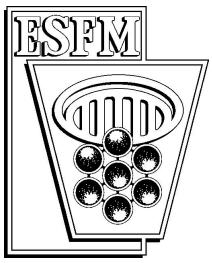

INSTITUTO POLITÉCNICO NACIONAL

ESCUELA SUPERIOR DE FÍSICA Y MATEMÁTICAS

Sobre algunos resultados de la teoría de caracteres en grupos finitos

T E S I S

QUE PARA OBTENER EL TÍTULO DE LICENCIADO EN FÍSICA Y MATEMÁTICAS

P R E S E N T A

HÉCTOR HUGO CORRALES SÁNCHEZ

ASESOR DE TESIS
DR. PABLO LAM ESTRADA

MÉXICO, D. F. **SEPTIEMBRE DE 2008**

A todos aquellos que durante
tanto tiempo han compartido
conmigo el sueño que hoy se
transforma en tinta y papel

. . . twilight! twilight!

Índice general

Introducción

Este trabajo ha sido escrito con la intención de dar una breve introducción a la teoría de caracteres en grupos finitos y ejemplificar con algunos resultados básicos la importancia que juega ésta en la teoría de grupos. Para esto, se presupone todo el material básico sobre grupos, y algunos conocimientos extras tales como álgebra lineal y un poco de teoría de anillos y campos; siempre que mencionemos la palabra grupo, nos referiremos a un grupo finito a menos que se diga explícitamente lo contrario. El trabajo está dividido en dos grandes capítulos, a grandes razgos podríamos decir que el primero es "la teoría" y el segundo "los ejemplos".

En la Sección 1.1 se introducen los conceptos de álgebras y módulos, siendo estos últimos tratados siempre sobre álgebras; se desarrolla todo el material que sobre de estos utilizaremos y para concluir se demuestra una versión simplificada del Teorema de Wedderburn (1.1.12) y el Teorema de Mashke (1.1.13), juntos justifican el desarrollo posterior. Si bien el concepto de módulo es mucho más extenso de lo que aquí se presenta, para los fines de este trabajo es suficiente con tratarlo de esta manera.

La definición de representación se introduce en la Sección 1.2 junto con la de caracter, los resultados de la sección previa son utilizados para demostrar lo que a juicio del autor son las 3 propiedades fundamentales (que este trabajo presenta) de los caracteres irreducibles (1.2.8, 1.2.12, 1.2.17). Cabe aclarar que no se profundiza demasiado en la basta teoría de representaciones, solo se desarrolla el material que será necesario para justificar lo expuesto.

Hasta este punto los caracteres están siempre ligados a una representación, esto se abandona en la siguiente sección donde se presentan diversas maneras de obtener un caracter sin tener una de antemano. De entre todos los métodos expuestos la inducción es quizá el mas importante y el menos trivial, es importante recalcar que no se hace mención alguna sobre las representaciones inducidas; esto es motivado primeramente por cuestiones de extensión y en segundo lugar por que el objetivo del capítulo (y de todo el trabajo) son los caracteres. Sin embargo es importante observar que este es un muy buen ejemplo de como los caracteres motivan la teoría de

representaciones; históricamente los caracteres inducidos aparecieron primero, posteriormente al intentar recuperar"su procedencia surgió el concepto de representación inducida.

Aunque me hubiese gustado incluir el Teorema de Inducción de Brauer y el concepto de *grupo p-elemental*, esto inevitablemente llevaría el trabajo por una línea muy "teórica", siendo que desde un principio esta tesis fue planeada para presentar tanto teoría como aplicaciones; por esta misma razón los resultados expuestos en el Capítulo 2 poseen demostraciones relativamente breves, de hecho, este fue el principal criterio de selección. También se intentó no ser repetitivo y exponer resultados variados (en su conclusión o en su demostración) para mostrar el largo alcance de la teoría de caracteres.

En la sección 2.1 se presentan algunos teoremas que involucran caracteres y conmutadores, siendo 2.1.6 y 2.1.9 los resultados principales, además de los resultados esta sección pretende ejemplificar la manera en como se manipulan algunas operaciones que involucran caracteres, ya que estos no siempre son fáciles de manipular. La siguiente sección expone un resultado clásico de Frobenius 2.2.1, es importante mencionar que la demostración que desarrollo no es la primera que Frobenius publicó. La primera se basó en un estudio del producto exterior de la representación regular y no se presenta aquí ya que el mencionado producto exterior requiere una construcción demasiado extensa para ser incluida.

La siguiente sección (2.3) es quizá la más espectacular en el sentido de que "con poco desarrollo se logra obtener mucho", y trata brevemente de un problema surgido también de la teoría de caracteres el cual es determinar un grupo (simple) a partir del centralizador de una involución ([3] pág. 54 Teo. 4.12). En esta misma línea se encuentra el Teorema de Brauer-Suzuki-Wall el cual fue uno de los primeros resultados sobresalientes en esta dirección, posee una demostración muy similar a la que aquí desarrollamos de 2.3.2; lamentablemente hace uso de un par de detalles fuera del alcance de este trabajo.

La última sección desarrolla una versión extensa y detallada del Teorema de Nagao (2.4.1), el cual afirma que un grupo simétrico esta determinado unívocamente por su tabla de caracteres; en la misma manera en como se expone aquí se puede demostrar que esto también es válido para los grupos alternantes ([11]). Estos resultados estan muy relacionados con la clasificación de grupos finitos, uno de los problemas fundamentales en la teoría de grupos, mi mayor área de interés y el mejor ejemplo de que la teoría de caracteres es una de las herramientas mas poderosas en la teoría de grupos.

Capítulo 1

Teoría Básica de Caracteres

1.1. Álgebras y módulos

En esta sección se exponen conceptos básicos que serán usados a lo largo de todo este trabajo. Muchos resultados en álgebra lineal y en teoría de anillos serán usados sin demostración. Primeramente recordemos dos importantes conceptos.

1.1.1 Definición
Un ***campo*** *es un conjunto no vacío F junto con dos operaciones internas, llamadas* ***adición*** *"$+$" y* ***multiplicación*** *"$\cdot$" de forma tal que:*

$$F,+ \quad y \quad F^*,\cdot \quad \textit{son grupos abelianos} \quad y$$

$$\alpha_1(\alpha_2+\alpha_3)=\alpha_1\alpha_2+\alpha_1\alpha_3, \quad \forall\ \alpha_1,\alpha_2,\alpha_3 \in F,$$

donde $F^*=F\setminus\{0\}$.

La **característica** de un campo es el menor número natural (si hay alguno) n tal que $n\cdot 1=0$; si un número tal no existe, la característica se define como cero. En todo campo la característica es cero o un número primo.

1.1.2 Definición
Dados un conjunto no vacío V, un campo F y dos funciones $+ : V\times V \to V$ y $\cdot : F\times V \to V$ llamamos a V un ***espacio vectorial sobre*** *F si $V,+$ es un grupo abeliano y $\forall\ v,w\in V$, $\alpha,\beta\in F$:*

$$(\alpha+\beta)v=\alpha v+\beta w,$$

$$\alpha(v+w) = \alpha v + \alpha w,$$

$$(\alpha\beta)v = \alpha(\beta v)\ y$$

$$1v = v.$$

En este trabajo, todos los espacios vectoriales se considerarán de dimensión finita.

Sean V, W dos espacios vectoriales sobre F y $f : V \to W$ una función tal que $f(v+w) = f(v) + f(w)$ y $f(\alpha v) = \alpha f(v)$ si $v, w \in V$ y $\alpha \in F$, entonces f se denomina **lineal**, también llamada **transformación lineal**. Al conjunto de todas las funciones lineales de V en W se le denota por $\mathrm{Hom}(V, W)$. Cuando una función lineal es biyectiva se dice que es un **isomorfismo**.

Tomemos $f, g \in \mathrm{Hom}(V, W)$ y $\alpha \in F$, entonces podemos definir dos nuevas funciones:

$$[f+g](v) := f(v) + g(v)\ y$$

$$[\alpha f](v) := \alpha f(v).$$

Así, el conjunto $\mathrm{Hom}(V, W)$ es un espacio vectorial sobre F con elemento identidad $1(v) = v$. A los elementos de $\mathrm{End}(V) = \mathrm{Hom}(V, V)$ los llamamos **endomorfismos**. Sobre éstos podemos además definir el producto de f y g por:

$$[fg](x) := [f \circ g](x) = f(g(x)).$$

Al conjunto de los elementos invertibles bajo esta operación (es decir, a las funciones invertibles) se le llama el **grupo lineal general de** V y se denota por $\mathrm{GL}(V)$.

1.1.3 Definición

*Sea F un campo. Una **F-álgebra** es un espacio vectorial A sobre F en el cual existe un elemento llamado unidad (1_A) y una operación $\cdot : A \times A \to A$ tales que:*

$$a1_A = 1_A a = a$$

$$a(bc) = (ab)c$$

$$a(b+c) = ab + ac$$

$$(a+b)c = ac + bc$$

$$\alpha(ab) = (\alpha a)b = a(\alpha b),$$

siempre que $\alpha, \beta \in F$ y $a, b, c \in A$.

Las primeras cuatro condiciones de la definición anterior, establecen que A es un anillo unitario, y la última nos asegura la compatibilidad entre las operaciones de F y A. Si A' es un subconjunto de A tal que $1_A \in A'$ y A' es por si solo una álgebra decimos que A' es una **subálgebra** de A.

Dadas dos F-álgebras A, A', una función $\sigma : A \to A'$ se denomina **F-homomorfismo**, o simplemente **homomorfismo** (si el contexto es claro), cuando:

$$\sigma \in \mathrm{Hom}(A, A'),$$

$$\sigma(ab) = \sigma(a)\sigma(b) \quad \forall\ a, b \in A\ y$$

$$\sigma(1_A) = 1_{A'}.$$

La más importante de las álgebras que trataremos es la llamada álgebra de grupo.

1.1.4 Definición
Sean G un grupo y F un campo. Al conjunto de sumas formales:

$$\sum_{g\in G} a_g g \qquad con\ a_g \in F, \quad \forall\ g \in G,$$

se le suele denotar por $F[G]$ y junto con las operaciones:

$$\sum_{g\in G} a_g g + \sum_{g\in G} b_g g = \sum_{g\in G} (a_g + b_g) g,$$

$$\sum_{g\in G} a_g g \cdot \sum_{g\in G} b_g g = \sum_{g\in G} \Big(\sum_{xy=g} a_x b_y \Big) g \qquad y$$

$$\alpha \cdot \sum_{g\in G} a_g g = \sum_{g\in G} (\alpha a_g) g, \qquad \alpha \in F,$$

*forma una F-álgebra denominada el **álgebra del grupo** G **sobre** F.*

Otros ejemplos importantes de álgebras son $\mathrm{M}_n(F)$ el álgebra de matrices de grado n sobre F; y cuando V es un espacio vectorial, el conjunto $\mathrm{End}(V)$ es una F-álgebra con las operaciones antes definidas.

1.1.5 Definición
*Si A es una F-álgebra, entonces un espacio vectorial V sobre F, en el cual está definida una función $\cdot : A \times V \to V$, es llamado un **A-módulo** si:*

$$a(bv) = (ab)v,$$

$$1_A v = v,$$
$$(a+b)v = av + bv,$$
$$a(v+w) = av + aw,$$
$$(\alpha a)v = \alpha(av) = a(\alpha v),$$

cuando $\alpha \in F,\ a, b \in A$ *y* $v, w \in V$.

Dada una álgebra A, un módulo importante es el que se obtiene tomando $V = A$ y definiendo el producto de un elemento de A por uno de V como su producto en A, a este módulo se le llama **módulo regular de** A y se denota por ${}_AA$ o A^o.

Un subespacio W de V que bajo las operaciones de V es un A-módulo por sí solo se denomina **submódulo** de V y escribimos $W < V$. Si $v \in V$ definimos el conjunto $v+W := \{v+w : w \in W\}$. En $V/W = \{v+W : v \in V\}$ podemos introducir la estructura de A-módulo definiendo para $v, v' \in V$, $\alpha \in F$ y $a \in A$:

$$(v+W) + (v'+W) = (v+v') + W,$$
$$\alpha(v+W) = \alpha v + W,$$
$$a(v+W) = av + W.$$

Al módulo resultante se le conoce como **módulo cociente** de V y W.

Un **homomorfismo** entre dos A-módulos V y W es una función $f \in \mathrm{Hom}(V, W)$ (es decir, una función lineal) tal que $f(av) = af(v)$, cuando $a \in A$ y $v \in V$. Al conjunto de estas funciones lo denotamos por $\mathrm{Hom}_A(V, W)$, y claramente tenemos $\mathrm{Hom}_A(V, W) \subseteq \mathrm{Hom}(V, W)$. Si decimos que g es un homomorfismo de V en W, esto debe entenderse como homomorfismo lineal, y si lo llamamos un A-homomorfismo es porque $f \in \mathrm{Hom}_A(V, W)$. Cuando podemos definir un A-homomorfismo f de V en W que además sea una función biyectiva, llamamos a f un **A-isomorfismo** y escribimos $V \cong W$. Si $f \in \mathrm{Hom}_A(V, W)$, los conjuntos $K = \mathrm{Ker}(f)$ e $\mathrm{Im}(f)$ son submódulos de V y W respectivamente, los cuales cumplen $V/K \cong \mathrm{Im}(f)$. Un **A-endomorfismo** es un elemento del conjunto $\mathrm{End}_A(V) = \mathrm{Hom}_A(V, V)$ siendo este último una subálgebra de $\mathrm{End}(V)$. Si $f \in \mathrm{End}_A(V)$, $v \in V$ y definimos $f \cdot v := f(v)$, esta operación hace de V un $\mathrm{End}_A(V)$-módulo.

Un módulo V no trivial (es decir, $\neq \langle 0 \rangle$), cuyos únicos submódulos son $\langle 0 \rangle$ y V se denomina módulo **irreducible**, y **reducibles** en caso contrario. Si para todo submódulo W_1 podemos encontrar otro submódulo W_2 tal que $V = W_1 \oplus W_2$, entonces decimos que V es **completamente reducible**.

Supongamos que V y W son módulos irreducibles sobre A, si $f \in \mathrm{Hom}_A(V, W)$ entonces $\mathrm{Ker}(f) = \langle 0 \rangle,\ \mathrm{Im}(f) = W$ o $\mathrm{Ker}(f) = V,\ \mathrm{Im}(f) = \langle 0 \rangle$. Si f no se anula en

todo V, entonces su kernel es trivial y, por lo tanto, es inyectiva. Además, $\mathrm{Im}(f)=W$ y f es también sobre; no es difícil ver que, en este caso, $f^{-1} \in \mathrm{Hom}_A(W,V)$. Este análisis demuestra parte de la siguiente proposición.

1.1.6 Proposición (Schur)
Si V y W son dos A-módulos irreducibles, entonces todo elemento no cero de $\mathrm{Hom}_A(V,W)$ *tiene un inverso en* $\mathrm{Hom}_A(W,V)$. *En particular,* $\mathrm{End}_A(V)$ *es una álgebra de división* (*es decir, una en la cual todo elemento no cero tiene un inverso*). *Si F es algebraicamente cerrado, entonces* $\mathrm{End}_A(V) = F \cdot id_V$.

Demostración. Sólo resta probar la última aseveración. Para esto, tomemos $f \in \mathrm{End}_A(V)$ y consideremos el polinomio $g(X) = \det(f - X \cdot id_V)$; por ser F algebraicamente cerrado existe al menos una raíz de $g(X)$ en F, sea ésta λ . Entonces, $f - \lambda \cdot id_V$ es no invertible y, por lo tanto, identicamente nulo. Tenemos así que $\mathrm{End}_A(V) \subseteq F \cdot id_V$, y como la otra inclusión es trivialmente cierta se tiene la afirmación.

□

Tomemos un módulo no trivial V y $\mathcal{F} = \{W < V : W \neq \langle 0 \rangle\}$. Si V es irreducible, entonces $\mathcal{F} = \emptyset$. Si $\mathcal{F} \neq \emptyset$ tomemos $V_1 \in \mathcal{F}$, entonces V_1 es irreducible ó existe un módulo no trivial $V_2 < V_1 < V$. De nuevo, V_2 es irreducible ó podemos continuar este proceso; lo importante radica en que después de un número finito de pasos, debemos obtener un módulo irreducible no trivial, de lo contrario existiría una torre infinita de subespacios anidados de V, lo cual no puede ser cuando V tiene dimensión finita. En otras palabra, todo módulo no trivial debe contener al menos un submódulo irreducible no trivial. La relación entre los módulos irreducible y los completamente reducibles va mucho más allá del simple parecido en los nombres.

1.1.7 Proposición
Un módulo es completamente reducible si y sólo si es suma directa de una familia de submódulos irreducibles.

Demostración. Sea A una álgebra. Supongamos que V es una A-módulo completamente reducible y que $\{V_\alpha\}$ es la colección de todos los submódulos irreducibles de V. Definimos $W = \sum V_\alpha$. Si suponemos que $W < V$, podríamos encontrar un submódulo $W_1 \neq \langle 0 \rangle$ de V tal que $V = W \oplus W_1$, como W_1 es no trivial debe contener un submódulo irreducible no trivial, digamos W_1'; por la definición de W, tenemos $W_1' \subseteq W$, por lo tanto $W_1' \subseteq W \cap W_1 = \langle 0 \rangle$, lo cual es una contradicción, entonces $W = V$. Ahora, V es de dimensión finita y por lo tanto podemos elegir $W' \leq V$ maximal con la propiedad de ser suma directa de elementos de $\{V_\alpha\}$. Si $W' < V$ existe un elemento $V' \in \{V_\alpha\}$ tal que $V' \not\subseteq W'$; por ser V' irreducible, $W' \cap V' = \langle 0 \rangle$

y por lo tanto $W' \subset W' \oplus V'$, lo cual no puede ocurrir por haberse elegido a W' maximal, entonces tenemos $W' = V$.

Supongamos ahora que V es suma directa de una familia $\{V_\alpha\}$ de submódulos irreducibles. Tomemos $W<V$ y $\mathcal{F}=\{U<V : W\cap U=\langle 0\rangle\}$. Por ser V de dimensión finita, y por un argumento similar al del parágrafo que precede a esta proposición, existe al menos un elemento maximal en $\mathcal{F}$, denotémoslo por W'. Si $W \oplus W' \neq V$, existe $V_0 \in \{V_\alpha\}$ con $V_0 \nsubseteq W \oplus W'$ y por ser V_0 irreducible $(W \oplus W') \cap V_0 = \langle 0\rangle$. Ahora, tomemos $w \in W \cap (V_0 + W')$, entonces existen $v_0 \in V_0$ y $w' \in W'$ tales que $w = v_0 + w'$, luego $v_0 = w - w' \in W \oplus W'$, por lo tanto $v_0 = 0$. Así, $w = w' \in W \cap W' = \langle 0\rangle$, como w se eligió arbitrariamente, $W \cap (V_0 + W') = \langle 0\rangle$, lo cual contradice la maximalidad de W'. Por lo tanto, $V = W \oplus W'$.

□

Así pues, los módulos irreducibles sirven como bloques básicos para construir módulos completamente reducibles, por lo tanto si queremos conocer todos los módulos completamente reducibles nos basta con tener todos los módulos irreducibles. Esto es relativamente fácil con ayuda del siguiente resultado.

1.1.8 Proposición

Si A es una álgebra, todo A-módulo irreducible es isomorfo a un módulo cociente de ${}_AA$. Cuando A es semisimple, todo A-módulo irreducible es isomorfo a un submódulo de ${}_AA$.

Demostración. Sea V un A-módulo irreducible no trivial y tomemos $0 \neq v_0 \in V$. Definimos $f : {}_AA \to V$ por $f(a) = av_0$. Si $a, b \in A, \alpha \in F$ y $x \in {}_AA$ tenemos:

$$\begin{aligned} f(a+b) &= (a+b)v_0 = av_0 + bv_0 = f(a) + f(b), \\ f(\alpha a) &= (\alpha a)v_0 = \alpha(av_0) = \alpha f(a), \\ f(xa) &= (xa)v_0 = x(av_0) = xf(a). \end{aligned}$$

Por lo tanto, $f \in \mathrm{Hom}_A({}_AA, V)$. Como $1_A v_0 = v_0$, $\mathrm{Im}(f) \neq \langle 0\rangle$ y, por ser V irreducible, $V = \mathrm{Im}(f) \cong {}_AA/\mathrm{Ker}(f)$. Si A es semisimple, existe $W < {}_AA$ tal que ${}_AA = \mathrm{Ker}(f) \oplus W$ y por lo tanto $W \cong {}_AA/\mathrm{Ker}(f)$.

□

Así, cuando A es semisimple nuestro problema anterior se reduce a explorar el módulo regular de A. De ahora en adelante, supondremos que A es semisimple, podemos por lo tanto encontrar un conjunto de submódulos irreducibles de ${}_AA$ con la propiedad de que todo A-módulo irreducible sea isomorfo a uno y sólo a uno de sus elementos. A un conjunto tal lo denotaremos por $\mathcal{M}_i(A)$.

1.1.9 Definición
*Sea V un A-módulo irreducible. La **parte homogénea** de V (en A), denotada por $V(A)$, se define como la suma de todos los submódulos de ${}_AA$ isomorfos a V.*

Por la Proposición 1.1.7, sabemos que ${}_AA = \sum\cdot W_i$, con W_i submódulos irreducibles. Entonces, $\sum_{W_i\cong V} W_i \subseteq V(A)$. Sean p_j la proyección de ${}_AA$ en W_j y $W' < {}_AA$ con $W' \cong V$, entonces $p_j(W') = \langle 0\rangle$ ó W_i, por ser W_i irreducible. Cuando $p_j(W') = W_j$, $W'/K_j \cong W_j$, donde $K_j = \mathrm{Ker}(p_j) \cap W' \leq W'$ con este último irreducible. Si $K_j = W'$ tendríamos $W' \subseteq \mathrm{Ker}(p_j)$, lo cual no puede ser en vista de que $p_j(W') = W_j$; por lo tanto, $K_j = \langle 0\rangle$ y $W' \cong W_j$. Tenemos por lo tanto $p_j(W') \subseteq \sum_{W_i\cong V} W_i$ y, como $W' = \sum p_i(W')$, $W' \subseteq \sum_{W_i\cong V} W_i$. Dado que W' es cualquier submódulo de A isomorfo a V, $V(A) = \sum\cdot_{W_i\cong V} W_i$.

Así que $n_V(A) := |\{W_i : W_i \cong V\}|$ no depende de la familia $\{W_i\}$, pues $\dim V(A) = n_V(A)\dim V$. Si V' es otro A-módulo irreducible y $V \cong V'$, entonces $V(A) = V'(A)$. Cuando $V \ncong V'$, la relación entre $V(A)$ y $V'(A)$ se vuelve más interesante, pues como $V'(A) = \sum\limits_{W_i\cong V'} \cdot W_i$ y $\{W_i : W_i \cong V\} \cap \{W_i : W_i \cong V'\} = \emptyset$, tenemos $V(A) \cap V'(A) = \langle 0\rangle$.

De todo esto podemos deducir que:

$$ {}_AA = \sum_{V\in\mathcal{M}_i(A)}\cdot V(A). $$

Como $\dim V(A) > 0 \ \ \forall\ V \in \mathcal{M}_i(A)$ y $\dim A < \infty$, $|\mathcal{M}_i(A)| < \infty$. Además,

$$ \dim A = \sum_{V\in\mathcal{M}_i(A)} \dim V(A) = \sum_{V\in\mathcal{M}_i(A)} (n_V(A) \ \cdot\ \dim V)\,. $$

Nos falta ahora determinar $|\mathcal{M}_i(A)|$ y $n_V(A)$ para $V \in \mathcal{M}_i(A)$. El siguiente resultado nos servirá como un paso intermedio.

Tomemos V cualquier A-módulo y $a \in A$. Definamos $a_V : V \to V$ por $a_V(v) = av$. Por la definición de un A-módulo, $a_V \in \mathrm{End}(V)$ y la función $a \to a_V$ es un homomorfismo de álgebras de A en $\mathrm{End}(V)$. A su imagen la denotaremos por A_V.

1.1.10 Proposición
Sea V un A-módulo irreducible. Entonces:

1) *$V(A)$ es un $End_A({}_AA)$-submódulo de ${}_AA$.*

2) *$V(A)$ es un ideal minimal de A.*

3) *Si V' es un A-módulo irreducible y $V \ncong V'$, entonces $xV' = 0 \ \forall \ x \in V(A)$.*

4) *$V(A)$ es un F-álgebra isomorfa a A_V.*

Demostración. Tomemos ${}_AA = \sum \cdot W_i$ con W_i irreducibles. Si $\gamma \in \mathrm{End}_A({}_AA)$ y $\gamma(W_j) \neq \langle 0 \rangle$, entonces $\mathrm{Ker}(\gamma) \cap W_j = \langle 0 \rangle$ (por ser W_j irreducible), luego $\gamma(W_j) \cong W_j \cong V$ lo que significa que $\gamma(W_j) \subseteq V(A)$. Como $\gamma(V(A)) = \sum_{W_i \cong V} \gamma(W_i)$ tenemos $\gamma(V(A)) = \gamma \cdot V(A) \subseteq V(A)$, lo cual demuestra 1).

Si $a \in {}_AA$ y definimos $\gamma_a : {}_AA \to {}_AA$ por $\gamma_a(x) = xa$, tenemos que $\gamma_a \in \mathrm{End}_A({}_AA)$, luego $V(A)a = \gamma_a \cdot V(A) \subseteq V(A)$, pero también $aV(A) \subseteq V(A)$ (esto por ser $V(A)$ un módulo). Así, $V(A)$ es un ideal de A. Cuando $x \in V(A)$, $xV'(A) \subseteq V'(A)$, pues $V'(A)$ es un A-módulo, pero también $xV'(A) \subseteq V(A)$ por ser este último un ideal; entonces $xV'(A) = \langle 0 \rangle$. Ahora tomemos $W_j \cong V'$ y denotemos el A-isomorfismo por μ, entonces $xV' = x\mu(W_j) = \mu(xW_j) = \langle 0 \rangle$, pues $W_j \subseteq V'(A)$, y por lo tanto 3) ha sido demostrado. Si $W \in \mathcal{M}_i(A)$ y $x \in W(A)$, por 3) tenemos que $xV = \langle 0 \rangle \ \ \forall \, W \ncong V$. Sea p_W la proyección de ${}_AA$ respecto a $W(A), \ W \in \mathcal{M}_i(A)$. Si $a \in A$ tenemos que $a = \sum_{W \in \mathcal{M}_i} p_W(a)$; por lo tanto, si $v \in V$

$$a_V(v) = av = \sum_{W \in \mathcal{M}_i} p_W(a)v = xv = x_V(v), \qquad \text{con } x \in V(A).$$

Entonces, $a_V = x_V$ y la función $\Gamma : a \mapsto a_V$ mapea $V(A)$ en todo A_V. Representamos la proyección sobre $W(A)$, con $V \cong W \in \mathcal{M}_i(A)$, por p_V. Si $x \in V(A)$ y $x_V = 0$,

$$x = x1 = x \sum_{W \in \mathcal{M}_i(A)} p_W(1) = xp_V(1) = x_V(p_V(1)) = 0.$$

Luego, $\mathrm{Ker}(\Gamma) = \sum_{W \in \mathcal{M}'_i} W_i$, donde $\mathcal{M}'_i$ es la familia de elementos de $\mathcal{M}_i(A)$ no isomorfos a V. En otras palabras, ${}_AA = V(A) \oplus \mathrm{Ker}(\Gamma)$. Ahora, $V(A)$ es un subespacio de A y, al ser un ideal, $xy \in V(A)$ si $x, y \in V(A)$, es decir, la multiplicación de A es cerrada en $V(A)$; además, el elemento $1_{V(A)} = p_V(1_A)$ es la identidad en $V(A)$ y, por lo tanto, $V(A)$ es una F-álgebra; luego, se tiene 4). En consecuencia, $\Gamma(1_{V(A)}) = \Gamma(1_A) = 1_{A_V}$. Así, al ser Γ inyectiva en $V(A)$, tenemos $V(A) \cong A_V$.

Sólo resta probar la minimalidad de $V(A)$ como un ideal de A. Tomemos pues I un ideal de A, con $I \subsetneq V(A)$. Por la definición de $V(A)$, podemos encontar $V_0 \cong V$ con $V_0 \subset V(A)$ y $V_0 \not\subseteq I$. Como $V_0 \cap I < V_0$ y V_0 es irreducible, tenemos que $V_0 \cap I = \langle 0 \rangle$. Si $x \in I$, $xV_0 \subset V_0$ por ser este último un módulo, y $xV_0 \subset I$ al ser I un ideal; por lo tanto, $xV = xV_0 = \langle 0 \rangle$, o equivalentemente $x_V = 0$; como $x \in V(A)$, se tiene que $x = 0$ y, finalmente, $I = \langle 0 \rangle$.

□

Por el resultado anterior, estudiar $V(A)$ se reduce a estudiar A_V.

1.1.11 Teorema
Sea V un A-módulo irreducible y $B=\mathrm{End}_A(V)$. Entonces, $A_V=\mathrm{End}_B(V)$.

Demostración. Primeramente, recordemos que ya vimos que B es una álgebra y que V es un B-módulo. Si $a_V \in A_V$, $\phi \in \mathrm{End}_A(V)$ y $v \in V$, entonces $a_V(\phi \cdot v) = a\phi(v) = \phi(av) = \phi \cdot (a_V(v))$ y, como claramente $a_V \in \mathrm{End}(V)$, $a_V \in \mathrm{End}_B(V)$, es decir, $A_V \subseteq \mathrm{End}_B(V)$. Pero como A es semisimple, podemos suponer que $V \subseteq {}_AA$. Sea $0 \neq v_0 \in V$ fijo, tenemos que $v_0 \in Av_0A \subseteq AV(A)A \subseteq V(A)$, por ser $V(A)$ un ideal. Como Av_0A también es un ideal, la minimalidad de $V(A)$ garantiza que $Av_0A = V(A)$, por lo cual existen $a_i, a_i' \in A$ tales que $1_{V(A)} = \sum a_i v_0 a_i'$. Si $v \in V$, $v = 1_{V(A)}v = \sum (a_i v_0)(a_i' v)$. Tomemos $\psi \in \mathrm{End}_B(V)$ y, para $v \in V$, definamos $\varphi_v \in B$ por $\varphi_v(x) = xv$, entonces $\psi(xy) = \psi(\varphi_y(x)) = \varphi_y(\psi(x)) = \psi(x)y, \ \forall \ x, y \in V$. Como $a_i v_0, a_i' v \in V$, si $v \in V$, tenemos:

$$\psi(v) = \sum \psi\big((a_i v_0)(a_i' v)\big) = \sum \psi(a_i v_0) a_i' v = av = a_V(v),$$

donde $a = \sum \psi(a_i v_0) a_i'$. Por lo tanto, $\psi = a_V \in A_V$ y $\mathrm{End}_B(V) \subseteq A_V$. □

Combinando la mayor parte de los resultados de esta sección, podemos demostrar un resultado muy importante debido a Wederburn.

1.1.12 Teorema
Si F es un campo algebraicamente cerrado y A una F-álgebra semisimple, entonces

$$\dim\, A = \sum_{V \in \mathcal{M}_i(A)} (\dim\, V)^2 \quad \text{y}$$

$$\dim\, \mathrm{Z}(A) = |\mathcal{M}_i(A)|,$$

donde $\mathrm{Z}(A)$ es el centro de A.

Demostración. Sea $V \in \mathcal{M}_i(A)$. Por la Proposición 1.1.6 y el Teorema 1.1.11, respectivamente tenemos que $\mathrm{End}_A(V) = F \cdot id_V$ y $A_V = End(V)$. Como $End(V) \cong M_n(F)$, con $n = \dim(V)$ y $V(A) \cong A_V$, se tiene que $\dim V(A) = \dim\, \mathrm{End}(V) = (\dim V)^2$, de donde se deduce la primera igualdad del enunciado del teorema.

Afirmamos que $\mathrm{Z}(A) = \sum \mathrm{Z}(V(A))$. Si $x \in \sum \mathrm{Z}(V(A))$, digamos que $x = \sum x_V$, con $x_V \in \mathrm{Z}(V(A)) \ \forall \ V \in \mathcal{M}_i(A)$, y $y \in A$ con $y = \sum y_V$, en virtud de la Proposición 1.1.10, se tiene que

$$xy = \Big(\sum_{V \in \mathcal{M}_i(A)} x_V\Big)\Big(\sum_{V \in \mathcal{M}_i(A)} y_V\Big) = \sum_{V \in \mathcal{M}_i(A)} x_V y_V = \sum_{V \in \mathcal{M}_i(A)} y_V x_V = yx.$$

Por lo tanto, $x \in \mathrm{Z}(A)$ y $\sum \mathrm{Z}(A) \subseteq \mathrm{Z}(A)$. Tomemos ahora $x \in \mathrm{Z}(V(A))$ y escribimos $x = \sum x_V$ con $x_V \in V(A),\ \forall\ V \in \mathcal{M}_i(A)$; si W es cualquier elemento de $\mathcal{M}_i(A)$ y $y_W \in W(A)$ tenemos:

$$x_W y_W = x y_W = y_W x = y_W x_W.$$

Entonces, $x_W \in \mathrm{Z}(W(A))$ como W es arbitario $x \in \sum \mathrm{Z}(V(A))$.

Si $a_V \in \mathrm{Z}(A_V)$, entonces $\forall\ a' \in A$, $(aa')_V = a_V a'_V = a'_V a_V = (a'a)_V$. Luego, para $v \in V$, $a_V(a'v) = a_V(a'_V(v)) = [aa']_V(v) = [a'a]_V(v) = a'_V(a_V(v)) = a' a_V(v)$, con lo cual $a_V \in End_A(V)$ y $\mathrm{Z}(A(V)) \subseteq A(V) \cap \mathrm{End}_A(V)$. Al tomar $a_V \in \mathrm{End}_A(V)$ y $a' \in A$ cualesquiera, $\forall\ v \in V$ tenemos que $a_V(a'_V(v)) = a_V(a'v) = a' a_V(v) = a'_V(a_V(v))$, luego $a_V \in \mathrm{Z}(A_V)$; en consecuencia, $A_V \cap \mathrm{End}_A(V) \subseteq \mathrm{Z}(A_V)$. Finalmente, $\mathrm{Z}(A_V) = A_V \cap \mathrm{End}_A(V)$, pero como $\mathrm{End}_A(V) = F \cdot id_V$, se tiene que $\mathrm{Z}(A_V) = F \cdot id_V$, con lo cual obtenemos que $\dim \mathrm{Z}(V(A)) = \dim \mathrm{Z}(A_V) = 1$ y $\dim \mathrm{Z}(A) = \sum_{V \in \mathcal{M}_i(A)} 1 = |\mathcal{M}_i(A)|$. Esto termina la demostración del teorema. □

Todo lo que hemos hecho sobre una álgebra semisimple es útil debido al siguiente teorema.

1.1.13 Teorema (Maschke)
Sea G un grupo, F un campo cuya característica no divide a $|G|$. Entonces, todo $F[G]$-módulo es completamente reducible. En particular, $F[G]$ es semisimple.

Demostración. Sean V un $F[G]$-módulo y W un submódulo de V. Sea W' un subespacio de V tal que $V = W \oplus W'$ (como espacios vectoriales). Tomemos T como la proyección de V en W. Definamos $f : V \to W$ por:

$$f(v) = \frac{1}{|G|} \sum_{g \in G} g^{-1} T(gv).$$

Así $f \in \mathrm{Hom}(V, W)$ y, si tomamos $h \in G$, tenemos:

$$f(hv) = \frac{1}{|G|} \sum_{g \in G} g^{-1} T(ghv) = h \frac{1}{|G|} \sum_{g \in G} (gh)^{-1} T(ghv) = h f(v).$$

Luego, $f \in \mathrm{Hom}_{F[G]}(V, W)$. Si $w \in W$ y $g \in G$, se tiene que $T(gw) = gw$, por lo tanto $f(w) = w$. Tomemos $W_1 = \mathrm{Ker}(f)$, entonces W_1 es un submódulo de V. Para todo $v \in V$, $f(v) \in W$ y $f(f(v)) = f(v)$; en consecuencia,

$$v = f(v) + [v - f(v)] \in W + W_1.$$

Por lo tanto, $V = W + W_1$ (como módulos). Sea $w \in W \cap W_1$, entonces $w = f(w) = 0$ y $V = W \oplus W_1$. □

1.2. Representaciones y Caracteres

El propósito principal de esta sección es la definición de un caracter y el desarrollo de sus principales propiedades. Los caracteres se derivan de una teoría más general, la de representaciones; veremos cómo se relacionan los módulos con las representaciones, que son el paso inicial para construir caracteres.

1.2.1 Definición
Si A es una F-álgebra y V un F-espacio vectorial. Por una ***representación de*** A ***en*** V *entendemos un homomorfismo de álgebras $\Phi : A \to \mathrm{End}(V)$. La representación correspondiente al módulo regular se llama* ***regular*** *y la representaremos por ρ.*

Dada otra representación Ψ de A en un F-espacio W, decimos que Φ y Ψ son ***equivalentes*** *si existe $f \in \mathrm{Hom}(V, W)$ biyectiva tal que:*

$$\Phi(a) = f^{-1}\Psi(a)f, \quad \forall\ a \in A.$$

A $\dim V$ se le llama el ***grado de la representación*** *y se denota por* $\deg\ \Phi$.

Si Φ es una representación de A en V. Para cada $a \in A$, $\Phi_a := \Phi(a)$ es un endomorfismo de V y, por lo tanto, la correspondencia:

$$(a, v) \longmapsto \Phi_a(v)$$

define una función $\cdot : A \times V \to V$. Si $a, b \in A$, $v, w \in V$ y $\alpha \in F$, entonces:

$$\Phi_{ab} = \Phi(ab) = \Phi(a)\Phi(b) = \Phi_a\Phi_b,$$

$$a(bv) = \Phi_a(\Phi_b(v)) = [\Phi_a\Phi_b](v) = \Phi_{ab}(v) = (ab)v,$$

$$1_A v = \Phi_{1_A}(v) = id_V(v) = v,$$

$$(a+b)v = \Phi_{a+b}(v) = [\Phi_a + \Phi_b](v) = \Phi_a(v) + \Phi_b(v) = av + bv,$$

$$a(v+w) = \Phi_a(v+w) = \Phi_a(v) + \Phi_a(w) = av + aw \quad \text{y}$$

$$(\alpha a)v = \Phi_{\alpha a}(v) = [\alpha\Phi_a](v) = \alpha(\Phi_a(v)) = \alpha(av) = \Phi_a(\alpha v) = a(\alpha v),$$

es decir, V adquire la estructura de A-módulo.

1.2.2 Definición
Una reprensentación se dice ser ***irreducible, reducible o completamente irreducible*** *si el módulo arriba construido es irreducible, reducible o completamente irreducible, respectivamente.*

Supongamos ahora que V es un A-módulo, entonces podemos definir una función $\Phi : A \to \mathrm{End}(V)$ por $\Phi(a) := \Phi_a$, donde $\Phi_a(v) = av$; así, $\Phi_a \in \mathrm{End}(V)$, $\forall\ a \in A$. Además, Φ es una representación de A en V la cual adquirirá las características de irreducibilidad, etc., si V las posee. En otras palabras, un A-módulo y una representación de A son diferentes formas de ver la misma operación $a \cdot v$.

Si $\dim(V) = n$ y tomamos una base $\mathcal{B} = \{v_1, v_2, \ldots, v_n\}$, entonces dado $f \in \mathrm{End}(V)$ e $i \in \{1, 2, \ldots, n\}$ existen únicos $\alpha_{1i}, \alpha_{2i}, \ldots, \alpha_{ni} \in F$ tales que

$$f(v_i) = \sum_{j=1}^{n} \alpha_{ji} v_j.$$

A la matriz $[f]_{\mathcal{B}} = [\alpha_{ij}]$ se le conoce como **representación matricial de f respecto a $\mathcal{B}$**; si $[v]_{\mathcal{B}}$ representa el vector de coordenadas de $v \in V$ respecto a $\mathcal{B}$, tenemos:

$$[f(v)]_{\mathcal{B}} = [f]_{\mathcal{B}}[v]_{\mathcal{B}}, \quad \forall\ v \in V.$$

Además, la matriz $[f]_{\mathcal{B}}$ es única bajo esta propiedad. Tomando $f' \in \mathrm{End}(V)$, tenemos que

$$[ff']_{\mathcal{B}}[v]_{\mathcal{B}} = [f(f'(v))]_{\mathcal{B}} = [f]_{\mathcal{B}}[f'(v)]_{\mathcal{B}} = [f]_{\mathcal{B}}[f']_{\mathcal{B}}[v]_{\mathcal{B}}.$$

Lo que significa que $[f'f]_{\mathcal{B}} = [f]_{\mathcal{B}}[f']_{\mathcal{B}}$, es decir, la función dada por $M_{\mathcal{B}}(f) := [f]_{\mathcal{B}}$ es un homomorfismo del semigrupo $\mathrm{End}(V)$ en $\mathrm{M}_n(F)$. Supongamos que $f \in \mathrm{GL}(V)$, entonces

$$I_n = M_{\mathcal{B}}(id_V) = M_{\mathcal{B}}(ff^{-1}) = M_{\mathcal{B}}(f)M_{\mathcal{B}}(f^{-1}).$$

Así que $M_{\mathcal{B}}(f)$ es invertible y $M_{\mathcal{B}}(f)^{-1} = M_{\mathcal{B}}(f^{-1})$. Por lo tanto, $\mathrm{GL}(V) \cong \mathrm{GL}(n, F)$, toda vez que $M_{\mathcal{B}}(\mathrm{GL}(V)) = \mathrm{GL}(n, F)$.

Sea Φ una representación de una álgebra A en un espacio V. Supongamos que exiten V_1 y V_2 submódulos no triviales de V tales que $V = V_1 \oplus V_2$. Como V_1 y V_2 son submódulos de V, $\forall\ a \in A$, se tiene que $\Phi_a(V_1) = aV_1 = V_1$ y $\Phi_a(V_2) = aV_2 = V_2$, por lo tanto $\Phi_i : A \to \mathrm{End}(V_i)$ dada por $\Phi_i(a) = \Phi(a)|_{V_i}$ es una representación de A en V_i, $i = 1, 2$. Tomemos $\mathcal{B}_1 = \{v_1, \ldots, v_m\}$ una base de V_1 y $\mathcal{B}_2 = \{v_{m+1}, \ldots, v_n\}$ una base de V_2; así, $\mathcal{B} = \mathcal{B}_1 \cup \mathcal{B}_2$ es una base de V y

$$[\Phi(a)]_{\mathcal{B}} = \begin{pmatrix} [\Phi_1(a)]_{\mathcal{B}_1} & 0 \\ 0 & [\Phi_2(a)]_{\mathcal{B}_2} \end{pmatrix}.$$

Bajo estas circunstancias, decimos que la representación Φ se ha **descompuesto** en Φ_1 y Φ_2, simbólicamente $\Phi = \Phi_1 + \Phi_2$. Cuando V es completamente reducible, podemos continuar este proceso hasta tener $V = \sum W_i$, con W_i submódulos irreducibles,

y descomponer a $[\Phi(a)]_{\mathcal{B}}$ en una matriz por bloques donde cada bloque corresponderá a una representación de A en un módulo irreducible, es decir, la representación completamente reducible se descompone en una "suma" de representaciones irreducibles.

Usando el Teorema 1.1.11, podemos obtener un resultado muy útil.

1.2.3 Proposición
Sean $\Phi : A \to \mathrm{End}(V)$ *y* $\Psi : A \to \mathrm{End}(W)$ *dos representaciones irreducibles de una álgebra* A. *Supongamos que exiten bases* $\mathcal{B}$ *y* $\mathcal{B}'$ *de* V *y* W, *respectivamente, y una matriz* $S \neq 0$ *en* $\mathrm{M}_{\dim V \times \dim W}(F)$ *tales que*

$$[\Phi(a)]_{\mathcal{B}} S = S[\Psi(a)]_{\mathcal{B}'}, \quad \forall\ a \in A.$$

Entonces, $\dim V = \dim W$, S *es invertible y* Φ, Ψ *son equivalentes. Si* $\Phi = \Psi$, $\mathcal{B} = \mathcal{B}'$ *y* F *es algebraicamente cerrado, entonces* $S \in F \cdot I_{\dim V}$.

Demostración. Para todo $v \in V$ exite un único elemento $f(v) \in W$ tal que

$$[v]_{\mathcal{B}} = S[f(v)]_{\mathcal{B}'}.$$

Así, hemos definido una función f de V en W la cual es claramente lineal, es decir, $f \in \mathrm{Hom}(V, W)$. Ahora, si $a \in A$ y $v \in V$, se tiene que

$$\begin{aligned}[av]_{\mathcal{B}} &= [\Phi_a(v)]_{\mathcal{B}} = [\Phi(a)]_{\mathcal{B}}[v]_{\mathcal{B}} = [\Phi(a)]_{\mathcal{B}} S[f(v)]_{\mathcal{B}'} \\ &= S[\Psi(a)]_{\mathcal{B}'}[f(v)]_{\mathcal{B}'} = S[\Psi_a(f(v))]_{\mathcal{B}'} = S[af(v)]_{\mathcal{B}'}.\end{aligned}$$

lo cual implica que

$$f(av) = af(v).$$

Entonces $f \in \mathrm{Hom}_A(V, W)$, f no cero, con V y W irreducibles; por la Proposición 1.1.6, f es invertible, luego $\dim V = \dim W$. Para ver que S es invertible basta con notar que S es la representación matricial de f^{-1} repecto a $\mathcal{B}'$ y $\mathcal{B}$; como $\Phi(a) = f^{-1}\Psi(a)f$, tenemos que Φ y Ψ son equivalentes. Si $\Phi = \Psi$, $\mathcal{B} = \mathcal{B}'$ y F es algebraicamente cerrado, de nuevo por la Proposición 1.1.6, $f \in F \cdot id_V$, de donde se desprende que S es una matriz escalar.

□

Este resultado es útil porque permite obtener, entre otras cosas, las llamadas **relaciones de Schur** que son de gran importancia en la teoría de caracteres.

1.2.4 Proposición
Sean $\Phi : A \to \text{End}(V)$ *y* $\Psi : A \to \text{End}(W)$ *representaciones irreducibles de* $\mathbb{C}[G]$. *Tomemos* $\mathcal{B}$ *y* $\mathcal{B}'$ *bases cualesquiera de* V *y* W, *respectivamente. Definimos las funciones* a_{ij} *y* b_{ij} *de* G *en* $\mathbb{C}$ *como el elemento* (i,j) *de* $[\Phi(g)]_{\mathcal{B}}$ *y de* $[\Psi(g)]_{\mathcal{B}'}$, *respectivamente. Sea:*

$$\langle a_{ij}, b_{kl} \rangle = \sum_{g \in G} a_{ij}(g) b_{kl}(g^{-1}).$$

Entonces:

1) $\langle a_{ij}, b_{kl} \rangle = 0$ *si* Φ *y* Ψ *no son equivalentes.*

2) *Si* $\Phi = \Psi$ *y* $\mathcal{B} = \mathcal{B}'$, *entonces*

$$\langle a_{ij}, b_{kl} \rangle = \delta_{il}\delta_{jk} \frac{|G|}{\deg \Phi},$$

donde δ_{ij} *es la delta de Kronecker.*

Demostración. Sean $\dim V = n$ y $\dim W = m$, y E_{ij} la matriz en $F_{n \times m}$ con todas sus entradas cero excepto en (i,j) la cual es 1. Sea

$$P_{ij} = \sum_{g \in G} [\Phi(g)]_{\mathcal{B}} E_{ij} [\Psi(g)]^{-1}_{\mathcal{B}'} .$$

Tomemos $h \in G$, entonces la relación

$$[\Phi(h)]_{\mathcal{B}} P_{ij} [\Psi(h)]^{-1}_{\mathcal{B}'} = \sum_{g \in G} [\Phi(hg)]_{\mathcal{B}} E_{ij} [\Psi(hg)]^{-1}_{\mathcal{B}'} = P_{ij},$$

implica que

$$[\Phi(h)]_{\mathcal{B}} P_{ij} = P_{ij} [\Psi(h)]_{\mathcal{B}'}, \qquad \forall\ h \in G.$$

De la igualdad anterior, y dado que Φ y Ψ son $\mathbb{C}$-lineales, tenemos:

$$[\Phi(a)]_{\mathcal{B}} P_{ij} = P_{ij} [\Psi(a)]_{\mathcal{B}'}, \quad \forall\ a \in \mathbb{C}[G].$$

Ahora,

$$[\Phi(g)]_{\mathcal{B}} E_{ij} = \sum_{k=1}^{n} a_{ki}(g) E_{kj} \quad \text{y}$$

$$E_{kj} [\Psi(g)]^{-1}_{\mathcal{B}'} = \sum_{l=1}^{m} b_{jl}(g^{-1}) E_{kl}.$$

Por lo tanto,

$$P_{ij} = \sum_{g\in G} \sum_{k=1}^{n} \sum_{l=1}^{m} a_{ki}(g) b_{jl}(g^{-1}) E_{kl} = \sum_{k=1}^{n} \sum_{l=1}^{m} \langle a_{ki}, b_{jl} \rangle E_{kl}. \tag{1.1}$$

Si Φ y Ψ no son equivalentes, por la Proposición 1.2.3, obtenemos que $P_{ij} = 0$. Como $\langle a_{ki}, b_{jl} \rangle$ es la entrada (k,l) de P_{ij}, se tiene que $\langle a_{ki}, b_{jl} \rangle = 0$. Luego, se tiene 1).

Por otro lado, supongamos ahora las hipótesis de 2); por la Proposición 1.2.3, sabemos que $P_{ij} = \alpha I_n$ para algún $\alpha \in F$. Además,

$$n\alpha = tr(P_{ij}) = \sum_{g\in G} tr([\Phi(g)]_{\mathcal{B}} E_{ij} [\Phi(g)]_{\mathcal{B}}^{-1}) = \sum_{g\in G} tr(E_{ij}) = |G|\delta_{ij},$$

lo cual implica que

$$\alpha = \frac{|G|}{n} \delta_{ij} \ .$$

Así, el elemento (k,l) de P_{ij} se puede escribir como:

$$\delta_{kl}\delta_{ij} \frac{|G|}{n} \ .$$

Según la ecuación (1.1), la entrada (k,l) de P_{ij} es $\langle a_{ki}, b_{jl} \rangle$, de donde se obtiene el resultado.

□

Sea V un espacio vectorial, y tomemos $\mathcal{B} = \{v_1, \ldots, v_n\}$ y $\mathcal{B}' = \{v'_1, \ldots, v'_n\}$ dos bases de V. Si elejimos $\alpha_{ij} \in F$ de forma tal que $v_i = \sum \alpha_{ji} v'_j$, entonces $\forall\ v \in V$ se tiene:

$$[v]_{\mathcal{B}'} = {}_{\mathcal{B}'}M_{\mathcal{B}} [v]_{\mathcal{B}},$$

donde ${}_{\mathcal{B}'}M_{\mathcal{B}} = (\alpha_{ij})$ es la conocida como **matriz de cambio de base de $\mathcal{B}$ a $\mathcal{B}'$**; es bien sabido que ${}_{\mathcal{B}'}M_{\mathcal{B}}\, {}_{\mathcal{B}}M_{\mathcal{B}'} = I_n$. Además, si W es otro espacio vectorial y $f \in \mathrm{Hom}(V,W)$, entonces

$$[f]_{\mathcal{B}'}[v]_{\mathcal{B}'} = [f(v)]_{\mathcal{B}'} = {}_{\mathcal{B}'}M_{\mathcal{B}} [f(v)]_{\mathcal{B}} = {}_{\mathcal{B}'}M_{\mathcal{B}} [f]_{\mathcal{B}} [v]_{\mathcal{B}} = {}_{\mathcal{B}'}M_{\mathcal{B}} [f]_{\mathcal{B}\mathcal{B}} M_{\mathcal{B}'} [v]_{\mathcal{B}'},$$

por lo tanto, $[f]_{\mathcal{B}'} = {}_{\mathcal{B}'}M_{\mathcal{B}}\, [f]_{\mathcal{B}}\, {}_{\mathcal{B}}M_{\mathcal{B}'}$. Entonces, si Φ es cualquier representación de $F[G]$ en V, representaciones matriciales de Φ en diferentes bases son equivalentes (como matrices) y de aquí que

$$tr([f]_{\mathcal{B}'}) = tr({}_{\mathcal{B}'}M_{\mathcal{B}} [f]_{\mathcal{B}\mathcal{B}} M_{\mathcal{B}'}) = tr([f]_{\mathcal{B}\mathcal{B}'} M_{\mathcal{B}\mathcal{B}} M_{\mathcal{B}'}) = tr([f]_{\mathcal{B}}).$$

En otras palabras, podemos definir la **traza de** f, $tr(f)$, como el valor de la traza de cualquier representación matricial de f, ya que esta no depende de la base elegida.

De ahora en adelante, siempre trabajaremos sobre el campo $\mathbb{C}$ a menos que se diga otra cosa. Pero es importante mencionar que la mayoria de los resultados se pueden enunciar sobre cualquier campo de característica cero y algebraicamente cerrado, salvo aquellos que requieren propiedades especificas de $\mathbb{C}$.

1.2.5 Definición
Dada una representación Φ *de* $\mathbb{C}[G]$*, a la función* $\chi : G \to \mathbb{C}$ *definida por* $\chi(g) = tr(\Phi(g))$ *se le llama el* ***caracter de*** G ***aportado por*** Φ*. Al conjunto de caracteres de* G *lo denotamos por* $\mathrm{Ch}(G)$*. Llamamos a un caracter* ***irreducible*** *si es aportado por una representación irreducible, y al conjunto de caracteres irreducible se le denota por* $\mathrm{Irr}(G)$*. Un caracter que es aportado por una representación de grado* 1 *se denomina* ***lineal****, al conjunto de estos lo representamos por* $\mathrm{Lin}(G)$*.*

Una ventaja de los caracteres radica en que existen maneras de construirlos sin necesidad de tener una representación. Algunos de los métodos básicos serán expuestos posteriormente; sin embargo, mencionemos aquí al más simple de todos, la **restricción**. Supongamos que Φ es una representación de $\mathbb{C}[G]$ aportando el caracter χ. Si $H < G$, entonces $\Phi|_{\mathbb{C}[H]}$ es una representación de H que aporta el caracter $\chi|_H$. Es importante mencionar que χ irreducible no necesariamente implica $\chi|_H$ irreducible. Más adelante hablaremos también acerca de cómo deducir propiedades de un grupo conociendo sus caracteres.

Es claro de la definición que $\chi(e) = \deg \Phi > 0$. Si χ es un caracter lineal, necesariamente es irreducible, pués el módulo que genera tiene dimensión 1; por lo tanto $\mathrm{Lin}(G) \subseteq \mathrm{Irr}(G)$. Al conjunto de caracteres irreducibles de grado mayor a uno lo denotaremos por $\mathrm{Irr}_1(G)$. Por lo dicho anteriormente, $\mathrm{Irr}_1(G) = \mathrm{Irr}(G) \backslash \mathrm{Lin}(G)$. Si V es cualquier espacio vectorial de dimensión 1, el homomorfismo trivial de $\mathbb{C}[G]$ en $\mathrm{End}(V)$ aporta un caracter de valor constante 1; a este caracter irreducible se le nombra **principal** y se denota por 1_G.

Otro ejemplo de un caracter lo podemos obtener de la representación regular ρ de $\mathbb{C}[G]$. Tomemos $G = \{e = g_1, g_2, \ldots, g_n\}$, como G es una base de $\mathbb{C}[G]$, podemos calcular $[\rho(g_k)]_G$,

$$\rho_{g_k}(g_i) = g_k g_i = \sum_{j=1}^{n} \alpha_{ji}^{k}\, g_j,$$

donde $\alpha_{ji}^k = 1$ si $g_k g_i = g_j$ y 0 en otro caso. Al carater aportado por ρ también lo representaremos por ρ, entonces:

$$\rho(g_k) = tr\ [\rho(g_k)]_G = tr\ (\alpha_{ij}^k) = \sum_{i=1}^{n} \alpha_{ii}^k.$$

Para que $\alpha_{ii}^k \neq 0$, se debe cumplir que $g_k g_i = g_i$; por lo tanto, si $k \neq 1$ $\alpha_{ii}^k = 0$, y $\alpha_{ii}^1 = 1,\ \forall\ i$. Así

$$\rho(g) = 0 \quad \text{si } g \neq e \quad \text{y} \quad \rho(e) = |G|.$$

Una **función de clases** es una función definida sobre un grupo de forma tal que es constante en cada clase de conjugación. La propiedad más importante de un caracter es sin duda que es una función de este tipo.

1.2.6 Teorema

Todo caracter es una función de clase.

Demostración. Sean G un grupo y χ un caracter de G aportado por una representación Φ. Entonces, si $g, h \in G$ se tiene que

$$\chi(h^{-1}gh) = tr(\Phi(h^{-1}gh)) = tr(\Phi(h^{-1})\Phi(g)\Phi(h)) = tr(\Phi(g)) = \chi(g).$$

□

Supongamos que Φ y Ψ son dos representaciones equivalentes de $\mathbb{C}[G]$. Sean V y W módulos correspondientes a Φ y Ψ, respectivamente. Por definición, existe una función biyectiva f de V en W tal que

$$\Phi(a) = f^{-1}\Psi(a)f, \quad \forall\ a \in A.$$

Sea P la representación matricial de f respecto a dos bases $\mathcal{B}$ y $\mathcal{B}'$ de V y W, respectivamente. Entonces tenemos:

$$[\Phi(a)]_{\mathcal{B}} = P^{-1}[\Psi(a)]_{\mathcal{B}'}P.$$

Por lo tanto, se tiene el siguiente resultado:

1.2.7 Proposición

Dos representaciones similares aportan un mismo caracter.

□

Fijemos $\mathcal{M}_i(\mathbb{C}[G])$, y supongamos que Φ es irreducible, entonces V es irreducible como $\mathbb{C}[G]$-módulo, por lo tanto existen $W \in \mathcal{M}_i(\mathbb{C}[G])$ y $f \in \mathrm{Hom}_{\mathbb{C}[G]}(W, V)$ biyectiva. Sea Ψ la representación correspondiente a W, es decir, definimos $\Psi(a) = \Psi_a$ y $\Psi_a(w) = aw$, $\forall\ a \in \mathbb{C}[G]$. Entonces

$$\Psi_a(w) = aw = af^{-1}(f(w)) = f^{-1}(af(w)) = f^{-1}(\Phi_a(f(w))) = [f^{-1}\Phi_a f](w).$$

Así, Φ y Ψ son equivalentes y aportan un mismo caracter. Por lo tanto, el número de caracteres irreducibles no sobrepasa a $|\mathcal{M}_i(\mathbb{C}[G])|$. De aquí en adelante si G es un grupo cualquiera al conjunto de clases de conjugación de elementos de G lo denotaremos por $\mathrm{CL}[G]$.

1.2.8 Proposición

Sea G un grupo. Entonces:

$$|\mathrm{Irr}(G)| = |\mathrm{CL}[G]| \quad \text{y}$$

$$|G| = \sum_{\chi \in\ \mathrm{Irr}(G)} \chi(e)^2$$

Demostración. Por el Teorema 1.1.12, se tiene que $|\mathcal{M}_i(\mathbb{C}[G])| = \dim \mathrm{Z}(\mathbb{C}[G])$. Sea $\mathrm{CL}[G] = \{\mathcal{K}_1, \ldots, \mathcal{K}_n\}$ y $K_i \in \mathbb{C}[G]$ la suma de los elementos de $\mathcal{K}_i$. Tomemos $g \in G$, como la conjugación permuta los elementos de una clase de conjugación, tenemos que $gK_ig^{-1} = K_i$, por lo tanto $gK_i = K_ig$ y de ahí que $aK_i = K_ia$ $\forall\ a \in \mathbb{C}[G]$; así, $K_1, \ldots, K_n \in \mathrm{Z}(\mathbb{C}[G])$. Ahora, tomemos $a = \sum a_g g \in \mathrm{Z}(\mathbb{C}[G])$ y $h \in G$, entonces

$$\sum a_g g = h^{-1}(\sum a_g g)h = \sum a_g h^{-1}gh = \sum a_{hgh^{-1}} g,$$

lo cual implica que

$$a_g = a_{hgh^{-1}},\ \forall\ g \in G.$$

Es decir, a_g es constante en clases de conjugación y, por lo tanto, a es combinación lineal de $K_1, \ldots, K_n$; además, estos últimos son claramente linealmente independientes. Por lo tanto, $\dim \mathrm{Z}(\mathbb{C}[G]) = |CL[G]| \geq |\mathrm{Irr}(G)|$.

Para finalizar, mostraremos que los caracteres aportados por las representaciones correspondientes a los elementos de $\mathcal{M}_i(\mathbb{C}[G])$ son distintos, es decir, $|\mathrm{CL}[G]| = |\mathcal{M}_i(\mathbb{C}[G])| \leq |\mathrm{Irr}(G)|$. Tomemos $\mathcal{M}_i(\mathbb{C}[G]) = \{V_1, \ldots, V_n\}$. Entonces:

$$\mathbb{C}[G]^\circ = \sum_{i=1}^{n} V_i(\mathbb{C}[G]).$$

Sea e_i la proyección de e sobre $V_i(\mathbb{C}[G])$ y Φ^i la representación correspondiente a V_i. Tomemos $j=1,\ldots,n$ y $j\neq i=1,\ldots,n$. Si $v\in V_j$, por la Proposición 1.1.10, tenemos:

$$\Phi^j_{e_i}(v)=e_iv=0 \qquad \Rightarrow \qquad \Phi^j(e_i)=0$$
$$\Rightarrow \qquad \Phi^j(e)=\Phi^j(e_j)=id_{V_j}.$$

Así, si χ_j es el caracter aportado por Φ^j, entonces

$$\chi_j(e_i)=\delta_{ji}\text{deg }\Phi^j, \qquad \forall\ i=1,\ldots,n. \tag{1.2}$$

Luego, los caracteres χ_j son diferentes como funciones en $\mathbb{C}[G]$ y, por lo tanto, diferentes en G. La segunda igualdad es inmediata de la primera y del Teorema 1.1.12.

□

Si G es un grupo, $\text{CL}[G]=\{\mathcal{K}_1,\ldots,\mathcal{K}_n\}$ e $\text{Irr}(G)=\{\chi_1,\ldots,\chi_n\}$, entonces al arreglo

$$X(G)=\begin{bmatrix} \chi_1(\mathcal{K}_1) & \cdots & \chi_1(\mathcal{K}_n) \\ \vdots & \ddots & \vdots \\ \chi_n(\mathcal{K}_1) & \cdots & \chi_n(\mathcal{K}_n) \end{bmatrix}$$

se le conoce como **Tabla de Caracteres de** G y la denotaremos por $\text{X}(G)$. Aunque no existe una regla acerca de la forma para ordenar a las clases o a los caracteres, si hay una convención. A las clases se les suele ordenar por el orden de sus elementos en forma ascendente y a los caracteres por su grado. Si G_1 es cualquier otro grupo, $Cl[G_1]=\{\mathcal{K}'_1,\ldots,\mathcal{K}'_m\}$, decimos que G y G_1 tienen la misma tabla de caracteres si $\big|\text{CL}[G]\big|=\big|\text{CL}[G_1]\big|$ y bajo una permutación entre filas y columnas podemos obtener $X(G)=X(G_1)$ (como matrices); cuando esto sucede escribimos $X(G)=X(G_1)$. El objetivo de la Teoría de Caracteres es estudiar la relación entre G y $\text{X}(G)$; como un primer ejemplo tenemos:

1.2.9 Proposición

Un grupo es abeliano si y sólo si todos sus caracteres irreducibles son lineales.

Demostración. De la Proposición 1.2.8, se deduce que $|G|=|\text{CL}(G)|=|\text{Irr}(G)|$ si y sólo si $\text{deg }\chi=\chi(e)=1,\ \forall\ \chi\in\text{Irr}(G)$.

□

De este resultado podemos derivar que toda representación irreducible de un grupo abeliano G es de grado 1 y, por lo tanto, los bloques de la descomposición de cualquier representación de G son de tamaño 1. Es decir, para toda representación $\Phi:\mathbb{C}[G]\rightarrow$

End(V) podemos encontar una base de V de forma tal que la representación matricial de $\Phi(g)$ es diagonal $\forall\ g \in G$.

Denotemos por Cl(G) al conjunto de las funciones de clase en un grupo G; claramente Cl(G) es un espacio vectorial sobre $\mathbb{C}$ (con las operaciones usuales sobre funciones) cuya dimensión es $|\mathrm{CL}[G]|$.

1.2.10 Proposición

$$\mathrm{Cl}(G) = \langle \mathrm{Irr}(G) \rangle_{\mathbb{C}} \quad \text{y}$$
$$\mathrm{Ch}(G) = \langle \mathrm{Irr}(G) \rangle_{\mathbb{Z}^+}.$$

Demostración. Ya sabemos que dim Cl(G) = |Irr(G)|, entonces para obtener que Irr(G) es una base para Cl(G) basta mostrar que es un conjunto linealmente independiente sobre $\mathbb{C}$. Si $\sum \alpha_j \chi_j = 0$, con $\alpha_j \in \mathbb{C}$, evaluando esta suma en los e_i construidos en la demostración de 1.2.8, obtenemos $\alpha_i = 0\ \forall\ i$.

Sea Φ cualquier representación de G, entonces podemos descomponer ésta en una "suma" finita de representaciones irreducibles por el proceso descrito en la página 12. Así, el caracter aportado por Φ es combinacion lineal con coeficientes enteros no negativos de caracteres irreducibles, por lo tanto $\mathrm{Ch}(G) \subseteq \langle \mathrm{Irr}(G) \rangle_{\mathbb{Z}^+}$. Para obtener la igualdad, debemos mostrar que todo elemento de $\langle \mathrm{Irr}(G) \rangle_{\mathbb{Z}^+}$ es un caracter; de hecho, basta con mostrar que la suma de dos caracteres es un caracter. Para esto, sean χ_1 y χ_2 dos caracteres cualesquiera, y $\Phi_i : \mathbb{C}[G] \to \mathrm{End}(V_i)$ representaciones que aporten el caracter χ_i, con $i = 1, 2$. Definimos un nuevo $\mathbb{C}[G]$-módulo por $V = V_1 \times V_2$; la representación de este módulo aporta el caracter $\chi_1 + \chi_2$. □

1.2.11 Proposición

Dos representaciones son similares si y sólo si aportan el mismo caracter.

Demostración. Sean Ψ_1 y Ψ_2 dos representaciones de un grupo G que aportan un mismo caracter. Sean $\Phi_1, \ldots, \Phi_n$ las representaciones correspondientes a los submódulos de $\mathcal{M}_i(\mathbb{C}[G])$. Entonces, existen $m_1, \ldots, m_n, k_1, \ldots, k_n \in \mathbb{Z}^+$ tales que

$$\Psi_1 = \sum_{i=1}^{n} m_i \Phi_i \quad \text{y} \quad \Psi_2 = \sum_{i=1}^{n} k_i \Phi_i\ .$$

Sea χ_i el caracter irreducible aportado por Φ_i, y sea ϑ_1 y ϑ_2 los caracteres aportados por Ψ_1 y Ψ_2, respectivamente. Entonces:

$$\vartheta_1 = \sum_{i=1}^{n} m_i \chi_i \quad \text{y} \quad \vartheta_2 = \sum_{i=1}^{n} k_i \chi_i\ .$$

Como $\vartheta_1 = \vartheta_2$, al ser $\{\chi_1, \ldots, \chi_1\}$ linealmente independientes, tenemos que $m_i = k_i$, $\forall\ i$. Por lo tanto, Ψ_1 y Ψ_2 tienen idénticas descomposiciones en bloques irreducibles y, de aquí que son similares. Para finalizar, basta aplicar la Proposición 1.2.7.

□

Una propiedad fundamental de los caracteres irreducibles son las llamadas **relaciones de ortogonalidad**.

1.2.12 Proposición (Primera Relación de Ortogonalidad)
Sean G un grupo y $\mathrm{Irr}(G) = \{\chi_1, \ldots, \chi_n\}$. *Entonces,*

$$\frac{1}{|G|}\sum_{g\in G}\chi_i(g)\overline{\chi_j(g)} = \delta_{ij} \quad \forall\ g \in G.$$

Demostración. Sea $\Phi_i : G \to \mathrm{End}(V_i)$ una representación que aporte χ_i, y $\mathcal{B}_i$ una base del espacio vectorial correspondiente. Entonces,

$$[\Phi_i(g)]_{\mathcal{B}_i} = [a^i_{kl}(g)] \quad \text{con} \quad k, l = 1, \ldots,\ \dim V_i = n_i \quad \text{y}$$

$$\chi_i = \sum_{k=1}^{n_i} a^i_{kk}\ .$$

Luego

$$\begin{aligned}
\frac{1}{|G|}\sum_{g\in G}\chi_i(g)\overline{\chi_j(g)} &= \frac{1}{|G|}\sum_{g\in G}\Big(\sum_{k=1}^{n_i} a^i_{kk}(g)\Big)\Big(\sum_{l=1}^{n_j} a^j_{ll}(g^{-1})\Big) \\
&= \frac{1}{|G|}\sum_{g\in G}\sum_{k=1}^{n_i}\sum_{l=1}^{n_j} a^i_{kk}(g)a^j_{ll}(g^{-1}) \\
&= \frac{1}{|G|}\sum_{k=1}^{n_i}\sum_{l=1}^{n_j}\langle a^i_{kk}, a^j_{ll}\rangle\ .
\end{aligned}$$

Si $i \neq j$, por la Proposición 1.2.11, se tiene que Φ_i y Φ_j no son similares. Aplicando la Proposición 1.2.4, tenemos que $\langle a^i_{kk}, a^j_{ll}\rangle = 0\ \forall\ k, l$ lo cual implica que

$$\frac{1}{|G|}\sum_{g\in G}\chi_i(g)\overline{\chi_j(g)} = 0$$

y si $i = j$, entonces

$$\langle a^i_{kk}, a^j_{ll}\rangle = \delta_{kl}\frac{|G|}{n_i} \quad \forall\ k,l$$

con lo cual

$$\frac{1}{|G|}\sum_{g\in G}\chi_i(g)\overline{\chi_j(g)} = \frac{1}{n_i}\sum_{k=1}^{n_i}\sum_{l=1}^{n_i}\delta_{kl} = 1.$$

□

La proposición anterior motiva la siguiente definición.

1.2.13 Definición
Sean $\phi,\psi\in$ Cl(G). Se define el ***producto interno de*** ϕ ***y*** ψ *por:*

$$\langle\phi,\psi\rangle = \frac{1}{|G|}\sum_{g\in G}\phi(g)\overline{\psi(g)}.$$

La ventaja de introducir este producto interno en $\mathrm{Cl}(G)$ es que, por la Primera Relación de Ortogonalidad, $\mathrm{Irr}(G)$ es una base ortonormal y, por lo tanto, para determinar si una cierta función de clase ϑ es o no un caracter, basta con calcular $\langle\vartheta,\chi\rangle\ \ \forall\ \chi\in\mathrm{Irr}(G)$ y aplicar la Proposición 1.2.10. También nos proporciona una manera de calcular los coeficientes de la representación de un caracter en la base $\mathrm{Irr}(G)$. Por ejemplo, si $\chi\in\mathrm{Irr}(G)$, entonces $\langle\rho,\chi\rangle=\chi(e)$ y de aquí que:

$$\rho = \sum_{\chi\in\mathrm{Irr}(G)}\chi(e)\chi$$

1.2.14 Proposición
Si $\phi,\psi\in$ Ch(G), entonces $\langle\phi,\psi\rangle=\langle\psi,\phi\rangle\in\mathbb{Z}^+$. Además, $\langle\phi,\phi\rangle=1\ \Leftrightarrow\ \phi\in$ Irr(G).

Demostración. Sea $\mathrm{Irr}(G)=\{\chi_1,\ldots,\chi_n\}$. Por la Proposición 1.2.10, se tiene que $\phi=\sum m_i\chi_i$ y $\psi=\sum k_i\chi_i$, con $m_1,\ldots,m_n,k_1\ldots,k_n\in\mathbb{Z}^+$, luego

$$\langle\phi,\psi\rangle = \sum m_ik_i = \sum k_im_i = \langle\psi,\phi\rangle\,.$$

Por otro lado, se tiene que $\langle\phi,\phi\rangle=\sum m_i^2=1$ si, y sólo si, todos excepto uno de los m_i valen 0 y el restante 1, es decir, si, y sólo si $\phi\in\mathrm{Irr}(G)$.

□

Es importante aclarar que si $\vartheta \in \mathrm{Cl}(G)$ y $\langle \vartheta, \vartheta \rangle = 1$, no necesariamente tenemos que $\vartheta \in \mathrm{Irr}(G)$, pues puede darse el caso de que ϑ no sea un caracter. Por ejemplo, considérese $G = \mathbb{Z}/4\mathbb{Z}$ con la función de clase $\vartheta(g) = 2$ si $g \neq e$, y $\vartheta(e) = -2$; aquí, $\langle \vartheta, \vartheta \rangle = 1$ pero claramente ϑ no puede ser un caracter.

Otra observación importante es que $\langle \phi, \psi \rangle = \langle \overline{\phi}, \overline{\psi} \rangle$ y, por lo tanto, $\overline{\chi} \in \mathrm{Irr}(G) \Leftrightarrow \chi \in \mathrm{Irr}(G)$.

1.2.15 Proposición (Segunda Relación de Ortogonalidad)
Sea G un grupo, entonces

$$\sum_{\chi \in \mathrm{Irr}(G)} \chi(g)\overline{\chi(h)} = \widehat{\delta}_{gh} \left| \mathrm{C}_G(g) \right|, \quad \forall\ g, h \in G,$$

donde $\widehat{\delta}_{gh} = 1$ si $\mathrm{Cl}[g] = \mathrm{Cl}[h]$ y 0 en otro caso.

Demostración. Tomemos $\mathrm{CL}[G] = \{\mathcal{K}_1, \ldots, \mathcal{K}_n\}$, $k_i = |\mathcal{K}_i|$, $g_i \in \mathcal{K}_i$ e $\mathrm{Irr}(G) = \{\chi_1, \ldots, \chi_n\}$. Como los caracteres son funciones de clase, por la Proposición 1.2.12 tenemos que

$$\frac{1}{|G|} \sum_{m=1}^{n} k_m \chi_i(g_m)\overline{\chi_j(g_m)} = \delta_{ij}.$$

Sean

$$X(G) = \begin{pmatrix} \chi_1(\mathcal{K}_1) & \cdots & \chi_1(\mathcal{K}_n) \\ \vdots & \ddots & \vdots \\ \chi_n(\mathcal{K}_1) & \cdots & \chi_n(\mathcal{K}_n) \end{pmatrix} \quad \text{y}$$

$$M = \frac{1}{|G|} \begin{pmatrix} k_1 & & 0 \\ & \ddots & \\ 0 & & k_n \end{pmatrix} \overline{X(G)^t} = \sum_{i=1}^{n} \sum_{j=1}^{n} k_i \overline{\chi_j(g_i)} E_{ij}$$

donde E_{ij} son retomados de la Proposición 1.2.4. Tomando en cuenta que $E_{ij}E_{kl} = 0$ si $j \neq k$ y $E_{ij}E_{jl} = E_{il}$, tenemos que

$$\begin{aligned} X(G)M &= \frac{1}{|G|} \Big(\sum_{i=1}^{n} \sum_{j=1}^{n} \chi_i(g_j) E_{ij} \Big) \Big(\sum_{i=1}^{n} \sum_{j=1}^{n} k_i \overline{\chi_j(g_i)} E_{ij} \Big) \\ &= \frac{1}{|G|} \sum_{i=1}^{n} \sum_{j=1}^{n} \sum_{m=1}^{n} k_m \chi_i(g_m) \overline{\chi_j(g_m)} E_{ij} \\ &= \sum_{i=1}^{n} \sum_{j=1}^{n} \delta_{ij} E_{ij} = I_n. \end{aligned}$$

Por lo tanto, $MX(G) = I_n$. Así,

$$\begin{aligned} I_n &= \frac{1}{|G|}\Big(\sum_{i=1}^{n}\sum_{j=1}^{n} k_i\overline{\chi_j(g_i)}E_{ij}\Big)\Big(\sum_{i=1}^{n}\sum_{j=1}^{n}\chi_i(g_j)E_{ij}\Big) \\ &= \frac{1}{|G|}\sum_{i=1}^{n}\sum_{j=1}^{n}\sum_{m=1}^{n} k_i\chi_m(g_j)\overline{\chi_m(g_i)}E_{ij}, \end{aligned}$$

con lo cual

$$\frac{k_i}{|G|}\sum_{m=1}^{n}\chi_m(g_j)\overline{\chi_m(g_i)} = \delta_{ij}.$$

Recordando que $|\mathrm{C}_G(g_i)| = |G| \,/\, |\mathrm{Cl}[g_i]|$ terminamos.

□

Una consecuencia importante del anterior resultado es la fórmula:

$$\sum_{\chi\in\mathrm{Irr}(G)} |\chi(g)|^2 = |\mathrm{C}_G(g)|\,, \quad \forall\ g \in G.$$

Otra propiedad importante de un caracter es que sus valores son enteros algebraicos; un **entero algebraico** es un número complejo raíz de un polinomio mónico en $\mathbb{Z}[X]$. Al conjunto de los enteros algebraicos lo denotaremos por E. Las siguientes son propiedades bien conocidas sobre el conjunto E:

1.2.16 Proposición

1) *E es un subanillo de $\mathbb{C}$.*

2) *$E \cap \mathbb{Q} = \mathbb{Z}$.*

3) *Si S es un anillo con $\mathbb{Z} \subseteq S \subseteq \mathbb{C}$ y S es finitamente generado como $\mathbb{Z}$-módulo, entonces $S \subseteq E$.*

Una demostración de estas propiedades se puede encontrar en [12].

□

1.2.17 Teorema

Sean G un grupo y χ un caracter de G de grado n. Si $g \in G$, entonces

1) $\chi(g) = \sum_{i=1}^{n} \varepsilon_i, \quad$ *donde* $\quad \varepsilon_i^{o(g)} = 1 \quad \forall\ i = 1, \ldots, n.$

2) $|\chi(g)| \leq \chi(e)$.

3) $\chi(g^{-1}) = \overline{\chi(g)} = \sum_{i=1}^{n} \varepsilon_i^{-1}$.

Demostración. Sea Φ una representación de G sobre un espacio V que aporta χ, entonces $\Phi|_{\langle g \rangle}$ es una representación de $\langle g \rangle$ sobre V. Como $\langle g \rangle$ es abeliano, por la Proposición 1.2.9, podemos encontar una base $\mathcal{B}$ de V tal que

$$[\Phi(g)]_{\mathcal{B}} = \begin{pmatrix} \varepsilon_1 & & & 0 \\ & \varepsilon_2 & & \\ & & \ddots & \\ 0 & & & \varepsilon_n \end{pmatrix},$$

$$\Rightarrow \quad I_n = [\Phi(g^{o(g)})]_{\mathcal{B}} = [\Phi(g)]_{\mathcal{B}}^{o(g)} = \begin{pmatrix} \varepsilon_1^{o(g)} & & & 0 \\ & \varepsilon_2^{o(g)} & & \\ & & \ddots & \\ 0 & & & \varepsilon_n^{o(g)} \end{pmatrix}.$$

De donde se tiene 1). Como $|\varepsilon_i| = 1 \quad \forall\ i = 1, \ldots, n$ (pues $\varepsilon_i^{o(g)} = 1$) tenemos:

$$|\chi(g)| \leq \sum_{i=1}^{n} |\varepsilon_i| = n = \chi(e).$$

Tambien $\overline{\varepsilon_i} = \varepsilon_i^{-1}$ y

$$[\Phi(g^{-1})]_{\mathcal{B}} = [\Phi(g)]_{\mathcal{B}}^{-1} = \begin{pmatrix} \varepsilon_1^{-1} & & & 0 \\ & \varepsilon_2^{-1} & & \\ & & \ddots & \\ 0 & & & \varepsilon_n^{-1} \end{pmatrix}.$$

□

Existen varios subconjuntos de G naturalmente asociados a un caracter.

1.2.18 Definición
Sea $\chi \in \mathrm{Ch}(G)$. *El* ***kernel*** *de* χ *se define como* $\ker \chi = \{g \in G : \chi(g) = \chi(e)\}$, *el* ***quasikernel*** *de* χ *es* $\mathrm{Z}(\chi) = \{g \in G : |\chi(g)| = \chi(e)\}$, *al* ***conjunto de ceros*** *de* χ *se le denota por* $\mathrm{T}(\chi)$ *y, finalmente, al conjunto de elementos de* g *con* $|\chi(g)| = 1$ *se denota por* $\mathrm{U}(\chi)$ *y se llama conjunto de* ***elementos*** χ***-unitarios***.

1.2.19 Proposición
Sean $\Phi : \mathbb{C}[G] \to \mathrm{End}(V)$ *una representación y* φ *el caracter aportado por ésta. Entonces:*

1) $\ker\varphi = G \cap \mathrm{Ker}\Phi$ *y por lo tanto* $\ker\varphi \triangleleft G$.

2) $\ker\varphi = \bigcap\{\ker\chi : \chi \in \mathrm{Irr}(G),\ \langle\varphi,\chi\rangle > 0\}$.

3) $\bigcap\{\ker\chi : \chi \in \mathrm{Irr}(G)\} = \langle e\rangle$.

Demostración. Tomemos $n = \deg\varphi$. Sean $g \in G \cap \mathrm{Ker}\Phi$ y $\mathcal{B}$ una base de V, entonces $[\Phi(g)]_{\mathcal{B}} = I_n$ y, por lo tanto, $\varphi(g) = \varphi(e)$. Supongamos ahora que $\varphi(g) = \varphi(e)$, de la demostración de la Proposicion 1.2.17, inferimos que existe una base $\mathcal{B}'$ de V tal que $[\Phi(g)]_{\mathcal{B}'} = \mathrm{diag}(\epsilon_1, \ldots, \epsilon_n)$. Como $\varphi(g) = \epsilon_1 + \cdots + \epsilon_n = n$, con $|\epsilon_i| = 1$, necesariamente tenemos $\epsilon_1 = \cdots = \epsilon_n = 1$ y, por lo tanto, $[\Phi(g)]_{\mathcal{B}'} = I_n$. Para obtener la última aseveración de 1), basta notar que $\Phi|_G$ es un homomorfismo de G en el grupo $\mathrm{End}(V)$.

Sabemos que

$$\varphi = \sum_{\chi \in \mathrm{Irr}(G)} \langle\varphi,\chi\rangle\,\chi\ , \qquad \text{con } \langle\varphi,\chi\rangle \geq 0.$$

Si $g \in \bigcap\{\ker\chi : \chi \in \mathrm{Irr}(G),\ \langle\varphi,\chi\rangle > 0\} = A$, entonces

$$\varphi(g) = \sum_{\chi \in\ \mathrm{Irr}(G)} \langle\varphi,\chi\rangle\,\chi(g) = \sum_{\chi \in Irr(G)} \langle\varphi,\chi\rangle\,\chi(e) = \varphi(e),$$

lo cual implica que

$$A \subseteq \ker\varphi.$$

Supongamos ahora que $g \in\ \ker\varphi$; como

$$|\varphi(g)| \leq \sum_{\chi \in\ \mathrm{Irr}(G)} \langle\varphi,\chi\rangle\,|\chi(g)| \leq \sum_{\chi \in\ \mathrm{Irr}(G)} \langle\varphi,\chi\rangle\,\chi(e) = \varphi(e),$$

la condición $\varphi(g) = \varphi(e)$, junto con la independencia lineal de $\mathrm{Irr}(G)$, obliga a que $\chi(g) = \chi(e)$,$\forall\ \chi \in\ \mathrm{Irr}(G)$ con $\langle\varphi,\chi\rangle > 0$; es decir a que $g \in A$. Para obtener 3) basta aplicar 2) al caracter regular de G y recordar lo dicho sobre éste en las páginas 16 y 22.

□

El quasikernel al igual que el kernel de un caracter nos proporciona información valiosa sobre éste. Algunas de sus propiedades básicas se resumen en la siguiente proposición.

1.2.20 Proposición
Sean $\Phi:\mathbb{C}[G]\to \mathrm{End}(V)$ *una representación,* χ *el caracter aportado por ésta,* n *el grado de* χ *y* $\mathcal{B}$ *una base de* V*. Entonces,*

1) $\mathrm{Z}(\chi)=\{g\in G:[\Phi(g)]_{\mathcal{B}}=\alpha I_n\}$.

2) $\mathrm{Z}(\chi)<G$.

3) $\chi|_{\mathrm{Z}(\chi)}=n\lambda$, *con* $\lambda\in \mathrm{Lin}(\mathrm{Z}(\chi))$.

4) $\mathrm{Z}(\chi)/ker\chi$ *es cíclico.*

5) $\mathrm{Z}(\chi)/ker\chi\subseteq \mathrm{Z}(G/\ker\chi)$.

6) *Si* χ *es irreducible,* $\mathrm{Z}(\chi)/\ker\chi=\mathrm{Z}(G/\ker\chi)$.

Demostración. Sea $g\in G$; si $[\Phi(g)]_{\mathcal{B}}=\epsilon I_n$, entonces $\chi(g)=n\epsilon$. Como $I_n=[\Phi(g)]_{\mathcal{B}}^{o(g)}$, ϵ es una raíz $o(g)$-ésima de la unidad, por lo tanto $|\epsilon|=1$ y de aquí que $|\chi(g)|=n=\chi(e)$. Supongamos ahora que $g\in \mathrm{Z}(\chi)$, por la Proposición 1.2.17, existe una base $\mathcal{B}'$ de V tal que $[\Phi(g)]_{\mathcal{B}'}= \mathrm{diag}(\epsilon_1,\ldots,\epsilon_n)$, con $|\epsilon_i|=1$; la condición $n=|\chi(g)|=|\epsilon_1+\cdots+\epsilon_n|$, obliga a que $\epsilon_1=\cdots=\epsilon_n$ y, por lo tanto, tenemos $[\Phi(g)]_{\mathcal{B}'}=\!=\epsilon_1 I_n$, la cual es similar a la matriz $[\Phi(g)]_{\mathcal{B}}$, de donde obtenemos que $[\Phi(g)]_{\mathcal{B}}=\epsilon_1 I_n$.

Para cada $g\in \mathrm{Z}(\chi)$, existe $\alpha_g\in\mathbb{C}$ tal que $[\Phi(g)]_{\mathcal{B}}=\alpha_g I_n$. Si $g,h\in \mathrm{Z}(\chi)$, entonces

$$[\Phi(gh)]_{\mathcal{B}}=[\Phi(g)]_{\mathcal{B}}[\Phi(h)]_{\mathcal{B}}=\big(\alpha_g I_n\big)\big(\alpha_h I_n\big)=\alpha_g\alpha_h I_n,$$

lo cual implica que

$$gh\in \mathrm{Z}(\chi)$$

y, en consecuencia, $\mathrm{Z}(\chi)<G$. Además, $\alpha_{gh}=\alpha_g\alpha_h$, con lo cual la función λ dada por la correspondencia $g\longmapsto\alpha_g$ es un homomorfismo de $\mathrm{Z}(\chi)$ en $\mathbb{C}^*$. Si W es un espacio de dimensión 1, $\mathrm{End}(W)=\mathbb{C}^*$ y, de aquí que, λ sea un caracter de $\mathrm{Z}(\chi)$ que, además, satisface $\chi(g)=\alpha_g n=\lambda(g)n,\ \forall\ g\in \mathrm{Z}(\chi)$.

Para obtener 4), notamos en primer lugar que en vista de 3) $\ker\chi=\ker\lambda$ y, aplicando el Primer Teorema de Isomorfismo, $\mathrm{Z}(\chi)/\ker\chi$ es isomorfo a un subgrupo finito de $\mathbb{C}^*$; como éste último es necesariamente cíclico, obtenemos 4).

Para demostrar 5), tomemos $g\in \mathrm{Z}(\chi)$ y $h\in G$, entonces tenemos que

$$[\Phi([g,h])]_{\mathcal{B}}=\big(\alpha_g^{-1}I_n\big)[\Phi(h^{-1})]_{\mathcal{B}}\big(\alpha_g I_n\big)[\Phi(h)]_{\mathcal{B}}=I_n,$$

con lo cual

$$\chi([g,h]) = n \quad \text{y} \quad [g,h] \in \ker\chi.$$

Por lo tanto, $g\ker\chi \in \mathrm{Z}(G/\ker\chi)$, y al ser g arbitrario en $\mathrm{Z}(\chi)$, obtenemos 5).

Supongamos ahora que χ es irreducible. Sea $g\ker\chi \in \mathrm{Z}(G/\ker\chi)$, entonces

$$\forall\ h\in G, \quad [g,h]\in\ker\chi = G\cap\mathrm{Ker}\Phi \quad \Rightarrow \quad \forall\ h\in G, \quad [\Phi([g,h])]_{\mathcal{B}} = I_n$$
$$\Rightarrow \quad [\Phi(g)]_{\mathcal{B}} \in \mathrm{Z}([\Phi(G)]_{\mathcal{B}}) \quad \Rightarrow \quad \Phi(g) \in \mathrm{Z}(\Phi(G)).$$

Por lo tanto, si $v\in V$ y $h\in G$ se cumple que

$$\Phi_g(h\cdot v) = (\Phi_g\circ\Phi_h)(v) = (\Phi_h\circ\Phi_g)(v) = h\cdot\Phi_g(v),$$

lo cual implica que

$$\Phi(g) \in \mathrm{End}_{\mathbb{C}[G]}(V).$$

Como $\mathbb{C}$ es algebraicamente cerrado, por la Proposición 1.1.6, $\mathrm{End}_{\mathbb{C}[G]}(V) = \mathbb{C}\cdot id_V$ y, por lo tanto, $[\Phi(g)]_{\mathcal{B}}$ es diagonal. Aplicando 1), obtenemos que $g\in \mathrm{Z}(\chi)$. □

Discutimos ahora una importante relación entre un caracter y el centro de $G[\mathbb{C}]$.

1.2.21 Proposición
Si $\chi \in Irr(G)$ existe un único homomorfismo $\Gamma_\chi : \mathrm{Z}(\mathbb{C}[G]) \to \mathbb{C}$ tal que si $\Phi : \mathbb{C}[G] \to \mathrm{End}(V)$ es cualquier representación aportando χ entonces:

$$\Phi(a) = \Gamma_\chi(a)\, id_V, \qquad \forall\ a \in \mathrm{Z}(\mathbb{C}[G]).$$

Demostración. Primeramente tomemos una representación Φ que aporte χ y sea $a \in \mathrm{Z}(\mathbb{C}[G])$. Si $b \in \mathbb{C}[G]$, entonces:

$$\Phi_a\circ\Phi_b = \Phi(ab) = \Phi(ba) = \Phi_b\circ\Phi_a$$

$$\Rightarrow \qquad \Phi_a(b\cdot v) = [\Phi_a\circ\Phi_b](v) = [\Phi_b\circ\Phi_a](v) = b\cdot\Phi_a(v).$$

Para cualquiera $v \in V$. Por lo tanto $\Phi_a \in \mathrm{End}_{\mathbb{C}[G]}(V)$, como V es un $\mathbb{C}[G]$-módulo irreducible por 1.1.6 concluimos que existe $\alpha_a \in \mathbb{C}$ tal que $\Phi_a = \alpha_a\, id_V$, así que es lógico definir:

$$\Gamma_\chi(a) = \alpha_a$$

Así, si $b \in \mathrm{Z}(\mathbb{C}[G])$ tendremos:

$$\Gamma_\chi(ab)\, id_V = \Phi(ab) = \Phi_a\circ\Phi_b = (\Gamma_\chi(a)\, id_V)\circ(\Gamma_\chi(b)\, id_V) = \Gamma_\chi(a)\Gamma_\chi(b)\, id_V$$

$$\Rightarrow \Gamma_\chi(ab) = \Gamma_\chi(a)\Gamma_\chi(b).$$

De donde se sigue que $\Gamma_\chi : \mathrm{Z}(\mathbb{C}[G]) \to \mathbb{C}^*$ es un homomorfismo.

Ahora, supongamos que Ψ es una representación sobre algún módulo W la cual también aporta χ, entonces por 1.2.11 Φ y Ψ son similares lo cual significa que existe $f \in \mathrm{Hom}(W, V)$ biyectivo y tal que:

$$\Psi(a) = f^{-1}\Phi(a)f$$

$$\Rightarrow \qquad \Psi(a) = f^{-1} \circ (\Gamma_\chi(a)\, id_V) \circ f = \Gamma_\chi(a)\, f^{-1} id_V f = \Gamma_\chi(a)\, id_V.$$

□

Siguiendo la notación de 1.2.8 sabemos que $K_1, \ldots, K_n$ es una base para $\mathrm{Z}(\mathbb{C}[G])$ y por lo tanto nos interesa calcular $\Gamma_\chi(K_i)$, para esto sea Ψ una representación aportando χ como

$$\Psi(K_i) = \Gamma_\chi(K_i)\, id_V \quad \text{y}$$

$$K_i = \sum_{g \in \mathcal{K}_i} g,$$

tenemos que

$$\Gamma_\chi(K_i)\chi(e) = tr(\Psi(K_i)) = \sum_{g \in \mathcal{K}_i} tr(\Psi(g)) = |\mathcal{K}_i|\chi(g)$$

$$\Rightarrow \qquad \Gamma_\chi(K_i) = \frac{\chi(g)|\mathcal{K}_i|}{\chi(e)}, \qquad g \in \mathcal{K}_i. \tag{1.3}$$

Por lo tanto solo necesitamos los valores de χ. Con ayuda de las funciones Γ_χ podemos demostrar la importante relación entre $\mathrm{CL}[G]$ y $\mathrm{X}(G)$.

1.2.22 Proposición
Sean $\mathcal{K}_1, \mathcal{K}_2, \ldots, \mathcal{K}_r$ las clases de conjugación de un grupo G, K_1, $K_2, \ldots, K_r$ las sumas correspondientes en $\mathbb{C}[G]$, $g_i \in \mathcal{K}_i$ y $CL[G] = \{K_1, \ldots, K_r\}$. Como $K_iK_j \in \mathrm{Z}(\mathbb{C}[G])$ y $CL[G]$ es una base de éste, existen $a_{ij1}, \ldots, a_{ijr} \in \mathbb{C}$ tales que:

$$K_iK_j = \sum_{m=1}^{r} a_{ijm}K_m. \tag{1.4}$$

Al arreglo:

	K_1	$\cdots$	K_r
K_1	K_1K_1	$\cdots$	K_1K_r
$\vdots$	$\vdots$	$\ddots$	$\vdots$
K_r	K_rK_1	$\cdots$	K_rK_r

Se le conoce como **tabla de multiplicación de clases**, los numeros a_{ijm} cumplen:

$$a_{ijm} = |\{(x,y) \in \mathcal{K}_i \times \mathcal{K}_j : xy = g_m\}| \in \mathbb{Z}^+. \tag{1.5}$$

También se tiene:

$$a_{ijm} = \frac{|\mathcal{K}_i||\mathcal{K}_j|}{|G|} \sum_{\chi \in Irr(G)} \frac{\chi(g_i)\chi(g_j)\overline{\chi(g_m)}}{\chi(e)}. \tag{1.6}$$

Por lo tanto X(G) determina unívocamente los coeficientes a_{ijm} y con estos la tabla de multiplicación de clases.

Demostración. Por como se ha definido la multiplicación en $\mathbb{C}[G]$ la igualdad 1.5 es inmediata . Para demostrar 1.6 sea $\chi \in Irr(G)$ y aplicamos Γ_χ en ambos lados de 1.4 para obtener:

$$\Gamma_\chi(K_i)\Gamma_\chi(K_j) = \sum_{m=1}^{r} a_{ijm}\Gamma_\chi(K_m).$$

Aplicando 1.3 tenemos:

$$\frac{\chi(g_i)\chi(g_j)|\mathcal{K}_i||\mathcal{K}_j|}{\chi(e)^2} = \sum_{m=1}^{r} a_{ijm}\frac{\chi(g_m)|\mathcal{K}_m|}{\chi(e)}.$$

Multiplicando por $\overline{\chi(g_n)}$

$$\frac{\chi(g_i)\chi(g_j)\overline{\chi(g_n)}|\mathcal{K}_i||\mathcal{K}_j|}{\chi(e)} = \sum_{m=1}^{r} a_{ijm}\chi(g_m)\overline{\chi(g_n)}|\mathcal{K}_m|.$$

De donde se sigue que:

$$|\mathcal{K}_i||\mathcal{K}_j| \sum_{\chi \in Irr(G)} \frac{\chi(g_i)\chi(g_j)\overline{\chi(g_n)}}{\chi(e)} = \sum_{m=1}^{r} a_{ijm}|\mathcal{K}_m| \sum_{\chi \in Irr(G)} \chi(g_m)\overline{\chi(g_n)}.$$

Aplicando la segunda relación de ortogonalidad tenemos:

$$|\mathcal{K}_i||\mathcal{K}_j| \sum_{\chi \in Irr(G)} \frac{\chi(g_i)\chi(g_j)\overline{\chi(g_n)}}{\chi(e)} = a_{ijn}|\mathcal{K}_n||\mathrm{C}(g_n)| = a_{ijn}|G|.$$

□

Siguiendo con esta notación demostremos el siguiente resultado.

1.2.23 Proposición
$\Gamma_\chi(K_i)$ *es un entero algebraico*

Demostración. Sea $S = \langle \Gamma_\chi(K_1), \Gamma_\chi(K_1) \ldots, \rangle_{\mathbb{Z}}$, entonces claramente S es cerrado bajo la suma y por la ecuación (1.5) también lo es bajo la multiplicación. Dado que $\Gamma_\chi(\langle e \rangle) = 1$ (por 1.3), entonces S es un subanillo de $\mathbb{C}$ y $\mathbb{Z} \subseteq S \subseteq \mathbb{C}$. Por definici'on S es un $\mathbb{Z}$-módulo finitamente generado y por lo tanto podemos aplicar 1.2.16. □

La proposición 1.2.8 proporciona restricciones sobre el grado de los caracteres irreducibles de G, existen muchas otras restricciones sobre estos. Con ayuda de las funciones Γ_χ y la proposicíon anterior podemos demostrar una de ellos.

1.2.24 Teorema
Si $\chi \in \mathrm{Irr}(G)$, *entonces* $\chi(e) \big| |G|$

Demostración. De nuevo retomemos la notación de 1.2.8. Sea $g_1, \ldots, g_n \in G$ un conjunto completo de representantes de clase, aplicando la igualdad 1.3 (pag 29) a la primera relación de ortogonalidad tenemos:

$$|G| = \sum_{i=1}^{n} |\mathcal{K}_i| \chi(g_i)\chi(g_i^{-1}) = \sum_{i=1}^{n} \chi(e)\Gamma_\chi(K_i)\chi(g_i^{-1})$$

$$\Rightarrow \qquad \frac{|G|}{\chi(e)} = \sum_{i=1}^{n} \Gamma_\chi(K_i)\chi(g_i^{-1}).$$

Así que $|G|/\chi(e) \in E \cap \mathbb{Q}$ aplicando 1.2.16 obtenemos $|G|/\chi(e) \in \mathbb{Z}$. □

1.3. Construcción de Caracteres

En esta sección estudiaremos algunos métodos para construir caracteres sin una representación.

1.3.1 Proposición
Supongamos que $N \triangleleft G$, *sean:*

$$\mathcal{A} = \{\chi \in Ch(G/N)\} \quad \text{y}$$

$$\mathcal{B} = \{\chi \in Ch(G) : N \subseteq ker\chi\}$$

Si $\chi \in \mathcal{A}$ *y definimos:*

$$\hat{\chi}(g) = \chi(gN) \quad \text{para } g \in G,$$

entonces $\hat{\chi} \in \mathcal{B}$. *Recíprocamente, si* $\hat{\chi} \in \mathcal{B}$ *y tomamos:*

$$\chi(gN) = \hat{\chi}(g),$$

entonces $\chi \in \mathcal{A}$. *Además:*

$$\langle \chi, \chi \rangle = \langle \hat{\chi}, \hat{\chi} \rangle .$$

En particular $\hat{\chi} \in \mathrm{Irr}(G)$ *si y solo si* $\chi \in \mathrm{Irr}(G/N)$ *y por lo tanto:*

$$\mathrm{Irr}(G/N) = \{\chi : \hat{\chi} \in \mathrm{Irr}(G), N \subseteq ker\chi\}.$$

Demostración. Sea $\chi \in \mathcal{A}$ y Φ una representación de G/N que aporte χ. Definimos:

$$\Phi' : G \to Hom(V), \qquad \text{por} \qquad \Phi'(g) = \Phi(gN)$$

Obtenemos así una representación de $\mathbb{C}[G]$ sobre V la cual claramente aporta como caracter a $\hat{\chi}$. Además, si $g \in N$:

$$\Phi'(g) = \Phi(N) = \Phi'(e) \qquad \Rightarrow \qquad \hat{\chi}(g) = \hat{\chi}(e),$$

es decir $g \in ker\hat{\chi}$ y como g es un elemento arbitrario en N tenemos $N \subseteq Ker\hat{\chi}$. Por lo tanto $\hat{\chi} \in \mathcal{B}$, lo cual demuestra la primera parte.

Ahora, si $\Psi : G \to \mathrm{End}(W)$ es una representación de $\mathbb{C}[G]$ que aporta el caracter $\hat{\chi} \in \mathcal{B}$ y $gN = g'N \in G/N$, entonces:

$$g^{-1}g' \in N \qquad \Rightarrow \qquad g^{-1}g' \in Ker\hat{\chi}.$$

Pero en vista de 1.2.19 $\ker\hat{\chi} \subseteq \mathrm{Ker}\Psi$ y por lo tanto:

$$\Psi(g^{-1}g') = id_W \qquad \Rightarrow \qquad \Psi(g)^{-1}\Psi(g') = \Psi(g^{-1})\Psi(g') = \Psi(g^{-1}g') = id_W$$

$$\Rightarrow \qquad \Psi(g) = \Psi(g').$$

Asi que podemos definir $\Psi'(gN) = \Psi(g)$. Para obtener una representación de G/N la cual aporta el caracter $\chi \in \mathcal{A}$. Por último:

$$\langle \hat{\chi}, \hat{\chi} \rangle = \frac{1}{|G|} \sum_{g \in G} |\hat{\chi}(g)|^2 = \frac{1}{|G|} \sum_{g \in G} |\chi(gN)|^2.$$

Ahora, $G = \bigcup_{gN \in G/N} gN$. Ya demostramos que χ es constante en gN, por lo tanto:

$$\frac{1}{|G|} \sum_{g \in G} |\chi(gN)|^2 = \frac{|N|}{|G|} \sum_{gN \in G/N} |\chi(gN)|^2 = \langle \chi, \chi \rangle .$$

□

Cabe mencionar que normalmente no se hace ninguna distinción entre χ y $\hat{\chi}$, simplemente se diferencian con solo escribir $\chi(g)$ o $\chi(gN)$ según sea el caso. Este resultado puede parecer trivial pero en realidad es muy útil cuando intentamos encontrar caracteres en grupos no simples.

Supongamos que $N \triangleleft G$ y sea ρ la representación regular de G/N, entonces $\mathrm{Ker}\rho = N/N$. Siguiendo la notación anterior ρ' es una representación de G tal que $\mathrm{Ker}\rho' = N$, si ϕ es el caracter aportado por ρ' entonces de acuerdo con la proposición 1.2.19

$$N = \bigcap\{ker\chi : \chi \in \mathrm{Irr}(G/N)\}.$$

Aplicando el resultado anterior tenemos:

$$N = \bigcap\{\ker\chi : \chi \in \mathrm{Irr}(G),\ N \subseteq \ker\chi\}. \tag{1.7}$$

Así, todos los subgrupos normales de G se construyen a partir de la familia $\{\ker\chi : \chi \in \mathrm{Irr}(G)\}$ y de aquí que un grupo sea simple si y solo si $\ker\chi = \langle e\rangle$ o $G\ \forall\, \chi \in \mathrm{Irr}(G)$.

1.3.2 Teorema
Si G es un grupo y $G' = [G, G]$, entonces:

1) $\mathrm{Irr}(G/G') = \mathrm{Lin(G)}$.

2) $G' = \bigcap\{\ker\lambda : \lambda \in \mathrm{Lin}(G)\}$.

3) $[G : G'] = |\mathrm{Lin(G)}|$.

Demostración. Por 1.3.1 tenemos que $\mathrm{Irr}(G/G') \subseteq \mathrm{Irr}(G)$, pero G/G' es abeliano por lo tanto según 1.2.9 $\mathrm{Irr}(G/G')$ consta solo de caracteres lineales y por lo tanto $\mathrm{Irr}(G/G') \subseteq \mathrm{Lin}(G)$. Sea ahora $\lambda \in \mathrm{Lin}(G)$, entonces λ es un homomorfismo de G en $\mathbb{C}$ así que $G' \subseteq \ker\lambda$, por la proposición anterior $\lambda \in \mathrm{Irr}(G/G')$, con lo cual queda demostrado 1).

De la ecuación (1.7)

$$G' = \bigcap\{\ker\chi : \chi \in \mathrm{Irr}(G),\ G' \subseteq \ker\chi\}$$

Pero $G' \subseteq \ker\chi$ equivale según 1.3.1 a que $\chi \in \mathrm{Irr}(G/G') = \mathrm{Lin}(G')$ y por lo tanto a que $\chi \in \mathrm{Lin}(G)$. Además al ser G/G' abeliano por 1.2.9 tenemos:

$$[G : G'] = |G/G'| = |\mathrm{Irr}(G/G')| = |\mathrm{Lin}(G)|$$

□

Una herramienta muy usada en la teoría de grupos son las acciones de un grupo, por esto es importante el siguiente concepto.

1.3.3 Teorema
Supongamos que un grupo G actua en un conjunto no vacio Ω, entonces la función $\vartheta(g) = |\{x \in \Omega : x^g = x\}|$ es un caracter de G. A ϑ se le llama el ***caracter asociado a la acción de*** *G* ***en*** *Ω*

Demostración. Sea V el conjunto de sumas formales de la forma:

$$\sum_{x\in G} \alpha_x x \qquad \text{con} \quad \alpha_x \in \mathbb{C} \ \forall \ x \in \Omega.$$

Claramente V es un espacio vectorial (con las operaciones usuales) y Ω una base de éste. Definimos una acción de G en V por:

$$g \cdot \sum_{x\in G} \alpha_x \, x = \sum_{x\in G} \alpha_x \, x^g.$$

Si extendemos esta operación linealmente a $\mathbb{C}[G]$ hacemos de V un $\mathbb{C}[G]$-módulo. Tomemos $\Omega = \{x_1, \ldots, x_n\}$ y sea Λ la representación de $\mathbb{C}[G]$ sobre V correspondiente a esta acción, entonces:

$$[\Lambda_g]_\Omega = (a_{ij}^g) \in \mathcal{M}_n(\mathbb{C}).$$

Donde $a_{ij}^g = 1$ si ${x_j}^g = x_i$, y $a_{ij}^g = 0$ en otro caso. Por lo tanto:

$$tr([\Lambda_g]_\Omega) = \sum_{i=1}^{n} a_{ii}^g = \sum_{x_i^g = x_i} 1 = |\{x_i : x_i^g = x_i\}| = \vartheta(g).$$

□

Otra manera de construir un caracter fue descrita en 1.2.10 donde se demostró que la suma de dos caracteres es de nuevo un caracter. Esto motiva la pregunta ¿el producto de dos caracteres es también un caracter?

1.3.4 Teorema
Sean G un grupo y $\chi, \psi \in Ch(G)$, entonces $\chi\psi \in Ch(G)$.

Demostración. Supongamos que $\Phi : \mathbb{C}[G] \to \mathrm{End}(V)$ y $\Psi : \mathbb{C}[G] \to \mathrm{End}(W)$ son dos representaciones de G que aportan χ y ϕ respectivamente.

Tomemos $\mathcal{B} = \{v_1, \ldots, v_n\}$ y $\mathcal{B}' = \{w_1, \ldots, w_m\}$ cualesquiera bases de V y W, definimos nm simbolos formales $v_i \otimes w_j$ y el conjunto:

$$V \otimes W = \Big\{ \sum_{i,j} \alpha_{ij}\ v_i \otimes w_j : \alpha_{ij} \in \mathbb{C} \Big\}.$$

Al cual llamamos producto tensorial de V y W, si $v = \sum a_i v_i$ y $w = \sum b_j w_j$, entonces definimos:

$$v \otimes w = \sum_{i,j} a_i b_j\ v_i \otimes w_j.$$

Es bien sabido que $V \otimes W$ es un espacio vectorial sobre $\mathbb{C}$, para dar a éste la estructura de $\mathbb{C}[G]$-módulo primeramente notamos que si $g \in G$, entonces $gv_i \in V$ y $gw_j \in W$; por lo tanto tiene sentido definir:

$$g \cdot (v_i \otimes w_j) = gv_i \otimes gw_j.$$

Recuerdese que $gv = \Phi_g(v)\ \forall\ v \in V$, y $gw = \Psi_g(w)\ \forall\ w \in W$.

Extendiendo linealmente a $V \otimes W$ obtenemos que si $\omega = \sum_{i,j} \alpha_{ij}\ v_i \otimes w_j$:

$$g \cdot \omega = \sum_{i,j} \alpha_{ij}\ gv_i \otimes gw_j.$$

Finalmente si extendemos este producto linealmente a $\mathbb{C}[G]$ y tomamos:

$$a = \sum_{g \in G} a_g g \in \mathbb{C}[G].$$

Definimos

$$a \cdot \omega = \sum_{g \in G} a_g\ g \cdot \omega. \tag{1.8}$$

Primeramente notemos que:

$$e \cdot \omega = \sum_{i,j} \alpha_{ij}\ ev_i \otimes ew_j = \sum_{i,j} \alpha_{ij}\, v_i \otimes w_j = \omega.$$

Para demostrar que con esta operación $V \otimes W$ es un $\mathbb{C}[G]$-módulo introducimos la siguiente notación:

$$gv_i = \sum_r \xi_{ir}^g\, v_r$$

$$gw_j = \sum_s \zeta_{js}^g\, w_s$$

Así:

$$gv_i \otimes gw_j = \sum_{r,s} \xi_{ir}^{g}\, \zeta_{js}^{g}\, v_r \otimes w_s$$

$$\Rightarrow \quad g \cdot \omega = \sum_{r,s} \Big(\sum_{i,j} \alpha_{ij} \xi_{ir}^{g} \zeta_{js}^{g} \Big) v_r \otimes w_s.$$

Si $g' \in G$, entonces:

$$g' \cdot (g \cdot \omega) = \sum_{r,s} \Big(\sum_{i,j} \alpha_{ij} \xi_{ir}^{g} \zeta_{js}^{g} \Big) g' v_r \otimes g' w_s$$

$$= \sum_{r,s} \Big(\sum_{i,j} \alpha_{ij} \xi_{ir}^{g} \zeta_{js}^{g} \Big) \sum_{r',s'} \xi_{rr'}^{g'}\, \zeta_{ss'}^{g'}\, v_{r'} \otimes w_{s'}$$

$$= \sum_{r',s'} \Big(\sum_{i,j,r,s} \alpha_{ij}\, \xi_{ir}^{g}\, \zeta_{js}^{g}\, \xi_{rr'}^{g'}\, \zeta_{ss'}^{g'} \Big) v_{r'} \otimes w_{s'}.$$

Por otra parte:

$$(g'g)v_i = g'(gv_i) = g'\Big(\sum_{r} \xi_{ir}^{g}\, v_r \Big) = \sum_{r} \xi_{ir}^{g}\, g' v_r$$

$$= \sum_{r} \xi_{rr}^{g} \Big(\sum_{r'} \xi_{rr'}^{g'}\, v_{r'} \Big) = \sum_{r'} \Big(\sum_{r} \xi_{ir}^{g}\, \xi_{rr'}^{g'} \Big) v_{r'}.$$

Similarmente:

$$(g'g)w_j = \sum_{s'} \Big(\sum_{s} \zeta_{js}^{g} \zeta_{ss'}^{g'} \Big) w_{s'}.$$

Por lo tanto:

$$(g'g)v_i \otimes (g'g)w_j = \sum_{r',s'} \Big(\sum_{r,s} \xi_{ir}^{g}\, \xi_{rr'}^{g'} \zeta_{js}^{g} \zeta_{ss'}^{g'} \Big) v_{r'} \otimes w_{s'}$$

$$\Rightarrow \quad (g'g) \cdot \omega = \sum_{i,j} \alpha_{ij}\ (g'g)v_i \otimes (g'g)w_j = \sum_{r',s'} \Big(\sum_{i,j,r,s} \alpha_{ij}\, \xi_{ir}^{g}\, \xi_{rr'}^{g'} \zeta_{js}^{g} \zeta_{ss'}^{g'} \Big) v_{r'} \otimes w_{s'}.$$

Entonces:

$$g' \cdot (g \cdot \omega) = (g'g) \cdot \omega \qquad \forall\ g', g \in G, \ \ \forall\ \omega \in V \otimes W \tag{1.9}$$

Ahora, si $\omega' = \sum_{i,j} \alpha'_{ij} v_i \otimes w_j$ tenemos:

$$g \cdot (\omega + \omega') = g\Big(\sum_{i,j} (\alpha_{ij} + \alpha'_{ij}) v_i \otimes w_j \Big) = \sum_{i,j} (\alpha_{ij} + \alpha'_{ij}) g v_i \otimes g w_j = g \cdot \omega + g \cdot \omega'.$$

Es decir:

$$g \cdot (\omega + \omega') = g \cdot \omega + g \cdot \omega' \qquad \forall\ g \in G, \ \ \forall\ \omega, \omega' \in V \otimes W. \tag{1.10}$$

Además si $\alpha \in \mathbb{C}$, entonces:

$$g \cdot (\alpha\, \omega) = g\Big(\sum_{i,j} \alpha\alpha_{ij}\ v_i \otimes w_j \Big) = \sum_{i,j} \alpha\alpha_{ij}\ gv_i \otimes gw_j = \alpha(g \cdot \omega).$$

Por lo tanto:

$$g \cdot (\alpha\, \omega) = \alpha(g \cdot \omega) \qquad \forall\ \alpha \in \mathbb{C}, \quad \forall\ g \in G, \quad \forall\ \omega \in V \otimes W. \tag{1.11}$$

Asi, si tomamos $b = \sum_{g\in G} b_g g \in \mathbb{C}[G]$ y $\alpha \in \mathbb{C}$ tenemos:

$$\begin{aligned}
(a+b)\cdot w &= \sum_{g\in G} (a_g + b_g)\ g \cdot w = \sum_{g\in G} \big(a_g\, g\cdot w + b_g\, g \cdot w\big) \\
&= a \cdot \omega + b \cdot \omega.
\end{aligned}$$

$$\begin{aligned}
(\alpha a)\cdot \omega &= \sum_{g\in G} (\alpha a_g)\ g \cdot \omega \\
&= \sum_{g} a_g\ g \cdot (\alpha\omega) = a \cdot (\alpha\omega) && \text{por 1.11} \\
&= \alpha\Big(\sum_{g} a_g\ g \cdot \omega \Big) = \alpha(a \cdot \omega).
\end{aligned}$$

$$\begin{aligned}
a(\omega + \omega) &= \sum_{g\in G} a_g\ g \cdot (\omega + \omega) = \sum_{g} a_g (g \cdot \omega + g \cdot \omega') && \text{por 1.10} \\
&= a \cdot \omega + a \cdot \omega'.
\end{aligned}$$

$$\begin{aligned}
a \cdot (b \cdot w) &= \sum_{g\in G} a_g\ g \cdot (b \cdot w) && \text{por 1.8} \\
&= \sum_{g} a_g\ g \cdot \Big(\sum_{g'\in G} b_{g'}\ g' \cdot \omega \Big) && \text{por 1.8} \\
&= \sum_{g} a_g\ \Big(\sum_{g'} g \cdot (b_{g'} g' \cdot \omega) \Big) && \text{por 1.10} \\
&= \sum_{g} a_g\ \Big(\sum_{g'} b_{g'} g \cdot (g' \cdot \omega) \Big) && \text{por 1.11} \\
&= \sum_{g} a_g\ \Big(\sum_{g'} b_{g'} (gg') \cdot \omega \Big) && \text{por 1.9} \\
&= \sum_{g,g'} a_g b_{g'} (gg') \cdot \omega = (ab) \cdot \omega.
\end{aligned}$$

Así, hemos logrado hacer de $V \otimes W$ un $\mathbb{C}[G]$-módulo. Si Λ es la representación de $\mathbb{C}[G]$ sobre este:

$$\Lambda_g(\omega) = g \cdot \omega.$$

Como $\mathcal{B} \otimes \mathcal{B}' = \{v_1 \otimes w_1, \ldots, v_1 \otimes w_m, \ldots, v_n \otimes w_m\}$ es una base de $V \otimes W$ y:

$$\Lambda_g(v_i \otimes w_j) = \sum_{r,s} \xi_{ir}^g \, \zeta_{js}^g \, v_r \otimes w_s.$$

Entonces:

$$[\Lambda_g]_{\mathcal{B}\otimes\mathcal{B}'} = \begin{pmatrix} \xi_{11}^g \zeta_{11}^g & \cdots & \xi_{11}^g \zeta_{m1}^g & \cdots & \xi_{n1}^g \zeta_{m1}^g \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \xi_{11}^g \zeta_{1m}^g & \cdots & \xi_{11}^g \zeta_{mm}^g & \cdots & \xi_{n1}^g \zeta_{mm}^g \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \xi_{1n}^g \zeta_{1m}^g & \cdots & \xi_{1n}^g \zeta_{mm}^g & \cdots & \xi_{nn}^g \zeta_{mm}^g \end{pmatrix} \in \mathcal{M}_{nm}(\mathbb{C}).$$

Por lo tanto:

$$tr(\Lambda_g) = \sum_{i,j} \xi_{ii}^g \zeta_{jj}^g = \left(\sum_{i=1}^{n} \xi_{ii}^g \right) \left(\sum_{j=1}^{m} \zeta_{jj}^g \right) = \chi(g)\phi(g).$$

Lo cual significa que $\chi\phi \in Ch(G)$.

□

El anterior resultado junto con 1.2.10 motiva la siguiente definición.

1.3.5 Definición
A los elementos de $Ch'(G) = \langle \mathrm{Irr}(G) \rangle_{\mathbb{Z}}$ *los llamamos* ***caracteres generalizados****.*

Notemos que $Ch'(G)$ es cerrado bajo la suma y resta. Además si θ es un caracter generalizado de G y $\mathrm{Irr}(G) = \{\chi_1, \ldots, \chi_n\}$, entonces existen $m_1, \ldots, m_n \in \mathbb{Z}$ tales que $\theta = m_1\chi_1 + \cdots + m_n\chi_n$, definamos:

$$\theta_1 = \sum_{m_i > 0} m_i \chi_i \quad \text{y}$$

$$\theta_2 = \sum_{m_i < 0} (-m_i) \chi_i.$$

Entonces $\theta_1, \theta_2 \in Ch(G)$ y $\theta = \theta_1 - \theta_2$, es decir, todo caracter generalizado es la diferencia de dos caracteres. Si tomamos $\varphi \in Ch'(G)$ y $\varphi = \varphi_1 - \varphi_2$, con $\varphi_1, \varphi_2 \in Ch(G)$, entonces:

$$\theta\varphi = (\theta_1\varphi_1 + \theta_2\varphi_2) - (\theta_1\varphi_2 + \theta_2\varphi_1).$$

Por el teorema 1.3.4, $\theta_1\varphi_1, \theta_2\varphi_2, \theta_1\varphi_2, \theta_2\varphi_1 \in Ch(G)$ y por lo tanto $\theta\varphi \in Ch'(G)$, es decir, $Ch'(G)$ es cerrado bajo la multiplicación de donde se sigue que $Ch'(G)$ es un anillo.

Una forma más de obtener un nuevo caracter a partir de uno ya conocido es inspirado por 1.2.14. Si ϕ es un caracter cualquiera, entonces $\langle \phi, \chi \rangle \in \mathbb{Z}^+ \ \forall \ \chi \in \mathrm{Irr}(G)$, por lo tanto:

$$\overline{\langle \phi, \chi \rangle} = \langle \overline{\phi}, \overline{\chi} \rangle \in \mathbb{Z}^+ \ \forall \ \chi \in Irr(G)$$

Por la observación que sigue a 1.2.14 la conjugación permuta $\mathrm{Irr}(G)$, entonces:

$$\langle \overline{\phi}, \chi \rangle \in \mathbb{Z}^+, \quad \forall \ \chi \in \mathrm{Irr(G)}.$$

Aplicando 1.2.10 obtenemos que $\overline{\phi} \in \mathrm{Ch}(G)$. La idea ahora es cambiar la conjugación en $\mathbb{C}$ por la conjugación de Galois. Recordemos que el **exponente de un grupo** es el menor entero positivo n tal que $g^n = e \ \forall \ g \in G$.

1.3.6 Teorema
Sean G un grupo con exponente n, $\mathbb{Q}_n = \mathbb{Q}(e^{2\pi i/n})$ y $\sigma \in Gal(\mathbb{Q}_n/\mathbb{Q})$. Si $\chi \in \mathrm{Ch}(G)$ por 1.2.17 *sabemos que $\chi(g) \in \mathbb{Q}_n \ \forall \ g \in G$. Si definimos χ^σ por:*

$$\chi^\sigma(g) = \sigma(\chi(g)).$$

Entonces $\chi^\sigma \in Ch(G)$. Además, $\langle \chi^\sigma, \chi^\sigma \rangle = \langle \chi, \chi \rangle$, en particular $\chi \in \mathrm{Irr}(G)$ si y solo si $\chi^\sigma \in \mathrm{Irr}(G)$.

Demostración. Denotemos por $\mathbb{E}$ a la cerradura algebraica de $\mathbb{Q}$ en $\mathbb{C}$, así $\mathbb{Q}_n \subset \mathbb{E}$.

Sea $\chi \in Ch(G)$ de grado m y supongamos que podemos encontrar una representación Φ sobre un espacio vectorial V y una base $\mathcal{B}$ de V tales que:

$$[\Phi(g)]_{\mathcal{B}} \in \mathcal{M}_m(\mathbb{E}) \quad \forall \ g \in G.$$

Dado que $\mathbb{E}$ es algebraico sobre $\mathbb{Q}_n$, podemos extender σ a un automorfismo de $\mathbb{E}$ y definir Φ^σ por:

$$[\Phi^\sigma(g)]_{\mathcal{B}} = \sigma([\Phi(g)]_{\mathcal{B}}) \in \mathcal{M}_m(\mathbb{E}) \quad \forall \ g \in G.$$

Así:

$$[\Phi^\sigma(gh)]_{\mathcal{B}} = \sigma([\Phi(gh)]_{\mathcal{B}}) = \sigma([\Phi(g)]_{\mathcal{B}}[\Phi(h)]_{\mathcal{B}})$$

$$= \sigma([\Phi(g)]_{\mathcal{B}})\sigma([\Phi(h)]_{\mathcal{B}}) = [\Phi^\sigma(g)]_{\mathcal{B}}[\Phi^\sigma(h)]_{\mathcal{B}} \quad \forall \ g, h \in G.$$

Entonces $\Phi^\sigma(gh) = \Phi^\sigma(g)\Phi^\sigma(h) \ \forall \ g, h \in G$, y si extendemos linealmente Φ^σ a todo $\mathbb{C}[G]$ tenemos que:

$$\Phi^\sigma(ab) = \Phi^\sigma(a)\Phi^\sigma(b) \ \forall \ a, b \in \mathbb{C}[G].$$

Por lo tanto, Φ^σ es una representación de G sobre V que claramente aporta el caracter χ^σ. Además

$$\langle \chi^\sigma, \chi^\sigma \rangle = \frac{1}{|G|} \sum_{g \in G} \chi^\sigma(g)\overline{\chi^\sigma(g)} = \frac{1}{|G|} \sum_{g \in G} \sigma(\chi(g))\overline{\sigma(\chi(g))} =$$

$$= \frac{1}{|G|} \sum_{g \in G} \sigma(\chi(g)\overline{\chi(g)}) = \sigma(\langle \chi, \chi \rangle) = \langle \chi, \chi \rangle .$$

Para terminar demostraremos que siempre se pueden encontrar tales Φ, V y $\mathcal{B}$.

Supongamos que Φ' es una representación de $\mathbb{C}[G]$ sobre un $\mathbb{E}$-espacio vectorial V'; sean χ' el $\mathbb{E}$-caracter aportado por Φ' y $n = \deg(\Phi') = \chi'(e)$. Tomemos $\mathcal{B}_1 = \{v_1, \ldots, v_n\}$ una base cualquiera de V'. Definimos W como el conjunto de sumas formales $\sum \alpha_i v_i$, donde $\alpha_i \in \mathbb{C}$, entonces W es un $\mathbb{C}$-espacio vectorial con base $\mathcal{B}_1$ y por lo tanto de dimensión $|\mathcal{B}_1| = n$, además podemos considerar que $V' \subset W$. Si $a \in \mathbb{C}[G]$ definimos $\Psi'_a \in \mathrm{End}(W)$ por:

$$\Psi'_a\Big(\sum \alpha_i v_i\Big) = \sum_{i=1}^{n} \alpha_i \, \Phi'_a(v_i).$$

Notemos que la parte derecha esta bien definida ya que $\Phi'_a \in \mathrm{End}(V)$ y por lo tanto $\Phi'_a(v_i) \in W \ \forall \ i$. Así, Ψ' dada por $\Psi'(a) = \Psi'_a$ es una $\mathbb{C}$-representación de $\mathbb{C}[G]$ sobre el $\mathbb{C}$-espacio vectorial W. Dado que $\Psi'_a(v_i) = \Phi'_a(v_i) \ \forall \ i$, entonces:

$$[\Psi'_a]_{\mathcal{B}_1} = [\Phi'_a]_{\mathcal{B}_1} \ \forall \ a \in \mathbb{C}[G]$$

$$\Rightarrow \quad tr([\Psi'_g]_{\mathcal{B}_1}) = tr([\Phi'_g]_{\mathcal{B}_1}) = \chi'(g) \ \forall \ g \in G.$$

Así, χ' es un $\mathbb{C}$-caracter. Ahora, la cantidad de distintos $\mathbb{E}$-caracteres es según 1.2.8 igual a la $|\mathrm{Irr}(G)|$ (recuerdese que todo lo dicho sobre $\mathbb{C}$-caracteres es válido para F-caracteres cuando F es algebraicamente cerrado y de característica cero), por lo tanto todo $\mathbb{C}$-caracter es también un $\mathbb{E}$-caracter con lo cual termina la demostración.

□

Este resultado es útil cuando tenemos un caracter cuyos valores no son todos racionales o mejor dicho enteros (ver 1.2.16). Otro método extremadamente útil es un proceso llamado inducción de caracteres, y es en cierto sentido inverso a la restricción.

Supongamos que $H < G$, claramente $Cl(G)$ y $Cl(H)$ son dos $\mathbb{C}$-espacios vectoriales de Hilbert finito dimensionales; si definimos $R : Cl(G) \to Cl(H)$ como la restricción

de ϑ a H, entonces R es una transformación lineal y por lo tanto existe una unica transformación lineal $I : Cl(H) \to Cl(G)$ (llamada dual de R) tal que:

$$\langle R(\vartheta), \theta \rangle = \langle \vartheta, I(\theta) \rangle \quad \forall\ \vartheta \in Cl(G), \theta \in Cl(H).$$

Cabe aclarar que el producto interno de la izquierda es calculado en H y el de la derecha en G. Sean $R(\vartheta) = \vartheta_H$ e $I(\theta) = \theta^G$, entonces:

$$\langle \vartheta_H, \theta \rangle = \left\langle \vartheta, \theta^G \right\rangle.$$

Esta igualdad es conocida como **Ley de Reciprocidad de Frobenius**. A θ^G se le llama **función de clase inducida**. Lo importante sobre las funciones inducidas es que podemos calcularlas explícitamente.

1.3.7 Teorema
Supongamos que $H < G$ y que $\theta \in Cl(H)$, si $g \in G$ definimos $\theta^o(g) = \theta(g)$ si $g \in H$ y $\theta^o(g) = 0$ si $g \notin G$. Entonces:

$$\theta^G(g) = \frac{1}{|H|} \sum_{x \in G} \theta^o(g^x).$$

Y por lo tanto $\theta^G(e) = [G : H]\theta(e)$.

Demostración. Denotemos por $\widehat{\theta}$ a la función definida por la fórmula de la parte derecha de la igualdad anterior, entonces $\widehat{\theta} \in Cl(G)$ ya que $\forall\ y \in G$:

$$\widehat{\theta}(g^y) = \frac{1}{|H|} \sum_{x \in G} \theta^o(g^{yx}) = \frac{1}{|H|} \sum_{x \in G} \theta^o(g^x) = \widehat{\theta}(g).$$

Ya que yx toma una vez todos los valores de G al ir recorriendo x sobre G.

Sea $\vartheta \in Cl(G)$, entonces:

$$\left\langle \vartheta, \widehat{\theta} \right\rangle = \frac{1}{|G|} \sum_{g \in G} \vartheta(g) \left(\frac{1}{|H|} \sum_{x \in G} \overline{\theta^o(g^x)} \right) = \frac{1}{|G||H|} \sum_{x \in G} \sum_{g \in G} \vartheta(g) \overline{\theta^o(g^x)}.$$

Si $x \in G$ es fijo $(xg)^x = gx$ y por lo tanto:

$$\sum_{g \in G} \vartheta(g) \overline{\theta^o(g^x)} = \sum_{g \in G} \vartheta(xg) \overline{\theta^o(gx)}.$$

Sea $g_1 = gx$, $xg = xg_1x^{-1}$; así $\vartheta(xg) = \vartheta(xg_1x^{-1}) = \vartheta(g_1)$ y:

$$\sum_{g \in G} \vartheta(xg) \overline{\theta^o(gx)} = \sum_{g_1 \in G} \vartheta(g_1) \overline{\theta^o(g_1)} = \sum_{g_1 \in H} \vartheta(g_1) \overline{\theta(g_1)} = |H| \left\langle \vartheta_H, \theta \right\rangle.$$

Sustiyuyendo tenemos que:

$$\left\langle \vartheta, \widehat{\theta}\,\right\rangle = \frac{\left\langle \vartheta_H, \theta\,\right\rangle}{|G|}\sum_{x\in G} 1 = \left\langle \vartheta_H, \theta\,\right\rangle.$$

La función $\theta \to \widehat{\theta}$ es claramente lineal y por la unicidad del operador dual concluimos que $\theta^G = \widehat{\theta}$.

□

Otra forma de calcular θ^G es tomar $g_1, \ldots, g_n \in G$ tales que:

$$G = \dot{\bigcup_i} g_i H.$$

Entonces:

$$\theta^G(g) = \frac{1}{|H|}\sum_{x\in G}\theta^o(g^x) = \frac{1}{|H|}\sum_i\sum_{h\in H}\theta^o(g^{g_i h}).$$

Ahora, si $h \in H$, entonces $g^{g_i h} = h^{-1}(g^{g_i})h \in H$ si y solo si $g^{g_i} \in H$ y por lo tanto $\theta^o(g^{g_i h}) = \theta^o(g_i^g)$, entonces:

$$\theta^G(g) = \sum_{i=1}^{n}\theta^o(g^{g_i}). \tag{1.12}$$

1.3.8 Teorema
Si $H < G$ *y* $\chi \in \mathrm{Ch(H)}$ *entonces* $\chi^G \in \mathrm{Ch(G)}$ *el cual es llamado* ***caracter inducido*** *por* χ.

Demostración. Sea $\phi \in \mathrm{Irr}(G)$, entonces $\phi_H, \chi \in Ch(H)$ y por 1.2.14 $\langle \phi_H, \chi\rangle \in \mathbb{Z}^+$ y por lo tanto $\langle \phi, \chi^G\rangle \in \mathbb{Z}^+$ aplicando 1.2.10 concluimos que $\chi^G \in Ch(G)$.

□

Otra consecuencia inmediata de la definición de un caracter inducido es que si $K < H < G$, entonces:

$$(\chi^H)^G = \chi^G \quad \forall\ \chi \in \mathrm{Ch(K)}.$$

Ya que si $\phi \in \mathrm{Cl}(G)$ entonces:

$$\left\langle (\chi^H)^G, \phi\right\rangle = \left\langle \chi^H, \phi_{\,H}\right\rangle = \langle \chi, \phi_K\rangle = \left\langle \chi^G, \phi\right\rangle.$$

Donde cada igualdad se deduce de la ley de reciprocidad de Frobenius y del hecho de que $(\phi_H)_K = \phi_K$.

Como un ejemplo del teorema anterior tomemos $G = S_3$ y $H = A_3$. Sean $\sigma = (1,2) \notin H$ y $\pi = (1,2,3) \in H$ entonces $G = \langle \sigma, \pi\rangle$ y $H = \langle \pi\rangle$. Ademas $|CL[G]| = 3$ a

saber $K(e) = \{e\}$, $K(\sigma) = \{\sigma, \sigma\pi, \sigma\pi^2\}$ y $K(\pi) = \{\pi, \pi^2\}$. Sea $\chi = 1_H$ y calculemos χ^G tenemos:

$$\chi^G(e) = [S_3 : A_3]\chi(e) = 2.$$

Como $S_3 = A_3 \bigcup \sigma A_3$ aplicando 1.12 tenemos que:

$$\chi^G(\sigma) = \chi^o(\sigma) + \chi^o(\sigma^\sigma) = 0 + 0 = 0.$$

$$\chi^G(\pi) = \chi^o(\pi) + \chi^o(\pi^\sigma) = 1 + 1 = 2.$$

Notemos que si definimos $\phi : G \to \{1, -1\}$ por $\phi(g) = 1$ si $g \in H$ y $\phi(g) = -1$ si $g \notin H$, entonces $\phi \in \mathrm{Hom}(G, \mathbb{C})$ y por lo tanto $\phi \in Lin(G)$ además $\chi^G = 1_G + \phi$. Otro caracter de H se puede definir como:

$$\chi_1(e) = 1, \qquad \chi_1(\pi) = \omega, \qquad \chi_1(\pi^2) = \omega^2, \qquad \omega = e^{2\pi i/3}$$

El cual es un caracter ya que $\chi_1 \in \mathrm{Hom}(H, \mathbb{C})$ pues $|H| = 3$. Usemos 1.12 para calcular χ_1^G :

$$\chi_1^G(e) = [S_3 : A_3]\chi_1(e) = 2,$$

$$\chi_1^G(\sigma) = \chi_1^o(\sigma) + \chi_1^o(\sigma^\sigma) = 0 + 0 = 0,$$

$$\chi_1^G(\pi) = \chi_1^o(\pi) + \chi_1^o(\pi^\sigma) = \omega + \omega^2 = -1.$$

Ahora:

$$\langle \chi_1^G, \chi_1^G \rangle = \frac{1}{6} \sum_{g \in S_3} |\chi_1^G(g)|^2 = \frac{1}{6}(2^2 + 2(-1)^2) = 1$$

Así:

$$\mathrm{Irr}(G) = \{\, 1_G \,,\, \phi \,,\, \chi_1^G \,\}.$$

El siguiente concepto se encuentra íntimamente ligado a los caracteres inducidos.

1.3.9 Definición
Sea $X \subseteq G$ decimos que X es un ***conjunto T.I. (trivial intersection)*** *en G si:*

$$X^g = X \quad o \quad X^g \cap X \subseteq \{e\} \qquad \forall\ g \in G.$$

Los conjuntos T.I. juegan un papel importante en la teoría de caracteres, principalmente en los llamados "Grupos de Frobenius" los cuales no son tratados en este trabajo pero que son fundamentales en la clasificación de Grupos Finitos. Además, los conjuntos T.I. suelen relacionarse con el problema de "extensión" de un caracter, como un ejemplo de esto último tenemos:

1.3.10 Proposición
Sean X un conjunto T.I. en G; $\phi,\ \chi$ funciones de clase en $N = \mathrm{N}_G(X)$. Supongamos que ϕ y χ se anulan en $N - X$ y que $\chi(e) = 0$. Entonces $\langle \phi^G, \chi^G \rangle = \langle \phi, \chi \rangle$, y $\chi^G(x) = \chi(x) \quad \forall\ x \in X$.

Demostración. Primeramente, $\chi^G(e) = [G:N]\chi(e) = 0$, así que tomemos $x \in X - e$. Si $\chi^0(yxy^{-1}) \neq 0,\ e \neq yxy^{-1} \in X \cap X^{y^{-1}}$, entonces $X = X^{y^{-1}}$ y por lo tanto $y \in N$. Así:

$$\chi^G(x) = \frac{1}{|N|} \sum_{y \in G} \chi^0(yxy^{-1}) = \frac{1}{|N|} \sum_{y \in N} \chi^0(x) = \chi(x).$$

Luego, $\chi^G(x) = \chi(x) \quad \forall\ x \in X$. También, $\langle \phi^G, \chi^G \rangle = \langle \phi, (\chi^G)_N \rangle$. Como ϕ se anula en $N - X$ y $(\chi^G)_N - \chi$ se anula en X, $\langle \phi, (\chi^G)_N - \chi \rangle = 0$ de donde se obtiene el resultado.

□

Capítulo 2

Algunas aplicaciones de la teoría

2.1. . . . en conmutadores

En esta sección presentaremos los teoremas de Gallagher y Burnside en caracteres y conmutadores. Todo lo expuesto desde aquí y hasta el Teorema 2.1.7 fue publicado por Gallagher en [7]

2.1.1 Proposición
Sea $\chi \in \mathrm{Irr}(G)$ *entonces:*

$$e_\chi = \frac{\chi(e)}{|G|} \sum_{g \in G} \overline{\chi(g)} g \in \mathrm{Z}(\mathbb{C}[G])$$

$$\text{y} \quad e_\chi^2 = e_\chi.$$

Demostración. Sean $\mathcal{K}_i, \ldots, \mathcal{K}_n$ y $K_1, \ldots, K_n$ como en 1.2.8 ,si $g_i \in \mathcal{K}_n$ entonces:

$$\sum_{g \in G} \overline{\chi(g)} g = \sum_{i=1}^{n} \overline{\chi(g_i)} \sum_{g \in \mathcal{K}_i} g = \sum_{i=1}^{n} \overline{\chi(g_i)} K_i.$$

Por lo tanto $e_\chi \in \mathrm{Z}(\mathbb{C}[G])$. Además:

$$e_\chi^2 = \frac{\chi(e)^2}{|G|^2} \left(\sum_{i=1}^{n} \overline{\chi(g_i)} K_i \right) \left(\sum_{i=1}^{n} \overline{\chi(g_i)} K_i \right) = \frac{\chi(e)^2}{|G|^2} \sum_{i=1}^{n} \sum_{j=1}^{n} \overline{\chi(g_i)}\, \overline{\chi(g_j)} K_i K_j.$$

Según 1.2.22:

$$e_\chi^2 = \frac{\chi(e)^2}{|G|^2} \sum_{i=1}^{n} \sum_{j=1}^{n} \sum_{m=1}^{n} \sum_{\phi \in \mathrm{Irr}(G)} \frac{|\mathcal{K}_i||\mathcal{K}_j| \overline{\chi(g_i)}\, \overline{\chi(g_j)} \phi(g_i) \phi(g_j) \overline{\phi(g_m)}}{|G| \phi(e)} K_m$$

$$= \frac{\chi(e)^2}{|G|} \sum_m \sum_\phi \left(\frac{1}{|G|} \sum_i \phi(g_i)\overline{\chi(g_i)}|\mathcal{K}_i| \right) \left(\frac{1}{|G|} \sum_j \phi(g_j)\overline{\chi(g_j)}|\mathcal{K}_j| \right) \frac{\overline{\phi(g_m)}}{\phi(e)} K_m.$$

Como $\phi(g)\overline{\chi(g)}$ es constante para $g \in K_i$, la primera relación de ortogonalidad nos dice que:

$$\frac{1}{|G|} \sum_{i=1}^{n} \phi(g_i)\overline{\chi(g_i)}|\mathcal{K}_i| = \delta_{\phi\chi}.$$

Por lo tanto, dado que $\delta_{\phi\chi}^2 = \delta_{\phi\chi}$ tenemos:

$$e_\chi^2 = \frac{\chi(e)^2}{|G|} \sum_{m=1}^{n} \left[\sum_\phi \frac{\overline{\phi(g_m)}}{\phi(e)} \delta_{\phi\chi} \right] K_m = \frac{\chi(e)^2}{|G|} \sum_{m=1}^{n} \frac{\overline{\chi(g_m)}}{\chi(e)} K_m = e_\chi.$$

□

2.1.2 Proposición
$\forall\ n \in \mathbb{N}$ y $g \in G$:

$$\sum_{g_1 \cdots g_n = g} \chi(g_1) \cdots \chi(g_n) = \chi(g) \left(\frac{|G|}{\chi(e)} \right)^{n-1}.$$

Demostración. Tomemos $G = \{h_1, \ldots, h_m\}$, entonces:

$$e_\chi^n = \left[\frac{\chi(e)}{|G|} \sum_{i=1}^{n} \overline{\chi(h_i)} h_i \right]^n = \left[\frac{\chi(e)}{|G|} \right]^n \sum_{i_1=1}^{m} \cdots \sum_{i_n=1}^{m} \overline{\chi(h_{i_1})} \cdots \overline{\chi(h_{i_n})} h_{i_1} \cdots h_{i_n}.$$

Reescribiendo la última expresión y usando el hecho de que $e_\chi^n = 1$ tenemos:

$$\frac{\chi(e)}{|G|} \sum_{g \in G} \overline{\chi(g)} g = \left[\frac{\chi(e)}{|G|} \right]^n \sum_{g_1 \cdots g_n = g} \overline{\chi(g_1)} \cdots \overline{\chi(g_n)} g.$$

El resultado final de obtiene comparando coeficientes.

□

2.1.3 Proposición
Si $\chi \in \mathrm{Irr}(G)$; $\forall\ g, h \in G$ se cumple:

$$\sum_{t \in G} \chi(g[t,h]) = \frac{|G|}{\chi(e)} \chi(gh)\overline{\chi(h)}.$$

Demostración. Sean $s \in G$, $\mathcal{K}_s = CL(s)$ y K_s la suma de la clase $\mathcal{K}_s$. Entonces:

$$K_s = \frac{1}{|\mathrm{C}_G(s)|} \sum_{t \in G} s^t.$$

Retomemos las funciones Γ_χ definidas en 1.2.21, $\forall\ x, y \in G$ se cumple:

$$\Gamma_\chi(K_xK_y) = \Gamma_\chi(K_x)\Gamma_\chi(K_y) = \frac{\chi(x)\chi(y)|\mathcal{K}_x||\mathcal{K}_y|}{\chi(e)^2}.$$

Además:

$$K_xK_y = \left(\frac{1}{|\mathrm{C}_G(x)|}\sum_{t\in G} x^t\right)\left(\frac{1}{|\mathrm{C}_G(y)|}\sum_{t\in G} y^t\right) = \frac{1}{|\mathrm{C}_G(x)||\mathrm{C}_G(y)|}\sum_{t_1\in G}\sum_{t_2\in G} x^{t_1}y^{t_2}$$

$$\Rightarrow \chi(K_xK_y) = \frac{1}{|\mathrm{C}_G(x)||\mathrm{C}_G(y)|}\sum_{t_1,t_2}\chi(xy^{t_2t_1^{-1}}).$$

Queremos escribir esta última expresión en una suma sobre solo un elemento de G, sea $t\in G$ fijo ¿De cuantas maneras podemos tomar t_1, t_2 para que $t_2t_1^{-1}=t$? Una vez elegido t_2 solo queda una posibilidad para t_1 y como tenemos $|G|$ formas diferentes de elegir a t_2; por lo tanto:

$$\sum_{t_2t_1^{-1}=t}\chi(xy^{t_2t_1^{-1}}) = |G|\chi(xy^t) \quad \Rightarrow \quad \sum_{t_2,t_1}\chi(xy^{t_2t_1^{-1}}) = |G|\sum_{t\in G}\chi(xy^t).$$

Así:

$$\Gamma_\chi(K_xK_y) = \frac{\chi(K_xK_y)}{\chi(e)} = \frac{|\mathcal{K}_x|\,|\mathcal{K}_y|}{|G|\,\chi(e)}\sum_{t\in G}\chi(xy^t).$$

Comparando las dos expresiones para $\Gamma_\chi(K_xK_y)$ tenemos:

$$\sum_{t\in G}\chi(xy^t) = \frac{|G|}{\chi(e)}\chi(x)\chi(y).$$

Ahora $xy^t = xt^{-1}yt = xt^{-1}yty^{-1}y = x[t,y^{-1}]y$, como x, y son arbitrarios tenemos:

$$\sum_{t\in G}\chi(x[t,y]y^{-1}) = \frac{|G|}{\chi(e)}\chi(x)\chi(y^{-1}).$$

Como $CL(ab) = CL(ba)\ \forall\ a, b \in G$:

$$\sum_{t\in G}\chi(y^{-1}x[t,y]) = \frac{|G|}{\chi(e)}\chi(x)\overline{\chi(y)}.$$

Tomando $y=h$ y $x=hg$ terminamos.

□

2.1.4 Proposición
Si $\chi \in \mathrm{Irr}(G)$*;* $\forall\ g, h_1, \ldots, h_n \in G$ *se cumple:*

$$\sum_{t_1,\ldots,t_n \in G} \chi(g[t_1,h_1]\cdots[t_n,h_n]) = \left(\frac{|G|}{\chi(e)}\right)^n \chi(gh_1\cdots h_n)\overline{\chi(h_1)}\cdots\overline{\chi(h_n)}.$$

Demostración. Procederemos por inducción sobre n. El caso $n=1$ es la proposición 2.1.3, de esta podemos además deducir que si $n>1$ tenemos:

$$\sum_{t_1,\ldots,t_n} \chi(g[t_1,h_1]\cdots[t_n,h_n]) = \sum_{t_1,\ldots,t_{n-1}} \frac{|G|}{\chi(e)}\chi(g[t_1,h_1]\cdots[t_{n-1},h_{n-1}]h_n)\overline{\chi(h_n)}$$

$$= \frac{|G|}{\chi(e)}\left[\sum_{t_1,\ldots,t_{n-1}} \chi(h_n g[t_1,h_1]\cdots[t_{n-1},h_{n-1}])\right]\overline{\chi(h_n)}.$$

Aplicando la hipótesis de inducción:

$$\sum_{t_1,\ldots,t_{n-1}} \chi\big(h_n g[t_1,h_1]\cdots[t_{n-1},h_{n-1}]\big) = \left(\frac{|G|}{\chi(e)}\right)^{n-1} \chi(h_n g h_1\cdots h_{n-1})\overline{\chi(h_1)}\cdots\overline{\chi(h_{n-1})}$$

Por lo tanto:

$$\sum_{t_1,\ldots,t_n} \chi(g[t_1,h_1]\cdots[t_n,h_n]) = \left(\frac{|G|}{\chi(e)}\right)^n \chi(h_n g h_1\cdots h_{n-1})\overline{\chi(h_1)}\cdots\overline{\chi(h_{n-1})}\,\overline{\chi(h_n)}.$$

□

2.1.5 Proposición
Si $\chi \in \mathrm{Irr}(G)$*;* $\forall\ g \in G$*:*

$$\sum_{a_1,\ldots,a_n,b_1,\ldots,b_n \in G} \chi(g[a_1,b_1]\cdots[a_n,b_n]) = \left(\frac{|G|}{\chi(e)}\right)^{2n} \chi(g).$$

Demostración. Por el resultado anterior tenemos:

$$\sum \chi(g[a_1,b_1]\cdots[a_n,b_n]) = \left(\frac{|G|}{\chi(e)}\right)^n \sum_{b_1,\ldots,b_n \in G} \chi(gb_1\cdots b_n)\chi(b_1^{-1})\cdots\chi(b_n^{-1}).$$

Si tomamos cualesquiera $s_1, \cdots, s_n \in G$ estos determinan un único elemento $s_0 \in G$ tal que $s_0 s_n \cdots s_1 = g$, por lo tanto:

$$\sum_{b_1,\ldots,b_n} \chi(gb_1\cdots b_n)\chi(b_n^{-1})\cdots\chi(b_1^{-1}) = \sum_{s_0 s_n\cdots s_1 = g} \chi(s_0)\chi(s_n)\cdots\chi(s_1) = \left(\frac{|G|}{\chi(e)}\right)^n \chi(g).$$

□

2.1.6 Teorema
Si n es tal que:

$$\sum_{\chi\in \mathrm{Irr}_1(G)} \chi(e)^{2(1-n)} < [\,G : G'\,].$$

Entonces todo elemento de G' es el producto de n conmutadores. En particular si:

$$|\mathrm{Irr}_1(G)| < |\mathrm{Lin}(G)|.$$

Todo elemento de G' es un conmutador

Demostración. Consideremos el caracter regular de G. Sabemos que:

$$\rho = \sum_{\chi\in \mathrm{Irr}(G)} \chi(e)\chi$$

Si $g\in G$, por la proposición anterior obtenemos:

$$\sum_{a_1,b_1,\ldots,a_n,b_n\in G} \rho(g[a_1,b_1]\cdots[a_n,b_n]) = |G|^{2n}\left[\sum_{\chi\in Lin(G)} \frac{\chi(g)}{\chi(e)^{2n-1}} + \sum_{\chi\in \mathrm{Irr}_1(G)} \frac{\chi(g)}{\chi(e)^{2n-1}}\right].$$

Como $\chi(g)=1=\chi(e)$ si $\chi \in Lin(G)$ y $g\in G'$, tenemos:

$$\sum \rho(g[a_1,b_1]\cdots[a_n,b_n]) = |G|^{2n}\left[|Lin(G)| + \sum_{\chi\in \mathrm{Irr}_1(G)} \frac{\chi(g)}{\chi(e)^{2n-1}}\right].$$

Sea $X\subseteq G'$ el conjunto de los elementos de G que se pueden escribir como el producto de n conmutadores, es decir:

$$X = \{[x_1,y_1]\cdots[x_n,y_n] : x_1,\ldots,x_n,y_1\ldots,y_n \in G\}.$$

Entonces $g\notin X$ si y solo si $g[a_1,b_1]\cdots[a_n,b_n]\neq e$ para cualesquiera $a_1,\ldots,a_n$, $b_1\ldots,b_n\in G$ (recuerdese que el inverso de un conmutador es un conmutador), por lo tanto:

$$\sum \rho(g[a_1,b_1]\cdots[a_n,b_n]) = 0 \Leftrightarrow g\notin X$$

$$\Rightarrow \qquad |\mathrm{Lin}(G)| + \sum_{\chi\in \mathrm{Irr}_1(G)} \frac{\chi(g)}{\chi(e)^{2n-1}} = 0 \Leftrightarrow g\in G' - X$$

Si $G'-X\neq\emptyset$ aplicando 1.3.2 y 1.2.17:

$$[\,G : G'\,] = |\mathrm{Lin}(G)| \leq \sum_{\chi\in \mathrm{Irr}_1(G)} |\chi(g)|\,\chi(e)^{1-2n} \leq \sum_{\chi\in \mathrm{Irr}_1(G)} \chi(e)^{2(1-n)}$$

Lo cual contradice la elección de n. Para demostrar la última afirmación notemos:

$$\sum_{\chi\in \mathrm{Irr}(G)} \chi(e)^0 = |\mathrm{Irr}_(G)|.$$

Así que en este caso podemos tomar $n=1$.

□

2.1.7 Teorema
Supongamos que G es no abeliano, sea $c=\min\{\chi(e):\chi\in \mathrm{Irr}_1(G)\}$. Si $n\in\mathbb{N}$ cumple:

$$|G'| \leq c^{2n}.$$

Entonces todo elemento de G es producto de n conmutadores.

Demostración. Por la definición de c tenemos:

$$\chi(e)^{-2n} \leq c^{-2n} \leq |G'|^{-1} \quad \forall\ \chi \in \mathrm{Irr}_1(G).$$

Además:

$$|G| = \sum_{\chi\in \mathrm{Irr}(G)} \chi(e)^2 = \sum_{\chi\in \mathrm{Irr}_1(G)} \chi(e)^2 + |\mathrm{Lin}(G)| = \sum_{\chi\in \mathrm{Irr}_1(G)} \chi(e)^2 + [\,G : G'\,]$$

$$\Rightarrow \quad \sum_{\chi\in \mathrm{Irr}_1(G)} \chi(e)^2 = |G| - [\,G : G'\,]$$

$$\Rightarrow \quad \sum_{\chi\in \mathrm{Irr}_1(G)} \chi(e)^{2(1-n)} \leq \frac{|G| - [\,G : G'\,]}{|G'\,|}$$

$$\Rightarrow \quad \sum_{\chi\in \mathrm{Irr}_1(G)} \chi(e)^{2(1-n)} \leq \frac{|G| - [\,G : G'\,]}{|G'|} < [\,G : G'\,].$$

□

Una forma de obtener el valor n sin necesidad de conocer $\mathrm{Irr}(G)$ es buscar n tal que $|G'| \leq p^n$, donde p es el menor divisor primo de $|G|$; esto porque 1.2.24 nos asegura que el valor minimo de c en la proposición anterior es p.

Desarrollamos ahora los teoremas de Burnside en conmutadores [8]

2.1.8 Teorema
Sean $g, h\in G$. Exite $x\in G$ tal que $g\in CL([h,x])$ si y solo si:

$$\sum_{\chi\in \mathrm{Irr}(G)} \frac{\chi(g)|\chi(h)|^2}{\chi(e)} > 0.$$

Demostración. Siguiendo la notación de 1.2.22 tenemos:

$$a_{ijm} = \frac{|\mathcal{K}_i||\mathcal{K}_j|}{|G|} \sum_{\chi\in \mathrm{Irr}(G)} \frac{\chi(g_i)\chi(g_j)\overline{\chi(g_m)}}{\chi(e)}.$$

Para cada i definimos el número i' de forma tal que $CL(g_i^{-1}) = \mathcal{K}_{i'}$. Entonces:

$$a_{i'im} = \frac{|\mathcal{K}_i|^2}{|G|} \sum_{\chi\in \mathrm{Irr}(G)} \frac{\chi(g_i^{-1})\chi(g_i)\overline{\chi(g_m)}}{\chi(e)} = \frac{|\mathcal{K}_i|^2}{|G|} \sum_{\chi\in \mathrm{Irr}(G)} \frac{|\chi(g_i)|^2\overline{\chi(g_m)}}{\chi(e)}.$$

Si $CL(g) = \mathcal{K}_l$ y $CL(h) = \mathcal{K}_j$, tenemos:

$$a_{j'jl} = \frac{|\mathcal{K}_i|^2}{|G|} \sum_{\chi\in \mathrm{Irr}(G)} \frac{|\chi(h)|^2\overline{\chi}(g)}{\chi(e)} = \frac{|\mathcal{K}_i|^2}{|G|} \sum_{\chi\in \mathrm{Irr}(G)} \frac{|\overline{\chi}(h)|^2\chi(g)}{\overline{\chi}(e)}$$

$$= \frac{|\mathcal{K}_i|^2}{|G|} \sum_{\chi\in \mathrm{Irr}(G)} \frac{\chi(g)|\chi(h)|^2}{\chi(e)}$$

Supongamos que $a_{j'jl} > 0$. Entonces existen $s \in \mathcal{K}_{j'}$ y $t \in \mathcal{K}_j$ cumpliendo $st = g$. Como $s \in CL(h^{-1})$ y $t \in CL(h)$, existen $a, b \in G$ tales que $s = a^{-1}h^{-1}a$ y $t = b^{-1}hb$, luego:

$$aga^{-1} = asta^{-1} = h^{-1}ab^{-1}hba^{-1} = h^{-1}(ba^{-1})^{-1}hba^{-1} = [h, ba^{-1}]$$

$$\Rightarrow \quad g \in \mathrm{CL}([h, ba^{-1}]).$$

Ahora, supongamos que $g = a[h, x]a^{-1}$ para algunos $a, x \in G$, entonces:

$$g = (ah^{-1}a^{-1})(ax^{-1}hxa^{-1}) = \Big(ah^{-1}a^{-1}\Big)\Big((xa^{-1})^{-1}h(xa^{-1})\Big).$$

Entonces $g \in \mathcal{K}_{j'} \cdot \mathcal{K}_j$ y por lo tanto $a_{j'jl} > 0$. □

2.1.9 Teorema

Un elemento $g \in G$ es un conmutador si y solo si:

$$\sum_{\chi\in \mathrm{Irr}(G)} \frac{\chi(g)}{\chi(e)} \neq 0.$$

Demostración. Continuado con la notación anterior, si $|\mathrm{Irr}(G)| = r$:

$$\sum_{i=1}^{r} \frac{a_{i'il}}{|\mathcal{K}_i|} = \frac{1}{|G|} \sum_{i=1}^{r} \sum_{\chi\in \mathrm{Irr}(G)} \frac{\chi(g)|\chi(g_i)|^2|\mathcal{K}_i|}{\chi(e)} = \sum_{\chi\in \mathrm{Irr}(G)} \frac{\chi(g)}{\chi(e)} \frac{1}{|G|} \sum_{i=1}^{r} |\mathcal{K}_i||\chi(g_i)|^2$$

$$= \sum_{\chi\in \mathrm{Irr}(G)} \frac{\chi(g)}{\chi(e)} \langle \chi, \chi \rangle = \sum_{\chi\in \mathrm{Irr}(G)} \frac{\chi(g)}{\chi(e)} = \tau_g$$

Luego, $\tau_g \neq 0 \Leftrightarrow \exists\ i$ tal que $a_{i'il} \neq 0$. Por el teorema anterior esta última condición es equivalente a que g sea conjugado a $[x, y]$, con $x \in \mathcal{K}_i$ y $y \in G$. Entonces $g = a^{-1}[x, y]a = [a^{-1}xa, a^{-1}ya]$, para algunos $a, x, y \in G$ si y solo si $\tau_g \neq 0$. □

Una aplicación del teorema anterior:

2.1.10 Teorema
Si g es un conmutador, entonces todo generador de $\langle\, g\,\rangle$ también lo es.

Demostración. Sea $n = o(g)$ y ϵ una n-ésima raíz primitiva de la unidad. Si g^m es un generador de $\langle\, g\,\rangle$ tenemos $(n, m) = 1$ y por lo tanto existe $\sigma \in \mathrm{Gal}(\mathbb{Q}(\epsilon)/\mathbb{Q})$ tal que $\sigma(\epsilon) = \epsilon^m$. Por 1.2.17 existe Φ_i una representación de $\langle\, g\,\rangle$ que aporta $\chi_i \in \mathrm{Irr}(G) = \{\chi_1, \ldots, \chi_k\}$ y tal que $\Phi_i(g)$ es diagonal, digamos:

$$\Phi_i(g) = \begin{pmatrix} \epsilon^{l_{i,1}} & & 0 \\ & \ddots & \\ 0 & & \epsilon^{l_{i,d_i}} \end{pmatrix} \quad \text{con} \quad d_i = \chi_i(e),$$

donde $l_{i,1}, \ldots, l_{i,d_i} \in \mathbb{Z}\ \forall\ i$. Entonces:

$$\sigma(\chi_i(g)) = \sigma\left(\sum_{j=1}^{d_i} \epsilon^{l_{i,j}}\right) = \sum_{j=1}^{d_i} \sigma(\epsilon)^{l_{i,j}}.$$

Además:

$$\Phi_i(g^m) = \begin{pmatrix} \epsilon^{l_{i,1}} & & 0 \\ & \ddots & \\ 0 & & \epsilon^{l_{i,d_i}} \end{pmatrix}^m = \begin{pmatrix} \sigma(\epsilon)^{l_{i,1}} & & 0 \\ & \ddots & \\ 0 & & \sigma(\epsilon)^{l_{i,d_i}} \end{pmatrix}.$$

Por lo tanto $\sigma(\chi_i(g)) = \chi_i(g^m)\ \forall\ i$. Entonces:

$$\sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(g^m)}{\chi(e)} = \sigma\left(\sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(g)}{\chi(e)}\right) \neq 0$$

□

El siguiente resultado aún cuando no trata sobre conmutadores se presenta debido a que aparecio por primera vez en [8] junto con los teoremas ya demostrados.

2.1.11 Teorema
Si $g, h \in G$ y $\chi \in \mathrm{Irr}(G)$, entonces:

$$\chi(g)\chi(h) = \frac{\chi(e)}{|G|} \sum_{z \in G} \chi(gh^z).$$

Demostración. Sean $\mathcal{K}_1, \ldots, \mathcal{K}_n$ las clases de conjugación de G, $g_m \in \mathcal{K}_m$ e i, j tales que $g \in \mathcal{K}_i$ y $h \in \mathcal{K}_j$. Si $K_m \in \mathbb{C}[G]$ es la suma de los elementos de $\mathcal{K}_m$, según 1.2.22:

$$K_i K_j = \sum_{m=1}^{n} \left[\frac{|\mathcal{K}_i||\mathcal{K}_j|}{|G|} \sum_{\phi \in \mathrm{Irr}(G)} \frac{\phi(g)\phi(h)\overline{\phi(g_m)}}{\phi(e)} \right] K_m.$$

Tomemos Φ una representación de G que aporte χ. Entonces:

$$\chi(K_i K_j) = \sum_{m=1}^{n} \left[\frac{|\mathcal{K}_i||\mathcal{K}_j|}{|G|} \sum_{\phi \in \mathrm{Irr}(G)} \frac{\phi(g)\phi(h)\overline{\phi(g_m)}}{\phi(e)} \right] \chi(K_m)$$

$$= \sum_{m=1}^{n} \left[\frac{|\mathcal{K}_i||\mathcal{K}_j|}{|G|} \sum_{\phi \in \mathrm{Irr}(G)} \frac{\phi(g)\phi(h)\overline{\phi(g_m)}}{\phi(e)} \right] |\mathcal{K}_m| \chi(g_m)$$

$$= \sum_{\phi} \frac{|\mathcal{K}_i||\mathcal{K}_j|\phi(g)\phi(h)}{\phi(e)} \left[\frac{1}{|G|} \sum_{m} \chi(g_m)\overline{\phi(g_m)}|\mathcal{K}_m| \right]$$

$$= \sum_{\phi} \frac{|\mathcal{K}_i||\mathcal{K}_j|\phi(g)\phi(h)}{\phi(e)} \langle \chi, \phi \rangle = \frac{|\mathcal{K}_i||\mathcal{K}_j|\chi(g)\chi(h)}{\chi(e)}$$

$$\Rightarrow \chi(g)\chi(h) = \frac{\chi(K_i K_j)\chi(e)}{|\mathcal{K}_i||\mathcal{K}_j|}.$$

Ahora:

$$K_i = \frac{1}{|\mathrm{C}_G(g)|} \sum_{x \in G} g^x$$

$$K_j = \frac{1}{|\mathrm{C}_G(h)|} \sum_{y \in G} h^y$$

$$\Rightarrow K_i K_j = \frac{1}{|\mathrm{C}(g)||\mathrm{C}(h)|} \sum_{x,y \in G} g^x h^y$$

$$\Rightarrow \chi(K_i K_j) = \frac{1}{|\mathrm{C}(g)||\mathrm{C}(h)|} \sum_{x,y \in G} \chi(g^x h^y).$$

Como $g^x h^y$ es conjugado con $g h^{y x^{-1}}$

$$\chi(K_i K_j) = \frac{1}{|\mathrm{C}(g)||\mathrm{C}(h)|} \sum_{x,y \in G} \chi(g h^{y x^{-1}}) = \frac{1}{|\mathrm{C}(g)||\mathrm{C}(h)|} \sum_{x,y \in G} \chi(g h^{yx})$$

La ecuación $yx=z$ con $z\in G$, fijo tiene $|G|$ soluciones entonces:

$$\chi(K_iK_j) = \frac{|G|}{|\mathrm{C}(g)||\mathrm{C}(h)|}\sum_{z\in G}\chi(gh^z)$$

$$\Rightarrow \chi(g)\chi(h) = \frac{\chi(e)}{|\mathcal{K}_i||\mathcal{K}_j|}\left[\frac{|G|}{|\mathrm{C}(g)||\mathrm{C}(h)|}\sum_{z\in G}\chi(gh^z)\right].$$

Para terminar basta recordar que $|G|=|\mathcal{K}_m|\,|\mathrm{C}_G(g_m)|\ \forall\ m$.

□

2.2. . . . a la ecuación $x^n = 1$

Tomemos G un grupo cualquiera y $n \in \mathbb{N}$ consideremos la ecuación:

$$x^n = e. \tag{2.1}$$

Si $(n, |G|) = 1$, existen $a, b \in \mathbb{Z}$ tales que:

$$1 = na + |G|b.$$

Sea $g \in |G|$ solucion de (2.1), entonces:

$$g = (g^n)^a(g^b)^{|G|} = e^a e = e.$$

Por lo tanto si $(n, |G|) = 1$ existe solo una solucion de (2.1).

Supongamos ahora que $(n, |G|) = m$ con $1 < m < n$. Entonces podemos encontrar un número primo p tal que:

$$p\big|n \quad \text{y} \quad p\not\big||G|. \tag{2.2}$$

Si g es solucion de (2.1), entonces:

$$e = g^n = (g^{n/p})^p.$$

Como p es primo $o(g^{n/p}) \in \{1, p\}$, pero como $p\not\big||G|$ entonces $o(g^{n/p}) = 1$; i.e. g es solución de la ecuación:

$$x^{n/p} = e.$$

Repitiendo sobre los primos que cumplen (2.2) obtenemos que 2.1 es equivalente a:

$$x^m = e,$$

donde $(m, |G|) = m$, ya que $m\big||G|$. Por esto cuando queremos estudiar la ecuación (2.1) basta con considerar el caso en que n es divisor de $|G|$.

El proposito de esta sección es demostrar el siguiente resultado concerniente a la ecuación (2.1) cuando $n\big||G|$.

2.2.1 Teorema (Frobenius)
Si $n\big||G|$*, el número de soluciones a la ecuación* $x^n = e$ *es divisible por* n*.*

Para demostrar este resultado Frobenius probo en [9] lo siguiente.

2.2.2 Teorema
Si $n\big||G|$ *y* $\chi \in \mathrm{Ch}(G)$*, entonces:*

$$\frac{1}{n}\sum_{g^n=1}\chi(g) \in \mathbb{Z}.$$

Tomando $\chi = 1_G$ en este último teorema tenemos:

$$\frac{1}{n}\sum_{g^n=1}1_G(g) = \frac{1}{n}\sum_{g^n=1}1 = \frac{1}{n}|\{g : g^n = e\}| \in \mathbb{Z}.$$

Lo cual demuestra 2.2.1. De ahora en adelante nos dedicaremos a demostrar 2.2.2, siempre supondremos que $n\big||G|$.

2.2.3 Definición
Sea $G_n = \{X \subseteq G : |X| = n\}$*. Como* $|X| = |gX|\ \forall\ X \subseteq G$*, podemos definir una acción de* G *en* G_n *por:*

$$X^g = gX.$$

Definimos θ_n *como el caracter de* G *asociado a esta acción* (ver 1.3.3)*.*

2.2.4 Proposición
Sean $g \in G$ *,* $a = o(g)$ *y* $c = |G|$*. Entonces:*

$$\theta_n(g) = \begin{cases} 0 & si\ a \not| n \\ \binom{c/a}{n/a} & si\ a|n \end{cases}$$

Demostración. Supongamos que $\theta_n(g) \neq 0$ por la definición de θ_n (1.3.3) existe $X \in G_n$ tal que $gX = X$, esto nos permite afirmar que $\langle\, g \,\rangle$ actua en X por:

$$g^m \cdot x = g^m x \quad \forall\ x \in X$$

Sea $\mathcal{O}_x$ la orbita de $x \in X$ correspondiente a esta última acción, entonces:

$$\mathcal{O}_x = \{hx : h \in \langle\, g \,\rangle\}$$

$$\Rightarrow \quad |\mathcal{O}_x| = |\langle\, g \,\rangle| = a.$$

Descomponiendo a X como la unión directa de un cierto número de órbitas y dado que todas las órbitas tiene la misma cardinalidad (a saber a) obtenemos:

$$a \Big| |X| = n.$$

Así, si $a \not| n$ se tiene $\theta_n(g) = 0$.

Si $a \Big| n$, sea $H = \langle\, g \,\rangle$ es claro que:

$$g \cdot Hg' = Hg' \qquad \forall\ Hg' \in G/H$$

Sea $m = n/a \leq c/a = [G : H] = |G/H|$, podemos por lo tanto elegir m elementos $Hg_1, \ldots, Hg_m \in {}_HG$ distintos a pares y formar $X = Hg_1 \cup \ldots \cup Hg_m$, entonces:

$$|X| = |Hg_1| + \cdots + |Hg_m| = m|H| = (n/a)a = n$$

$$\Rightarrow X \in G_n \qquad \text{y} \qquad X^g = g \cdot X = X.$$

Supongamos ahora que $X \in G_n$ es g-invariante, es decir, que $X^g = gX = X$; entonces:

$$Hy \subseteq X \quad \forall\ y \in X.$$

Y dado que $y \in Hy\ \forall\ y \in X$, tenemos:

$$X = \bigcup_{y \in X} Hy.$$

Podemos por lo tanto elegir $y_1, \ldots, y_k \in X$ tales que:

$$X = \dot{\bigcup_i} Hy_i$$

$$\Rightarrow n = |X| = |Hy_1| + \cdots + |Hy_k| = k|H| = ka$$

$$\Rightarrow k = n/a = m.$$

Así, hemos establecido una correspondencia 1–1 entre el número de elementos de G_n que son g-invariantes y el número de combinaciones de $|G/H|$ elementos tomados m a la vez, por lo tanto:

$$\theta_n(g) = |\{X \in G_n : X^g = X\}| = \binom{c/a}{m}.$$

Ya que $[G : H] = c/a$.

□

2.2.5 Definición
Sea $n \in \mathbb{N}$ *y* $n = p_1^{a_1} \cdots p_k^{a_k}$ *su descomposición canónica en primos distintos, definimos la Función de Möbius por:*

$$\mu(n) = \begin{cases} 1 & Si\ n = 1 \\ (-1)^k & Si\ a_1 = \cdots = a_k = 1 \\ 0 & En\ otro\ caso \end{cases}$$

Si $\mu(n) \neq 0$ *se dice que* n *es libre de cuadrado. Además,* $\mu(nm) = \mu(n)\mu(m)$ *si* $(n, m) = 1$.

Los siguientes lemas tratan sobre el coeficiente binomial y son independientes de la teoría de Grupos. Se presentan y demuestran ya que de ellos depende la demostración que aquí se presenta del Teorema de 2.2.2.

2.2.6 Lema
Supongamos que $n, m \in \mathbb{N}$, *con* $n \big| m$. *Si* p *es primo y* $r \in \mathbb{N}$ *tal que* $p^r \big| n$, *entonces:*

$$\binom{m-1}{n-1} \equiv \binom{m/p-1}{n/p-1} \bmod p^r.$$

Demostración. Definamos el siguiente polinomio:

$$f(X) = (X-1)(X-2)\cdots(X-p+1) = X^{p-1} + c_1 X^{p-2} + \cdots + c_{p-1}.$$

Entonces $c_i \in \mathbb{Z}\ \forall\ i = 1, \ldots, p-1$, ie. $f(X) \in \mathbb{Z}[X]$.

Si $a, b \in \mathbb{Z}$, entonces:

$$f(a) - f(b) = [a^{p-1} - b^{p-1}] + c_1[a^{p-2} - b^{p-2}] + \cdots + c_{p-2}[a-b] \tag{2.3}$$

Ahora, si $a \equiv b \bmod p^r$, entonces $a^q \equiv b^q \bmod p^r\ \forall\ q \in \mathbb{Z}$ y de (2.3) se sigue que:

$$f(a) \equiv f(b) \bmod p^r.$$

Además:

$$f(a+p) = (a+p-1)(a+p-2)\cdots(a+1)$$
$$= (-1)^{p-1}[(-a)-1][(-a)-2]\cdots[(-a)-p+1] = (-1)^{p-1} f(-a)$$
$$\Rightarrow \quad f(-a) = (-1)^{p-1} f(a+p).$$

Por definición:

$$\binom{m-1}{n-1} = \frac{(m-1)!}{(m-n)!(n-1)!} = \frac{(m-1)(m-2)\cdots(m-n+1)}{(n-1)(n-2)\cdots 1}$$

$$= \frac{f(m)(m-p)(m-p-1)\cdots(m-n+1)}{f(n)(n-p)(n-p-1)\cdots 1}$$

$$= \frac{f(m)(m-p)f(m-p)(m-2p)\cdots(m-n+1)}{f(n)(n-p)f(n-p)(n-2p+1)\cdots 1}$$

$$= \cdots = \frac{f(m)(m-p)f(m-p)\cdots(m-n+p)f(m-n+p)}{f(n)(n-p)f(n-p)\cdots pf(p)}$$

$$= \frac{f(m)f(m-p)\cdots f(m-n+p)}{f(n)f(n-p)\cdots f(p)}\left[\frac{(m-p)(m-2p)\cdots(m-n+p)}{(n-p)(n-2p)\cdots p}\right].$$

Pero:

$$(m-p)\cdots(m-n+p) = \prod_{k=1}^{n/p-1} m-kp = p^{(n/p-1)}\prod_{k=1}^{n/p-1}(m/p-k)$$

$$(n-p)\cdots p = \prod_{k=1}^{n/p-1} n-kp = p^{(n/p-1)}\prod_{k=1}^{n/p-1}(n/p-k).$$

Así que:

$$\frac{(m-p)\cdots(m-n+p)}{(n-p)\cdots p} = \frac{(m/p-1)\cdots(m/p-n/p+1)}{(n/p-1)\cdots 1} = \binom{m/p-1}{n/p-1}.$$

Luego:

$$\binom{m-1}{n-1} = \frac{f(m)f(m-p)\cdots f(m-n+p)}{f(n)f(n-p)\cdots f(p)}\binom{m/p-1}{n/p-1}.$$

Y por lo tanto:

$$\binom{m-1}{n-1} - \binom{m/p-1}{n/p-1} = \binom{m/p-1}{n/p-1}\left[\frac{f(m)\cdots f(m-n+p)}{f(n)\cdots f(p)} - 1\right]. \tag{2.4}$$

Sea $b \in \mathbb{Z}$, como $m - bp \equiv -bp \bmod p^r$, entonces:

$$f(m-bp) \equiv f(-bp) \equiv (-1)^{p-1} f(bp+p) \bmod p^r.$$

También $n - bp \equiv -bp \bmod p^r$ y por lo tanto:

$$f(n-bp) \equiv (-1)^{p-1} f(bp+p) \bmod p^r$$

$$\Rightarrow \quad f(m-bp) \equiv f(n-bp) \bmod p^r \ \forall\ b \in \mathbb{Z}.$$

Tomando $b = 0, 1, \ldots, n/p - 1$, obtenemos:

$$\begin{aligned} f(m) &\equiv f(n) && \mod p^r \\ f(m-p) &\equiv f(n-p) && \mod p^r \\ &\vdots \\ f(m-n+p) &\equiv f(p) && \mod p^r \end{aligned}$$

$$\Rightarrow \quad f(m)\cdots f(m-n+p) \equiv f(n)\cdots f(p) \mod p^r$$

$$\Rightarrow \quad \exists\, a \in \mathbb{Z} \text{ tal que:} \quad p^r a = f(m)\cdots f(m-n+p) - f(n)\cdots f(p).$$

Sean:

$$b = \binom{m/p-1}{n/p-1} \in \mathbb{Z},$$

$$c = f(n)f(n-p)\cdots f(p),$$

$$d = \binom{m-1}{n-1} - \binom{m/p-1}{n/p-1}.$$

Entonces:

$$d = \frac{p^k ab}{c} \in \mathbb{Z}. \tag{2.5}$$

Es claro de la definición que $p \not| f(x)\ \forall\ x \in p\,\mathbb{Z}$; por lo tanto:

$$p \not| f(n-kp) \quad \forall\ k = 0, 1, \ldots, n/p-1$$

$$\Rightarrow \quad p \not| f(n)f(n-p)\cdots f(p) = c$$

$$\Rightarrow \quad p^k \not| c \qquad \Rightarrow \quad (p^k, c) = 1.$$

Pero por (2.5) $p^k \big| cd$; entonces $p^k \big| d$, $d' = d/p^k \in \mathbb{Z}$ y $ab = cd'$. Así, de (2.5)

$$\binom{m-1}{n-1} - \binom{m/p-1}{n/p-1} = p^k d'$$

$$\Rightarrow \quad \binom{m-1}{n-1} \equiv \binom{m/p-1}{n/p-1} \mod p^k.$$

□

2.2.7 Lema

Supongamos que $n, m \in \mathbb{N}$ con $n \big| m$, entonces:

$$\frac{1}{m} \sum_{k|n} \binom{m/k}{n/k} \mu(k) \in \mathbb{Z}.$$

Demostración. Supongamos que $k\big|\, n$, entonces:

$$\binom{m/k}{n/k} = \frac{(m/k)(m/k-1)\cdots(m/k-n/k+1)}{(n/k)(n/k-1)\cdots 1}$$

$$= \frac{m/k}{n/k}\,\frac{(m/k-1)\cdots(m/k-n/k+1)}{(n/k-1)\cdots 1} = \frac{m}{n}\binom{m/k-1}{n/k-1}$$

$$\Rightarrow \quad \frac{1}{m}\sum_{k|n}\binom{m/k}{n/k}\mu(k) = \frac{1}{n}\sum_{k|n}\binom{m/k-1}{n/k-1}\mu(k).$$

Tomemos $A = \{k : k\big|\, n,\ \mu(k) \neq 0\}$, entonces:

$$\sum_{k|n}\binom{m/k-1}{n/k-1}\mu(k) = \sum_{k\in A}\binom{m/k-1}{n/k-1}\mu(k).$$

Sean p un numero primo, $a \in \mathbb{N}$ con $p^a\big|n$ y $p^{a+1}\not|n$, $B = \{k \in A : p \not| k\}$ y $C = \{k \in A : p\big|\, k\}$. Tomemos $k \in B$, entonces $k\big|n$, k es libre de cuadrado y su descomposición en primos no contiene a p, por lo tanto pk es libre de cuadrado ($\mu(pk) \neq 0$), $pk\big|n$ y $p\big|pk$ es decir, $pk \in C$; asi $pB \subseteq C$.

Tomemos ahora $k \in C$, como k es libre de cuadrado, $p \not|(k/p)$ y claramente k/p es libre de cuadrado además $(k/p)\big|k$ y $k\big|n$, por lo tanto $(k/p)\big|n$, es decir, $k/p \in B$; al ser k arbitrario $C/p \subseteq B$. Por lo tanto $C = pB$ y $A = B \cup C = B \cup pB$, entonces:

$$\sum_{k|n}\binom{m/k-1}{n/k-1}\mu(k) = \sum_{k\in B}\binom{m/k-1}{n/k-1}\mu(k) + \sum_{k\in pB}\binom{m/k-1}{n/k-1}\mu(k)$$

$$= \sum_{k\in B}\binom{m/k-1}{n/k-1}\mu(k) + \sum_{k\in B}\binom{m/pk-1}{n/pk-1}\mu(pk).$$

Pero si $k \in B$, entonces $(k,p) = 1 \Rightarrow\ \mu(pk) = \mu(p)\mu(k) = -\mu(k)$ luego:

$$\sum_{k|n}\binom{m/k-1}{n/k-1}\mu(k) = \sum_{k\in B}\left[\binom{m/k-1}{n/k-1} - \binom{m/pk-1}{n/pk-1}\right]\mu(k).$$

Si $k \in B$, como $p^a \,\big|\, n$ y $k \,\big|\, n$ con $(p^a, k = 1)$, entonces $kp^a \,\big|\, n$ o equivalentemente $p^a \,\big|\, (n/k)$ podemos por lo tanto aplicando 2.2.6 concluir que:

$$\binom{m/k-1}{n/k-1} \equiv \binom{m/pk-1}{n/pk-1} \bmod p^a \quad \forall\ k \in B$$

$$\Rightarrow \quad \sum_{k|n}\binom{m/k-1}{n/k-1}\mu(k) \equiv 0 \bmod p^a.$$

Como p es cualquier primo que divide a n, entonces:

$$\sum_{k|n} \binom{m/k-1}{n/k-1} \mu(k) \equiv 0 \bmod n.$$

□

Si $a, b \in \mathbb{Z}, b \neq 0$ para hacer más legibles algunos resultados escribiremos ab^* en lugar de ab^{-1}; si $b \big| a$, entonces $ab^* = a/b \in \mathbb{Z}$.

2.2.8 Lema
Supongamos que $k \big| n$ *y* $n \big| m$*, entonces:*

$$\frac{k}{m} \sum_{d|nk^*} \binom{m/kd}{n/kd} \mu(d) \in \mathbb{Z}.$$

Demostración. Como $nk^* \big| mk^*$ la Proposición 2.2.7 nos dice que:

$$\frac{1}{m/k} \sum_{d|nk^*} \binom{(m/k)/d}{(n/k)/d} \mu(d) \in \mathbb{Z}.$$

Simplificando obtenemos el resultado deseado.

□

El siguiente resultado es un hecho muy conocido y usado en teoría de números, una demostración se puede encontrar en [12].

2.2.9 Lema
Sean f, g *dos funciones aritméticas, definimos el producto de Dirichlet de* f *y* g *como la función* $f * g$ *dada por:*

$$[f * g](n) = \sum_{d|n} f(d) g(n/d).$$

Entonces el conjunto de funciones aritméticas junto con $*$ *forman un grupo abeliano cuya identidad es:*

$$I(n) = \begin{cases} 1 & \text{Si } n = 1 \\ 0 & \text{En otro caso} \end{cases}$$

Si definimos u *como la función aritmetica* $u(n) = 1$*, entonces:*

$$u * \mu = I.$$

2.2.10 Lema
Si f y g son dos funciones aritméticas, entonces:

$$\sum_{d|n} f(d)g(n/d) = \sum_{d|n} \sum_{r|nd^*} g(n/rd)\mu(r) \sum_{k|d} f(k).$$

Demostración. En vista de 2.2.9

$$f * g = f * g * I = (f * g) * (u * \mu) = (f * u) * (\mu * g).$$

Pero

$$[(f * u) * (g * \mu)](n) = \sum_{d|n} [f * u](d)[\mu * g](n/d),$$

y

$$[f * u](d) = \sum_{k|d} f(k)u(d/k) = \sum_{k|d} f(k)$$

$$[\mu * g](n/d) = \sum_{r|nd^*} \mu(r)g(n/rd).$$

□

Podemos ahora demostrar el Teorema 2.2.2, para esto sean $\chi \in \mathrm{Irr}(G)$ y $m = |G|$ definamos:

$$a_n(\chi) = \frac{1}{n} \sum_{g^n=1} \chi(g).$$

Para $n = 1$ es claro que $a_n(\chi) \in \mathbb{Z}$ podemos por lo tanto suponer que $n > 1$ y por inducción que $a_k(\chi) \in \mathbb{Z}\ \forall\ k \in \mathbb{N}\ k < n$. Como $\overline{\theta_n} = \theta_n$, entonces:

$$\langle \chi, \theta_n \rangle = \frac{1}{m} \sum_{g \in G} \chi(g)\theta_n(g) = \frac{1}{m} \sum_{d|m} \sum_{o(g)=d} \chi(g)\theta_n(g).$$

Usando 2.2.4

$$\langle \chi, \theta_n \rangle = \frac{1}{m} \sum_{d|n} \binom{m/d}{n/d} \sum_{o(g)=d} \chi(g).$$

Sean:

$$f(k) = \sum_{o(g)=k} \chi(g) \quad \text{y}$$

$$g(k) = \binom{km/n}{k}.$$

Entonces:

$$\langle \chi, \theta_n \rangle = \frac{1}{m} \sum_{d \Big| n} g(n/d)f(d).$$

En vista de 2.2.10

$$\langle \chi, \theta_n \rangle = \frac{1}{m} \sum_{d|n} \sum_{r|(n/d)} g(n/rd)\mu(r) \sum_{k|d} f(k)$$

$$= \frac{1}{m} \sum_{d|n} \sum_{r|nd^*} \binom{m/rd}{n/rd} \mu(r) \sum_{k|d} \sum_{o(g)=k} \chi(g).$$

Si notamos que:

$$o(g) | \, d \quad \Leftrightarrow \quad g^d = e.$$

Tenemos:

$$\sum_{k|d} \sum_{o(g)=k} \chi(g) = \sum_{g^d=e} \chi(g) = d \, a_d(\chi)$$

$$\Rightarrow \quad \langle \chi, \theta_n \rangle = \frac{1}{m} \sum_{d|n} \sum_{r|nd^*} \binom{m/rd}{n/rd} \mu(r) d \, a_d(\chi)$$

$$\Rightarrow \quad \langle \chi, \theta_n \rangle = \frac{n}{m} \binom{m/n}{1} a_n(\chi) + \frac{1}{m} \sum_{d|n,\, d<n} \sum_{r|nd^*} \binom{m/rd}{n/rd} \mu(r) d \, a_d(\chi).$$

Lo cual también podemos escribir como:

$$\langle \chi, \theta_n \rangle = a_n(\chi) + \sum_{d|n,\, d<n} \sum_{r|nd^*} \frac{d}{m} \binom{m/rd}{n/rd} \mu(r) \, a_d(\chi). \tag{2.6}$$

Pero $a_d \in \mathbb{Z} \; \forall \; d < n$, lo cual junto con 2.2.8 nos dice que:

$$\sum_{d|n,\, d<n} \sum_{r|nd^*} \frac{d}{m} \binom{m/rd}{n/rd} \mu(r) \, a_d(\chi) \in \mathbb{Z}.$$

Según 1.2.14 $\langle \chi, \theta_n \rangle \in \mathbb{Z}$, por lo tanto de (2.6) podemos concluir que $a_n(\chi) \in \mathbb{Z}$ con lo cual termina la demostración de 2.2.2.

2.3. . . . en grupos simples

Gran parte de las aplicaciones de la teoría de caracteres son concernientes a la caracterización de grupos a partir de diversas restricciones. Estas restricciones pueden o no referirse a los caracteres de dicho grupo. Esta sección y la próxima trabajan en esta línea, aquí presentamos un teorema muy sencillo de demostrar que ejemplifica como partiendo con una condición ajena a los caracteres se puede controlar mediante estos la estructura del grupo. Empezamos con un resultado auxiliar.

2.3.1 Proposición
Sean $S \in Syl_2(G)$, $M < S$ con $[S : M] = 2$ y $\tau \in S$ una involución tal que:

$$Cl_G(\tau) \cap M = \emptyset.$$

Entonces, $\tau \notin G'$.

Demostración. Sea $\Omega = \{gM : g \in G\}$ y consideremos la acción de G en Ω definida por:

$$h \cdot gM = hgM \quad si \quad h \in GygM \in \Omega.$$

Así:

$$h \cdot gM = gM \qquad \Leftrightarrow \qquad g^{-1}hg \in M.$$

Por lo tanto, la permutación inducida por τ no tiene puntos fijos en Ω y dado que $\tau^2 = e$ entonces:

$$\tau = (a_1, a_2)(a_3, a_4) \cdots (a_{n-1}, a_n),$$

donde

$$\{a_1, a_2, \ldots, a_{n-1}, a_n\} = \{1, 2, \ldots, |\Omega|\}.$$

Ahora:

$$|\Omega| = [G : M] = [G : S][S : M] = 2[G : S]$$
$$\Rightarrow \qquad \text{sig}(\tau) = (-1)^{[G:S]} = -1.$$

Pues $2 \nmid [G : S]$, por lo tanto:

$$A = \{g \in G : g \text{ es par}\} \lneqq G \quad y \quad [G : A] = 2.$$

Como G/A es abeliano, $G' \subseteq A$ y dado que $\tau \notin A$, $\tau \notin G'$. □

Probemos ahora el prometido ejemplo.

2.3.2 Teorema
Sea $G = G'$ y supongamos que $\tau \in G$ es una involución con $\mathrm{C}_G(\tau) = D_8$. Entonces, $|G|$ =168 ó 360.

Demostración. Sean $D = \mathrm{C}_G(\tau)$ y $x \in D$. Como $\tau = x\tau x^{-1}$, tenemos:

$$e = \tau^2 = \left(x\tau x^{-1}\right)^2 = x^2$$

Tenemos que D es un 2-grupo, sea $D \subseteq S \in Syl_2(G)$ y tomemos $x \in \mathrm{Z}(S)$, luego:

$$x\tau = \tau x \qquad \Rightarrow \qquad x \in D \quad y \quad xy = yx \quad \forall\, y \in D$$

$$\Rightarrow \quad x \in \mathrm{Z}(D) \qquad \Rightarrow \qquad \mathrm{Z}(S) \subseteq \mathrm{Z}(D) = \langle \tau \rangle.$$

Y dado que $\mathrm{Z}(S) \neq \langle e \rangle$, tenemos $\mathrm{Z}(S) = \langle \tau \rangle$

$$\Rightarrow \qquad x\tau = \tau x \quad \forall\, x \in S \qquad \Rightarrow \qquad S \subseteq \mathrm{C}_G(\tau) = D$$

$$\Rightarrow \qquad D = S = \mathrm{C}_G(\tau).$$

Tomemos $Z_4 \approx M < D = \langle a, b : a^2 = b^4 = e \rangle$ cíclico de orden 4, con $\tau \in M = \langle b \rangle$ su unica involución. Sea λ el caracter de M dado por:

$$\lambda(b^n) = i^n \qquad n = 0, 1, 2, 3.$$

Y sea

$$\vartheta = (1_M - \lambda)^D.$$

La tabla (2.1) contine los valores de ϑ, de estos obtenemos que:

$$[\vartheta : \vartheta] = 3, \qquad \vartheta(e) = 0, \qquad \vartheta|_{D-M} = 0.$$

	$\{e\}$	$\{b, b^3\}$	$\{b^2\}$	$\{a, ab^2\}$	$\{ab, ab^3\}$
ϑ	0	2	4	0	0

Tabla 2.1: Funcion ϑ

Supongamos que $x \in G$ y que $M \cap M^x \neq \langle e \rangle$, tendríamos entonces:

$$\tau \in M \cap M^x \qquad \Rightarrow \qquad \tau = \tau^x \qquad \Rightarrow \qquad x \in D$$

$$\Rightarrow \quad M = M^x \text{ pues } M \lhd D \qquad \Rightarrow \qquad M \text{ es un conjunto T.I. en } G$$

Del teorema 1.3.10 obtenemos:

$$[\vartheta^G : \vartheta^G] = 3 \quad \text{y} \quad (\vartheta^G)_M = \vartheta.$$

Ahora, ϑ^G es un caracter generalizado, por lo tanto:

$$\vartheta^G = \sum_{\chi \in \mathrm{Irr}(G)} n_\chi \chi \qquad \text{con} \quad n_\chi \in \mathbb{Z} \quad \text{y} \sum_{\chi \in \mathrm{Irr}(G)} n_\chi^2 = 3.$$

Es más, tenemos:

$$[\vartheta^G, 1_G] = [\vartheta : 1_D] = [1_M - \lambda : 1_M] = 1$$

$$\Rightarrow \qquad \vartheta^G = 1_G + n_1\chi + n_2\psi, \qquad \text{con} \quad n_1^2 + n_2^2 = 2 \quad \text{y} \quad \chi, \psi \in \mathrm{Irr}(G).$$

Como:

$$\vartheta^G(e) = 0 \quad \Rightarrow \quad 0 = 1 + n_1 \mathrm{deg}(\chi) + n_2 \mathrm{deg}(\psi) \quad \Rightarrow \quad n_1 = 1 \text{ y } n_2 = -1$$

Tenemos:

$$\vartheta^G = 1_G + \chi - \psi, \qquad \text{con} \quad \chi, \psi \in \mathrm{Irr}(G).$$

Ahora:

$$0 = \vartheta^G(e) = 1 + \chi(e) - \psi(e) \qquad \text{y} \qquad 4 = \vartheta^G(\tau) = 1 + \chi(\tau) - \psi(\tau).$$

Como $G = G'$, la Proposición 2.3.1 garantiza que toda involución de G es conjugada con τ, así que designemos por $\mathcal{K}$ a la única clase de conjugación de involuciones de G y definamos:

$$\varphi(g) = |\{(x, y) \in \mathcal{K} \times \mathcal{K} : \ xy = g\}|.$$

Así, φ es una función de clase. Además:

$$x, y \in \mathcal{K}, \ xy = g \qquad \Rightarrow \qquad g^x = g^{-1}.$$

Y si $x \in \mathcal{K}, \ x \neq g$:

$$g^x = g^{-1} \qquad \Rightarrow \qquad y = xg \in \mathcal{K}.$$

Por lo tanto:

$$\varphi(g) = |\{x \in \mathcal{K} : g^x = g^{-1} \ \ x \neq g\}|.$$

Tomemos $g \in M - \{e\}$ y sea $x \in \mathcal{K}$ tal que $g^x = g^{-1}$, entonces:

$$g = \tau \quad \text{o} \quad g^2 = \tau.$$

Si $g = \tau$, $\tau^x = \tau^{-1} = \tau$. Ahora, si $g = \tau^2$ tenemos:

$$\tau^x = x\tau x = (xgx)^2 = g^{-2} = g^2 = \tau.$$

En cualquier caso, $\tau^x = \tau$, es decir, $x \in \mathrm{C}_G(\tau) = D$. Podemos ahora deducir que:

$$\varphi(g) = 4 \quad \text{si} \quad g \in M - \{e\}.$$

Según la Proposición 1.2.22, $a_{11r} = \varphi(g)$ si $g \in \mathcal{K}_r \in Cl(G)$. Obtenemos así:

$$\varphi = \frac{|\mathcal{K}|^2}{|G|} \sum_{\xi \in \mathrm{Irr}(G)} \frac{\xi(\tau)^2}{\xi(e)} \overline{\xi}.$$

Como $[\bar{\xi} : \bar{\xi}] = [\xi : \xi]$, entonces:

$$\varphi = \frac{|\mathcal{K}|^2}{|G|} \sum_{\xi \in \mathrm{Irr}(G)} \frac{\overline{\xi}(\tau)^2}{\overline{\xi}(e)} \xi.$$

Claramente $\xi(e)$ es real y como $\overline{\xi(\tau)} = \xi(\tau^{-1}) = \xi(\tau)$:

$$\varphi = \frac{|\mathcal{K}|^2}{|G|} \sum_{\xi \in \mathrm{Irr}(G)} \frac{\xi(\tau)^2}{\xi(e)} \xi.$$

$$\Rightarrow \qquad [\vartheta^G, \varphi] = \frac{|\mathcal{K}|^2}{|G|} \left(1 + \frac{\chi(\tau)^2}{\chi(e)} - \frac{\psi(\tau)^2}{\psi(e)} \right).$$

Pero, por otro lado:

$$[\vartheta^G, \varphi] = [1_M - \lambda, \varphi_M] = \frac{1}{|M|} \sum_{x \in M} (1_M - \lambda)(x) \overline{\varphi_M(x)}$$

$$= \frac{1}{4} \sum_{x \in M - \{e\}} (1_M - \lambda)(x) \overline{\varphi_M(x)} = \sum_{x \in M - \{e\}} (1_M - \lambda)(x) = 4.$$

Ahora, $|G| = |\mathrm{C}(\tau)||\mathcal{K}| = 2^3 |\mathcal{K}|$, por lo tanto:

$$2^8 = |G| \left(1 + \frac{\chi(\tau)^2}{\chi(e)} - \frac{\psi(\tau)^2}{\psi(e)} \right).$$

Sean $a = \chi(e)$, $b = \chi(\tau) \in \mathbb{Z}$, entonces $\psi(e) = a + 1$ y $\psi(\tau) = b - 3$. Por la segunda relación de ortogonalidad tenemos:

$$8 = |\mathrm{C}_G(\tau)| = \sum_{\xi \in \mathrm{Irr}(G)} \xi(\tau)^2 \geqq 1 + b^2 + (b-3)^2$$

$$\Rightarrow \qquad b = 1 \text{ ó } 2$$

Si b=1, tenemos:

$$2^8 = |G| \left(1 + \frac{1}{a} - \frac{4}{a+1} \right) = |G| \frac{(a-1)^2}{a(a+1)}$$

$$\Rightarrow \qquad |G| = \frac{2^8 a(a+1)}{(a-1)^2} \qquad \Rightarrow \qquad |G|(a-1)^2 = 2^8 a(a+1).$$

Tenemos $2^3 \,\big|\, |G|$ y $2^4 \not| \, |G|$, como $a \in \mathbb{Z}$, $2 \big| a(a+1)$

$$\Rightarrow \qquad 2^6 \,\big|\, (a-1)^2 \qquad \Rightarrow \qquad 2^3 \,\big|\, (a-1).$$

Supongamos que $2^2 \,\big|\, a(a+1)$, entonces:

$$2^2 \,\big|\, a \quad \text{o} \quad 2^2 \,\big|\, (a+1).$$

En ambos casos tendríamos que $2^3 \nmid (a-1)$, por lo tanto $2^2 \nmid a(a+1)$. Así, $2^4 \nmid (a-1)$. Sea p un divisor impar de $a-1$, entonces:

$$p \big| 2^8 a(a+1) \Rightarrow p \big| a \text{ o } p \big| a+1 \Rightarrow p \big| 1 \Rightarrow p = \pm 1.$$

Luego $a = 2^3 + 1 = 9$ y por lo tanto:

$$|G| = \frac{2^8 \cdot 9 \cdot 10}{2^6} = 2^3 \cdot 3^2 \cdot 5 = 360.$$

Ahora, si b=2:

$$2^8 = |G| \left(1 + \frac{4}{a} - \frac{1}{a+1}\right) = |G| \frac{(a+2)^2}{a(a+1)}$$

$$\Rightarrow \qquad |G| = \frac{2^8 a(a+1)}{(a+2)^2} \qquad \Rightarrow \qquad |G|(a+2)^2 = 2^8 a(a+1).$$

De manera similar tenemos aqui $2^3 \big| |G|$ y $2^4 \nmid |G|$, como $a \in \mathbb{Z}$, $2 \big| a(a+1)$

$$\Rightarrow \qquad 2^6 \ \big| (a+2)^2 \qquad \Rightarrow \qquad 2^3 \ \big| (a+2).$$

Si $2^2 \ \big| a(a+1)$, entonces:

$$2^2 \ \big| a \quad \text{o} \quad 2^2 \ \big| (a+1) \qquad \Rightarrow \qquad 2^3 \nmid (a+2)!! \qquad \therefore \quad 2^2 \nmid a(a+1)$$

$$\Rightarrow \qquad 2^4 \nmid (a+2)$$

Si p es un divisor impar de $a+2$; entonces $p \big| 2^8 a(a+1) \Rightarrow p \big| a$ o $p \big| a+1$. En ambos casos tenemos que $p \big| 1$ y por lo tanto $a = 2^3 - 2 = 6$ y:

$$|G| = \frac{2^8 \cdot 6 \cdot 7}{2^6} = 2^3 \cdot 3 \cdot 5 = 168.$$

□

2.4. . . . en caracterización de grupos

Como los grupos D_8 y Q_8 demuestran, la tabla de caracteres no determina unívocamente a un grupo. Sin embargo en 1.2.22 (pág. 29) demostramos que $X(G)$ determina la tabla de multiplicación de clases la cual esta estrechamente relacionada con la estructura de G. Bajo estas premisas surge la pregunta ¿Cuando $X(G)$ determina unívocamente a G? El resultado expuesto en esta sección es un ejemplo de que para ciertos casos esto si sucede.

2.4.1 Teorema (Nagao)
Si G es un grupo tal que $X(G)=X(S_n)$, entonces $G \approx S_n$

A lo largo de esta sección supondremos que G es un grupo y $X(G) = X(S_n)$. Las siguientes son propiedades bien conocidas acerca de los grupos simétricos; la tercera de ellas es por decirlo de cierta forma la más sofisticada de ellas, una demostración de esta puede ser encontrada en [2] pág. 52.

1) Dos elementos de S_n son conjugados si y solo si tienen la misma estructura cíclica

2) S_3 es el único grupo no abeliano de orden 6

3) Si H es un grupo y $a_1, \ldots, a_m \in H$ cumplen:

   3.1) $a_1^2 = \cdots = a_m^2 = e$

   3.2) $a_i a_j = a_j a_i \quad$ si $i+1 < j \leq m$

   3.3) $(a_i a_{i+1})^3 = e \quad$ si $i < m$

   Entonces $\langle a_1, \ldots, a_m \rangle \approx S_{m+1}$

Si $n = 1, 2$ el Teorema de Nagao es trivialmente cierto ($|G|=|S_n|$). Si $n = 3$, dado que G tiene un caracter irreducible no lineal, es no abeliano, entonces por 2) el resultado también es cierto en este caso. En adelante supondremos que $n \geq 4$.

Por 1) podemos identificar una clase de conjugación en S_n por la estructura cíclica de sus elementos. Así $\mathcal{K}(2^{m_2}, 3^{m_3}, \ldots, n^{m_n})$ representará a la clase de conjugación en S_n cuyos elementos son producto de m_2 2-ciclos, m_3 3-ciclos, etc.; si para algún $j \in \{1, \ldots, n\}$ $n_j = 0$, podemos omitirlo. Así:

$$\begin{aligned} \mathcal{K}(1) &= CL(e). \\ \mathcal{K}(2) &= CL\big((1,2)\big). \\ \mathcal{K}(3) &= CL\big((1,2,3)\big). \\ \mathcal{K}(2^2) &= CL\big((1,2)(3,4). \end{aligned}$$

Como ya es usual $K(2^{m_2}, 3^{m_3}, \ldots, n^{m_n})$ representará la suma de los elementos de $\mathcal{K}(2^{m_2}, 3^{m_3}, \ldots, n^{m_n})$.

Dado que $X(G) = X(S_n)$ para cada clase $\mathcal{K}(2^{m_2}, 3^{m_3}, \ldots, n^{m_n})$ existe una clase de G para la cual las columnas correspondientes en $X(G)$ y en $X(S_n)$ son iguales, a esta clase la denotaremos por $\mathcal{K}[2^{m_2}, 3^{m_3}, \ldots, n^{m_n}]$ y a la suma de sus elementos por $K[2^{m_2}, 3^{m_3}, \ldots, n^{m_n}]$. Por 1.2.19, $\mathcal{K}[1]$ es la clase de la identidad en G.

2.4.2 Proposición

$$K[2]^2 = 3\,K[3] + 2\,K[2^2] + \binom{n}{2} K[1]. \tag{2.7}$$

$$K[2]K[3] = K[3]K[2] = K[2,3] + 4\,K[4] + 2\,K[2]. \tag{2.8}$$

$$K[2]K[2^2] = \cdots + 2\,K[4] + \cdots . \tag{2.9}$$

$$\mathcal{K}[4] \subset \mathcal{K}[2^2]\mathcal{K}[2]. \tag{2.10}$$

Si $m \leq [n/2]$:

$$K[2]^m = \cdots + m!\,K[2]^m + m\,K[2^{m-1}]K[2]. \tag{2.11}$$

$$\mathcal{K}[2^{m-1}]\mathcal{K}[2] \subseteq \mathcal{K}[2^m] \cup \mathcal{K}[2^{m-2},3] \cup \mathcal{K}[2^{m-2}] \cup \mathcal{K}[2^{m-3},4]. \tag{2.12}$$

Si $n \geq 6$:

$$\mathcal{K}[2]\mathcal{K}[4] \cap \mathcal{K}[2^3]\mathcal{K}[2] = \mathcal{K}[2^2] \cup \mathcal{K}[2,4]. \tag{2.13}$$

Demostración. Como la tabla de multiplicación de clases de G y S_n son iguales la primera igualdad es equivalente a:

$$K(2)^2 = 3\,K(3) + 2\,K(2^2) + \binom{n}{2} K(1).$$

Tomemos $(i,j),(k,l) \in \mathcal{K}(2)$ para determinar la clase de $(i,j)(k,l)$ notamos que:

1) $|\{i,j\} \cap \{k,l\}| = 2 \Leftrightarrow (i,j) = (k,l) \Leftrightarrow (i,j)(k,l) \in \mathcal{K}(1)$.

2) $|\{i,j\} \cap \{k,l\}| = 1 \Leftrightarrow (i,j)(k,l) \in \mathcal{K}(3)$.

3) $|\{i,j\} \cap \{k,l\}| = 0 \Leftrightarrow (i,j)(k,l) \in \mathcal{K}(2^2)$.

Por lo tanto existen $A, B, C \in \mathbb{Z}^+$ tales que:

$$K(2)^2 = A\,K(3) + B\,K(2^2) + C\,K(1)$$

Dado que existen $n(n-1)/2 = \binom{n}{2}$ transposiciones el caso 1) ocurre exactamente en $\binom{n}{2}$ ocasiones, ie. $C = \binom{n}{2}$.

Sea $(a,b,c) \in \mathcal{K}(3)$ y supongamos que $(i,j),(k,l) \in \mathcal{K}(2)$ son tales que:

$$(i,j)(k,l) = (a,b,c).$$

Por 2), $|\{i,j\}\cap\{k,l\}|=1$ y podemos suponer sin pérdida de generalidad que $j=k$, entonces:

$$(a,b,c)=(i,j)(j,l)=(i,j,l)$$
$$\Rightarrow \quad a\in\{i,j,l\},\ b=\sigma(a),\ c=\sigma(b)=\sigma^2(a).$$

Como podemos " elegir " a de 3 formas distintas y cada una de estas elecciones nos da una representación diferente de (a,b,c) como producto de 2 transposiciones a saber:

$$(a,b,c)=(a,b)(b,c)=(b,c)(c,a)=(c,a)(a,l),$$
$$\text{con}\quad (a,b)\neq(b,c)\neq(c,a)\neq(a,b).$$

Tenemos que $A=3$.

Por último supongamos que $\sigma=(a,b)(c,d)\in\mathcal{K}(2^2)$, razonando de la misma manera obtenemos que existen exactamente 2 maneras de representar a σ como elemento de $\mathcal{K}(2)^2$:

$$\sigma=(a,b)(c,d)=(c,d)(a,b).$$

Y por lo tanto $B=2$, lo que termina la demostración de la formula (2.7).

De la misma manera se puede demostrar (2.8), de hecho:

$$(a,b,c,d)=(a,d)(a,b,c)=(c,b)(a,c,d)=(a,b)(b,c,d)=(c,d)(a,b,d),$$

$$(a,b)=(a,c)(c,a,b)=(b,c)(c,b,a).$$

Para (2.9) consideremos que:

$$(a,b,c,d)=(a,c)[(a,b)(c,d)]=(b,d)[(a,d)(b,d)].$$

Si queremos demostrar (2.10)basta notar que si $(a,b,c,d)\in\mathcal{K}(4)$, entonces:

$$(a,b,c,d)=[(a,d)(b,c)](a,d)\in\mathcal{K}(2^2)\mathcal{K}(2).$$

La demostración de (2.13) se omite por ser un poco tediosa, pero se puede realizar de la misma manera en que se han hecho las demás. En cuanto al resto de las formulas, son evidentes de la defínción de estructura cíclica en S_n.

□

Sean $g\in\mathcal{K}[2^{m_2},3^{m_3},\ldots,n^{m_n}]$ y $\sigma\in\mathcal{K}(2^{m_2},3^{m_3},\ldots,n^{m_n})$, entonces por 1.2.15 y dado que $X(G)=X(S_n)$ tenemos:

$$|\mathrm{C}_{S_n}(\sigma)|=\sum_{\chi\in\mathrm{Irr}(S_n)}|\chi(\sigma)|^2=\sum_{\chi\in\mathrm{Irr}(G)}|\chi(g)|^2=|\mathrm{C}_G(g)|.$$

2.4.3 Proposición
Si $g \in \mathcal{K}[2]$*, entonces* $o(g) = 2$.

Demostración. Es bien sabido que:

$$|\mathcal{K}(2)| = \frac{n(n-1)}{2},$$

$$|\mathcal{K}(3)| = \frac{n(n-1)(n-2)}{3},$$

$$|\mathcal{K}(2^2)| = \frac{n(n-1)(n-2)(n-3)}{8}.$$

Por lo tanto, si $\sigma \in \mathcal{K}(2), \sigma_1 \in \mathcal{K}(3)$ y $\sigma_2 \in \mathcal{K}(2^2)$, entonces:

$$|\mathrm{C}(\sigma)| = \frac{|S_n|}{|\mathcal{K}(2)|} = 2(n-2)!,$$

$$|\mathrm{C}(\sigma_1)| = \frac{|S_n|}{|\mathcal{K}(3)|} = 3(n-3)!,$$

$$|\mathrm{C}(\sigma_2)| = \frac{|S_n|}{|\mathcal{K}(2)|} = 8(n-4)!.$$

Ahora, por la proposición anterior $g^2 \in \mathcal{K}[3] \cup \mathcal{K}[2^2] \cup \mathcal{K}[1]$. Tomemos $g_1 \in \mathcal{K}[3]$ y $g_2 \in \mathcal{K}[2^2]$, según lo dicho en las lineas anteriores a esta proposición:

$$|\mathrm{C}(g)| = |\mathrm{C}(\sigma)| = 2(n-2)!$$

$$|\mathrm{C}(g_1)| = |\mathrm{C}(\sigma_1)| = 3(n-3)!$$

$$|\mathrm{C}(g_2)| = |\mathrm{C}(\sigma_2)| = 8(n-4)!$$

Como $\mathrm{C}_G(g) < \mathrm{C}_G(g^2)$, tenemos

$$|\mathrm{C}_G(g)| = 2(n-2)! \,\big|\, |\mathrm{C}_G(g^2)|.$$

Y dado que:

$$2(n-2)! \not| \; 3(n-3)!$$

$$2(n-2)! \not| \; 8(n-4)!$$

Entonces $g^2 \notin \mathcal{K}[3] \cup \mathcal{K}[2^2]$ y por lo tanto $g^2 \in \mathcal{K}[1]$, ie. $g^2 = e$.

□

2.4.4 Proposición
Si $g \in \mathcal{K}[3]$*, entonces* $o(g) = 3$

Demostración. Por la fórmula 2.7 existen exactamente tres parejas de involuciones cuyo producto es g ie., existen $a_1, b_1, \ldots, a_3, b_3 \in \mathcal{K}[2]$ tales que:

1) $g = a_1b_1 = a_2b_2 = a_3b_3$.

2) $a_i \neq a_j$ y $b_i \neq b_j$ si $i \neq j$.

3) Si $a, b \in \mathcal{K}[2]$ y $g = ab$, entonces $\exists\ i$ tal que $a = a_i$ y $b = b_i$.

Supongamos que $g^2 = e$, entonces $g = a_ib_i = b_ia_i\ \forall\ i$. En particular, $g = b_1a_1$, según la propiedad 3) $\exists\ i$ tal que $b_1 = a_i$ y $a_1 = b_i$. Si $i = 1$, entonces $g = a_1b_1 = b_1^2 = e$ lo cual no puede ser. Tenemos por lo tanto que $i \in \{2, 3\}$.

Podemos suponer sin pérdida de generalidad que $i = 2$. Entonces $b_1 = a_2$ y $a_1 = b_2$; pero también $g = b_3a_3$ y por lo tanto $\exists\ j$ tal que $b_3 = a_j$ y $a_3 = b_j$, razonando como antes deducimos que $j \in \{1, 2\}$. Si $j = 1$, entonces $b_3 = a_1 = b_2$ lo cual contradice la propiedad 2), y si $j = 2$ entonces $a_3 = b_2 = a_1$ lo cual tambien contradice dicha propiedad. Por lo tanto $g^2 \neq e$.

Ahora, sean $a, b \in \mathcal{K}[2]$ tales que $g = ab$. Entonces dado que:

$$g = ab = b(bab) = (bab)(babab) = (babab)(bababab). \tag{2.14}$$

Tenemos 4 expresiones de g como el producto de dos involuciones; por la fórmula (2.7) sabemos que solo tres de ellas son diferentes es decir que entre estas al menos dos son iguales.

Dado que $a \neq b$ las primeras dos expresiones son diferentes; si la primera fuese igual a la tercera $a = bab$ lo cual nos daría $ba = ab$ lo cual ya sabemos que no puede pasar. Ahora si la segunda y la tercera expresión fuesen iguales tendríamos $b = bab$ y por lo tanto $e = ab = g$ *!!*

De todo esto se deduce que las primeras tres expresiones en la igualdad (2.14) son diferentes a pares, por lo tanto la cuarta coincide con alguna de las 3 primeras. Razonando de igual manera es fácil llegar a que:

$$a = babab \quad \Rightarrow \quad e = ababab = g^3.$$

□

2.4.5 Proposición
Si $g \in \mathcal{K}[2^2]$*, entonces* $o(g) = 2$.

Demostración. Por la fórmula (2.7) sabemos que g se puede escribir de exactamente 2 maneras diferentes como el producto de dos involuciones. Tomemos $a, b \in \mathcal{K}[2]$ tales que $g = ab$, entonces:

$$g = ab = b(bab) = (bab)(babab).$$

Tenemos así 3 maneras de escribir a g como un elemento de $\mathcal{K}[2]^2$, dado que $b \neq bab$ las dos primera expresiones son diferentes. Así, la ultima expresion coincide con alguna de las dos primeras. Si $b = bab$ entonces $e = ab$ lo cual no puede ser, por lo tanto la tercera expresión no coincide con la segunda. Así, la primera y tercera expresiones son iguales y por lo tanto $b = babab$ o equivalentemente $e = abab = g^2$. □

2.4.6 Proposición
Sean a y b dos elementos diferentes de $\mathcal{K}[2]$. Entonces:

1) $ab = ba \quad \Leftrightarrow \quad ab \in \mathcal{K}[2^2]$.

2) $ab \neq ba \quad \Leftrightarrow \quad ab \in \mathcal{K}[3]$.

Demostración. Por la fórmula (2.7) sabemos que $ab \in \mathcal{K}[1] \cup \mathcal{K}[3] \cup \mathcal{K}[2^2]$. Si $ab \in \mathcal{K}[1]$, entonces $a = b^{-1} = b$, lo cual no puede ser. Entonces $ab \in \mathcal{K}[3] \cup \mathcal{K}[2^2]$, así que basta con demostrar 1). Si $ab \in \mathcal{K}[2^2]$, entonces $(ab)^2 = e$, lo cual implica que $ab = ba$; supongamos ahora que $ab = ba$, entonces $(ab)^2 = e$; de 2.4.5 concluimos que $ab \notin \mathcal{K}[3]$ por lo tanto $ab \in \mathcal{K}[2^2]$. □

2.4.7 Proposición
Si $g \in \mathcal{K}[4]$, entonces $o(g) = 4$.

Demostración. En vista de la fórmula (2.8) de la página 70 existen $a \in \mathcal{K}[2]$ y $b \in \mathcal{K}[3]$ tales que $g = ab$. Si $g^2 = e$, entonces:

$$a(bab) = e \quad \Rightarrow \quad a = bab \quad \Rightarrow \quad g = babb = bab^{-1} \in CL(a) = \mathcal{K}[2].$$

Lo cual no puede ser. Ahora, por la fórmula (2.9) existen exactamente 2 maneras de escribir a $g = xy$, con $x \in \mathcal{K}[2]$ y $y \in \mathcal{K}[2^2]$. Si $gx = xg$ entonces $xyx = y$ y como $x^2 = e$ tendríamos $xy = yx$ y por lo tanto $g^2 = x^2y^2 = e$ lo cual sabemos que no pasa. Así:

$$g = xy = (gxg^{-1})(gyg^{-1}) = (g^2xg^{-2})(g^2yg^{-2}).$$

Son 3 expresiones de g como elemento de $\mathcal{K}[2]\mathcal{K}[2^2]$, de las cuales sabemos existen solo 2 y dado que $x \neq gxg^{-1}$ las dos primeras son diferentes; por lo tanto alguna de ellas coincide con la última; pero también $gxg^{-1} \neq g^2xg^{-2}$ lo cual significa que:

$$x = g^2xg^{-2} \quad \text{y} \quad y = g^2yg^{-2}$$

$$\Rightarrow \quad g^2 \in \mathrm{Z}(\langle x, y\rangle).$$

Como x y y son dos involuciones que no conmutan entre si $\langle x, y\rangle \approx D_n$ donde $n = o(xy = g)$, de esto deducimos que:

$$|\mathrm{Z}(\langle x, y\rangle)| = \begin{cases} 1 & \text{si } 2 \nmid n \\ 0 & \text{si } 2 \mid n \end{cases}$$

Como $e \neq g^2 \in \mathrm{Z}(\langle x, y\rangle)$, tenemos $|\mathrm{Z}(\langle x, y\rangle)| = 2$ y por lo tanto $g^4 = (g^2)^2 = e$. □

2.4.8 Proposición
Sea $k \leq [n/2]$ y $a_1, \ldots, a_k \in \mathcal{K}[2]$. Entonces:

1) *$a_1 \cdots a_k \in \mathcal{K}[2^k]$ si y solo si $a_1, \ldots, a_k$ son distintos y permutables a pares.*

2) *Todo elemento de $\mathcal{K}[2^k]$ se puede representar de manera única (salvo orden) como el producto de k elementos de $\mathcal{K}[2]$.*

Demostración. La demostración se hara por inducción sobre k.

Tomemos dos elementos $a_1, a_2 \in \mathcal{K}[2]$, si estos son permutables y distintos por 2.4.6 tenemos que $a_1a_2 \in \mathcal{K}[2^2]$; inversamente si $a_1a_2 \in \mathcal{K}[2^2]$, entonces $a_1 \neq a_2$ (pues de lo contrario $a_1a_2 \in \mathcal{K}[1]$) podemos aplicar de nuevo 2.4.6 para concluir que $a_1a_2 = a_2a_1$. De la fórmula (2.7) sabemos que un elemento g de $\mathcal{K}[2^2]$ se puede representar de 2 maneras como elemento de $\mathcal{K}[2]^2$; sea una de ellas ab, entonces como a y b conmutan:

$$g = ab = ba.$$

Son las únicas 2 expresiones de g en $\mathcal{K}[2]^2$. Sea ahora $k \geq 3$.

Primero demostraremos la *Existencia* en 2).

Tomemos $g \in \mathcal{K}[2^k]$, entonces de la fórmula (2.11) sabemos que existen exactamente $k!$ formas diferentes de escribir a g como producto de k elementos de $\mathcal{K}[2]$ y k maneras de escribirlo como elemento de $\mathcal{K}[2^{k-1}]\mathcal{K}[2]$.

Sean $x_1, \ldots, x_k \in \mathcal{K}[2^{k-1}]$ y $y_1, \ldots, y_k \in \mathcal{K}[2]$ tales que $g = x_iy_i$. Por la hipótesis de inducción aplicada a x_i existen $b_1^i, \ldots, b_{k-1}^i \in \mathcal{K}[2]$ distintos y permutables a pares tales que:

$$x_i = b_1^i \cdots b_{k-1}^i.$$

Por lo tanto:

$$x_i = b^i_{\sigma(1)} \cdots b^i_{\sigma(k-1)} \quad \forall\ \sigma \in S_{k-1}$$
$$\Rightarrow \qquad g = b^i_{\sigma(1)} \cdots b^i_{\sigma(k-1)} y_i \quad \forall\ \sigma \in S_{k-1}.$$

Tenemos así $|S_{k-1}| = (k-1)!$ expresiones diferentes de g como elemento de $\mathcal{K}[2]^k$ y dado que esto es válido para cualquier j en total tenemos $k(k-1)! = k!$ expresiones de g como elemento de $\mathcal{K}[2]^k$.

Supongamos que existen $x' \in \mathcal{K}[2]^{k-1}$ y $y' \in \mathcal{K}[2]$ tales que $g = x'y'$ pero $x' \notin \mathcal{K}[2^{k-1}]$, entonces la representación $g = x'y' \in \mathcal{K}[2]^k$ sería distinta de las $k!$ representaciones arriba construidas lo cual no puede ser en vista de la fórmula (2.11). Lo que hemos hecho se pude resumir de la siguiente forma:

$$\text{Si } ab \in \mathcal{K}[2^k] \text{ con } a \in \mathcal{K}[2]^{k-1} \text{ y } b \in \mathcal{K}[2] \ \therefore \ a \in \mathcal{K}[2^{k-1}]. \tag{2.15}$$

Probemos ahora el *Si* de 1).

Sean $a_1, \ldots, a_k \in \mathcal{K}[2]$ tales que $g = a_1 \cdots a_k \in \mathcal{K}[2^k]$, entonces:

$$a_1 \cdots a_k = (a_1 \cdots a_{k-1})a_k \in \mathcal{K}[2^k]$$

$$\Rightarrow \quad a_1 \cdots a_{k-1} \in \mathcal{K}[2^{k-1}] \qquad \text{por (2.15)}$$

$$\Rightarrow \quad a_1, \ldots, a_{k-1} \qquad \text{son distintos y permutables a pares}$$

Además:

$$(a_2 \cdots a_k)a_1 = a_1(a_1 \cdots a_k)a_1 \in \mathcal{K}[2^k]$$

$$\Rightarrow \quad a_2 \cdots a_k \in \mathcal{K}[2^{k-1}] \qquad \text{por (2.15)}$$

$$\Rightarrow \quad a_2, \ldots, a_k \qquad \text{son distintos y permutables a pares}$$

Si $a_1, \ldots, a_k$ no fuesen distintos en vista de lo anterior:

$$a_k = a_1$$

$$\Rightarrow \quad a_1 \cdots a_k = a_1 a_k a_2 \cdots a_{k-1} = a_2 \cdots a_{k-1} \in \mathcal{K}[2^k].$$

Como $a_2, \ldots, a_{k-1}$ son $k-2$ elementos de $\mathcal{K}[2]$ distintos y permutables a pares $a_2 \cdots a_{k-1} \in \mathcal{K}[2^{k-2}]$ contradicción. Asi que $a_1, \ldots, a_k$ son distintos, para ver que estos conmutan a pares solo falta demostrar que a_1 y a_k conmutan, para esto notemos que:

$$a_1 \cdots a_k = (a_1 \cdots a_{k-2}a_k)a_{k-1} \in \mathcal{K}[2^k].$$

Aplicando (2.15) $a_1, \ldots a_{k-2}, a_k$ son permutables a pares.

La *unicidad en 2)* es consecuencia de que con estos $a_1, \ldots, a_k$ elementos de $\mathcal{K}[2]$ podemos obtener las $k!$ representaciones de g como elemento de $\mathcal{K}[2]^k$.

Ahora podemos probar los siguiente resultados que nos seran útiles.

$$\text{Si } g \in \mathcal{K}[2^k], \qquad o(g) = 2. \tag{2.16}$$

$$\text{Si } g \in \mathcal{K}[2^k, 3], \quad o(g) = 6. \tag{2.17}$$

$$\text{Si } g \in \mathcal{K}[2^k, 4], \quad o(g) = 4. \tag{2.18}$$

Demostramos que si $g \in \mathcal{K}[2^k]$, entonces $\exists\ a_1, \ldots, a_k \in \mathcal{K}[2]$ tales que $g = a_1 \cdots a_k$ y que bajo estas condiciones $a_1, \ldots, a_k$ son distintos y permutables a pares. Así que:

$$g^2 = a_1^2 \cdots a_k^2 = e.$$

Lo cual demuestra la primera afirmación. Para demostrar las restantes sea $p = 2, 3$ y tomemos $g \in \mathcal{K}[2^k, p]$; en vista de que las tablas de multiplicación de G y S_n son iguales existen únicos $x \in \mathcal{K}[2^k]$ y $y \in \mathcal{K}[p]$ tales que $g = xy$. Además:

$$g = xy = (gxg^{-1})(gyg^{-1}).$$

Son dos representaciones de g en $\mathcal{K}[2^k]\mathcal{K}[p]$, en vista de la unicidad de x y y tenemos:

$$y = gyg^{-1} = (xy)y(y^{-1}x^{-1}) = xyx^{-1}.$$

Así que $xy = yx$ y por lo tanto $o(g) = 6$, si $p = 3$ y $o(g) = 4$ cuando $p = 2$.

Para terminar solo falta probar el *Solo si* en 1). Supongamos que $a_1, \ldots, a_k \in \mathcal{K}[2]$ son distintos y permutables a pares. Por la hipótesis de inducción:

$$x = a_1 \cdots a_{k-1} \in \mathcal{K}[2^{k-1}].$$

De donde se deduce con ayuda de (2.12) que:

$$g = xa_k \in \mathcal{K}[2^k] \cup \mathcal{K}[2^{k-2}, 3] \cup \mathcal{K}[2^{k-2}] \cup \mathcal{K}[2^{k-3}, 4].$$

Por lo arriba demostrado

$$g^2 = e \quad \Rightarrow \quad g \in \mathcal{K}[2^k] \cup \mathcal{K}[2^{k-2}].$$

Supongamos que $g \in \mathcal{K}[2^{k-2}]$, entonces existen $b_1, \ldots, b_{k-2} \in \mathcal{K}[2]$ tales que:

$$g = b_1 \cdots b_{k-2}.$$

Así que:

$$x = a_1 \cdots a_{k-1} = b_1 \cdots b_{k-2} a_k.$$

Por la unicidad de la representación de x en $\mathcal{K}[2]^{k-1}$, existe $j \in \{1, \ldots, k-1\}$ tal que:

$$a_k = a_j$$

Lo cual contradice que $a_1, \ldots, a_k$ sean distintos. Por lo tanto $g \in \mathcal{K}[2^k]$. □

2.4.9 Proposición
Si $a_1, a_2 \in \mathcal{K}[2]$ *y* $a_1a_2 \in \mathcal{K}[2^2]$, *entonces existe* $b \in \mathcal{K}[2]$ *tal que:*

1) $a_1a_2b \in \mathcal{K}[4]$.

2) $a_ib \in \mathcal{K}[3]$ $i = 1, 2$.

Demostración. Por 2.4.8, $a_1 \neq a_2$ y $a_1a_2 = a_2a_1$. Como $a_1a_2 \in \mathcal{K}[3]$ por (2.8) existe $b \in \mathcal{K}[2]$ tal que $a_1a_2b \in \mathcal{K}[4]$ y por lo tanto $a_1b \neq e \neq a_2b$ de lo cual deducimos (2.7) que $a_ib \in \mathcal{K}[2^2] \cup \mathcal{K}[3]$. Supongamos que $a_1b, a_2b \in \mathcal{K}[2^2]$, entonces por 2.4.8 tenemos que $a_ib = ba_i$ luego:

$$(a_1a_2b)^2 = a_1^2a_2^2b^2 = e.$$

Lo cual contradice 2.4.7. Así, a lo más podemos tener un elemento a_ib en $\mathcal{K}[2^2]$. Si este fuese el caso, entonces como a_1 y a_2 conmutan podemos suponer que $a_1b \in \mathcal{K}[2^2]$ y $a_2b \in \mathcal{K}[3]$. Entonces por 2.4.8

$$a_1b = ba_1 \quad \Rightarrow \quad a_1(a_2b) = (a_2b)a_1$$

$$\Rightarrow \quad e = (a_1a_2b)^4 = a_1^4(a_2b)^4 = (a_2b)^4.$$

Pero según 2.4.4 $o(a_2b) = 3$. Tenemos por lo tanto $a_1b, a_2b \in \mathcal{K}[3]$.

□

En este punto es posible demostrar el Teorema de Nagao para $n = 4$. En este caso tenemos que $\emptyset \neq K[2^2]$ y de (2.7) $K[2^2] \subset K[2]K[2]$, podemos por lo tanto elegir $a_1, a_2 \in K[2]$ tales que $a_1a_2 \in K[2^2]$. Por el resultado anterior existe $b \in K[2]$ el cual cumple:

$$a_1b, a_2b \in K[3].$$

Definiendo $c_1 = a_1, c_2 = b$ y $c_3 = a_2$ tenemos que:

$$c_1^2 = c_2^2 = c_3^2 = e,$$

$$c_1c_3 = c_3c_1,$$

$$(c_1c_2)^3 = (c_2c_3)^3 = e.$$

Así, $S_4 \approx H = \langle c_1, c_2, c_3 \rangle < G$. Pero $|G| = |S_4|$ y por lo tanto $G \approx S_4$; el caso $n = 5$ se retomara al final de la sección. De ahora en adelante supondremos que $n \geq 6$,

2.4.10 Proposición
Sean $a_1, a_2, b \in \mathcal{K}[2]$ *tales que* $a_1a_2 \in \mathcal{K}[2^2]$ *y* $a_ib \in \mathcal{K}[3]$, *entonces* $a_1a_2b \in \mathcal{K}[4]$.

Demostración. Sea $x = a_1a_2b$. Por (2.8) $x \in \mathcal{K}[2,3] \cup \mathcal{K}[4] \cup \mathcal{K}[2]$. Supongamos que $x \in \mathcal{K}[2]$, entonces dado que $a_1a_2 = xb \in \mathcal{K}[2^2]$ la parte 2) de 2.4.8 nos da que $b = a_2$ o $b = a_1$, en el primer caso tendríamos $e = a_2b \in \mathcal{K}[3]$ y en el segundo $e = a_1b \in \mathcal{K}[3]$, como ninguna de estas es posible $x \notin \mathcal{K}[2]$.

Si $x \in \mathcal{K}[2,3]$ como ya sabemos existe una única representación de x en $\mathcal{K}[2]\mathcal{K}[3]$; pero como a_1 y a_2 son diferentes y conmutan $x = a_1(a_2b) = a_2(a_1b)$ son dos diferentes representaciones en $\mathcal{K}[2]\mathcal{K}[3]$. Por lo tanto $x = a_1a_2b \in \mathcal{K}[4]$.

□

2.4.11 Proposición
Sean $a_1, a_2, a_3 \in \mathcal{K}[2]$ tales que $a_1a_2a_3 \in \mathcal{K}[2^3]$. Si $b \in \mathcal{K}[2]$ no conmuta con a_1 ni con a_2, entonces si conmuta con a_3.

Demostración. Supongamos que $a_3b \neq ba_3$. Entonces por 2.4.6 $a_ib \in \mathcal{K}[3]$ y como $a_2a_3 \in \mathcal{K}[2^2]$ (por 2.4.8) aplicando el resultado anterior a a_2, a_3, b tenemos que $a_2a_3b \in \mathcal{K}[4]$ (similarmente $a_1a_3b \in \mathcal{K}[4]$) y por lo tanto $x = a_1a_2a_3b \in \mathcal{K}[2]\mathcal{K}[4]$. Pero también $x \in \mathcal{K}[2^3]\mathcal{K}[2]$, entonces de 2.13 tenemos que $x \in \mathcal{K}[2^2] \cup \mathcal{K}[2,4]$.

Si $x \in \mathcal{K}[2^2]$, entonces por 2.4.8 existirían $c_1, c_2 \in \mathcal{K}[2]$ tales que $x = c_1c_2$, por lo tanto $xb = c_1c_2b = a_1a_2a_3 \in \mathcal{K}[2^3]$ y como $c_1, c_1, b \in \mathcal{K}[2]$ de nuevo por 2) de 2.4.8 $b = a_j$ para algun j, lo cual no puede pasar ya que b no conmuta con ninguno de los a_i; tenemos entonces $x \in \mathcal{K}[2,4]$. Como existe una única representación de x como elemento de $\mathcal{K}[2]\mathcal{K}[4]$ y $x = a_1(a_2a_3b) = a_2(a_1a_3b)$ son dos representaciones diferentes tenemos también aquí una contradicción.

□

2.4.12 Proposición
Sean $a_1, a_2, a_3 \in \mathcal{K}[2]$ tales que a_3 conmuta con a_1 y a_2. Si $a_1a_2 \in \mathcal{K}[3]$, entonces existe $b \in \mathcal{K}[2]$ que conmuta con a_1 y que no conmuta con a_2 y a_3.

Demostración. Por 2.4.9 existe un elemento $b \in \mathcal{K}[2]$ tal que $a_3a_2b \in \mathcal{K}[4]$ y $a_2b, a_3b \in \mathcal{K}[3]$, entonces por 2.4.6 b no conmuta con a_2 y a_3, además $a_2ba_3 = a_3(a_3a_2b)a_3 \in \mathcal{K}[3]$. Si b y a_1 conmutan terminamos.

Supongamos que a_1 y b no conmutan. Como $a_1a_2 \in \mathcal{K}[3]$, tenemos que $x = a_1a_2b \in \mathcal{K}[3]\mathcal{K}[2]$, aplicando 2.8 $x \in \mathcal{K}[2,3] \cup \mathcal{K}[4] \cup \mathcal{K}[2]$.

Si $x \in \mathcal{K}[3,2]$, notemos que:

$$x = (a_1a_2)b = (x^{-1}a_1a_2x)(x^{-1}bx).$$

En vista de que existe una única representación de x en $\mathcal{K}[3]\mathcal{K}[2]$ y como $x^{-1}a_1a_2x \in \mathcal{K}[3]$ y $x^{-1}bx \in \mathcal{K}[2]$, entonces:

$$a_1a_2 = x^{-1}a_1a_2x \quad \text{y} \quad b = x^{-1}bx$$

$$\Rightarrow \quad a_1a_2 = (ba_2a_1)a_1a_2(a_1a_2b) = b(a_1a_2b) = bx$$
$$\Rightarrow \quad x = (ba_1)a_2 = (a_1a_2)b.$$

Pero $ba_1 \in \mathcal{K}[3]$ y $a_2 \in \mathcal{K}[2]$, entonces dado que la representación de un elemento de $\mathcal{K}[2,3]$ en $\mathcal{K}[2]\mathcal{K}[3$ es única deberíamos tener $a_2 = b$, contradicción.

Supongamos que $x \in \mathcal{K}[2]$, entonces $xb = a_1a_2 \in \mathcal{K}[3]$ con $xb \in \mathcal{K}[2]^2$, además:

$$a_2(a_1a_2) \in \mathcal{K}[2]\mathcal{K}[3] \subseteq \mathcal{K}[2] \cup \mathcal{K}[2,3] \cup \mathcal{K}[4]$$

Pero dado que $(a_2a_1a_2)^2 = e$ por la Proposición 2.4.7 y el Resultado 2.17 (pag.77) tenemos que $a_2a_1a_2 \in \mathcal{K}[2]$, similarmente $a_1a_2a_1 \in \mathcal{K}[2]$, entonces:

$$xb = a_1a_2 = a_2(a_2a_1a_2) = (a_1a_2a_1)a_1.$$

Son cuatro representaciones de un mismo elemento de $\mathcal{K}[3]$ en $\mathcal{K}[2]^2$ de las cuales sabemos por la fórmula (2.7) hay a lo mas 3 diferentes, claramente las últimas 3 son diferentes y por lo tanto $b \in \{a_2, a_2a_1a_2, a_1\}$ lo cual no puede ser en vista de que estos elemento conmutan con a_3.

Tenemos entonces que $x \in \mathcal{K}[4]$. Por (2.9) $x \in \mathcal{K}[2^2]\mathcal{K}[2]$, así que existen $c_1, c_2, c_3 \in \mathcal{K}[2]$ tales que $c_1c_2 \in \mathcal{K}[2^2]$ y $x = c_1c_2c_3 \notin \mathcal{K}[2^3]$. Por 2.4.8 c_1 y c_2 conmutan además como $c_1c_2c_3 \notin \mathcal{K}[2^3]$, c_1, c_2, c_3 o no son todos diferentes o no conmutan a pares. Supongamos que no son todos diferentes, entonces dado que $c_1 \neq c_2$ se debe tener $c_2 = c_3$ o $c_1 = c_3$ pero en ambos casos tendríamos $c_1c_2c_3 = c_2c_1c_3 \in \mathcal{K}[2]$. Por lo tanto c_1, c_2, c_3 no conmutan a pares y dado que $c_1c_2 = c_2c_1$ es c_3 el que no conmuta con c_1 o con c_2, entonces podemos suponer sin pérdida de generalidad que $c_1c_3 \neq c_3c_1$ y por lo tanto $c_1c_3 \in \mathcal{K}[3]$. Si $c_2c_3 = c_3c_2$, entonces:

$$x^2 = c_1c_2c_3c_1c_2c_3 = (c_1c_3)^2$$
$$\Rightarrow \quad x^6 = e.$$

Lo cual contradice 2.4.7. Así que $c_1c_2 \in \mathcal{K}[2^2]$ y $c_1c_3, c_2c_3 \in \mathcal{K}[3]$.

Ahora, sea $y = c_1xc_1 \in \mathcal{K}[4]$, aplicando el mismo razonamiento podemos obtener $d_1, d_2, d_3 \in \mathcal{K}[2]$ diferentes y tales que $y = d_1d_2d_3$, $d_1d_2 \in \mathcal{K}[2^2]$ y $d_1d_3, d_2d_3 \in \mathcal{K}[3]$. Si definimos $f = c_1d_1$, tenemos:

$$f^{-1}xf = d_1c_1xc_1d_1 = d_1yd_1 = d_2d_3d_1$$
$$\Rightarrow \quad x = fd_2d_3d_1f^{-1}.$$

Sean:

$$h_1 = fd_2f^{-1}, \qquad h_2 = fd_3f^{-1} \quad \text{y} \quad h_3 = fd_1f^{-1}.$$

Obtenemos que $x = h_1h_2h_3$ con $h_i \in \mathcal{K}[2]$ distintos y tales que:

$$h_1h_3 = fd_2d_1f^{-1} \in \mathcal{K}[2^2] \quad \Rightarrow \quad h_1h_3 = h_3h_1.$$

$$h_1h_2 = fd_2d_3f^{-1} \in \mathcal{K}[3] \quad \Rightarrow \quad (h_1h_2)^3 = e.$$
$$h_2h_3 = fd_3d_1f^{-1} \in \mathcal{K}[3] \quad \Rightarrow \quad (h_2h_3)^3 = e.$$

Además:

$$xh_1x^{-1} = h_1h_2h_3h_1h_3h_2h_1 = (h_1h_2)^3h_2 = h_2$$
$$xh_2x^{-1} = h_1h_2h_3h_2h_3h_2h_1 = h_1(h_2h_3)^3h_3h_1 = h_1h_3h_1 = h_3$$
$$\Rightarrow \quad x^2h_1x^{-2} = xh_2x^{-1} = h_3$$

Si $x^3h_1x^{-3} = h_1$, entonces como $x^4 = e$ tendríamos:

$$h_1 = x^{-3}h_1x^3 = xh_1x^{-1} = h_2.$$

Lo cual no puede ser y por lo tanto $h_4 = x^3h_1x^{-3} \neq h_1$. Luego:

$$h_2h_4 = x(h_1)(x^2h_1x^{-2})x^{-1} = x(h_1h_3)x^{-1} \in \mathcal{K}[2^2].$$

$$h_3h_4 = x(xh_1x^{-1})(x^2h_1x^{-2})x^{-1} = x(h_2h_3)x^{-1} \in \mathcal{K}[3].$$
$$h_4h_1 = x(x^2h_1x^{-2})(x^3h_1x^{-3})x^{-1} = x(h_3h_4)x^{-1} \in \mathcal{K}[3].$$

Ahora, de las relaciones obtenidas deducimos que:

$$\begin{array}{rcrcl} x & = & h_1\big[(xh_1x^{-1})(x^2h_1x^{-2})\big] & = & h_1(h_2h_3). \\ x & = & (xh_1x^{-1})\big[(x^2h_1x^{-2})(x^3h_1x^{-3})\big] & = & h_2(h_3h_4). \\ x & = & (x^2h_2x^{-2})\big[(x^3h_1x^{-3})h_1\big] & = & h_3(h_4h_1). \\ x & = & (x^3h_1x^{-3})\big[h_1(xh_1x^{-1})\big] & = & h_4(h_1h_2). \end{array}$$

Son cuatro diferentes representaciones de x como elemento de $\mathcal{K}[2]\mathcal{K}[3]$ ($h_i \neq h_j$ si $i \neq j$); por (2.8) sabemos que solo existen 4 de tales representaciones por lo tanto una de ellas coincide con la representación $x = a_1[a_2b]$ (pues $a_2b \in \mathcal{K}[3]$ ya que $a_2b \neq ba_2$) lo cual significa que existe $i \in \{1, 2, 3, 4\}$ tal que:

$$a_1 = h_i \quad a_2b = h_{i+1}h_{i+2}$$

Donde se entiende que los índices se deben reducir modulo 4. Sean:

$$a_2' = h_{i+1} \in \mathcal{K}[2] \qquad\qquad b' = h_{i+2} \in \mathcal{K}[2].$$

Así, $x = a_1a_2'b'$ y $a_1b' = h_ih_{i+2} \in \mathcal{K}[2^2]$. Luego:

$$a_1x = a_2'b' = a_2b = (a_2ba_2)a_2 = b(ba_2b).$$

Son cuatro representaciones de $a_1x \in \mathcal{K}[3]$ como un elemento de $\mathcal{K}[2]\mathcal{K}[2]$, por (2.7) sabemos que solo 3 de ellas son diferentes. Nos referiremos a ellas como r1,r2,r3 y r4 respectivamente. Demostremos que r2≠r3≠r4≠r2.

Si r2=r3 o r2=r4, entonces $b = a_2$ y por lo tanto $a_1x = a_2b = a_2^2 = e \in \mathcal{K}[3]$, lo cual no puede ser. Si r3=r4, tendriamos $a_2ba_2 = b$, luego $(a_2b)^2 = a_2ba_2b = e$ lo cual contradice 2.4.4 ya que $a_2b \in \mathcal{K}[3]$ toda vez que a_2 y b no conmutan.

Así, r2≠r3≠r4≠r2 y por lo tanto r1 coincide con alguna de estas tres representaciones. Como b' conmuta con a_1 pero b y a_2 no, entonces r2≠r1≠r3. Así debe ser que r1=r4 es decir:

$$a_2' = b \quad \text{y} \quad b' = ba_2b.$$

Como $ba_2 \in \mathcal{K}[3]$ en vista de 2.4.4 $(ba_2)^3 = e$ por lo tanto:

$$(ba_2b)(a_2ba_2) = e$$

$$\Rightarrow \qquad b' = ba_2b = a_2ba_2$$

$$\Rightarrow \qquad b'a_2 = a_2b \neq ba_2 = a_2b'.$$

Es decir, b' no conmuta con a_2. Además en vista de que $a_2a_3 = a_3a_2$ tenemos:

$$b'a_3 = a_2ba_3a_2 \neq a_2a_3ba_2 = a_3b'.$$

Ya que $a_3b \neq ba_3$. Es decir, b' es el elemento buscado. □

Podemos ahora terminar de demostrar el resultado principal de esta sección.

Demostración. De 2.4.1 Distingimos dos casos. Supongamos que n es par y sea $m = n/2$.

Entonces por 2.4.8 existen $a_1, \ldots, a_m \in \mathcal{K}[2]$ tales que:

$$a_1 \cdots a_m \in \mathcal{K}[2^m]$$

Por 2.4.9 podemos encontrar $b_1 \in \mathcal{K}[2]$ tal que:

$$a_1a_2b_1 \in \mathcal{K}[4], \qquad b_1a_1 \neq a_1b_1 \quad \text{y} \quad b_1a_2 \neq a_2b_1$$

Si $b_1 \in \{a_3, \ldots, a_m\}$, tendríamos $a_1a_2b_1 \in \mathcal{K}[2^3]$. Por lo tanto $b_1 \notin \{a_3, \ldots, a_m\}$; sea $j \in \{3, \ldots, m\}$, como $a_1a_2a_j \in \mathcal{K}[3]$ y b no conmuta con a_1 ni con a_2 por 2.4.11 b conmuta con a_j, así:

$$b_1a_1 \neq a_1b_1, \qquad b_1a_2 \neq a_2b_1, \qquad b_1a_j = a_jb_1 \ \forall\ j = 3, \ldots, m$$

Aplicamos 2.4.12 a la tripleta b_1, a_2, a_3 para encontrar $b_2 \in \mathcal{K}[2]$ tal que:

$$b_1 b_2 = b_2 b_1, \qquad a_2 b_2 \neq b_2 a_2, \qquad a_3 b_2 \neq b_2 a_3$$

Si tuviesemos $m > 3$ usariamos de nuevo 2.4.9 para garantizar la existencia de $b_3 \in \mathcal{K}[2]$ tal que $a_3 a_4 b_3 \in \mathcal{K}[4]$, $a_3 b_3 \neq b_3 a_3$ y $a_4 b_3 \neq b_3 a_4$ razonando de la misma manera que se hizo con b_1 llegamos a que:

$$b_i b_3 = b_3 b_i \quad i = 1, 2$$

$$b_3 a_j = a_j b_3 \quad j \neq 3, 4$$

Y continuando de la misma manera obtenemos $b_1, \ldots, b_{m-1}$ tales que:

$$\begin{array}{rcll} b_i b_j & = & b_j b_i & \forall\ i, j. \\ a_i b_j & = & b_j a_i & \forall\ j, i \neq j, j+1. \\ a_i b_j & \neq & b_j a_i & \forall\ i = j, j+1. \end{array}$$

Sean:

$$\begin{array}{rcll} c_{2k-1} & = & a_k & k = 1, \ldots, m \\ c_{2k} & = & b_k & k = 1, \ldots, m-1 \end{array}$$

Definimos así $2m - 1 = n - 1$ elementos c_i tales que:

$$c_i^2 = e \qquad \forall\ i = 1, \ldots, n-1 \tag{2.19}$$

Afirmamos que:

$$c_i c_j = c_j c_i \qquad \text{si } i + 1 < j \tag{2.20}$$

Supongamos que $i = 2r$ y $j = 2s$, entonces:

$$c_i c_j = b_r b_s = b_s b_r = c_j c_i.$$

Si $j = 2s - 1$, tenemos:

$$c_i c_j = b_r a_s = a_s b_r = c_j c_i.$$

Ya que $r + 1 < s$. Cuando i es impar podemos hacer un análisis similar.

También se cumple:

$$c_i c_{i+1} \in \mathcal{K}[3] \qquad \forall\ i < n - 2. \tag{2.21}$$

Esto porque si $i = 2r$, entonces $i + 1 = 2r + 1 = 2(r + 1) - 1$ y por lo tanto:

$$c_i c_{i+1} = b_r a_{r+1} \in \mathcal{K}[3].$$

Y similarmente para $i = 2r - 1$. De (2.19), (2.20), (2.21) podemos concluir que:

$$S_n \approx \langle c_1, \ldots, c_{n-1} \rangle < G$$

Dado que $|G|=|S_n|$, tenemos $G = \langle c_1, \ldots, c_{n-1}\rangle \approx S_n$.

Supogamos ahora que n es impar e incluyamos aquí el caso $n=5$; sea $m = [n/2]$, entonces $n = 2m+1$ y podemos de la misma manera en que hicimos antes encontrar $c_1, \ldots, c_{n-2}$ elementos en G tales que:

$$S_{n-1} \approx \langle c_1, \ldots, c_{n-2}\rangle = H.$$

Como $|H| = (n-1)!$, entonces $[G : H] = n$. Sea $\Phi : G \to S_n$ el homomorfismo de Cayley y K su kernel, entonces $K \lhd G$ y sea ϕ el caracter de G aportado por la representación regular de G/K (ver 1.3.1). Asi:

$$\phi = \sum_{\chi_i \in \mathrm{Irr}(G)} a_i\chi_i \qquad a_i \in \mathbb{Z}^+.$$

Entonces, según 1.2.19 tenemos:

$$K = \bigcap_{a_i \neq 0} \ker \chi_i.$$

Sea χ_i' el caracter de S_n cuyos valores coincide con χ_i, definimos:

$$K' = \bigcap_{a_i \neq 0} ker\ \chi_i \subseteq S_n.$$

Así, $|K| = |K'|$ y $K' \lhd S_n$ de lo cual se sigue que:

$$K' \lhd S_n \quad \& \quad [S_n : K'] \geq n > 2.$$

Entonces $|K'| = 1 = |K|$ y por lo tanto G es isomorfo a un subgrupo de S_n; como $|G| = |S_n|$ se sigue que $G \approx S_n$.

□

Conclusiones

Durante la elaboración de este trabajo pude aplicar los conocimientos adquiridos en la ESFM, ampliarlos y dilucidar algunos conceptos de forma más precisa. Para poder alcanzar el objetivo del trabajo fue necesaria una labor de investigación bibliográfica mucho más extensa de lo que originalmente hubiese previsto, pero fue gracias a todos los artículos y libros que revise que pude darme cuenta del enorme desarrollo que tuvo esta teoría durante la segunda mitad del siglo XX y el papel fundamental que desempeña en gran parte de los resultados más sobresalientes en Teoría de Grupos.

Además de los nuevos conocimientos que fui absorbiendo, desarrollar esta tesis me permitió vislumbrar ligeramente las nuevas direcciones en que se ha orientado la investigación durante los años recientes; y comprobar que el concepto de caracter se ha extendido más allá de los grupos finitos dando lugar a importantes resultados.

Por último me gustaría mencionar que aunque desde la finalización del teorema de clasificación de grupos finitos simples pareciera que esta área ha despertado menos interés en la comunidad matemática, aún queda mucho material por explotar, principalmente en la teoría de caracteres modulares. Espero poder seguir mis estudios en esta dirección o similares.

Bibliografía

[1] Hungerford T. W., *Algebra*, Springer-Verlag New York Inc., 1974

[2] Robinson Dereck J. S., *A Course in the Theory of Groups*, Springer-Verlag New York Inc., 1996

[3] Isaacs I. M., *Character Theory of Finite Groups*, Academic Press Inc., 1976

[4] Berkovich Ya. G. y Zhmud' E. M., *Characters of Finite Groups Part. 1*, Translations of Mathematical Monographs, A.M.S., 1997

[5] Berkovich Ya. G. y Zhmud' E. M., *Characters of Finite Groups Part. 2*, Translations of Mathematical Monographs, A.M.S., 1998

[6] Ledermann W., *Introduction to group characters*, Cambridge Univ. Press, 1977

[7] Gallagher P., *Group characters and commutators*, Math. Z. Vol. 79, 1962

[8] Burnside W., *Theory of groups of finite order*, Dover Publications Inc., 1955

[9] Frobenius G., *Über einen Fundamentalsatz der Gruppentheorie II*, Sitzungsber Preuss. Akad. Wiss. Berlin, 1907

[10] Nagao H., *On the groups with the same table of characters as symmetric groups*, Journal of the Institute of Polytechnics Osaka City. Univ. Series A Vol.8, 1957

[11] Oyama T., *On the groups with the same table of characters as alternating groups*, Osaka Journal of Math. Vol. 1 1964

[12] Apostol T. M., *Introducción a la teoría analítica de números*, Ed. Reverte, 1984