TRABAJO FIN DE GRADO.
GRADO EN CIENCIAS MATEMÁTICAS.

DEPARTAMENTO DE MATEMÁTICAS FUNDAMENTALES.

REPRESENTACIONES DE GRUPOS FINITOS.

Alumno:
Angel Blasco Muñoz

Tutor:
Dr. Javier Perez Alvarez

Curso 2018 - 2019

A Mateo, mi hijo,
por enseñarme que lo imposible solo tarda un poco mas.
A Begoña, mi mujer,
por toda la paciencia que tiene conmigo.
A Angel y Juliana, mis padres,
por todas las oportunidades que me han dado, incluso cuando no las he merecido.

Agradecimientos.

Quisiera aprovechar este espacio para agradecer a todas aquellas personas que con su profesionalidad, interés, apoyo y ayuda, han hecho posible, de manera directa o indirecta, la redacción de este trabajo.

Asi pues, quiero agradecer al equipo docente de la UNED por todo lo que me han enseñado en estos años de estudio, y muy en especial al Dr. Javier Perez Alvarez por su dedicación y sus consejos a la hora de dirigir este trabajo, sin el no hubiese sido posible la realización del mismo. También me gustaria dedicar un agradecimiento al Dr. Jose Maria Leandro (Pepe), con quién he podido fraguar una grata amistad y el cual siempre me ha dado unos valiosos consejos a la hora de enfrentarme a mis estudios.

No puedo dejar pasar la oportunidad de agradecer a mi mujer, Begoña, la paciencia que ha tenido conmigo mientras realizaba el presente trabajo que tantas horas me ha quitado de estar junto a ella en nuestras particulares condiciones familiares.

Evidentemente es obligatorio agradecer a mis padres, Angel y Juliana, que siempre creyeron en mi, incluso en los momentos mas complicados, y nunca dejaron de apoyarme en esta aventura que es estudiar una carrera a distancia. Espero hacer que se sientan orgullosos.

Por último, pero no por ello menos importante, quisiera dar las gracias a una personita que lleva relativamente poco tiempo entre nosotros, pero que sin duda es quien mas tiempo me roba y quien mas feliz me hace, mi hijo, Mateo, el hace que todo esto tenga un sentido y su lucha diaria es fuente de mi inspiración y motivación.

Gracias.

Resumen

Este trabajo versa sobre los grupos finitos y sus representaciones. Es importante destacar que en todo el trabajo al referirnos a *grupo* nos referimos a un **conjunto finito** en el cual se definirá una operación que debe cumplir unos condicionantes, al igual que en los grupos algebraicos propiamente dichos. En los grupos finitos se deben cumplir y respetar las mismas propiedades que en los grupos en general.

Se introducirá el concepto de representación de un grupo finito, haciendo especial énfasis en el concepto de irreducibilidad, asi como en la teoría de caracteres para la determinación de todas las representaciones irreducibles de un grupo dado. Se definirá a su vez la matriz de caracteres y se calcularán las representaciones irreducibles de algunos grupos finitos.

Índice general

Capitulos **Pagina**

Introducción.

Hasta el siglo XIX no se tenía claro el concepto de grupo abstracto. Los comienzos llegaron de la mano de Gauss con varios grupos, pero hasta el año 1896 no se introdujo la Teoría de Representaciones en el mundo de las matemáticas. El gran pionero fue *Georg Ferdinand Frobenious*, quién se centró en el estudio de caracteres de grupos finitos (en particular, grupos no abelianos). Otros nombres a destacar son *Hermann Weyl*, *Michael Artin* e *Isaai Schur*, quienes desarrollaron importantes resultados posteriormente.

Durante el siglo XX se siguió profundizando en esta rama algebraica que consiste en la descripción de un grupo (en general, no necesariamente finito) como grupo concreto de transformaciones (o grupo de automorfismos) de un cierto objeto matemático, obteniendo de esta forma resultados muy significativos sobre cuerpos algebraicamente cerrados. Durante este siglo se han obtenido, a su vez, importantes resultados en las relaciones de ortogonalidad en los caracteres de grupos; estos resultados se extendieron a otros objetos y se usaron para definir las representaciones de álgebras definidas sobre un cuerpo k.

Por otra parte, esta teoría se aplica en distintos ámbitos de las matemáticas como por ejemplo en la teoria de códigos de corrección de errores y en combinatoria. Esta teoría también sirve como aplicación en otras ciencias como por ejemplo la cristalografia.

Capítulo 1

Conceptos básicos.

1.1. Grupos.

Comencemos por definir el concepto de grupo:

Definicion 1.1.1 *Un grupo es un conjunto no vacio G en el que está definida una operación que toma dos elementos $a, b \in G$ y nos devuelve otro elemento $ab \in G$*

$$G \times G \to G$$

que escribiremos

$$(a, b) \mapsto ab$$

tal que:

1. *$(ab)c = a(bc)$ para cada terna de elementos a, b y c de G. Se dice que la operación es asociativa.*
2. *Existe un elemento $u \in G$ tal que*

   $$ua = a = au$$

   para todos los elementos a de G. A este elemento le llamaremos elemento neutro o elemento identidad.
3. *Para cada elemento $a \in G$ existe $x \in G$ tal que*

   $$ax = u = xa$$

   A este elemento le llamaremos inverso de a.

Diremos que ab es el producto de a por b.

Como ejemplos de grupos (infinitos) podemos citar los conjuntos $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ y $\mathbb{C}$ con la suma usual. Otro ejemplo lo podemos tomar escogiendo un conjunto X no vacio compuesto por las aplicaciones $X \to X$ que son biyectivas, este es un grupo con la operación composición de aplicaciones.

Definicion 1.1.2 *Se dice que un grupo G es abeliano si $ab = ba$ para cada par de elementos $a, b \in G$.*

Sobre los grupos abelianos es importante enunciar que todo grupo formado por dos elementos es abeliano, pues si u es el elemento neutro y $a \neq u$ es el elemento restante,

$$uu = uu$$

$$aa = aa$$

$$au = u = ua$$

Definicion 1.1.3 *El número de elementos de un grupo G se llama orden de G y se denota como $o(G)$. Si $o(G)$ es finito, entonces se dice que G es un grupo finito.*

1.2. Subgrupos.

En este apartado se definira el concepto de subgrupo, y como caracterizarlo, y se enunciarán dos importantes operaciones con subgrupos: la intersección de varios subgrupos y el producto de dos subgrupos.

Definicion 1.2.1 *Un subconjunto no vacio H de un grupo G es un subgrupo de G si, con la misma operación de G, H es un grupo.*

Proposicion 1.2.1 *Podemos afirmar que un conjunto no vacio H es un subgrupo de G si y solo si:*

1. $\forall x, y \in H \rightarrow xy \in H$
2. $1_G \in H$, *siendo* 1_G *el elemento neutro de* G
3. $\forall x \in H \rightarrow x^{-1} \in H$

La siguiente proposición puede ser muy util para caracterizar subgrupos:

Proposicion 1.2.2 *Un subconjunto no vacio H es un subgrupo de G si y solo si:*

$$\forall x, y \in H \rightarrow xy^{-1} \in H$$

Trivialmente se tiene que G es subgrupo de G y 1_G es también subgrupo de G. Estos subgrupos se llaman *impropios.*

Intersección de subgrupos.

Proposicion 1.2.3 *La intersección de una cantidad cualquiera de subgrupos de G, es otro subgrupo.*

Demostracion: Sea $\Lambda \neq \emptyset$ un conjunto cualquiera y sea $\{H_\lambda\}_{\lambda \in \Lambda}$ una familia de subgrupos de G. Entonces,

$$x, y \in \cap_{\lambda \in \Lambda} H_\lambda \rightarrow x, y \in H_\lambda, \forall \lambda \in \Lambda \rightarrow$$
$$\rightarrow xy^{-1} \in H_\lambda, \forall \lambda \in \Lambda \rightarrow xy^{-1} \in \cap_{\lambda \in \Lambda} H_\lambda.$$

■

En particular, dados H, K subgrupos de G, se tendra que $H \cap K$ es subgrupo de G.

Producto de dos subgrupos.

Dados dos subconjuntos no vacíos H y K de un grupo G, el conjunto

$$HK = \{g = xu \,|\, x \in H, u \in K\}$$

de todos los resultados de operar un elemento de H con otro de K, se nombra como el *producto de H por K.*
Suponiendo que H y K sean subgrupos, en general HK no va a ser otro subgrupo.
Vamos a desarrollar una de las condiciones suficientes para que HK sea subgrupo, y vamos a señalar una propiedad que poseé HK en caso de ser subgrupo.

Proposicion 1.2.4 *Si H y K son subgrupos de un grupo abeliano G, se cumple que HK es otro subgrupo de G.*

Demostracion: Sea $g = xu$, $h = yv$, donde $x, y \in H$ y $u, v \in K$, dos elementos de HK. Entonces, aplicando las propiedades asociativa y conmutativa, tenemos

$$gh^{-1} = (xu)(yv)^{-1} = (xu)(v^{-1}y^{-1}) = (xy^{-1})(uv^{-1}) \in HK$$

porque, al tratarse de subgrupos, sabemos que

$$x, y \in H \to xy^{-1} \in H, uv \in K \to uv^{-1} \in K$$

A su vez, la relación $gh^{-1} \in HK$ implica que HK es subgrupo. ■

Proposicion 1.2.5 *Supongamos dos subgrupos H y K de G tales que HK también sea subgrupo. Sea L un tercer subgrupo. Entonces,*

1. $H \cup K \subseteq HK$.
2. $H \cup K \subseteq L \to HK \subseteq L$.

Demostracion:

1. Todo elemento $x \in H$ se puede escribir de la forma xe, con $e \in K$ (recordemos que e representa el elemento neutro), luego $x \in HK$. Igualmente, si $u \in K$ escribiendo $u = eu$ con $e \in H$, vemos que $u \in HK$. Así HK contiene a H y contiene a K, y, por ello,
$$H \cup K \subseteq HK$$
2. Sea L un subgrupo tal que $H \cup K \subseteq L$. Dado un elemento $g \in HK$, se tendrá $g = xu$, donde $x \in H$ y $u \in K$. Como los dos factores pertenecen a $H \cup K$, pertenecerán a L. Siendo L subgrupo, su producto también. Así queda probado que $HK \subseteq L$.

■

Esta proposición significa que si HK es subgrupo, tiene la propiedad de ser el mínimo subgrupo (para la relación de contenido) que contiene a la unión.

Subgrupo generado.

Definicion 1.2.2 *Si S es un subconjunto no vacío de un grupo G, el conjunto*

$$\langle S \rangle = \{s_1^{h_1} \dots s_n^{h_n} : n \in \mathbb{N}, s_i \in S, h_i \in \mathbb{Z}, 1 \leq i \leq n\}$$

es un subgrupo de G que contiene a S, llamado subgrupo generado por S.

Un caso particular y muy importante es aquel en que $S = \{a\}$ para algún $a \in G$. Obviamente

$$\langle a \rangle = \{a^k : k \in \mathbb{Z}\}$$

y se le llama *subgrupo generado por a.*

Definicion 1.2.3 *Un subconjunto no vacío S de un grupo G se llama sistema generador de G si $G = \langle S \rangle$*

Conjunto conjugado.

Si S es un subconjunto no vacío de un grupo G y $a \in G$, se llama *conjugado de S por a* al conjunto

$$S^a = \{a^{-1}xa \,:\, x \in S\}$$

Este conjunto tiene las siguientes propiedades que pasaremos a enunciar:

1. $S \to S^a \,:\, x \mapsto a^{-1}xa$ es biyectiva.
2. $(S^a)^b = S^{ab}$ para cualesquiera $a, b \in G$.
3. $S = S^1$
4. Si S es subgrupo de G, tambien lo es S^a.
5. Si $S \subset T$, entonces $S^a \subset T^a$.

Normalizador.

Si S es un subconjunto no vacío de un grupo G, se llama *normalizador de S en G* a

$$N_G(S) = \{a \in G \,:\, S^a = S\}$$

que es un subgrupo de G.

1.3. Orden de un elemento.

Sea a un elemento de un grupo G de orden g y consideremos la sucesión de potencias de a

$$1_G, a, a^2, a^3, \ldots$$

todas las cuales son, por supuesto, elementos de G. Como G es finito, estos elementos no pueden ser todos distintos, debemos tener la igualdad:

$$a^k = a^l$$

en la que podemos suponer $k > l$, por ejemplo. Por consiguiente,

$$a^{k-l} = 1_G$$

lo que demuestra que en un grupo finito cada elemento tiene alguna potencia igual al elemento unidad.

Definicion 1.3.1 *El menor entero positivo h, para el que a^h es igual al elemento unidad se llama orden de a.*

De modo que si h es el orden de a entonces $a^h = 1_G$, mientras que $a^x \neq 1_G$ cuando $0 < x < h$. Ademas, si m es multiplo de h, es decir $m = hq$, tenemos que:

$$a^m = (a^h)^q = 1_G^q = 1_G$$

Si a es de orden h, entonces $a^m = 1_G$ si y solo si, m es multiplo de h.

Las siguientes propiedades, referentes al orden de un elemento, son de uso frecuente:

1. El único elemento de orden 1 es el elemnto unidad.

2. Los elementos a y a^{-1} tienen siempre el mismo orden.

3. Si $b = p^{-1}ap$, en donde p es un elemento arbitrario, entonces a y b son del mismo orden. Porque
$$b^2 = (p^{-1}ap)(p^{-1}ap) = p^{-1}a1_G ap = p^{-1}a^2p$$
y, en general,
$$b^k = p^{-1}a^k p$$
de modo que si $a^k = 1_G$, tenemos $b^k = p^{-1}1_G p = 1_G$, y reciprocamente.

1.4. Grupos cíclicos.

Definicion 1.4.1 *Se llama grupo cíclico aquel cuyos elementos pueden expresarse por las potencias de uno solo de ellos.*

La forma general de un grupo cíclico G de orden c es:

$$G = \{1_G,\, a,\, a^2, \ldots, a^{c-1}\}$$

en donde c es el menor entero positivo que verifica la igualdad $a^c = 1_G$. Y decimos que a genera el grupo G o que es el *elemento generador* del grupo.

El orden de un grupo cíclico es igual al del elemento generador; reciprocamente, si un grupo de orden c contiene un elemento también de orden c, entonces el grupo es cíclico. El elemento generador no está unívocamente determinado; en efecto, si e es un entero cualquiera primo con c y $0 < e < c$, entonces se puede tomar a^e por elemento generador del grupo.

Todos los grupos cíclicos del mismo orden son isomorfos como se ve haciendo que se correspondan sus elementos generadores; en efecto, existe un grupo cíclico (abstracto) y solo uno para cada orden dado.

Proposicion 1.4.1 *Todos los grupos cíclicos son abelianos.*

Demostracion: Sea $G = \langle a \rangle$ un grupo cíclico. Dados $x, y \in G$, seran $x = a^k$, $y = a^l$, para ciertos enteros k y l. Por lo tanto
$$xy = a^{k+l} = yx$$
lo que implica que G es abeliano. ■

1.5. Coclases, índice de un grupo y Teorema de Lagrange.

Definicion 1.5.1 *Sea H un subgrupo de un grupo G, y sea x un elemento de G. El subconjunto de G formado por los productos hx $(h \in H)$ se denomina coclase derecha de H en G y se denota por Hx. La coclase izquierda de H en G, xH, se define de forma similar.*

Definicion 1.5.2 *El número de las distintas coclases derechas de H se llama índice de H en G y se denota por $[G : H]$*

Para cada subconjunto S de G, S^{-1} será el conjunto de los elementos inversos de S:

$$S^{-1} = \{s^{-1} : s \in S\}$$

Si S es una coclase derecha de H , entonces $S = Hx$ para algún $x \in G$. La inversa de un elemento de hx de S es $x^{-1}h^{-1}$, así que S^{-1} coincide con la coclase izquierda $x^{-1}H$. De igual forma $(yH)^{-1} = Hy^{-1}$. Así que, el número de las distintas coclases derechas de H es igual al numero de las distintas coclases izquierdas de H.
Podriamos haber definido el índice usando las coclases izquierdas de igual manera.

A continuación se enunciarán las propiedades básicas de las coclases:
Sea H un subgrupo de G,

1. Todo elemento $g \in G$ esta contenido en una y solo una coclase de H. Esta coclase es Hg.
2. Dos coclases distintas de H no tienen elementos comunes.
3. El grupo G esta particionado en una unión disjunta de coclases de H.
4. La función $h \to hx$ tiene una correspondencia uno-a-uno entre los elementos del conjunto H y los de la coclase Hx. Al tratarse H de un subgrupo finito cada coclase de H tiene el mismo número de elementos que H.
5. Dos elementos $x, y \in G$ están contenidos en la misma coclase de H si y solo si $xy^{-1} \in H$.

Pasemos ahora a enunciar y demostrar el Teorema de Lagrange:

Teorema 1.5.1 (Teorema de Lagrange) *Sean G un grupo y H un subgrupo de G, tenemos que $o(G) = o(H) \cdot [G : H]$. En particular, el orden de H y el indice de H en G dividen al orden de G.*

Demostracion: Utilizando las propiedades básicas de las coclases, en concreto por 3) y 4), el conjunto G está particionado en una unión disjunta de $[G : H]$ conjuntos que contienen, cada uno, $o(H)$ elementos. Contando el número de elementos en G, obtenemos que:

$$o(G) = o(H) \cdot [G : H].$$

■

El teorema de Lagrange implica los siguientes corolários que no demostraremos:

Corolario 1.5.1 *El orden de un elemento de un grupo finito G divide a $o(G)$.*

Corolario 1.5.2 *Si el orden de un grupo finito G es n, entonces todo elemento $x \in G$ satisface $x^n = 1_G$.*

1.6. Subgrupos normales. Grupo cociente.

1.6.1. Subgrupos normales.

Dado un grupo G y un subgrupo H de G, formaremos un nuevo grupo cuyos elementos son las clases laterales izquierdas de H en G. Estos subgrupos los denominaremos *subgrupos normales* y su definición es:

Definicion 1.6.1 *Sea G un grupo. Un subgrupo H de G es un subgrupo normal si*

$$ghg^{-1} \in H, \forall g \in G, h \in H$$

Si H es un subgrupo normal de G se representa como $H \triangleleft G$.

Teorema 1.6.1 *Si G es un grupo abeliano y H es un subgrupo de G, entonces H es un subgrupo normal de G.*

Demostracion: Como G es abeliano, $ghg^{-1} = hgg^{-1} = h \in H$ para todo $g \in G$ y todo $h \in H$, luego $H \triangleleft G$. ■

Sea G un grupo. Sea $H \triangleleft G$. Recordemos que, para $g \in G$, las clases laterales izquierda y derecha son, respectivamente,

$$gH = \{gh \,:\, h \in H\}$$

$$Hg = \{hg \,:\, h \in H\}$$

Para un subgrupo normal estas clases son iguales pues si $h \in H$, entonces $ghg^{-1} \in H$, luego $ghg^{-1} = h_1$ para algún $h_1 \in H$, luego $gh = h_1 g$. Esto muestra que $gH = Hg$.
Notar también que $gH = Hg$ significa que para cada $h \in H$ hay $h_1 \in H$ tal que $gh = gh_1$.
Lo anterior no ocurre cuando H no es subgrupo normal.

1.6.2. Grupo cociente.

Sea $H \triangleleft G$ (no usamos un símbolo especial para la operación). Denotamos por G/H el conjunto de las clases laterales izquierdas de H en G, es decir

$$G/H = \{gH \,:\, g \in G\}$$

Observar que $gH = Hg$ pues H es un subgrupo normal. Definiremos una operación en este conjunto de clases.

Teorema 1.6.2 *Sea $H \triangleleft G$. Dados $a, b \in G$ sea*

$$(aH)(bH) = (ab)H$$

Esto define una operación en G/H.

Demostracion: Si $aH = cH$ y $bH = dH$, queremos probar que $(ab)H = (cd)H$. Como $a \in aH = cH$, entonces $a = ch_1$, algún $h_1 \in H$. De $b \in bH = dH$ obtenemos $b = dh_2$, algún $h_2 \in H$. Ahora $ab = ch_1 dh_2$ y ya que $dH = Hd$, hay $h_3 \in H$ tal que $h_1 d = dh_3$, luego $ch_1 dh_2 = cdh_3 h_2 = cdh_4$, donde $h_4 = h_3 h_2$. Tenemos entonces que $ab = cdh_4$ y por lo tanto $(ab)H = (cdh_4)H = (cd)H$. ■

Sea $H \triangleleft G$. El conjunto G/H es un grupo con la operación

$$(aH)(bH) = (ab)H$$

1.7. Homomorfismos de grupos.

Definicion 1.7.1 *Sean G_1 y G_2 grupos, y sea $f : G_1 \to G_2$ una aplicación entre ellos. Se dice que f es un homomorfismo de grupos si*

$$f(xy) = f(x)f(y)$$

Un homomorfismo inyectivo recibe el nombre de monomorfismo; un homomorfismo suprayectivo recibe el nombre de epimorfismo; un homomorfismo biyectivo recibe el nombre de isomorfismo; y un isomorfismo de G en si mismo es un automorfismo.
Si existe un isomorfismo entre G_1 y G_2 se dice que ambos grupos son isomorfos.

Proposicion 1.7.1 *Sean G y H grupos, y sea $f : G \to H$ un homomorfismo entre ellos. Entonces, para todo $x, y \in G$*

$$f(xy^{-1}) = f(x)f(y)^{-1}$$
$$f(y^{-1}x) = f(y)^{-1}f(x)$$

Demostracion: Utilizando que f es un homomorfismo,

$$f(xy^{-1})f(y) = f((xy^{-1})y) = f(x)$$

y basta componer con $f(y)^{-1}$ por la derecha. La demostracion de la segunda igualdad es análoga. ■

Proposicion 1.7.2 *Sean G y H grupos, y sea $f : G \to H$ un homomorfismo entre ellos. Entonces,*

$$1.\ f(1_G) = 1_H$$
$$2.\ f(g^{-1}) = f(g)^{-1},\ \forall g \in G$$

Demostracion: Para 1) basta aplicar la proposición anterior al caso $x = y$. Para 2) basta aplicar la proposición anterior al caso $x = 1_G$, $y = g$. ■

Definicion 1.7.2 *Sean G y H grupos, y sea $f : G \to H$ un homomorfismo entre ellos. Se llaman núcleo e imagen de f a los conjuntos:*

$$ker\, f = \{g \in G : f(g) = 1_G\}$$

$$im\, f = \{h \in H : \exists g \in G : f(g) = h\}$$

Es importante indicar que el nucleo de f es un subgrupo de G, mientras que la imagen de f es un subgrupo de H.

Proposicion 1.7.3 *Sean G y H grupos, y $f : G \to H$ un homomorfismo. Si G es abeliano, $f(G)$ es abeliano.*

Demostracion:

$$f(x)f(y) = f(xy) = f(yx) = f(y)f(x)$$

■

1.7.1. Teorema de Cayley.

Este teorema afirma que todo grupo finito es isomorfo a un subgrupo de un grupo S_n para algún natural n. Primero a cada elemento de un grupo G le asociaremos una función biyectiva.

Teorema 1.7.1 *Dado un conjunto no vacío X, el conjunto S_x de todas las funciones biyectivas de X en X es un grupo con la operación $\circ$ de composición de funciones.*

La demostración es trivial usando las condiciones que debe cumplir un grupo.

Teorema 1.7.2 *Dado un grupo G,*

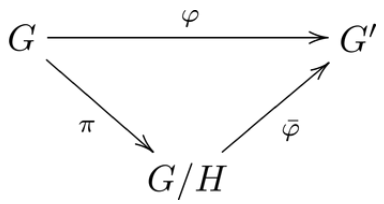
1. *Para cada $g \in G$ la función $\alpha_g : G \to G$, $\alpha_g(x) = gx$ es biyectiva.*
2. *La función inversa de α_g es α_g^{-1}.*
3. *Dados $a, b \in G$, $\alpha_a \circ \alpha_b = f_{ab}$.*
4. *El conjunto $\{\alpha_g : g \in G\}$ es un grupo de S_G con la operación composición.*

Teorema 1.7.3 (Teorema de Cayley.) *Si G es un grupo finito de orden n, entonces G es isomorfo a un subgrupo del grupo simétrico S_n.*

Demostracion: La función $\alpha : G \to S_G$, $\alpha(g) = \alpha_g$ es un homomorfismo. Si $g \in ker\,\alpha$, entonces $\alpha(g)$ es la identidad de S_G, luego $\alpha_g(x) = gx = x$, todo $x \in G$, de donde $g = 1_G$. Así α es inyectiva y G es isomorfo con $\alpha(G)$, que es un subgrupo de S_G.
Ahora si G es un grupo de orden n veremos que S_G es isomorfo con S_n. Si $o(G) = n$, entonces existe una función biyectiva $\beta : G \to N_n$ y también $\beta^{-1} : N_n \to G$ es biyectiva. Dado $\sigma \in S_n$, la función $\beta^{-1} \circ \sigma \circ \beta : G \to G$ es una biyección y la función $S_n \to S_G : \sigma \mapsto \beta^{-1} \circ \sigma \circ \beta$ es un isomorfismo. ■

1.7.2. Factorización de homomorfismos.

Sean G y G' grupos arbitrarios y $\varphi : G \to G'$ un homomorfismo de grupos. Sea H un subgrupo de $ker(\varphi)$; observar que H es subgrupo normal de G porque el núcleo es normal. Sea $\pi : G \to G/H$ la proyección al cociente.Entonces existe un único homomorfismo de grupos $\overline{\varphi} : G/H \to G'$ que hace conmutar el siguiente diagrama:



Es decir, para todo $x \in G$ dicho homomorfismo cumple que $\varphi(x) = \overline{\varphi}(\pi(x))$.

Demostracion: Existencia. Sea $\varphi : G/H \to G'$ la aplicación dada por $\overline{x} \to \varphi(x)$. Está bién definida porque si $\overline{x} = \overline{y}$, entonces $1 = \overline{xy}^{-1}$, con lo cual $xy^{-1} \in H \subseteq ker(\varphi)$. Por lo tanto $\varphi(xy^{-1}) = 1$, y entonces $\varphi(x) = \varphi(y)$. Además, define un homomorfismo porque $\overline{\varphi}(\overline{xy}) = \varphi(xy) = \varphi(x)\varphi(y) = \overline{\varphi}(\overline{x})\overline{\varphi}(\overline{y})$. Para ver que hace conmutar el diagrama, notar que para todo $x \in G$ se cumple $\varphi(x) = \overline{\varphi}(\overline{x}) = \overline{\varphi}(\pi(x))$.
Unicidad. Para la unicidad, basta observar que la manera en que fue definido el homomorfismo $\overline{\varphi}$ es la única manera de definirlo de tal manera que conmute con el diagrama. Es decir, si se tiene un homomorfismo ψ que conmuta con el diagrama, $\psi(\overline{x}) = \varphi(x)$ para todo $x \in G$, y entonces $\psi = \overline{\varphi}$. ■

1.7.3. Teoremas de isomorfía.

Primer teorema de isomorfía.

Teorema 1.7.4 *Sean G y G' grupos arbitrarios y sea $\varphi : G \to G'$ Un homomorfismo de grupos. Entonces $G/ker(\varphi) \simeq im(\varphi)$.*

El simbolo $\simeq$ indica que los dos elementos son isomorfos.

Demostracion: Usando la factorización de homomorfismos de grupos sobre el núcleo $ker(\varphi)$, se tiene que existe un único homomorfismo $\overline{\varphi} : G/ker(\varphi) \to G'$ tal que $\varphi = \overline{\varphi} \cdot \pi$.
Si consideramos dicho homomorfismo $\overline{\varphi}$ restringiendo su dominio a $im(\varphi)$ tendriamos un epimorfismo, porque por definición de la imagen, para todo $y \in im(\varphi)$ existe un $x \in G$ tal que $\varphi(x) = y$, y por lo tanto $\overline{\varphi}(\overline{x}) = y$.
Ademas, es un monomorfismo, porque $\overline{\varphi}(\overline{x}) = \varphi(x)$. Entonces si, $\overline{\varphi}(x) = 0$ se tiene que $x \in ker(\varphi)$, con lo cual $\overline{x} = 0$.
Así, $\overline{\varphi} : G/ker(\varphi) \to im(\varphi)$ resulta un isomorfismo. ■

Segundo teorema de isomorfía.

Teorema 1.7.5 *Sean N y H subgrupos normales de un grupo G, tales que $N \subset H$. Entonces $H/N \triangleleft G/N$ y*

$$(G/N)/(H/N) \simeq G/H$$

Demostracion: Consideramos la aplicación

$$f : G/N \to G/H : aN \mapsto aH$$

que sabemos que esta bien definida, pues si $aN = bN$, entonces $a^{-1}b \in N \subset H$, por lo que $aH = bH$.
Como $f((aN)(bN)) = f(abN) = abH = (aH)(bH) = f(aN)f(bN)$, f es homomorfismo.
Cada $aH \in G/H$ es $aH = f(aN)$, luego f es sobreyectiva. Finalmente $aN \in ker(f)$ si y solo si $aH = f(aN) = H$, esto es,

$$ker(f) = \{aN \in G/N \,:\, a \in H\} = H/N$$

Como f es un homomorfismo de gupos, aplicando el primer teorema de isomorfia tenemos que

$$(G/N)/ker(f) \simeq im(f)$$

esto es,

$$(G/N)/(H/N) \simeq G/H$$

■

Tercer teorema de isomorfía.

Teorema 1.7.6 *Sean G un grupo y S, T subgrupos de G. Sea S un subgrupo normal de G. Entonces se tiene que $ST/S = T/(S \cap T)$.*

Demostracion: Para empezar, se debe verificar que las expresiones del enunciado están bién definidas. Por un lado ST es subgrupo de G porque S es normal en G. Teniendo esto en cuenta se cumple también que S es subgrupo normal de ST, por que dado cualquier $x \in ST$, en particular $x \in G$, y por lo tanto $xSx^{-1} = S$. Por último $S \cap T$ es subgrupo normal de T. Para

ello, dados $t \in T$ y $s \in S \cap T$, se debe ver que $tst^{-1} \in S \cap T$. En efecto, $tst^{-1} = S$ porque S es normal, y está en T porque todos sus factores lo están.
Para el isomorfismo, vamos a considerar primero la aplicación $\varphi : T \to ST/S$ definida por $t \mapsto \overline{t} = 1tS$. Se tiene que φ es un homomrfismo de grupos porque $\varphi(tt') = \overline{tt'} = \varphi(t)\varphi(t')$.
Por un lado, φ es un epimorfismo. Para ver esto, considerar un elemento $stS \in ST/S$ arbitrario. Por ser S normal, se sabe que st se escribe como $t\widetilde{s}$ para algún $\widetilde{s} \in S$. Se tiene entonces que $stS = t\widetilde{s}S = tS = \varphi(t)$.
Por otro lado, el núcleo $ker(varphi)$ es el conjunto $\{t \in T : tS = S\}$, es decir, $T \cap S$.
Resumiendo, $\varphi : T \to ST/S$ es un epimorfismo cuyo núcleo es $T \cap S$. Por el primer teorema de isomorfia se concluye entonces que $T/(T \cap S) \simeq ST/S$. ■

1.8. Teorema de estructura de los grupos abelianos finitos.

El teorema de estructura de los grupos abelianos finitos constituye, por su naturaleza, una primera aproximación a la clasificación de los grupos, en nuestro caso de los grupos abelianos finitos.
Apuntemos que todo grupo cíclico es abeliano, pero no todo grupo abeliano es ciclico, ademas, los grupos abelianos finitos son producto directo de grupos ciclicos.
Enunciamos a continuación el teorema de estructura de los grupos abelianos finitos, del cual omitiremos su demostracion:

Teorema 1.8.1 (Estructura de los Grupos Abelianos Finitos.) *Si G es un grupo abeliano finito, existen enteros positivos $m_1, \ldots, m_r$ tales que:*

$$G \simeq Z/m_1Z \times \ldots \times Z/m_rZ$$

y cada m_i divide a m_{i-1}.

Queda claro que $o(G) = m_1 \ldots m_r$. Ademas, los numeros $r, m_1, \ldots, m_r$ son únicos con esta propiedad. Se dice que $m_1, \ldots, m_r$ son los coficientes de torsión de G.
Este teorema nos permite calcular el numero de grupos abelianos finitos no isomorfos de un orden dado.
Pongamos un ejemplo aclarador de aplicación de este teorema:

Supongamos que deseamos calcular cuantos grupos abelianos no isomorfos existen de orden 200. El teorema de estructura reduce la cuestión a obtener todas las -uplas $(r, m_1, \ldots, m_r)$ tales que $m_1 \ldots m_r = 200$ con m_i divide a m_{i-1}. Asi tenemos que para:

$r = 1$:

$$m_1 = 200$$

para $r = 2$:

$$m_1 = 100\,;\, m_2 = 2$$

$$m_1 = 40\,;\, m_2 = 5$$

$$m_1 = 20\,;\, m_2 = 10$$

para $r = 3$:

$$m_1 = 50\,;\, m_2 = 2\,;\, m_3 = 2$$

$$m_1 = 10\,;\, m_2 = 10\,;\, m_3 = 2$$

ya no es posible encontrar mas -uplas que cumplan las condiciones del teorema. Por lo tanto hay 6 grupos abelianos, no isomorfos, de orden 200 que son:

$$Z/200Z$$

$$Z/100Z \times Z/2Z$$

$$Z/400Z \times Z/5Z$$

$$Z/20Z \times Z/10Z$$

$$Z/500Z \times Z/2Z \times Z/2Z$$

$$Z/10Z \times Z/10Z \times Z/2Z$$

por lo tanto, todos los grupos abelianos de orden 200 son isomorfos a alguno de ellos.

1.9. Automorfismos de grupos.

Los homomorfismos biyectivos de un grupo G en si mismo se conocen como los automorfismos de G. Estas funciones conforman un grupo que tiene información importante relativa al grupo G.

1.9.1. Automorfismos interiores.

Veremos la relación entre los automorfismos de un grupo, sus automorfismos interiores y su centro.

Si H es un subgrupo de un grupo G, se llama *centralizador* de H en G a

$$C_G(H) = \{x \in G : ax = xa \ \forall a \in H\}$$

Al centralizador de G en G, simbolizado por $Z(G)$ y llamado *centro* de G, es un grupo normal de G el cual esta definido como

$$Z(G) = \{x \in G \ : \ xa = ax, \ \forall a \in G\}$$

Notese que G es abeliano si y solo si $G = Z(G)$.

Definicion 1.9.1 *Sea G un grupo, un **automorfismo** de G es un homomorfismo biyectivo de G en si mismo. Sea $x \in G$ la función definida por*

$$\phi_x : G \to G$$

$$a \mapsto x^{-1}ax$$

*es un automorfismo de G y se denomina **automorfismo interior** de G determinado por x. El conjunto de los automorfismos interiores de G lo denotaremos como $Int(G)$.*

Enunciamos ahora la siguiente proposición que nos sera de utilidad para demostrar el próximo teorema:

Proposicion 1.9.1 *Sean G un grupo y H un subgrupo de G. La aplicación*

$$\phi : N_G(H) \to Aut(H) \ : \ a \mapsto \phi_a$$

es homomorfismo de grupos con imagen $Int(H)$ y núcleo $C_G(H)$.

Teorema 1.9.1 *Sea G un grupo, $Aut(G)$ su colección de automorfismos y sea $Int(G)$ el conjunto de automorfismos interiores de G. Entonces:*

1. *$Aut(G)$ es un subgrupo de grupo S_G de funciones biyectivas de G en G.*
2. *$Int(G) \triangleleft Aut(G)$*

Demostracion: 1) La primera afirmación es evidente. 2) Por comodidad, llamando $K = Int(G)$ se trata de probar, como vimos en la definición 1.6.1, que:

$$K^f \subset K, \ \forall f \in Aut(G)$$

Sea pues $g \in K^f$. Asi $f \circ g \circ f^{-1} \in K$, luego existe $a \in G$ tal que $f \circ g \circ f^{-1} = \phi_a$, donde ϕ_a es un automorfismo interior, y asi $g = f^{-1} \circ \phi_a \circ f$. Entonces, dado $x \in G$ y llamando $b = f^{-1}(a)$ se tiene

$$g(x) = (f^{-1} \circ \phi_a)(f(x)) = f^{-1}(af(x)a^{-1}) = bxb^{-1} = \phi_b(x)$$

por tanto, $g = \phi_b \in K$.
Por último, de la proposición 1.9.1 se deduce que la aplicación

$$\phi : G \to Int(G) \ : a \mapsto \phi_a$$

es homomorfismo sobreyectivo con núcleo $Z(G)$, y por ello

$$G/Z(G) \cong Int(G)$$

■

1.9.2. Acción de un grupo sobre un conjunto.

El concepto de grupo tomó importancia en la matemática cuando Lagrange y luego Galois consideraron las sustituciones de las raices de una ecuación polinomial; los patrones de intercambios de las raices aportan información sobre la solubilidad de la ecuación mediante fórmulas explícitas. Posteriormente, Felix Klein enfatizó la importancia de las simetrias admisibles en la clasificación de las geometrias. En los dos casos, los elementos de un grupo aparecen como transformación de otros objetos (raices de una ecuación algebraica; o puntos de un plano) y los objetos transformados no son menos importantes que las propias transformaciones.

Definicion 1.9.2 *Una acción (a la izquierda) de un grupo G sobre un conjunto X es una función $\phi : G \times X \to X$ tal que:*

1. *$\phi(g, \phi(h, x)) = \phi(gh, x)$ para todo $g, h \in G$, $x \in X$.*
2. *$\phi(1_G, x) = x$ para todo $x \in X$.*

Se acostumbra a escribir $g \cdot x$ en lugar de $\phi(g, x)$; con esta notación, las propiedades de una acción son:

$$g \cdot (h \cdot x) = (gh) \cdot x$$

$$1_G \cdot x = x$$

Definicion 1.9.3 *Una acción de grupo define una relación de equivalencia sobre X: $x \sim y$ si y solo si $x = g \cdot y$ para algún $g \in G$.*

La **órbita** de $x \in X$ bajo la acción de G es la clase de equivalencia de x bajo esta relación:

$$G \cdot x = \{g \cdot x \in X \ : \ g \in G\} \subseteq X$$

Una acción de un grupo G en un conjunto X se dice que es *transitiva* si para todo par de elementos $x, y \in X$ existe un $g \in G$ tal que $g \cdot x = y$.

Definicion 1.9.4 *Sea $\phi : G \times X \to X$ una acción de un grupo sobre un conjunto. El **subgrupo estabilizador** para un elemento $x \in X$ es el subgrupo*

$$G_x = \{g \in G \ : \ g \cdot x = x\} \subseteq G$$

Proposicion 1.9.2 *Dada una acción de un grupo G sobre un conjunto X, el número de elementos de la órbita $G \cdot x$ coincide con el índice $[G : G_x]$.*

Demostracion: Si $h, g \in G$ y $x \in X$, entonces

$$g \cdot x = h \cdot x \iff g^{-1}h \cdot x = x \iff g^{-1}h \in G_x \iff gG_x = hG_x \in G/G_x$$

luego la aplicación $g \cdot x \mapsto gG_x$ es una biyección de la órbita $G \cdot x$ en el conjunto cociente G/G_x. Por lo tanto $o(G \cdot x) = o(G/G_x) = [G : G_x]$ ■

Definicion 1.9.5 *Una acción $\phi : G \times X \to X$ es **eficaz** (o **fiel**) si el homomorfismo $\psi : G \to S_X$ es inyectivo. Una acción es eficaz si $g \cdot x = x$ para todo $x \in X$ implica $g = 1_G$.*

Un grupo G también actúa por conjugación sobre el conjunto de todos sus subgrupos, $X = \{H : H \subseteq G\}$. Esta acción está dada por la fórmula $g \cdot H = gHg^{-1}$. La órbita de H bajo esta acción es la familia de subgrupos conjugados de H.
El subgrupo estabilizador de H en este caso es el **normalizador** de H, definido como:

$$N_G(H) = \{g \in G : gHg^{-1} = H\}$$

Se puede observar que $N_G(H)$ es un subgrupo de G, no necesariamente normal, pero H es un subgrupo normal de él: $H \triangleleft N_G(H)$.

1.9.3. Teorema de Sylow.

Antes de enunciar los teoremas de Sylow debemos introducir el concepto de *p-grupo* y el *Teorema de Cauchy.*

Definicion 1.9.6 *Sea p un número primo. Un grupo finito G se denomina p-grupo si $o(G) = p^r$, con $r \in \mathbb{Z}^+$.*

Antes de continuar es importante destacar dos resultados que usaremos en la demostración del Teorema de Syllow:

1. *Congruencia de los puntos fijos.* Si G es un *p-grupo* y G opera sobre un conjunto finito X, entonces:
$$o(X) \equiv o(X_0)(mod\, p)$$
Donde $X_0 \subseteq X$ es el conjunto de puntos fijos,
$$X_0 = \{x \in X; Gx = \{x\}\}$$

2. *Congruencia del normalizador.* Es un caso particular del resultado anterior. Sea H un *p-subgrupo* de un grupo finito G. Entonces:

$$[N(H) : H] \equiv [G : H](mod\, p)$$

Teorema 1.9.2 (Teorema de Cauchy) *Sea G un grupo finito de orden n y p un número primo que divide a n. Entonces G tiene un elemento (y por lo tanto un subgrupo) de orden p.*

Demostracion: Sea $X = \{(x_1, \ldots, x_p) \in G^p \,:\, x_1 \ldots x_p = 1\}$. Si $k \in \mathbb{Z}_p$, la relación

$$k(x_1, \ldots, x_p) = (x_{k+1}, \ldots, x_p, x_1, \ldots, x_k)$$

define una acción de $\mathbb{Z}_p$ en X. Como $\mathbb{Z}_p$ es un p-grupo y $o(X) = n^{p-1}$, se tiene que $o(X_0)$ es multiplo de p, siendo

$$X_0 = \{(x, \ldots, x) \,:\, x \in G\,, x^p = 1\}$$

Dado que X_0 contiene el elemento $(1, 1, \ldots, 1)$, resulta que G tiene un elemento de orden p. ■

Sea G un grupo finito, ante el problema de estudiar los subgrupos de G es natural empezar con los p-subgrupos, para cada primo p. El conocimiento de estos subgrupos es muy útil para determinar la estructura de G.
Con los teoremas de Sylow podremos conocer, si, dado un grupo finito G y un primo p que divida a $o(G)$, si existen p-subgrupos de cualquier orden permitido por el teorema de Lagrange, cuantos hay, y que relación hay entre ellos.

Teorema 1.9.3 (Primer teorema de Sylow) *Sea G un grupo finito, p un número primo y $r > 0$ un número entero tales que p^r divide a $o(G)$. Entonces existen subgrupos $H_1, \ldots, H_r$ de G tales que $o(H_i) = p^i$ para $i = 1, \ldots, r$ y de modo que $H_i \triangleleft H_{i+1}$ para $i = 1, \ldots, r-1$.*

Demostracion: Si $r = 1$ el resultado es consecuencia directa del teorema de Cauchy. Supongamos pues que $r \geq 2$. Entonces existen, por inducción, subgrupos $H_1, \ldots, H_{r-1}$ de G tales que $o(H_i = p^i\, (1 \leq i \leq r-1)$ y con H_i normal en $H_{i+1}\, (1 \leq r \leq r-2)$. Como p divide a $[G : H_{r-1}]$, por la congruencia del normalizador, vemos que p divide a $[N(H_{r-1}) : H_{r-1}]$. Por el teorema de Cauchy el grupo cociente $N(H_{r-1})/H_{r-1}$ tiene un subgrupo H_r/H_{r-1} de orden p, o lo que es lo mismo, H_r es un subgrupo de $N(H_{r-1})$ que contiene a H_{r-1} como subgrupo normal. Como H_r tiene orden p^r, por el teorema de Lagrange, la demostración es completa. ■

Si p es un divisor del orden n, de un grupo finito G, entonces existen p-subgrupos de Sylow de G. Basta con observar que si $n = p^r m$, m primo con p, los p-subgrupos de Sylow de G son los subgrupos de orden p^r. Si G posee un único p-subgrupo de Sylow H, entonces $H \triangleleft G$.

Teorema 1.9.4 (Segundo teorema de Sylow) *Sea G un grupo finito, H un p-subgrupo de G y S un p-subgrupo de Sylow de G. Entonces existe $x \in G$ tal que*

$$H \subseteq xSx^{-1}$$

en particular, dos p-subgrupos de Sylow de G son conjugados.

Demostracion: Consideremos la acción de H en $X = G/S$ por traslaciones por la izquierda. Una clase $xS \in X$ es invariante por la acción anterior si y solo si $hxS = xS$ para todo $h \in H$, es decir, si y solo si $x^{-1}hx \in S$ para todo $h \in H$. Como esta relación es equivalente a $H \subseteq xSx^{-1}$, vemos que

$$X_0 = \{xS \in X \,:\, H \subseteq xSx^{-1}\}$$

Ahora bien, como H es un p-grupo y $o(X) = [G : S]$, la congruencia de puntos fijos nos da

$$o(X_0) \equiv [G : S] \ (mod\, p)$$

Como p no divide a $[G : S]$, concluimos que X_0 no es divisible por p y por tanto que X_0 no es vacío. ■

El segundo teorema de Sylow se deduce trivialmente que la condición de que G posea un único p-subgrupo de Sylow es equivalente a que G posea un p-subgrupo de Sylow normal.

Teorema 1.9.5 (Tercer teorema de Sylow) *Sea G un grupo finito, y n_p el número de p-subgrupos de Sylow de G. Entonces $n_p = [G : N(S)]$, para todo p-subgrupo de Sylow S de G. Puesto que $[G : N(S)]$ divide a $[G : S]$, en particular tenemos que n_p divide a $[G : S]$ para todo p-subgrupo de Sylow S de G. Por último, se verifica que $n_p \equiv 1(mod\, p)$.*

Demostracion: Por el segundo teorema de Sylow, n_p es el cardinal de la órbita de un p-subgrupo de Sylow S por la acción de G (por conjugación) en el conjunto de subgrupos de G. De ello se deduce que

$$n_p = [G : N(S)]$$

dado que el grupo estabilizador de S es $N(S)$. La primera parte del enunciado se sigue de la relación

$$[G : S] = [G : N(S)][N(S) : S]$$

Sea ahora X el conjunto de p-subgrupos de Sylow de G. Consideremos la acción de S en X por conjugación. Entonces

$$X_0 = \{T \in X \ : \ sTs^{-1} = T, \forall s \in S\} = \{T \in X \ : \ S \subseteq N(T)\}$$

Veamos que $X_0 = \{S\}$. En efecto, si $T \in X_0$, entonces S y T son p-subgrupos de Sylow de $N(T)$ y $T \lhd N(T)$, de donde, por el segundo teorema de Sylow, $T = S$. Como $o(X) = n_p$ y $o(X_0 = 1$, obtenemos la congruencia enunciada usando la congruencia de puntos fijos. ■

Capítulo 2

Representaciones de grupos.

Una representación de un grupo finito G nos proporciona una manera de visualizar G como un grupo de matrices. Para ser mas preciso diremos que una representación es un homomorfismo de G en el grupo de matrices invertibles.
La estructura de estos homomorfismos y sus propiedades seran objeto de estudio en este capitulo.

2.1. Representaciones de grupos.

Sea V un espacio vectorial sobre el cuerpo $\mathbb{C}$ de los números complejos, y sea $GL(V)$ el grupo de isomorfismos de V. Un elemento $a \in GL(V)$ es, por definición, una aplicación lineal de V en V que admite inversa a^{-1}; a^{-1} es también lineal. Si V admite una base finita (e_i) de n elementos, toda aplicación lineal $a : V \to V$ se representa por una matriz cuadrada (a_{ij}) de orden n. Los coeficientes a_{ij} son números complejos; se calculan expresando $a(e_j)$ en la base (e_i):

$$a(e_j) = \sum_i a_{ij} e_i$$

Decir que a es un isomorfismo equivale a decir que el determinante de a es no nulo. El grupo $GL(V)$ se identifica así como el grupo de matrices cuadradas invertibles de orden n. En algunas ocasiones escribiremos $GL(n, V)$.

Definicion 2.1.1 *Sea G un grupo finito. Una representación de G en V es un homomorfismo ρ del grupo G en el grupo $GL(V)$:*

$$\rho : G \to GL(V)$$

de modo que:

$$\rho(st) = \rho(s)\rho(t)$$

cualesquiera que sean $s, t \in G$.

Supongamos que V es de dimensión finita, y sea n su dimensión; se dice también que n es el *grado* de la representación considerada.

Ejemplo 2.1.1 *Sea G el grupo dihedral $D_8 = \langle a, b : a^4 = b^2 = 1, b^{-1}ab = a^{-1} \rangle$. Definimos las matrices A y B como:*

$$A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, B = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

se comprueba que:

$$A^4 = B^2 = I, B^{-1}AB = A^{-1}$$

la función

$$\rho : G \to GL(2, V)$$

definida como $\rho : a^i b^j \to A^i B^j$ *para* $0 \leq i \leq 3$, $0 \leq j \leq 1$, *es una representación de* D_8 *sobre* V. *Es una representación de grado 2.*
En la siguiente tabla se representan las imágenes de ρ *para cada elemento de* D_8*:*

g	$\rho(g)$
1	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
a	$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$
a^2	$\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$
a^3	$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$
b	$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$
ab	$\begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}$
a^2b	$\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$
a^3b	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

Cuadro 2.1: Representación del grupo dihedral 8.

Ejemplo 2.1.2 *Sea* G *un grupo cualquiera. Definimos* $\rho : G \to GL(n, V)$ *como* $\rho(g) = I_n$ *para todo* $g \in G$, *donde* I_n *es la matriz identidad* $n \times n$. *Entoces:*

$$\rho(gh) = I_n = I_n I_n = \rho(g)\rho(h)$$

para todo $g, h \in G$, *por lo tanto,* ρ *es una representación de* G. *Esto nos indica que todo grupo tiene representaciones de cualquier grado.*

2.2. Representaciones equivalentes.

Sean ρ y ρ' representaciones lineales de un grupo G en espacios vectoriales V y V' respectivamente. Se dice que estas representaciones son equivalentes (o isomorfas) si existe un isomorfismo lineal $\tau : V \to V'$ que transforma ρ en ρ', es decir, que verifica la identidad:

$$\tau \cdot \rho(s) = \rho'(s) \cdot \tau$$

para todo $s \in G$.

Si ρ y ρ' se dan en forma matricial por R y R' respectivamente, el isomorfismo se traduce en una matriz invertible T tal que:

$$T \cdot R = R' \cdot T$$

o, equivalentemente, tal que:

$$R' = TRT^{-1}$$

Sea $\rho : G \to GL(V)$ una representación, Y sea T una matriz invertible $n \times n$ de V. Para todas las $n \times n$ matrices A y B tenemos:

$$(T^{-1}AT)(T^{-1}BT) = T^{-1}(AB)T$$

Usamos esto para crear una reprsentacion σ desde ρ; definimos

$$\sigma(g) = T^{-1}\rho(g)T$$

para todo $g \in G$. Por lo tanto, para todo $g, h \in G$, tenemos:

$$\begin{aligned}\sigma(gh) &= T^{-1}\rho(gh)T \\ &= T^{-1}\rho(g)\rho(h)T \\ &= T^{-1}\rho(g)T \cdot T^{-1}\rho(h)T \\ &= \sigma(g)\sigma(h)\end{aligned}$$

por lo que, σ es, en efecto, una representación.

Con esto podemos ya dar la siguiente definición:

Definicion 2.2.1 *Sean $\rho : G \to GL(m, V)$ y $\sigma : G \to GL(n, V)$ representaciones de G sobre V. Decimos que ρ es equivalente a σ si $n = m$ y existe una matriz invertible $n \times n$ T tal que, para todo $g \in G$,*

$$\sigma(g) = T^{-1}\rho(g)T$$

Dadas las representaciones ρ, σ y τ de G sobre V, se tiene que:

1. ρ es equivalente a ρ. (Prop. Reflexiva).
2. si ρ es equivalente a σ, entonces σ es equivalente a ρ. (Prop. Simétrica).
3. si ρ es equivalente a σ y σ es equivalente a τ, entonces ρ es equivalente a τ. (Prop. Transitiva).

Esto nos indica que ser equivalentes es una relación de equivalencia.

Demostracion: Sean ρ, σ y τ representaciones de G sobre V, y sea $g \in G$. Tenemos:

1. Prop. Reflexiva:
   Sea I la matriz identidad, que ademas es una matriz cuadrada e invertible, siempre podemos poner
   $$\rho(g) = I^{-1}\rho(g)I$$
   por lo que ρ es equivalente a ρ.
2. Prop. Simétrica:
   Por ser ρ equivalente a σ, tenemos que existe una matriz cuadrada invertible T que cumple:
   $$\begin{aligned}\sigma(g) &= T^{-1}\rho(g)T \\ T\sigma(g) &= \rho(g)T \\ T\sigma(g)T^{-1} &= \rho(g)\end{aligned}$$
   lo que concluye que σ es equivalente a ρ.

3. Prop. Transitiva.
   Por ser ρ equivalente a σ, tenemos que existe una matriz cuadrada invertible T que cumple:
   $$\sigma(g) = T^{-1}\rho(g)T$$
   Del mismo modo, por ser σ equivalente a τ, tenemos que existe una matriz cuadrada invertible P que cumple:
   $$\tau(g) = P^{-1}\sigma(g)P$$
   Sustituyendo tenemos que:
   $$\tau(g) = P^{-1}T^{-1}\rho(g)TP$$
   $$\tau(g) = (TP)^{-1}\rho(g)TP$$
   por lo que ρ es equivalente a τ.

■

2.3. Subrepresentaciones.

Antes de avanzar en este punto, vamos a tratar, de manera muy breve, algunas nociones relativas a los espacios vectoriales.

Sea V un espacio vectorial, W y W' subespacios de V. Se dice que V es *suma directa* de W y W' si todo $x \in V$ se puede escribir de manera única en la forma $x = w + w'$, $w \in W$ y $w' \in W'$; equivale a decir que $W \cap W' = 0$ y $dim(V) = dim(W) + dim(W')$; se escribe entonces $V = W \oplus W'$, y se dice que W' es *suplementario* de W en V. La aplicación p que hace corresponder a cada $x \in V$ su componente $w \in W$ se llama *proyector* de V sobre W (asociado a la descomposición $V = W \oplus W'$); la imagen de p es W, y $p(x) = x$ si $x \in W$; recíprocamente, si p es un endomorfismo de V que verifica estas propiedades, inmediatamente se prueba que V es suma directa de W y del núcleo W' de p. Se establece así una correspondencia biyectiva entre los proyectores de V sobre W y los suplementarios de W en V.

Sea $\rho : G \to GL(V)$ una representación, y sea W un subespacio de V. Si W es estable por la acción de G, esto es, si $gW \subset W$, $\forall g \in G$, entonces ρ define por restricción una representación $\rho' : G \to GL(W)$.

2.4. Núcleo de una representación.

Sea una representación $\rho : G \to GL(V)$. El núcleo de una representación consiste en un grupo de elementos $g \in G$ para los cuales $\rho(g)$ es la matriz identidad.

$$Ker\,\rho = \{g \in G : \rho(g) = I_n\}$$

El núcleo de ρ es un subgrupo normal de G.

Puede ocurrir que el núcleo de una representación es el propio grupo G.

Definicion 2.4.1 *Una representación $\rho : G \to GL(1, V)$ definida como:*

$$\rho(g) = 1_G$$

para todo $g \in G$, se denomina representación trivial de G.

2.5. Representaciones irreducibles.

Definicion 2.5.1 *Una representación lineal $\rho : G \to GL(V)$ se dice irreducible si $V \neq 0$ y ningún subespacio de V es estable por G, excepto, claro está, 0 y V.*

Esto equivale a decir que V no es suma directa de dos subrepresentaciones, salvo la descomposición trivial $V = 0 \oplus V$.

Toda representacion de grado 1 es evidentemente irreducible. La suma directa de representaciones irreducibles da cualquier representación.

Teorema 2.5.1 *Toda representación es suma directa de representaciones irreducibles.*

Demostracion: Sea V una representación lineal de G. Se razona por inducción sobre $dim(V)$. Si $dim(V) = 0$, el teorema es evidente, 0 es suma directa de la familia vacia de representaciones irreducibles. Si $dim(V) \geq 1$ y V es irreducible, también es cierto el teorema. En el resto de casos podemos descomponer V como suma directa de $V' \oplus V''$, con $dim(V') < dim(V)$ y $dim(V'') < dim(V)$. Por inducción, V' y V'' son suma directa de representaciones irreducibles y por tanto lo mismo le ocurre a V. ■

Sea V una representación y sea $V = W_1 \oplus \ldots \oplus W_k$ una descomposición de V en suma directa de representaciones irreducibles. El numero de las W_i isomorfas a una representación irreducible dada no depende de la descomposición elegida.

2.6. FG-módulos.

Sea G un grupo, y sea $F = \mathbb{R}$ o $F = \mathbb{C}$. Escribiremos como $V = F^n$ el espacio vectorial formado por los vectores fila $(\lambda_1, \ldots \lambda_n)$ con $\lambda_i \in F$. Para todo $v \in V$ y $g \in G$, el producto matricial

$$v\rho(g)$$

de el vector fila v con la matriz de dimensión $n \times n$ $\rho(g)$, es un vector fila en V.

Basandonos en el producto matricial $v\rho(g)$ definimos el FG-módulo.

Definicion 2.6.1 *Sea V un espacio vectorial sobre F y sea G un grupo. Entonces V es un FG-modulo si esta definida la multiplicación vg, para $v \in V$ y $g \in G$, y ademas satisfacen las siguientes condiciones para todo $u, v \in V$, $\lambda \in F$ y $g, h \in G$:*

1. $vg \in V$
2. $v(gh) = (vg)h$
3. $v1 = v$
4. $(\lambda v)g = \lambda(vg)$
5. $(u + v)g = ug + vg$

Las condiciones (1), (4) y (5) de la definición aseguran que para todo $g \in G$, la función

$$v \to vg$$

es un endomorfismo de V.

Sea V un FG-módulo, y sea $\mathscr{B}$ una base de V. Para cada $g \in G$, denotamos como

$$[g]_{\mathscr{B}}$$

a la matriz del endomorfismo $v \to vg$ de V, relativo a la base $\mathscr{B}$.
La relación entre los FG-módulos y las representaciones de G sobre F se verá en el siguiente teorema:

Teorema 2.6.1 *(1) Si $\rho : G \to GL(F)$ es una representación de G sobre F, y $V = F^n$, entonces V sera un FG-módulo si definimos la multiplicación vg como*

$$vg = v\rho(g)$$

ademas, existe una base $\mathscr{B}$ de V tal que

$$\rho(g) = [g]_{\mathscr{B}}$$

para todo $g \in G$.

(2) Sea V un FG-módulo y sea $\mathscr{B}$ una base de V. Entonces la función

$$g \to [g]_{\mathscr{B}}$$

es una representación de G sobre F.

Demostracion: (1) Sabemos que $v\rho(g) \in F^n$, ademas por ser ρ un homomorfismo tenemos que $v(\rho(gh)) = v(\rho(g)\rho(h))$ y $v(\rho(1)) = v$. Del mismo modo, por las propiedades de la multiplicación matricial tenemos que $(\lambda v)\rho(g) = \lambda(v\rho(g))$ y $(u+v)\rho(g) = u\rho(g) + v\rho(g)$ para todo $u, v \in F^n$, $\lambda \in F$ y $g, h \in G$.
Por lo tanto, F^n se convertirá en un FG-módulo si definimos

$$vg = v\rho(g)$$

para todo $v \in F^n, g \in G$.
Ademas, si consideramos la base $\mathscr{B}$ como

$$(1,0,0,...,0),(0,1,0,...,0),...,(0,0,0,...,1)$$

de F^n, entonces $\rho(g) = [g]_{\mathscr{B}}$ para todo $g \in G$.

(2) Sea V un FG-módulo con base $\mathscr{B}$. De $v(gh) = (vg)h$ para todo $g, h \in G$ y todo $v \in \mathscr{B}$, se sigue que

$$[gh]_{\mathscr{B}} = [g]_{\mathscr{B}}[h]_{\mathscr{B}}$$

En particular,

$$[1]_{\mathscr{B}} = [g]_{\mathscr{B}}[g^{-1}]_{\mathscr{B}}$$

para todo $g \in G$. Ahora $v1 = v$ para todo $v \in V$, asi que $[1]_{\mathscr{B}}$ es la matriz identidad.
Por lo tanto cada matriz $[g]_{\mathscr{B}}$ es invertible.
Hemos probado que la función $g \to [g]_{\mathscr{B}}$ es un homomorfismo de G a $GL(F)$ y por lo tanto es una representación de G sobre F. ■

Podemos construir FG-módulos sin usar una representación. Para hacer esto transformamos

un espacio vectorial V sobre F en un FG-módulo especificando la acción de los elementos del grupo en una base $v_1, \dots v_n$ de V y haciendo que sea lineal la acción en el entorno de V, es decir, primero definimos $v_i g$ para cada i y cada $g \in G$, y entonces definimos

$$(\lambda_1 v_1 + \ldots + \lambda_n v_n)g$$

para $\lambda_i \in F$, como

$$\lambda_1(v_1 g) + \ldots + \lambda_n(v_n g)$$

Como era de esperar existen restricciones a la hora de definir los vectores $v_i g$.

Teorema 2.6.2 *Sea $v_1, \dots v_n$ una base de un espacio vectorial V sobre F. Supongamos que tenemos una multiplicación vg para todo $v \in V$ y $g \in G$, la cual satisface las siguientes condiciones para todo i con $1 \leq i \leq n$, para todo $g, h \in G$ y para todo $\lambda_1, \dots, \lambda_n \in F$:*

1. $v_i g \in V$
2. $v_i(gh) = (v_i g)h$
3. $v_i 1 = v$
4. $(\lambda_1 v_1 + \ldots + \lambda_n v_n)g = \lambda_1(v_1 g) + \ldots + \lambda_n(v_n g)$

Entonces V es un FG-módulo.

Demostracion: Es trivial ver de (3) y (4) que $v1 = v$ para todo $v \in V$. Las condiciones (1) y (4) nos aseguran que, para todo $g \in G$, la función $v \to vg$ ($v \in V$) es un endomorfismo de V. Esto es:

$$vg \in V,$$
$$(\lambda v)g = \lambda(vg),$$
$$(u + v)g = ug + vg,$$

para todo $u, v \in V$, $\lambda \in F$ y $g \in G$. Por lo tanto

$$(\lambda_1 u_1 + \ldots + \lambda_n u_n)h = \lambda_1(u_1 h) + \ldots + \lambda_n(u_n h)$$

para todo $\lambda_1, \dots, \lambda_n \in F$, todo $u_1, \dots, u_n \in V$, y todo $h \in G$.
Ahora sea $v \in V$ y $g, h \in G$. Entonces $v = \lambda_1 v_1 + \ldots + \lambda_n v_n$ para algún $\lambda_1, \dots, \lambda_n \in F$, y

$$\begin{aligned} v(gh) &= \lambda_1(v_1(gh)) + \ldots + \lambda_n(v_n(gh)) \\ &= \lambda_1((v_1 g)h) + \ldots + \lambda_n((v_n g)h) \\ &= (\lambda_1(v_1 g) + \ldots + \lambda_n(v_n g))h \\ &= (vg)h \end{aligned}$$

Con esto hemos comprobado todos los axiomas requeridos para que V sea un FG-módulo. ■

Definicion 2.6.2 *El FG-módulo trivial es un espacio vectorial V sobre F 1-dimensional con*

$$vg = v$$

para todo $v \in V$, $g \in G$.

Definicion 2.6.3 *Un FG-módulo V es fiel si el elemento unitario de G es el único elemento g para el cual*

$$vg = v$$

para todo $v \in V$.

2.6.1. FG-módulos y representaciones equivalentes.

Veamos ahora las relaciones entre los FG-módulos y las representaciones equivalentes de G sobre F. Un FG-módulo tiene varias representaciones, todas de la forma

$$g \to [g]_{\mathscr{B}}$$

para una base $\mathscr{B}$ de V. El siguiente resultado muestra que todas estas representaciones son equivalentes entre si.

Teorema 2.6.3 *Sea V un FG-módulo con una base $\mathscr{B}$, y sea ρ la representación de G sobre F definida por*

$$\rho : g \to [g]_{\mathscr{B}}$$

(1) Si $\mathscr{B}'$ es una base de V, entonces la representación

$$\phi : g \to [g]_{\mathscr{B}'}$$

de G es equivalente a ρ.
(2) Si σ es una representación de G la cual es equivalente a ρ, entonces existe una base $\mathscr{B}''$ de V tal que

$$\sigma : g \to [g]_{\mathscr{B}''}$$

Demostracion: (1) Sea T la matriz del cambio de base de $\mathscr{B}$ a $\mathscr{B}'$. Para todo $g \in G$, tenemos

$$[g]_{\mathscr{B}} = T^{-1}[g]_{\mathscr{B}'}T$$

Por lo tanto ϕ es equivalente a ρ.
(2) Supongamos que ρ y σ son representaciones equivalentes de G. Entonces, para la matriz invertible T tenemos

$$g\rho = T^{-1}(g\sigma)T$$

para todo $g \in G$. Sea $\mathscr{B}''$ la base de V para la cual la matriz del cambio de base de $\mathscr{B}$ a $\mathscr{B}''$ es T. Entonces para todo $g \in G$

$$[g]_{\mathscr{B}} = T^{-1}[g]_{\mathscr{B}''}T$$

por lo que $g\sigma = [g]_{\mathscr{B}''}$. ■

2.6.2. FG-submódulos.

En lo sucesivo G sera un grupo y F sera $\mathbb{R}$ o $\mathbb{C}$.

Definicion 2.6.4 *Sea V un FG-módulo. Un subconjunto W de V se dice que es un FG-submódulo de V si W es un subespacio y $wg \in W$ para todo $w \in W$ y $g \in G$.*

2.6.3. FG-módulos irreducibles.

Definicion 2.6.5 *Un FG-módulo V se dice que es irreducible si es diferente a $\{0\}$ y no tiene FG-submódulos aparte de $\{0\}$ y V.*
Si V tiene un FG-submódulo W donde W es distinto a $\{0\}$ o V, entonces V es recucible.

Del mismo modo, una representación $\rho : G \to GL(F)$ es irreducible si el correspondiente FG-módulo F^n dado por

$$vg = v(\rho(g))$$

es irreducible; y ρ es reducible si F^n es reducible.

Supongamos ahora que V es un FG-módulo reducible, por lo tanto hay un FG-submódulo W con 0 < dim W < dim V. Tomando una base $\mathscr{B}$ de W y extendiéndola a una base $\mathscr{B}$ de V. Entonces para todo $g \in G$, la matriz $[g]_{\mathscr{B}}$ tiene la forma

$$\left(\begin{array}{c|c} X_g & 0 \\ \hline Y_g & Z_g \end{array}\right) \tag{2.6.1}$$

para las matrices X_g, Y_g y Z_g, donde X_g es $k \times k$ para $k = dim(W)$.

Una representación de grado n es reducible si, y solo si, es equivalente a una representación de la forma (2.6.1), donde X_g es $k \times k$ y $0 < k < n$. Notemos que en (2.6.1), las funciones $g \to X_g$ y $g \to Z_g$ son representaciones de G.

2.6.4. FG-homomorfismos.

Definicion 2.6.6 *Sean V y W FG-módulos. Una función $\vartheta : V \to W$ se dice que es un FG-homomorfismo si ϑ es una transformación lineal y*

$$\vartheta(vg) = \vartheta(v)g$$

En otras palabras, si ϑ envia v a w entonces envia vg a wg.

Como G es un grupo finito y $\vartheta : V \to W$ es un FG-homomorfismo, entonces para todo $v \in V$ y $r = \sum_{g \in G} \lambda_g g \in FG$, tenemos

$$\vartheta(vr) = \vartheta(v)r$$

Proposicion 2.6.1 *Sea V y W FG-módulos y sea $\vartheta : V \to W$ un FG-homomorfismo. Entonces $Ker\,\vartheta$ es un FG-submódulo de V y $Im\,\vartheta$ es un FG-submódulo de W.*

Demostracion: $Ker\,\vartheta$ es un subespacio de V y $Im\,\vartheta$ es un subespacio de W ya que ϑ es una transformación lineal.
Sea $v \in Ker\,\vartheta$ y $g \in G$, entonces

$$\vartheta(vg) = \vartheta(v)g = 0g = 0$$

asi que $vg \in Ker\,\vartheta$. Ademas $Ker\,\vartheta$ es un FG-submodulo de V.
Sea $w \in Im\,\vartheta$, tal que $w = \vartheta(v)$ para algún $v \in V$. Para todo $g \in G$,

$$wg = \vartheta(v)g = \vartheta(vg) \in Im\,\vartheta$$

por lo que $Im\,\vartheta$ es un FG-submódulo de W. ■

2.6.5. Isomorfismos de FG-módulos.

Definicion 2.6.7 *Sean V y W FG-módulos. Decimos que $\vartheta : V \to W$ es un FG-isomorfismo si ϑ es un FG-homomorfismo y ademas posee inversa. Si $\vartheta : V \to W$ es un FG-isomorfismo, entonces V y W son FG-módulos isomorfos y los representaremos como $V \cong W$.*

En el siguiente teorema veremos que si $V \cong W$ entonces $W \cong V$.

Teorema 2.6.4 *Si $\vartheta : V \to W$ es un FG-isomorfismo, entonces la inversa $\vartheta^{-1} : W \to V$ es tambien un FG-isomorfismo.*

Demostracion: Es evidente que ϑ^{-1} es una transformación lineal invertible, por lo que, unicamente, debemos demostrar que ϑ^{-1} es un FG-homomorfismo. Sean $w \in W$ y $g \in G$,

$$\vartheta(\vartheta^{-1}(w)g) = g(\vartheta(\vartheta^{-1}(w))$$

como ϑ es un FG-homomorfismo,

$$= wg$$
$$\vartheta(\vartheta^{-1}(wg))$$

Así que $\vartheta^{-1}(w)g = \vartheta^{-1}(wg)$ como se buscaba. ■

Sea $\vartheta : V \to W$ un FG-isomorfismo, entonces podemos usar ϑ y ϑ^{-1} para cambiar entre los FG-módulos isomorfos V y W, y probar que V y W comparten la mismas propiedades estructurales; algunos ejemplos pueden ser:

1. $\dim V = \dim W$ (cada $v_1, \ldots, v_n$ es una base de V si y solo si $\vartheta(v_1), \ldots, \vartheta(v_n)$ es base de W).

2. V es irreducible si y solo si W es irreducible (cada X es un FG-submódulo de V si y solo si $\vartheta(X)$ es un FG-submódulo de W).

3. V contiene un FG-submódulo trivial si y solo si W contiene un FG-submódulo trivial (cada X es un FG-submódulo trivial de V si y solo si $\vartheta(X)$ es un FG-submódulo trivial de W).

Teorema 2.6.5 *Sea V un FG-módulo con una base $\mathscr{B}$, y sea W un FG-módulo con una base $\mathscr{B}'$. Entonces V y W son isomorfas si y solo si las representaciones*

$$\rho : g \to [g]_{\mathscr{B}}$$

$$\sigma : g \to [g]_{\mathscr{B}'}$$

son equivalentes.

Demostracion: Para la demostración del anterior teorema primero estableceremos lo siguiente:

1. Los FG-módulos V y W son isomorfos si y solo si existe una base $\mathscr{B}_1$ de V y una base $\mathscr{B}_2$ de W tal que
$$[g]_{\mathscr{B}_1} = [g]_{\mathscr{B}_2}$$
para todo $g \in G$.

Para ver esto supongamos, primero, que ϑ es un FG-isomorfismo de V a W, y sea $v_1, \ldots, v_n$ una base $\mathscr{B}_1$ de V; entonces $\vartheta(v_1), \ldots, \vartheta(v_n)$ es una base de $\mathscr{B}_2$ de W. Sea $g \in G$. Ya que $\vartheta(v_i g) = \vartheta(v_i)g$ para cada i, se sigue que $[g]_{\mathscr{B}_1} = [g]_{\mathscr{B}_2}$.
De modo inverso, supongamos que $v_1, \ldots, v_n$ una base $\mathscr{B}_1$ de V y $w_1, \ldots, w_n$ una base $\mathscr{B}_2$ de W tal que $[g]_{\mathscr{B}_1} = [g]_{\mathscr{B}_2}$ para todo $g \in G$. Sea ϑ la transformación lineal invertible de V a W para la cuál $\vartheta(v_i) = w_i$. Y que $[g]_{\mathscr{B}_1} = [g]_{\mathscr{B}_2}$, se deduce que $\vartheta(v_i g) = \vartheta(v_i)g$ y por lo tanto cada ϑ es un FG-isomorfismo. Esto completa la demostración de (1).
Ahora asumimos que V y W son FG-módulos isomorfos. Por (1) hay una base $\mathscr{B}_1$ de V y una base $\mathscr{B}_2$ de W tal que $[g]_{\mathscr{B}_1} = [g]_{\mathscr{B}_2}$ para todo $g \in G$. Definimos ahora una representación ϕ de G como $\phi : g \to [g]_{\mathscr{B}_1}$. Según el teorema 2.6.3(1), ϕ es equivalente a ρ y a σ, por lo que ρ y σ son equivalentes.
A la inversa, supongamos que ρ y a σ son equivalentes, entonces, por el teorema 2.6.3(2) hay una base $\mathscr{B}''$ de V tal que $\sigma(g) = [g]_{\mathscr{B}''}$ para todo $g \in G$; esto es, $[g]_{\mathscr{B}'} = [g]_{\mathscr{B}''}$ para todo $g \in G$. Por lo tanto V y W son FG-módulos isomorfos, por (1). ■

2.6.6. Suma directa de FG-módulos.

Sea V un FG-módulo, y supongamos que

$$V = U \oplus W$$

donde U y W son FG-submódulos de V. Sea $u_1, \ldots, u_m$ una base $\mathscr{B}_1$ de U, y $w_1, \ldots, w_n$ una base $\mathscr{B}_2$ de W. Entonces sabemos, por los primeros cursos de álgebra lineal, que $u_1, \ldots, u_m, w_1, \ldots, w_n$ es una base $\mathscr{B}$ de V, y para $g \in G$

$$\left(\begin{array}{c|c} [g]_{\mathscr{B}_1} & 0 \\ \hline 0 & [g]_{\mathscr{B}_2} \end{array}\right)$$

Generalizando aun mas, si $V = U_1 \oplus \ldots \oplus U_r$, es suma directa de los FG-submódulos U_i y $\mathscr{B}_i$ es una base de U_i, entonces podemos unir $\mathscr{B}_1, \ldots, \mathscr{B}_r$, para obtener una base $mathscrB$ de V, y para $g \in G$,

$$[g]_{\mathscr{B}} = \begin{pmatrix} [g]_{\mathscr{B}_1} & & 0 \\ & \ddots & \\ 0 & & [g]_{\mathscr{B}_r} \end{pmatrix}$$

Proposicion 2.6.2 *Sea V un FG-módulo, y supongamos que*

$$V = U_1 \oplus \ldots \oplus U_r$$

donde cada U_i es un FG-submódulo de V. Para $v \in V$, tenemos que $v = u_1 + \ldots + u_r$ para $u_i \in U_i$, y definimos $\pi_i : V \to V$ como

$$\pi_i(v) = u_i$$

Entonces cada π_i es un FG-homomorfismo, y es, ademas, una proyección de V.

Demostracion: Evidentemente π_i es una transformación lineal; y es también un FG-homomorfismo, ya que para $v \in V$ con $v = u_i + \ldots + u_r$ siendo $u_j \in U_j$ para todo j, y $g \in G$, tenemos que

$$\pi_i(vg) = \pi_i(u_1 g + \ldots + u_r g) = u_i g = \pi_i(v)g$$

por lo tanto

$$\pi_i^2(v) = \pi_i(u_i) = u_i = \pi_i(v)$$

asi que $\pi_i^2 = \pi_i$. Lo que implica que π_i es una proyección. ■

Veamos, por último, un resultado concerniente a la suma de FG-módulos irreducibles del cual no daremos una demostración.

Proposicion 2.6.3 *Sea V un FG-módulo, y supongamos que*

$$V = U_1 + \ldots + U_r$$

donde cada U_i es un FG-submódulo irreducible de V. Entonces V es una suma directa de algunos FG-submódulos U_i.

Capítulo 3

Caracteres.

3.1. El lema de Schur.

Teorema 3.1.1 (Lema de Schur.) *Sea $f : V \to V'$ una aplicación lineal entre G-módulos irreducibles. Entonces, o bien $f = 0$, o bien f es un isomorfismo; ademas, en este caso, f es una homotecia.*

Demostracion: Como Ker(f) es un G-submódulo estable de V, o bien Ker(f)=V, lo que significa que $f = 0$, o bien Ker(f)=0. En este caso la condición $f(gv) = gf(v)$, para $v \in V$, implica que Im(f) es también un G-submódulo invariante de V', con lo que Im(f)=V'. Sobre los numeros complejos f ha de tener algún valor propio λ, ello supone que $f - \lambda Id$ tiene núcleo no nulo, con lo que por lo anterior $f - \lambda Id$ es el morfismo nulo y por lo tanto $f = \lambda Id$. ■

Corolario 3.1.1 *Toda representación irreducible V de un grupo abeliano es de grado 1.*

Demostracion: Sea g un elemento de G y consideremos la aplicación lineal que induce $g : V \to V$. Puesto que para todo $h \in G$ se cumple que $gh = hg$, se tiene que g es un morfismo de G-módulos, con ello g es una homotecia. Asi la representación de G en V convierte a G en un grupo de homotecias. Puesto que una homotecia deja invariante cualquier espacio, si V es irreducible ha de ser de dimensión 1. ■

3.2. Carácter de una representación.

Para comprender lo que es el carácter de una representación necesitamos conocer primero el concepto de traza. Este concepto se estudió en los primeros cursos de Algebra Lineal, pero debido a su importancia en esta sección procedemos, de nuevo, a dar su definición:

Definicion 3.2.1 *Sea V un espacio vectorial de dimension n y a un endomorfismo, cuya matriz, en una base (e_i) de V, es (a_{ij}). La traza de a es el escalar*

$$Tr(a) = \sum_i a_{ii}$$

la traza de a no depende de la base (e_i) elegida.

Sea $\rho : G \to GL(V)$ una representación lineal de un grupo finito G en el espacio vectorial V. Dado $s \in G$, pongamos

$$\chi_\rho(s) = Tr(\rho(s))$$

Se obtiene así una aplicación χ_ρ definida en G, a valores complejos

$$\chi_\rho : G \to \mathscr{C}$$

llamada *carácter* de la representación ρ, la importancia de esta aplicación proviene de que caracteriza la representación considerada.

Proposicion 3.2.1 *Si χ es el carácter de una representación ρ de grado n, entonces,*

1. $\chi(1) = n$
2. $\chi(s^{-1}) = \chi(s)^*$ *para todo* $s \in G$
3. $\chi(tst^{-1}) = \chi(s)$ *cualquiera que sean* $s\,, t \in G$

(Si x es un número complejo, denotamos a su conjugado por x^*.)

Demostracion: Como $\rho(1) = 1$ y $Tr(1) = n$ por ser V de dimensión n, tendremos $\chi(1) = n$.

$\rho(s)$ es de orden finito; sus valores propios $\lambda_1, \ldots . \lambda_n$ tambien serán de orden finito y por lo tanto de módulo 1. Entonces:

$$\chi(s^*) = Tr(\rho(s^*)) = \sum \lambda_i^* = \sum \lambda_i^{-1} = Tr(\rho(s^{-1})) = \chi(s^{-1})$$

■

Capítulo 4

Capitulo 4.

Bibliografía

[1] J. L. Alperin, R. B. Bell, *Groups and representations*, Springer-Verlag, 1995.

[2] E. Bujalance, J. J. Etayo, J. M. Gamboa, *Teoría elemental de grupos*, Publicaciones UNED, Madrid, 2007.

[3] E. Bujalance, J. A. Bujalance, A. F. Costa, E. Martinez, *Elementos de matemática discreta*, Sanz y Torres, Madrid, 2005.

[4] W. Lederman, *Grupos finitos*, Dossat, Manchester, 1952.

[5] W. Fulton, J. Harris, *Representation theory*, Springer-Verlag, 1991.

[6] D. Griffiths, D. Higham, *Learning LaTex*, Society for Industrial and Applied Mathematics, Filadelfia, 1997.

[7] G. James, M. Liebeck, *Representations and characters of groups*, Cambridge University Press, Londres, 2001.

[8] J. P. Serre, *Representaciones lineales de los grupos finitos*, Omega, Barcelona, 1970.

[9] J. C. Varilly, *Grupos y anillos*, Escuela de Matemática, Universidad de Costa Rica, 2014.

[10] M. Suzuki, *Group theory I*, Springer-Verlag, 1982.

[11] S. Xambó, F. Delgado, C. Fuertes, *Introducción al álgebra*, Editorial Complutense, Madrid, 1993.