Lema 3.3 (*Lema de Schur*) *Si V y W son representaciones irreducibles de G y $\varphi : V \to W$ es un homomorfismo de G-módulos, entonces, o bien φ es un isomorfismo, o bien $\varphi = 0$.*

Demostración.
Vamos a seguir la primera parte de la demostración de [1, Lemma 1.7].
Como $\ker(\varphi)$ y $\mathrm{Im}(\varphi)$ son subespacios invariantes y V y W son representaciones irreducibles solo tenemos 2 posibilidades, o bien la imagen es el total y el núcleo es el 0 y entonces φ isomorfismo por ser biyectiva y homomorfismo, o bien el núcleo es el total y entonces $\varphi = 0$. $\square$

El Lema de Schur nos permite demostrar la unicidad de la descomposición del Teorema 3.2.

Corolario 3.4 *Toda representación sobre un cuerpo cuya característica no divide al orden de G se escribe de manera única como suma directa de representaciones irreducibles.*

Demostración.
Supongamos que no, sean $W_1, \cdots, W_r$ y $W_1', \cdots, W_s'$ representaciones irreducibles de G tales que $V = W_1 \oplus \cdots \oplus W_r$ y $V = W_1' \oplus \cdots \oplus W_s'$ y todas distintas dos a dos. Por el Lema de Schur, existen homomorfismos $\varphi_{i,j} : W_i \to W_j'$ que son, o bien isomorfismos, o bien constantemente 0.
Tenemos también una aplicación inyectiva de cada W_i en V y, por tanto, en $W_1' \oplus \cdots \oplus W_s'$. Por consiguiente, no pueden ser todos los $\varphi_{i,j}$ constantemente 0.
De forma análoga, existe una aplicación inyectiva de cada W_j' en V y, por tanto, en $W_1 \oplus \cdots \oplus W_r$.
Vamos a ver que cada W_i está en biyección con una W_j' y, por tanto, $r = s$ y tenemos una contradicción. Si existe W_i tal que todas las $\varphi_{i,j}$ con i fijo son 0, entonces la inclusión de W_i en V tendría que ser también la aplicación 0, pero entonces W_i sería el 0 de V y no seria una representación irreducible de G. Luego, para todo i existe j tal que $\varphi_{i,j}$ es isomorfismo. De forma simétrica, lo tenemos para cada j. Entonces, existe una biyección entre las representaciones de la primera y la segunda descomposición, luego a cada i le corresponde un solo j tal que $\varphi_{i,j}$ isomorfismo, y viceversa, por tanto también se tiene $r = s$.
Luego la descomposición es única. □

El objetivo ahora es hallar todas las representaciones irreducibles de un grupo.

Definición 3.4. Dado G, grupo, y K cuerpo, $K(G)$ es el K-espacio vectorial de base $\{e_g \text{ con } g \epsilon G\}$. Con la operación dada por $e_g e_h = e_{gh}$, $K(G)$ tiene estructura de K-álgebra. Se denomina *representación regular* a la dada por la estructura de K-álgebra de $K(G)$.
Definición 3.5. Denotamos por P al conjunto de clases de conjugación de G y si $\lambda \epsilon P$, π_λ al conjunto de elementos de la clase de conjugación.

Teorema 3.5 *El centro de $K(G)$ que denotamos por $ZK(G)$ coincide con la subálgebra generada por los elementos:*

$$\alpha_\lambda = \Sigma_{h \epsilon \pi_\lambda} e_h$$

con λ clase de conjugación de G.

Demostración.
Vamos a probar la igualdad viendo un doble contenido.
$\subset$) Sea $\alpha = \Sigma_g a_g e_g$ un elemento de $K(G)$. Si α está en el centro, conmuta con todos los elementos de $K(G)$ luego $\alpha e_h = e_h \alpha$ para todo h en G.
Por un lado, $e_h \alpha = \Sigma_g a_g e_{hg}$, y por el otro, $\alpha e_h = \Sigma_g \ a_g e_{gh}$. Entonces, igualando ambas expresiones tenemos que el coeficiente de e_{hg} es $a_{h^{-1}hg}$ y también es $a_{hgh^{-1}}$, es decir que $a_{h^{-1}hg} = a_{hgh^{-1}}$. De donde, $a_g = a_{hgh^{-1}}$. Observamos que para todo g en G los coeficientes de hgh^{-1} son el mismo, luego todos los elementos de la clase de conjugación de g tienen el mismo coeficiente. Por tanto, α es combinación de elementos de la forma $\Sigma_{h \epsilon \pi_\lambda} e_h$.
$\supset$) Dado un α_λ, veamos que está en el centro de $K(G)$, es decir, que conmuta con todo e_g. En efecto,

$$\alpha_\lambda e_g = (\Sigma_{h \epsilon \Pi_\lambda} e_h) e_g = \Sigma_{h \epsilon \Pi_\lambda} e_{hg}$$

Tenemos que $e_{hg} = e_{gh}$ para todo h en $g^{-1}hg$, es decir, que está en la misma clase de conjugación que h. Por tanto, la suma de los e_{hg} es la suma de los e_{gh} si h varia en una misma clase de conjugación. De donde, tenemos la siguiente igualdad.

$$\Sigma_{h \epsilon \Pi_\lambda} e_{hg} = \Sigma_{h \epsilon \Pi_\lambda} e_{gh} = e_g \alpha_\lambda$$

$\square$

Es importante observar que $ZK(G)$ es un álgebra conmutativa y es finita, precisamente su dimension es el cardinal de P.

Teorema 3.6 *Para cada representación $\rho : G \to GL(V)$ donde V es un K-espacio vectorial, sea $\tilde{\rho} : K(G) \to End(V)$ el homomorfismo inducido por ρ. Entonces, se tiene:*
(i) Si G actúa en $End(V)$ como $gf = \rho(g) o f$, entonces $\tilde{\rho}$ es un morfismo de representaciones.
(ii) Un elemento $\alpha \epsilon K(G)$ es 0 si y sólo si esta en el $\ker(\tilde{\rho})$ *para toda representación de G.*
(iii) $\alpha \epsilon ZK(G)$ si y sólo si,para cualquier representación ρ de G,el homomorfismo $\tilde{\rho}(\alpha) : V \to V$ es morfismo de representaciones.

Demostración.
(i) Hay que ver que si $\alpha \epsilon K(G)$ entonces $\tilde{\rho}(g\alpha) = g\tilde{\rho}(\alpha)$, lo cual es obvio:

$\tilde{\rho}(g\alpha) = \tilde{\rho}(e_g\alpha) = \tilde{\rho}(e_g)\tilde{\rho}(\alpha) = \rho(g)o\tilde{\rho}(\alpha) = g\tilde{\rho}(\alpha)$.

(ii)
$\Rightarrow$)Trivial.
$\Leftarrow$)Sea α de $K(G)$ tal que está en el núcleo de toda $\tilde{\rho}$. En particular, está en el ker de la representación regular: $\tilde{\rho} : K(G) \to GL(K(G))$, es decir, $\tilde{\rho}(\alpha) = 0$. Entonces, α es la multiplicación por 0 en $K(G)$. Luego, para todo $\beta \epsilon K(G)$ se tiene: $\alpha\beta = 0$. Tomando β como el 1 de $K(G)$ tenemos que necesariamente $\alpha = 0$.

(iii) Sea $\alpha = \Sigma_{g\epsilon G} a_g \cdot e_g \epsilon ZK(G)$.Para cada $h \epsilon G$, tenemos:

$$\tilde{\rho}(\alpha)(hv) = \Sigma_{g\epsilon G} a_g \cdot g(hv)$$

que por la acción definida en (i) es igual a

$$(\Sigma_{g\epsilon G} a_g \cdot e_{gh})(v) = \alpha \cdot e_h(v)$$

Y, por tanto, $\tilde{\rho}(\alpha)(hv) = h\tilde{\rho}(\alpha)(v)$, es decir, es morfismo de representaciones si y sólo si $\alpha \epsilon ZK(G)$. $\square$

Vamos a demostrar, por último, unos resultados sencillos sobre el conjunto de endomorfismos de un espacio vectorial que utilizaremos más adelante en el trabajo.

Teorema 3.7 *Sea V un espacio vectorial de dimensión n, entonces la representación $End(V)$ se descompone como suma directa de V n veces.*

Demostración.
Sean $v_1, \cdots, v_n$ una base de V, la representación de $End(V)$ se descompone como suma directa de las representaciones V_i, donde V_i es el espacio vectorial de endomorfismos de V que mandan a cero todos los vectores de la base salvo el v_i. Cada V_i es una subrepresentación de $End(V)$ porque son subespacios vectoriales y quedan fijos por la acción de G, ya que si f pertenece a V_i se tiene $\rho(g)f(v_j) = 0$ si $j \neq i$.
Tenemos entonces que $End(V) = V_1 \oplus \cdots \oplus V_n$, falta ver que cada V_i es isomorfo a V como representaciones. Veamos para ello que $\{f_j^i : V \to V : f_j^i(v_i) = v_j; f_j^i(v_k) = 0, k \neq i\}$ con j de 1 hasta n es base de cada V_i.
-Linealmente independientes: Si existe una combinación $\Sigma_j \lambda_j f_j^i = 0$, actuando sobre v_i tendríamos: $\Sigma_j \lambda_j f_j^i(v_i) = 0$ lo cual es igual a $\Sigma_j \lambda_j v_j = 0$.

Como los v_j son base de V, esto implica que todos los λ_j son nulos.

-Sistema de generadores: Sea φ un elemento cualquiera de V_i, entonces se tiene $\varphi(v_k) = 0$ si $k \neq i$ y $\varphi(v_i) = w$ con w un elemento no nulo de V.
Sea u en V, $\varphi(u) = \varphi(\Sigma_k \lambda_k v_k) = \Sigma_k \lambda_k \varphi(v_k)$ y por lo dicho antes solo es distinto de cero si k es igual a i. Entonces, la igualdad queda $\Sigma_k \lambda_k \varphi(v_k) = \lambda_i w$ y, como w pertenece a V puede expresarse en función de la base. Por tanto, $\varphi(u) = \lambda_i w = \lambda_i \Sigma_k \alpha_k v_k = \Sigma_k \alpha_k \lambda_i v_k$. Veamos que $\lambda_i v_k$ es exactamente $f_k^i(u)$ y habremos acabado. Tenemos $f_k^i(u) = f_k^i(\Sigma_l \lambda_l v_l) = \Sigma_l \lambda_l f_k^i(v_l)$ que solo es distinto de 0 si l igual a i, luego queda $f_k^i(u) = \lambda_i v_k$ que es lo que queríamos, es decir, $\varphi = \Sigma_k \alpha_k f_k^i$.
Podemos definir la aplicación $\Phi_i : V \rightarrow V_i$ tal que a cada elemento v_j le asigna f_j^i. Tenemos que ver que Φ_i es isomorfismo de representaciones, es decir, morfismo de representaciones y biyectivo. Que es una biyección es claro porque manda cada elemento de la base de V a un único elemento de la base de V_i.
Para ver que es morfismo de representaciones basta ver que para todo g en G y para todo v en V se tiene que $\Phi_i(g \cdot v) = g \cdot \Phi_i(v)$. Y esto se tiene,

$$\Phi_i(g \cdot v) = \Phi_i(\rho(g) o v) = \Phi_i(\rho(g))\Phi_i(\Sigma_k \alpha_k v_k) = \rho(g) o \Sigma_k \alpha_k f_k^i = g \cdot \Phi_i(v)$$

En total, tenemos que la representación de $End(V)$ es igual a n veces la suma directa de V. $\square$

Teorema 3.8 *Dado V un espacio vectorial sobre un cuerpo K, el centro de $End(V)$ es el conjunto de aplicaciones de la forma μId donde μ es un elemento del cuerpo K.*

Demostración.
La prueba de esto es trivial ya que el centro son todos los endomorfismos que conmuten con el resto de elementos de $End(V)$ y solo la matriz identidad y sus múltiplos conmutan con todas las matrices. $\square$

4 Representaciones irreducibles y elementos idempotentes.

El objetivo de esta sección va a ser demostrar el Teorema de Artin-Wedderburn, que nos da la descomposición de la representación regular que aplicado a nuestro caso es la siguiente:

$$K(G) = \oplus_i End(V_i)$$

donde V_i son todas las representaciones irreducibles de G. Si el teorema es cierto, se tiene que el centro de $K(G)$, $ZK(G)$, es isomorfo a tantas copias de K como representaciones irreducibles tiene G. Por ello vamos a estudiar esta descomposición de $ZK(G)$ a base de geometría algebraica, lo cual nos hará interesarnos por los elementos idempotentes primitivos de esta álgebra. Todo ello nos llevará a ver que existen el mismo número de representaciones irreducibles de un grupo que clases de conjugación del mismo.
Primero observamos que $ZK(G)$ es una K-álgebra reducida, es producto directo finito de cuerpos, por ser finita. Y vamos a ver que, por tanto, existe un ideal I tal que $K[\mathbf{x}]/I \cong ZK(G)$ y es el ideal de $|P|$ puntos distintos.

Teorema 4.1 *Con la notación usada hasta ahora, sea G grupo y $\lambda' \epsilon P'$, clase de conjugación de G distinta de la clase del 1, fijamos $x_{\lambda'}$ y $\boldsymbol{x}$ el conjunto de $|P|-1$ indeterminadas $x_{\lambda'}$. Sea I el núcleo del homomorfismo de K-álgebras $F : K[\boldsymbol{x}] \to ZK(G)$ que manda cada $x_{\lambda'}$ a $\alpha_{\lambda'}$. Entonces, existe una extension finita $K \subset K'$ tal que I es el ideal de $|P|$ puntos distintos en el espacio afín $\mathbb{A}^{|P|-1}_{K'}$.*

Demostración.
Tenemos que $K[\mathbf{x}]/\ker(F) \cong ZK(G)$. Queremos probar que $I = \ker(F)$ es el ideal de $|P|$ puntos distintos y sabemos que $ZK(G)$ es un álgebra reducida y finita de dimensión $|P|$. Entonces, probar que I es el ideal de $|P|$ puntos distintos es equivalente a probar, por el Teorema 7.2, que $ZK(G)$ no tiene elementos nilpotentes diferentes del 0.
Sea $\alpha \ \epsilon \ ZK(G)$ nilpotente, entonces para cualquier representación irreducible V de G la aplicación inducida $\alpha : V \to V$ no tiene rango máximo, porque su matriz asociada es nilpotente y una matriz nilpotente nunca es de rango máximo, y, por el Lema de Schur, α es la multiplicación por 0 en V. Por el Corolario 3.4 $K(G)$ descompone en representaciones

irreducibles, entonces por el apartado (ii) del Teorema 3.6, se tiene que $\alpha = 0$. $\square$

Notación: Denotamos a partir de ahora a los $|P|$ puntos distintos del teorema como a_λ, que se obtienen como solución de ecuaciones que tienen como indeterminadas a los α_λ. Porque si $f \epsilon K[\mathbf{x}]$ podemos escribirlo como:

$$f = \Sigma_i b_{\lambda_i} x_{\lambda_i}$$

Y su imagen es de la forma siguiente,

$$F(f) = \Sigma_i b_{\lambda_i} \alpha_{\lambda_i}$$

Luego, los puntos buscados son soluciones de la ecuaciones de $I = \ker(F) = \{f \epsilon K[\mathbf{x}] : F(f) = 0\}$.
A partir de ahora, basta considerar K como un cuerpo que contenga a los puntos a_λ, en lugar de uno cuya característica no divida al orden de G.

Veamos un ejemplo que motiva la siguiente definición.

Ejemplo 4.1.: Sea K^n con n finito que tiene estructura de K-álgebra con el producto: $vw = (v_1w_1, \cdots, v_nw_n)$ donde v y w tienen sus coordenadas en K. Los idempotentes son aquellos elementos v de K^n tales que $v^2 = v$. Luego es claro que los elementos de la base canónica, $(0, \cdots, 1, \cdots, 0)$, son idempotentes. Además, son primitivos porque no se pueden descomponer como suma de otros idempotentes.
Y no hay más idempotentes primitivos porque cualquier otro idempotente se podrá expresar como combinación lineal de elementos de la base canónica y, por tanto, como suma de estos idempotentes primitivos.

Definición 4.1. Un elemento idempotente se dice *primitivo* si no puede descomponerse como suma de otros idempotentes.

Denotamos los elementos idempotentes de $K(G)$ como β_λ donde λ representa una clase de conjugación de G, que son idempotentes primitivos ya que vienen de idempotentes primitivos de $K^{|P|}$ mediante un isomorfismo.

Teorema 4.2 *Sea $H : ZK(G) \to K^{|P|}$ que consiste en evaluar las clases de los polinomios del ideal I tal que $ZK(G) \cong K[\boldsymbol{x}]/I$ en los puntos $\{a_\lambda\}_{\lambda \epsilon P}$, H*

es isomorfismo de K-álgebras. Además, las preimágenes de la base canónica de $K^{|P|}$ forman una base ortonormal $\{\beta_\lambda\}_{\lambda\epsilon P}$ de elementos idempotentes primitivos de $ZK(G)$ cuya suma es 1.

Demostración.
Como $I = \cap_{\lambda\epsilon P} I(a_\lambda)$, por el Teorema Chino del Resto se tiene que $K[\mathbf{x}]/I$ es isomorfo a $\oplus_{\lambda\epsilon P} K[\mathbf{x}]/I(a_\lambda)$ y cada $I(a_\lambda)$ es isomorfo a K mediante el homomorfismo de evaluación de las clases de polinomios en el a_λ correspondiente.
Luego, como $ZK(G) \cong K[X]/I$, $ZK(G)$ es isomorfo a $K^{|P|}$. Lo demás, se sigue de que H sea isomorfismo, ya que un isomorfismo manda elementos idempotentes a idempotentes. □

Vamos a probar ahora una forma de asignar a cada representación un idempotente primitivo que nos va a permitir descomponer $K(G)$.

Teorema 4.3 *Para cada representación V, se tiene una descomposición $\oplus\beta_\lambda V = V$. Además, si V es irreducible, entonces existe un único $\lambda_0 \epsilon P$ tal que $V = \beta_{\lambda_0} V$.*

Demostración.
Sabemos por el Teorema 4.2 que $\Sigma_{\lambda\epsilon P}\beta_\lambda = 1$, por tanto existe una descomposición de V que es la siguiente:

$$\Sigma_{\lambda\epsilon P}\beta_\lambda V = V$$

Y es suma directa porque, por el teorema ya nombrado, los idempotentes primitivos son una base y, por tanto, son linealmente independientes.
Veamos ahora que son representaciones. Un subespacio W de V es invariante por g si $g(W) \subset W$. Sea $v \epsilon V$,tenemos

$$g(\beta_\lambda v) = \beta_\lambda g(v)$$

que pertenece a $\beta_\lambda V$. Luego todo idempotente de $ZK(G)$ me da un subespacio de la forma $\beta_\lambda V$ invariante. Lo cual quiere decir que $\beta_\lambda V$ es una representación de G.
Si V es irreducible, como $\beta_\lambda V$ son invariantes, tiene que darse o $\beta_\lambda V = 0$ o $\beta_\lambda V = V$. Y es obvio que solo puede haber uno, λ_0, para el cual sea $\beta_{\lambda_0} V = V$.
□

Observación 4.1: Del teorema anterior, se deduce que $K(G) = \oplus_{\lambda \epsilon P} \beta_\lambda K(G)$.

Vamos a ver ahora unos resultados que nos van a permitir asignarle a cada idempotente primitivo una descomposición irreducible.

Lema 4.4 *Sean V' y V de dimensiones $n' < n$ sobre K. Suponemos que $Hom(V', V)$ tienen un subespacio lineal W de dimensión n tal que toda f no nula de W tiene rango n. Entonces, $n' = 1$.*

Demostración.
Sea $X_{n'-1} = \{\ [f] \ \epsilon\ \mathbb{P}(Hom(V', V)) : rango([f]) \leq n' - 1\} \subset \mathbb{P}^{nn'-1}$, por el Teorema 7.1, tenemos que $codim(X_{n'-1}) = n - n' + 1$.
Por hipótesis, el subespacio $\mathbb{P}(W)$ de dimensión $n - 1$ no corta a $X_{n'-1}$. Entonces, por el Teorema 7.3, $n - 1 < n - n' + 1$ y, por tanto, $n' < 2$. Luego solo puede ser $n' = 1$. □

Teorema 4.5 *Una representación $\rho : G \to GL(V)$ es irreducible si y sólo si $\tilde{\rho}$ es sobreyectiva.*

Demostración.
Veamos ambas implicaciones.
$\Leftarrow$) Si ρ no fuera irreducible, existiría $W \subset V$ tal que W es representación de G. En ese caso, la imagen de $\tilde{\rho}$ estaría contenida en los endomorfismos de V que conservan W, pero entonces $\tilde{\rho}$ no sería sobreyectiva. Contradicción. Luego tiene que ser ρ irreducible.
$\Rightarrow$) Supongamos ρ irreducible y veamos que $\tilde{\rho}$ es epimorfismo. Vamos a verlo en 3 pasos:

-Paso 1: Para cada $v, v' \ \epsilon\ V$ existe α que manda v a v'.
Para todo $v \ \epsilon\ V$ no nulo, consideramos la aplicación $\tilde{\rho}_v : K(G) \to V$ definida por $\tilde{\rho}_v(\alpha) = \tilde{\rho}(\alpha(v))$ que es morfismo de representaciones porque es una composición de morfismos de representaciones ($\tilde{\rho}$ y la evaluación en v) y como V es irreducible y la imagen no es 0, porque la imagen de 1 es v, se sigue que $\tilde{\rho}_v$ es suprayectiva que es lo que queríamos demostar.

-Paso 2: Existe un endomorfismo de V en Im($\tilde{\rho}$) tal que su rango es 1.
Sea r el menor rango de los endomorfismos de V no nulos que pertenecen

a la imagen de $\tilde{\rho}$. Sean $v'_1, \cdots, v'_n$ una base cualquiera de V y sea α tal que $\tilde{\rho}(\alpha)$ tenga rango r. Fijamos v perteneciente a V y sea $v' = \alpha(v)$. Podemos construir por el Paso 1 endomorfismos, $\alpha_i : V \to V$, tales que $\alpha_i(v') = v'_i$. El subespacio de $End(V)$ generado por los endomorfismos $\alpha_i o \alpha$ que mandan v a v'_i, al que llamamos V', tiene dimensión n y sus endomorfismos no nulos tienen como mucho rango r.
Todos los elementos del subespacio V' tienen un subespacio en su núcleo (concretamente el núcleo de α) de dimensión $n-r$, entonces V' puede verse como subespacio de $Hom(V/A, V)$. Aplicando entonces el Lema 4.4, se tiene $r = 1$. Por tanto,existe $f_1 \,\epsilon\, \mathrm{Im}(\tilde{\rho})$ de rango 1.

-Paso 3: Existe una base de endomorfismos de V en la imagen.
Sea $H_1 = ker(f_1)$ y tomamos v_1 que no pertenece a H_1 tal que $f_1(v_1) = v'$ que no es 0. Sea $v_2 \,\epsilon\, H_1$ y α_2 en $K(G)$ tal que $\alpha_2 \cdot v_2 = v_1$. Se define, entonces, $f_2 \,\epsilon\, End(V)$ como $f_2(v) = f_1(\alpha_2 \cdot v)$, y $H_2 = ker(f_2)$. En particular, tenemos $f_1(v_2) = 0$ y $f_2(v_2) = v'$. Tomamos v_3 en $H_1 \cap H_2$ de modo que $f_1(v_3) = 0$, $f_2(v_3) = 0$ y $f_3(v_3) = v'$. Repetimos el proceso hasta conseguir $v_1, ..., v_n$ y $f_1, ..., f_n$ de rango 1 en la imagen de $\tilde{\rho}$ tales que verifican $f_i(v_i) = v'$ y $f_i(v_j) = 0$ si j pertenece a $\{i+1, \cdots, n\}$.
Se tiene que $v_1, ..., v_n$ forman una base de V, ya que $v_{i+1}, ..., v_n \,\epsilon\, H_i$, luego v_i no es combinación lineal de $v_{i+1}, ..., v_n$. Consideramos ahora β_j tal que $\beta_j \cdot v' = v_j$ y definimos $f_{i,j}(v) = \beta_j \cdot f_i(v)$. Como $v_1, ..., v_n$ son base de V y $\beta_1, ..., \beta_n$ son base de $End(V)$, entonces $f_{i,j}$ son endomorfismos de V. Veamos que son linealmente independientes.
Sean $\lambda_{i,j}$ escalares tales que $\Sigma_{i,j}\lambda_{i,j}f_{i,j} = 0$. Como es una suma de endomorfismos por escalares es un endomorfismo y podemos aplicarlo a algún elemento de V. Lo aplicamos sobre v_n. Como v_n está en el núcleo de todas las $f_{i,j}$ para i desde 1 hasta $n-1$, tenemos que $\Sigma_{i,j}\lambda_{i,j}f_{i,j}(v_n) = \Sigma_j\lambda_{n,j}f_{n,j}(v_n) = 0$. Por otra parte, tenemos que $f_{n,j}(v_n) = v_j$ y, por tanto, lo anterior queda $\Sigma_j\lambda_{n,j}v_j = 0$. Y como los v_i son base de V, tenemos que todos los $\lambda_{n,j}$ son nulos.
Un vez tenemos esto, repetimos el proceso con v_{n-1}. Tenemos $\Sigma_{i,j}\lambda_{i,j}f_{i,j} = 0$ con i desde 1 hasta $n-1$ y lo aplicamos a v_{n-1}. Por el mismo razonamiento que antes, nos queda que $\Sigma_j\lambda_{n-1,j}v_j = 0$. Lo cual implica que todos los $\lambda_{n-1,j}$ son nulos.
Repetimos el proceso hasta llegar a que todos los $\lambda_{i,j}$ son nulos para todo (i,j). Por tanto, $f_{i,j}$ forman una base de los endomorfismos de V en $\mathrm{Im}(\tilde{\rho})$. Por tanto, $\tilde{\rho}$ es sobreyectiva. □

Observación 4.2: El teorema anterior caracteriza las representaciones irreducibles y no depende de la característica del cuerpo.

Corolario 4.6 *Si V es una representación irreducible y, suponiendo que la característica de K no divide al orden de G, hay una descomposición de K-álgebras unitarias que es la siguiente:*

$$K(G) \cong End(V) \oplus ker(\tilde{\rho})$$

En ese caso, dado un elemento idempotente primitivo β_λ existe una única representación irreducible, V, tal que $\beta_\lambda K(G) \cong End(V)$.

Demostración.
Como sabemos por el Teorema 4.5 que $\tilde{\rho}$ es morfismo de representaciones, $K(G)$ descompone por el Lema 3.1 como representaciones en $K(G) = W \oplus ker(\tilde{\rho})$, donde W es un subespacio complementario al núcleo de $\tilde{\rho}$.
Como $\tilde{\rho}$ restringida a W es un morfismo de representaciones entre W y $End(V)$ es también morfismo de K-álgebras y como W y $End(V)$ son isomorfos como espacios vectoriales, entonces la restricción de $\tilde{\rho}$ es biyectiva. Por tanto, $End(V) \cong W$ como representaciones pero también como K-álgebras.
Como álgebra $End(V)$ tiene una unidad, que es la identidad en V. Por tanto, $ker(\tilde{\rho})$ tiene también unidad que es el 1 de $K(G)$ menos el 1 de W. Se tiene entonces que la descomposición $K(G) \cong End(V) \oplus ker(\tilde{\rho})$ es descomposición de álgebras unitarias.

Veamos la segunda parte. Sea el elemento (1,0) ϵ $End(V) \oplus ker(\tilde{\rho})$, dicho elemento es idempotente primitivo y además está en el centro de $End(V) \oplus ker(\tilde{\rho})$.
Tomando centros en ambos lados del isomorfismo, tenemos:
$ZK(G) \cong Z(End(V) \oplus ker(\tilde{\rho}))$.
Por el Teorema 3.8, hay un isomorfismo del centro de K en $End(V)$ que es el siguiente:
$K \rightarrow Z(End(V))$: $\mu \rightarrow \mu Id$
De donde, $ZK(G) \cong K \oplus Z(Ker(\tilde{\rho}))$ y $ZK(G) \cong K^{|P|}$. Como (1,0) ϵ $K \oplus Z(ker(\tilde{\rho}))$ y (1,0) es un idempotente primitivo, su imagen por el isomorfismo es un elemento idempotente primitivo de $K(G)$, es decir, un β_λ. Además se tiene que $\beta_\lambda K(G) = End(V)$, este β_λ es aquel tal que $\beta_\lambda V = V$.
Para cualquier otra representación irreducible V' tal que $\beta_\lambda V' = V'$ se

tendría, por el mismo razonamiento, que $\beta_\lambda K(G) = End(V')$. Como por el Teorema 3.7 $End(V)$ es suma directa de V $\dim(V)$ veces y la descomposición de $\beta_\lambda K(G)$ en representaciones irreducibles es única, entonces $V = V'$. Luego tenemos la unicidad. $\square$

Los resultados anteriores nos permiten demostrar fácilmente el siguiente teorema:

Teorema 4.7 (*Teorema de Artin-Wedderburn*) *Si la característica de K no divide al orden de G, la representación regular se puede descomponer como $K(G) = \oplus_i End(V_i)$ donde V_i son todas las representaciones irreducibles de G. Además, hay el mismo número de representaciones irreducibles que clases de conjugación de G.*

Demostración.
Sabemos que $K(G) = \oplus_{\lambda \epsilon P} \beta_\lambda K(G)$ y que para cada idempotente primitivo se tiene que existe una única representación irreducible que denotamos por V_λ tal que $\beta_\lambda K(G) = End(V_\lambda)$. Por tanto, $K(G) = \oplus_{\lambda \epsilon P} End(V_\lambda)$.
Debido a todo lo probado anteriormente tenemos que existe una biyección entre $ZK(G)$ y las representaciones irreducibles de G, que vamos a denotar por $R(G)$ por comodidad, que es la siguiente:

$$\begin{array}{ccc} ZK(G) & \longleftrightarrow & R(G) \\ \beta_\lambda & \rightarrow & V : \beta_\lambda K(G) \cong End(V) \\ \beta_\lambda V = V : \beta_\lambda & \leftarrow & V \end{array}$$

$\square$

5 Ejemplos.

Ejemplo 5.1 *Ideal de $|P|$ puntos distintos de S_4*

$S_4 = \{id, (12), (23), (34), (13), (14), (24), (123), (124), (134), (234),$
$(214), (213), (324), (431), (1234), (1243), (1324), (1432), (2134), (12)(34), (23)(14), (13)(24)\}$
Como podemos ver hay 6 transposiciones, 8 3-ciclos, 6 4-ciclos y 3 transposiciones dobles. Denotamos las clases de conjugación de estos como: $\pi_{2,1,1}$,$\pi_{3,1}$,π_4 y $\pi_{2,2}$, respectivamente. Y, entonces, $ZK(S_4)$ está generado por $\alpha, \beta, \gamma, \delta$ y 1 donde :

$$1 = e_{id}$$

$$\alpha = \Sigma_{\sigma \epsilon \pi_{2,1,1}} e_\sigma$$

$$\beta = \Sigma_{\sigma \epsilon \pi_{3,1}} e_\sigma$$

$$\gamma = \Sigma_{\sigma \epsilon \pi_4} e_\sigma$$

$$\delta = \Sigma_{\sigma \epsilon \pi_{2,2}} e_\sigma$$

De modo que si representamos cada una con la matriz que lleva el vector e_i al $e_{\sigma(i)}$, tenemos:

$$\alpha = \begin{pmatrix} 3 & 1 & 1 & 1 \\ 1 & 3 & 1 & 1 \\ 1 & 1 & 3 & 1 \\ 1 & 1 & 1 & 3 \end{pmatrix}$$

$$\beta = \begin{pmatrix} 2 & 2 & 2 & 2 \\ 2 & 2 & 2 & 2 \\ 2 & 2 & 2 & 2 \\ 2 & 2 & 2 & 2 \end{pmatrix}$$

$$\gamma = \begin{pmatrix} 0 & 2 & 2 & 2 \\ 2 & 0 & 2 & 2 \\ 2 & 2 & 0 & 2 \\ 2 & 2 & 2 & 0 \end{pmatrix}$$

$$\delta = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}$$

Entonces, $ZK(S_4) \cong K[x,y,z,w]/I$ donde $I = ker(F)$, con $F : K[x,y,z,w] \to ZK(S_4)$,es el ideal: $I =< x^2 - 3y - 2w - 6, xy - 4x - 4z, y^2 - 4y - 8w - 8, yz - 4x - 4z, z^2 - 3y - 2w - 6, xw - x - 2z, yw - 3y, zw - 2x - z, w^2 - 2w - 3 >$
Cuyas raíces son: $V(I) = \{(6,8,6,3), (-6,8,-6,3), (2,0,-2,-1), (-2,0,2,-1), (0,-4,0,3)\}$
Además, observamos que estos puntos tienen coordenadas enteras y son distintos en cualquier cuerpo de característica distinta a 2 y 3.

Ejemplo 5.2 *Ideal de $|P|$ puntos distintos de A_4*

$A_4 = \{id, (123), (124), (134), (234), (214), (213), (324), (431),$
$(12)(34), (23)(14), (13)(24)\}$
Las clases de conjugación de A_4 son: π_{id}, $\pi_{(123)}$, $\pi_{(132)}$ y $\pi_{(12)(34)}$. Entonces, $ZK(A_4) = \langle 1, \alpha, \beta, \gamma \rangle$ donde:

$$1 = e_{id}$$

$$\alpha = \Sigma_{\sigma \epsilon \pi_{(123)}} e_\sigma$$

$$\beta = \Sigma_{\sigma \epsilon \pi_{(132)}} e_\sigma$$

$$\gamma = \Sigma_{\sigma \epsilon \pi_{(12)(34)}} e_\sigma$$

Por tanto, $ZK(A_4) \cong K[x,y,z]/I$ donde $I = ker(F)$, con $F : K[x,y,z] \to ZK(A_4)$, es el ideal generado por:
$\langle x^2 - 4y, xy - 4z - 4, y^2 - 4x, xz - 3x, yz - 3y, z^2 - 2z - 3 \rangle$
Cuyas raíces son: $\{(4,4,3), (4\omega, 4\omega^2, 0), (4, 4\omega^2, 4\omega, 0), (3,3,3,-1)\}$, donde ω es un raíz cúbica de la unidad. Observemos que son 4 puntos distintos en cualquier cuerpo de característica distinta a 2 y 3, sin embargo sus coordenadas ya no son enteras como en el caso de S_4.

Ejemplo 5.3 *Idempotentes primitivos de S_4*

A partir del ejemplo 5.1, se pueden sacar los elementos idempotentes del homomorfismo entre $ZK(S_4)$ y K^5 que es el siguiente:
$H : ZK(S_4) \to K^5$ tal que
$H(1) = (1, 1, 1, 1, 1)$
$H(\alpha) = (6, -6, 0, -2, 2)$
$H(\beta) = (8, 8, -4, 0, 0)$
$H(\gamma) = (6, -6, 0, 2, -2)$
$H(\delta) = (3, 3, 3, -1, -1)$
Si tomamos la inversa por dicha aplicación de los vectores e_i, estos nos darán los elementos idempotemtes primitivos que buscamos.
$H^{-1}(e_1) = \beta_1$
$H^{-1}(e_2) = \beta_2$
$H^{-1}(e_3) = \beta_3$
$H^{-1}(e_4) = \beta_4$
$H^{-1}(e_5) = \beta_5$
Cálculos de las preimágenes:
$e_1 = aH(1) + bH(\alpha) + cH(\beta) + dH(\gamma) + eH(\delta) \Rightarrow$

$$\left.\begin{array}{rcl} a + 6b + 8c + 6d + 3e & = & 1 \\ a - 6b + 8c - 6d + 3e & = & 0 \\ a - 4c + 3e & = & 0 \\ a - 2b + 2d - e & = & 0 \\ a + 2b - 2d - e & = & 0 \end{array}\right\}$$

$\Rightarrow \beta_1 = \frac{1+\alpha+\beta+\gamma+\delta}{24}$

Repitiendo el proceso con cada e_i, llegamos a:
$\beta_2 = \frac{1-\alpha+\beta-\gamma+\delta}{24}$
$\beta_3 = \frac{4-2\beta+4\delta}{24}$
$\beta_4 = \frac{9-3\alpha+3\gamma-3\delta}{24}$
$\beta_5 = \frac{9+3\alpha-3\gamma-3\delta}{24}$

6 Comparación con la teoría de caracteres. Ejemplos.

Definición 6.1. El *caracter* de una representación ρ es la función compleja $\chi_\rho(g) = Tr(\rho(g))$ donde Tr es la traza de la matriz $\rho(g)$.

Procedemos ahora a comparar los caracteres con los idempotentes primitivos de los cuales hemos hablado en la sección cuarta.
Primero observemos que parecería normal conocer el cuerpo K sobre el que vamos a trabajar a priori, sin embargo no es así. En teoría de caracteres suele suponerse $K = \mathbb{C}$, sin embargo en nuestro caso bastará con tomar un cuerpo que contenga las coordenadas de los puntos a los que hemos llamado a_λ.

Ejemplo 6.1 *Caracteres de S_4*

En este caso es suficiente trabajar con números racionales o cualquier cuerpo de característica distinta de 2 y 3.
Si miramos la tabla de caracteres del grupo S_4(veáse [1, Exercise 2.22])

	1	6	8	6	3
	(1)	(12)	(123)	(1234)	(12)(34)
ρ_1	1	1	1	1	1
ρ_2	1	-1	1	-1	1
ρ_3	3	1	0	-1	-1
ρ_4	3	-1	0	1	-1
ρ_5	2	0	-1	0	2

nos damos cuenta de que las 4 últimas columnas de la tabla multiplicadas por la primera fila nos dan justo las coordenadas de los puntos calculados en el ejemplo 5.1, es decir, cada punto no solo es distinto a los otros si no que se corresponde con una representación irreducible del grupo.

Ejemplo 6.2 *Caracteres de A_4*

Observamos que, como en el anterior ejemplo, los 4 puntos del ejemplo 5.2 son distintos en cualquier cuerpo de caracaterística distinta de 2 y 3 que, adems, corresponden cada uno con una representación irreducible de A_4, lo cual puede verse en su tabla de caracteres(veáse [1, Exercise 2.26]):

	1	4	4	3
	(1)	(123)	(132)	(12)(34)
ρ_1	1	1	1	1
ρ_2	1	ω	ω^2	1
ρ_3	1	ω^2	ω	1
ρ_4	3	0	0	-1

Es decir, como ya hemos demostrado a cada representación irreducible le corresponde un idempotente primitivo, y en este ejemplo hemos visto también que podemos asociar cada punto a_λ con dicha representación mediante los caracteres.

La teoría de carcateres permite demostrar resultados de teoría de representación de grupos, entre los cuales se incluyen aquellos que hemos demostrado a lo largo de este trabajo y para los cuales no hemos necesitado caracteres. Nuestro objetivo es "sustituir" los caracteres por los idempotentes primitivos, de modo que no sea necesario calcular los primeros.

7 APÉNDICE: Resultados Geometría Algebraica.

Teorema 7.1 *[1, Proposition 12.2] Sean V y V' dos espacios vectoriales sobre un cuerpo K de dimensiones $n < n'$,y $X_k = \{[f]\epsilon P(Hom(V, V')) : rango(f) \leq k\} \subset \mathbb{P}(Hom(V, V'))$. Entonces se tiene que $codim(X_k) = (n-k)(n'-k)$.*

Teorema 7.2 *Sea I un ideal de $K[x_1, \cdots, x_n]$ tal que $K[x_1, ..., x_n]/I$ tiene dimensión finita m sobre K. Entonces, si para cualquier extensión K' de K el ideal generado por I en $K'[x_1, \cdots, x_n]$ es radical, existe una extensión finita K' de K tal que el ideal generado por I en $K'[x_1, \cdots, x_n]$ es el ideal de m puntos de $\mathbb{A}^n_{K'}$.*

Demostración.
Como $K[x_1, ..., x_n]/I$ tiene dimensión finita m, para cada i las clases de $1, x_i, x_i^2, \cdots, x_i^m$ son linealmente dependientes luego existe combinación no trivial $\Sigma_{n=0}^m \lambda_i \bar{x_i^n} = \bar{0}$. Luego existe algún polinomio que solo depende de x_i y su clase es la clase del 0. Es decir, para cada i existe f_i que pertenece a $I \cap K[x_i]$.
Entones, $V(I)$ es finito porque está generado por los ceros de los f_i y sus puntos tienen coordenadas en una extensión finita de K, más concretamente en el cuerpo de descomposición de $f_1, \cdots, f_n$. A esta extensión la denotamos por K' y, abusando de notación, denotamos por I al ideal generado por I en $K'[x_1, \cdots, x_n]$.
Sea P ideal primo de $K'[x_1, \cdots, x_n]$ tal que P contiene a I. Como para cada i de 1 hasta n f_i está en P y f_i descompone en factores lineales en $K'[x_1, \cdots, x_n]$ y, por ser P primo, existe un $x_i - a_i$ en P para todo i. Por tanto, para todo P ideal primo que contiene a I, existe un punto $p = (a_1, \cdots, a_n)$ de $V(I)$ tal que P es el ideal asociado al punto p, $P = I(p)$. Si I es radical se tiene que es igual a la intersección de todos los ideales primos que lo contienen. Por tanto, como en este caso I es radical por ser K' extensión finita de K, tenemos que $I = \cap_{p \epsilon V(I)} I(p)$. Es decir, que el ideal generado por I en $K'[x_1, \cdots, x_n]$ es el ideal de m puntos de $\mathbb{A}^n_{K'}$. $\square$

Teorema 7.3 *[2, Proposition 11.4] Sea X subconjunto de un espacio proyectivo $\mathbb{P}^n$ de codimensión m, entonces corta a todo subespacio lineal de dimensión al menos m. Por tanto, si X no corta a un subespacio de dimensión n, $n < m$.*

Referencias

[1] William Fulton y Joe Harris, *Representation Theory: A First Course*, Springer-New York, 1991.

[2] Joe Harris, *Algebraic Geometry: A First Course*, Springer-New York, 1992.