USC
UNIVERSIDADE DE SANTIAGO DE COMPOSTELA
FACULTADE DE MATEMÁTICAS

Traballo Fin de Grao

Caracteres e teorema de Burnside

Manuel González Mora

2018/2019

UNIVERSIDADE DE SANTIAGO DE COMPOSTELA

GRAO DE MATEMÁTICAS

Traballo Fin de Grao

Caracteres e teorema de Burnside

Manuel González Mora

Xullo, 2019

UNIVERSIDADE DE SANTIAGO DE COMPOSTELA

Traballo proposto

Área de Coñecemento: Álxebra
Título: Caracteres e teorema de Burnside
Breve descrición do contido
Neste traballo deberase levar a cabo unha introdución ás representacións de grupos finitos mediante o uso da súa estreita relación cos módulos. Farase énfase especial nos caracteres, tendo como obxectivo final a demostración do teorema de Burnside.
Recomendacións
Ter cursadas as materias Estruturas Alxébricas e Ecuacións Alxébricas.

Índice xeral

Resumo

Se G é un grupo finito de orde n tal que n só ten dous factores primos, dito grupo é resoluble. Isto é o que nos dá o *Teorema p^aq^b de Burnside*, cuxa proba é o fin do traballo.

Para acadar este obxectivo existen dúas vías, a orixinal usando caracteres e outra máis moderna mediante teoría de grupos. Nós empregaremos a orixinal, polo que introduciremos os conceptos de representación dun grupo e a súa relación cos módulos sobre a álxebra de dito grupo, de representación irreducible, paralelamente ó de módulo simple ou de carácter irreducible, todos eles xunto coas súas propiedades. Deste xeito, tras este proceso disporemos dos resultados precisos para a demostración do teorema.

No transcurso da memoria porase de manifesto a versatilidade dos caracteres, especialmente dos caracteres irreducibles, para o estudo de grupos finitos, debido a algunhas das súas propiedades, como ser funcións de clase ou verificar as relacións de ortogonalidade.

Abstract

Whether G is a finite group of order n such that n does not have more than two primes factors, G is solvable. This is what *Burnside's p^aq^b theorem* provides, whose proof is the main objective of this dissertation.

There are two possible ways to prove that theorem, the original one, which uses character theory or another one which employs groups theory. We will use the original way, this is why we are going to introduce the following concepts: group representation and its relation with modules over the group algebra, irreducible representations and modules or irreducible characters, all of them with its properties. Therefore, after this process, we will get the neccesary results to prove the theorem.

Throughtout the dissertation, we realise the versatility of characters, especially the one of irreducible characters, to study finite groups due to some of its properties like being class functions or verifying the orthogonality relations.

Introdución

O inicio da teoría de representacións de grupos finitos pódese situar no 12 de abril de 1896, data na que Frobenius (1849-1917) deu resposta ó plantexamento feito por Dedekind (1831-1916) sobre como factorizar certo polinomio asociado a un grupo, ó que el chamaba "determinante do grupo". Dedekind asociaba a un grupo finito G unha matriz de tamaño $|G| \times |G|$ cuxo determinante era un polinomio. Cando G era un grupo abeliano, Dedekind foi capaz de factorizar este polinomio en factores lineais empregando os caracteres de G (neste caso, homomorfismos de G no grupo dos complexos non nulos). Pola súa banda, Frobenius fixo en pouco tempo o desenrolo da teoría xeral de caracteres e sentou as bases das representacións de grupos finitos. Outros matemáticos que xogaron un papel importante na teoría de representacións foron Schur (1875-1941), discípulo de Frobenius, e Burnside (1852-1927). Estes autores obtiveron os resultados fundamentais acerca das representacións irreducibles (sobre o corpo dos complexos), especialmente Schur, que fixo un uso sistemático do lema que leva o seu nome para estudar esas representacións, aínda que as relacións de ortogonalidade foron obtidas nos traballos de Burnside. Todos estes resultados, xunto cun *Teorema de Maschke*, sobre a semisimplicidade da álxebra dun grupo, relacionaron a teoría de representacións de grupos finitos coa de álxebras de dimensión finita.

A primeira referencia bibliográfica que fai unha presentación sistemática da teoría de representacións de grupos finitos é o libro de Burnside [2], no que se proban moitos resultados de grupos utilizando a teoría de caracteres. Entre eles destaca o seguinte teorema:

Teorema p^aq^b de Burnside: Sexan p e q primos e a e $b \in \mathbb{N}$. Se G é un grupo de orde p^aq^b, G é resoluble.

A partir da súa publicación, na segunda edición do libro en 1911, fixéronse varios intentos para atopar unha proba utilizando unicamente teoría de grupos. Non foi ata 1970 que Goldschmidt [8] a atopou para o caso no que p e q son primos impares, tres anos despois Matsuyama [13] demostrouno para $p = 2$ e finalmente Bender [1] obtivo unha proba para o caso xeral no mesmo ano. Estas probas empregan resultados de Feit e de Thompson e son demostracións que en si mesmas non son moi longas pero por exemplo a demostración de Goldschmidt, que consta de tres páxinas, utiliza un teorema de Glauberman, resultando

ser, en palabras de Curtis e Reiner [5], polo menos tan complicada como a orixinal usando caracteres. Na actualidade o *Teorema de Burnside* continúa a ser un bo exemplo de como a teoría de caracteres é útil para probar resultados de grupos finitos; de feito, hai algúns resultados importantes como o *Teorema de Frobenius*, que se pode consultar no texto de Isaacs [9], do cal non se coñece unha demostración sen utilizar teoría de caracteres, aínda que houbo algúns resultados parciais como os de Corrádi e Horváth [4] e Flavell [7].

A segunda etapa no desenrolo da teoría de representacións foi iniciada por Noether, nela destaca a aparición da teoría modular de representacións, debida sobre todo a Brauer. Pero nesta memoria non se fai ningún estudo nin tampouco aplicacións desta teoría e limitarémonos ó caso da teoría clásica de representacións.

O propósito deste traballo é facer unha proba do teorema de Burnside empregando a teoría de caracteres, para elo estruturamos a memoria do seguinte xeito:

Comézase facendo unha introdución á teoría de representacións dun grupo e as súas equivalencias e, xa asumindo que o grupo co que traballamos é finito, próbase que existe unha correspondencia entre as representacións dun grupo G sobre un corpo K e os $K[G]$-módulos, así como que as representacións equivalentes correspóndense con $K[G]$-módulos isomorfos. Definiremos tamén os conceptos de subrepresentación, suma de representacións e representación cociente.

O segundo capítulo está dedicado ás representacións irreducibles e para iso introducimos os módulos simples ós que van estar asociadas. Facemos unha proba do *Teorema de Maschke* e nas súas hipóteses obtemos resultados sobre os $K[G]$-módulos que trasladamos ás representacións, probando que todo $K[G]$-módulo é semisimple e como consecuencia que toda representación de G sobre K é completamente reducible. Para ter asegurados estes resultados pasamos a traballar sobre o corpo dos complexos, hipótese baixo a cal probaremos o *Lema de Schur*, que como xa se comentou, constitúe unha ferramenta esencial no estudo do número de representacións irreducibles dun grupo.

O terceiro capítulo versa sobre os caracteres de representación dun grupo e as súas propiedades, como ser función de clase ou as relacións de ortogonalidade. Para desenvolver dita teoría introduciranse as clases de conxugación dun grupo e resultados vinculados a elas, como que estas forman unha base de $Z(\mathbb{C}[G])$. Ademais, probaremos que os caracteres irreducibles forman unha base ortonormal do espazo das funcións de clase e que o número de caracteres irreducibles coincide co número de clases de conxugación dun grupo. Tamén veremos neste capítulo as táboas de caracteres e varios exemplos.

O traballo concluirá co cuarto capítulo cuxo fin é a proba do *Teorema* p^aq^b *de Burnside*, antes enunciado, para o que se empregará a teoría de caracteres previamente desenrolada. Ademais concluiremos o capítulo co *Teorema de Hall* que xeneraliza o teorema previo.

Na bibliografía coa que remata a memoria incluíronse os libros empregados para a realización do traballo e tamén referencias históricas, como as citadas previamente, algunhas das cales non foron consultadas directamente. Do mesmo xeito, debemos indicar que foron consultadas máis referencias das que figuran na bibliografía, pero limitámonos a incluír as que citamos explicitamente no texto.

Capítulo 1

Representacións.

Neste capítulo faremos unha introdución ás representacións de grupos e veremos a equivalencia entre representacións dun grupo G e os módulos sobre a álxebra do grupo G sobre un corpo K. Definiremos o concepto de representacións equivalentes e probaremos que os $K[G]$-módulos asociados a ditas representacións son isomorfos. Finalizaremos introducindo as definicións de suma de representacións, subrepresentacións e representacións cocientes, ilustrando en todo momento os conceptos con distintos exemplos. Cabe destacar que unha parte do capítulo segue os textos de Jacobson [11] e Curtis [5], así como tamén foron empregados os textos de Cárdenas [3] e James [12]. No que respecta á notación utilizada, cómpre dicir que V denotará un espazo vectorial de dimensión finita sobre un corpo K ó longo do capítulo.

1.1. Representacións de grupos.

En primeiro lugar introduciremos o concepto de representación dun grupo e estudaremos distintas vías de expresalo:

Definición 1.1. Se G é un grupo, unha **representación lineal** de G en V defínese como un homomorfismo de grupos, ρ, de G no grupo de automorfismos de V, $GL(V)$. V denominarase **espazo da representación** e a súa dimensión será o **grao** de ρ.

Nota 1.2. Na definición previa bastaría esixir que ρ fose un homomorfismo de monoides entre G e o anel de endomorfismos de V, $End_K(V)$; xa que de ser así $\rho(e) = Id$ e, para todo $g_1, g_2 \in G$, $\rho(g_1 g_2) = \rho(g_1)\rho(g_2)$ polo que $\rho(g)\rho(g^{-1}) = \rho(gg^{-1}) = Id$, de onde deducimos que, para todo $g \in G$, $\rho(g) \in GL(V) \subset End_K(V)$. Así, esta nova formulación da definición de representación dun grupo G sobre un corpo K implica a feita en 1.1.

Definición 1.3. Sexan $\rho_1 \colon G \longrightarrow GL(V)$ e $\rho_2 \colon G \longrightarrow GL(W)$ dúas representacións lineais. Diremos que ρ_1 e ρ_2 son **representacións lineais equivalentes** se existe un K-isomorfismo $f : V \longrightarrow W$ tal que

$$\rho_2(g) = f\rho_1(g)f^{-1} \text{ para todo } g \in G.$$

Definición 1.4. Unha **representación matricial** dun grupo G sobre K de **grao** m, defínese como un homomorfismo de grupos, ρ, de G no grupo de matrices invertibles $m \times m$, $GL(m, K)$.

Definición 1.5. Sexan $\rho_1 \colon G \longrightarrow GL(m, K)$ e $\rho_2 \colon G \longrightarrow GL(n, K)$ dúas representacións matriciais dun grupo G sobre K. Diremos que ρ_1 e ρ_2 son **representacións matriciais equivalentes** se $m = n$ e existe unha matriz invertible T tal que

$$\rho_2(g) = T\rho_1(g)T^{-1} \text{ para todo } g \in G.$$

Dada ρ unha representación lineal e $B = \{v_1, v_2, \dots, v_m\}$ unha base do seu espazo de representación, para cada $g \in G$ teremos:

$$\rho(g)(v_j) = \textstyle\sum_{i=1}^{m} a_{ij}v_i \text{ con } j \in \{1, \dots, m\}.$$

A matriz de $\rho(g)$ respecto da base B é unha matriz invertible, $(\rho(g))_B \in GL(m, K)$, e podemos definir a partir de ρ o seguinte homomorfismo de grupos, que será unha representación matricial de G sobre K asociada a ρ:

$$\begin{array}{rcl} \tilde{\rho} \colon G & \longrightarrow & GL(m, K) \\ g & \longmapsto & (\rho(g))_B. \end{array}$$

Se tomásemos outra base de V, B', as matrices $(\rho(g))_B$ e $(\rho(g))_{B'}$ serían semellantes.

Nota 1.6. No que segue empregarase indistintamente a palabra representación para representación lineal e matricial segundo o contexto.

Definición 1.7. Diremos que unha representación dun grupo G sobre un corpo K é **fiel** se é un monomorfismo.

Nesta situación, é claro que un grupo G presenta representacións de calquera grao, pois basta asociar a cada elemento $g \in G$ o elemento neutro de $GL(m, K)$, é dicir, a matriz identidade de orde m. Ademais, cabe destacar que a equivalencia de representacións define unha relación de equivalencia e que toda representación equivalente a unha fiel é fiel.

A continuación veremos algúns exemplos de representacións:

Exemplos 1.8.

1. O homomorfismo dado por $\rho(g) = Id$ para todo $g \in G$ denomínase **representación trivial**. Nótese que a representación trivial é fiel se, e só se, G é o grupo trivial.

2. Sexa G un **grupo cíclico** xerado por un elemento g de orde $n \in \mathbb{N}$, que denotaremos $\boldsymbol{C_n}$, e sexa K un corpo que contén tódalas raíces n-ésimas da unidade, $\omega_1, \ldots, \omega_n$. Unha posible representación de G sobre K sería $\rho\colon G \longrightarrow GL(n, K)$, tal que

$$\rho(g) = \begin{pmatrix} \omega_1 & 0 & \ldots & 0 \\ 0 & \omega_2 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & \omega_n \end{pmatrix}$$

para todo $g \in G$. Ademais,

$$\begin{array}{rcl} \rho\colon G & \longrightarrow & GL(m, \mathbb{C}) \\ g^r & \longmapsto & \rho(g)^r \end{array}$$

é unha representación de G sobre $\mathbb{C}$ se, e só se, $\rho(g)^n = I$.
Isto é doado de ver. Se ρ é unha representación $I = \rho(e) = \rho(g^n) = \rho(g)^n$. Por outra banda, se $\rho(g)^n = I$ tense de forma sinxela, pola definición de ρ, que $\rho(g^i g^j) = \rho(g^{i+j}) = \rho(g)^{i+j} = \rho(g)^i \rho(g)^j$ para $i, j \in \{1, \ldots, n\}$.

Sexa agora C_3, o grupo cíclico de orde tres, xerado por un elemento g e vexamos tres posibles representacións de grao 2 de dito grupo sobre $\mathbb{C}$, ρ_i con $i \in \{1, 2, 3\}$, onde

$$\rho_1(g) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \rho_2(g) = \begin{pmatrix} 1 & 0 \\ 0 & e^{2\Pi i/3} \end{pmatrix} \text{ e } \rho_3(g) = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}.$$

Para ver que efectivamente ρ_1, ρ_2 e ρ_3 son representacións, polo anterior, basta comprobar que se verifica que $\rho_1(g)^3 = I$, $\rho_2(g)^3 = I$ e $\rho_3(g)^3 = I$.

Nótese tamén, que ρ_1 non é fiel, xa que a imaxe de calquera elemento de C_3 é a identidade. Porén, ρ_2 e ρ_3 si o son, pois tanto $\rho_2(g^2)$ como $\rho_3(g^2)$ non son a identidade.

3. Sexa o **grupo diedral**, $\mathbf{D}_8 = \{s, t | s^4 = t^2 = 1, t^{-1}st = s^{-1}\}$. Podemos definir unha representación de grao dous de D_8 sobre $\mathbb{C}$, $\rho\colon D_8 \longrightarrow GL(2, \mathbb{C})$, determinada pola imaxe dos xeradores do grupo:

$$\rho(s) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \text{ e } \rho(t) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Posto que o único elemento de D_8 cuxa imaxe é a matriz identidade é o elemento neutro, ρ é unha representación fiel de D_8 sobre $\mathbb{C}$.

4. Sexan $\mathbf{S}_n$ o **grupo de permutacións (ou grupo simétrico)** e V un K-espazo vectorial de dimensión n con base $B = \{v_1, v_2, \dots, v_n\}$. Entón, podemos definir unha representación de S_n sobre K, $\rho\colon S_n \longrightarrow GL(V)$, que asocie a cada $\sigma \in S_n$ un automorfismo en V, $\rho(\sigma)$, tal que $\rho(\sigma)(v_i) = v_{\sigma(i)}$ para $i \in \{1, \dots, n\}$. Nótese que para dous elementos calquera de S_n, σ_1 e σ_2, verifícase que $\rho(\sigma_1\sigma_2) = \rho(\sigma_1)\rho(\sigma_2)$, polo que podemos concluír que ρ é un homomorfismo de grupos.

   Se particularizamos en $S_3 = \{\sigma_1 = (1), \sigma_2 = (12), \sigma_3 = (13), \sigma_4 = (23), \sigma_5 = (123), \sigma_6 = (132)\}$, posto que $\{(12), (123)\}$ é un conxunto de xeradores de dito grupo, ρ queda determinada por:

$$\rho(12) = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \text{ e } \rho(123) = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}.$$

5. Se partimos dun grupo arbitrario G, finito e de orde $n \in \mathbb{N}$, o *Teorema de Cayley* garante a existencia dun isomorfismo entre G e algún subgrupo de S_n. Así, compondo dito isomorfismo cun homomorfismo como o referido en 4 teremos o que denominaremos unha **representación regular** do grupo G sobre un corpo K. En concreto, supoñamos que $G = \{g_1, g_2, \dots, g_n\}$ é un grupo finito e V un K-espazo vectorial con base $B = \{v_1, v_2, \dots, v_n\}$. É coñecido que, dado $g \in G$ arbitrario, para cada $i \in \{1, \dots, n\}$ existe un único $j \in \{1, \dots, n\}$ tal que $gg_i = g_j$. Deste xeito definiremos $\rho_{reg}\colon G \longrightarrow GL(n, K)$ como a representación de G sobre K que verifica $\rho_{reg}(g)v_i = v_j$ se $gg_i = g_j$ con $i, j \in \{1, \dots, n\}$. Nótese que, pola súa construción, a representación regular dun grupo é fiel e en consecuencia todo grupo terá polo menos unha representación fiel, a regular. En particular, se G é un grupo cíclico, $G = \langle g \rangle$, a representación regular, $\rho_{reg}\colon G \longrightarrow GL(n, K)$, quedaría determinada por

$$\rho_{reg}(g) = \begin{pmatrix} 0 & 0 & \dots & 0 & 1 \\ 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 & 0 \end{pmatrix}.$$

   Outro caso particular de representación regular é a do grupo S_3, que ademais será de distinto grao á xa vista en 4. Xa que $\{(12), (123)\}$ é un conxunto de xeradores de

S_3, a representación regular, $\rho_{reg}\colon S_3 \longrightarrow GL(6,K)$, quedará determinada por

$$\rho_{reg}(12) = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix} \text{ e } \rho_{reg}(123) = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

Nótese que, dado $\sigma \in S_3$, a matriz $\rho_{reg}(\sigma)$ presenta un 1 na posición (i,j) se, e só se, $\sigma_i\sigma_j^{-1} = \sigma$. Así, a partir destas dúas matrices podemos construír a imaxe por ρ_{reg} de calquera elemento de S_3. Por exemplo $\rho_{reg}(23) = \rho_{reg}((12)(123)) = \rho_{reg}(12)\rho_{reg}(123)$.

6. Outro exemplo de representacións son as **representacións unidimensionais** dun grupo G sobre un corpo K, que de forma xeral son homomorfismos, ρ, entre G e K. En relación con estas representacións cabe dicir que se tomamos o grupo abeliano G/G', onde G' é o subgrupo conmutador de G ($G' = \langle gg'g^{-1}g'^{-1} | g, g' \in G\rangle$), posto que $\rho(gg'g^{-1}g'^{-1}) = \rho(g)\rho(g')\rho(g^{-1})\rho(g'^{-1}) = 1$ pódese construír a partir de ρ unha representación do grupo G/G':

$$\begin{array}{rcl} \hat{\rho}\colon G/G' & \longrightarrow & K \\ g''G' & \longmapsto & \rho(g''). \end{array}$$

En consecuencia, hai unha correspondencia biunívoca entre as representacións unidimensionais de G sobre K e as de G/G' sobre K.

Deseguido, comprobaremos se algunhas das representacións dos exemplos previos son equivalentes e buscaremos unha representación equivalente dalgún dos exemplos dados:

Exemplos 1.9.

1. Retomemos as representacións dun grupo cíclico G de orde n recollidas en 2 e 5 de 1.8, que denominaremos ρ_1 e ρ_2 respectivamente, e vexamos que son dúas representacións equivalentes de G sobre un corpo K. Definimos a matriz T referida en 1.5 como

$$T = \begin{pmatrix} 1 & \omega_1 & \omega_1^2 & \ldots & \omega_1^{n-1} \\ 1 & \omega_2 & \omega_2^2 & \ldots & \omega_2^{n-1} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 1 & \omega_n & \omega_n^2 & \ldots & \omega_n^{n-1} \end{pmatrix}.$$

T ten determinante de Van der Monde e, por ser as $\omega_1, \ldots, \omega_n$ distintas entre si e distintas de cero, podemos concluír que T é invertible. Ademais é sinxelo ver que $\rho_1(g) = T\rho_2(g)T^{-1}$.

2. En relación ás representacións do grupo cíclico de orde tres C_3, vistas en 2 de 1.8, cabe destacar que as representacións ρ_2 e ρ_3 non son equivalentes a ρ_1 pois esta última non é fiel a diferencia das outras.

3. Sexa agora o grupo diedral D_8 e a súa representación 3 de 1.8, que nomearemos agora como ρ_1. O obxectivo será buscar unha representación equivalente á que xa temos, para iso podemos tomar a seguinte matriz T nas condicións de 1.5:

$$T = \frac{\sqrt{2}}{2}\begin{pmatrix} 1 & 1 \\ i & -i \end{pmatrix} \text{ e } T^{-1} = \frac{\sqrt{2}}{2}\begin{pmatrix} 1 & -i \\ 1 & i \end{pmatrix}.$$

Deste xeito, a representación

$$\begin{array}{rccl} \rho_2 \colon & D_8 & \longrightarrow & GL(2,\mathbb{C}) \\ & g & \longmapsto & T\rho_1(g)T^{-1} \end{array}$$

será equivalente a ρ_1.

1.2. K[G]-módulos.

A continuación introduciremos os módulos definidos sobre a álxebra dun grupo e estudaremos o paralelismo entre ditas estruturas e as representacións do grupo.

Definición 1.10. Sexa K un corpo. Chamaremos **K-álxebra** a un anel A cun elemento identidade, que tamén sexa K-espazo vectorial. Ademais, pídese que a multiplicación por un escalar verifique

$$\alpha(ab) = (\alpha a)b = a(\alpha b) \text{ para todo } \alpha \in K \text{ e para todo } a, b \in A.$$

Deseguido, describiremos os elementos necesarios para definir o que denominaremos álxebra dun grupo G sobre un corpo K. A partir de agora asumiremos que o grupo G co que traballaremos é finito.

Consideremos tódalas sumas formais, $\sum_{g\in G} \alpha_g g$, con $\alpha_g \in K$ e $g \in G$. Dous destes elementos son iguais se teñen os mesmos coeficientes. Nótese tamén que unha suma formal pode interpretarse como unha aplicación de G en K. As operacións con estes elementos definiranse do seguinte modo:

1. $\sum_{g\in G} \alpha_g g + \sum_{g\in G} \beta_g g = \sum_{g\in G} (\alpha_g + \beta_g) g$.

2. $(\sum_{g\in G}\alpha_g g)(\sum_{g'\in G}\beta_{g'}g') = (\sum_{g,g'\in G}\alpha_g\beta_{g'}gg')$.

3. $\alpha(\sum_{g\in G}\alpha_g g) = \sum_{g\in G}\alpha\alpha_g g$.

Onde $\alpha, \alpha_g, \beta_{g'} \in K$. Se interpretamos as sumas formais como aplicacións definiremos as operacións da seguinte forma:

1. $(f+h)(g) = f(g) + h(g)$.

2. $(fh)(g) = k(g)$ con $k(g) = \sum_{g'g''=g} f(g')h(g'')$.

3. $(\alpha f)(g) = \alpha f(g)$ con $\alpha \in K$.

Definición 1.11. Definimos a **álxebra dun grupo G sobre un corpo K**, $\boldsymbol{K\,[G]}$, como a K-álxebra cuxos elementos son as sumas formais.

Así definida é sinxelo ver que o elemento neutro de $K\,[G]$ é $1 \cdot e$, con $1 \in K$ e e o elemento neutro de G. Ademais temos que, para todo $g \in G$, $1 \cdot g$ constitúe unha suma formal con tódolos coeficientes nulos agás un. Polo tanto, o conxunto formado por estas sumas formais para cada $g \in G$ é un conxunto de elementos linealmente independentes e forman unha base de $K\,[G]$ como K-espazo vectorial. Se ademais identificamos cada $g \in G$ con $1 \cdot g \in K\,[G]$, podemos considerar que G está mergullado en $K\,[G]$.

Proposición 1.12. *Existe unha correspondencia entre as representacións dun grupo G sobre un corpo K e os $K\,[G]$-módulos.*

Demostración. Sexa ρ unha representación de G sobre K. O dito previamente, que nos permite ver G mergullado en $K\,[G]$ e 1.2 proporcionan o seguinte diagrama:

$$\begin{array}{ccc} G & \xrightarrow{\ \rho\ } & GL(V) \\ \downarrow & & \downarrow \\ K\,[G] & & End_K(V) \end{array}$$

do cal extraemos que podemos definir un homomorfismo de aneis:

$$\begin{array}{rccc} \tilde{\rho}\colon & K\,[G] & \longrightarrow & End_K(V) \\ & \sum_{g\in G}\alpha_g g & \longmapsto & \sum_{g\in G}\alpha_g(\rho(g)) \end{array}$$

que induce en V unha estrutura de $K\,[G]$-módulo: $\alpha v = \tilde{\rho}(\alpha)(v)$ para $\alpha \in K\,[G]$ e $v \in V$.

Reciprocamente, se V é un $K\,[G]$-módulo tense un homomorfismo de aneis entre $K\,[G]$ e $End_K(V)$. Restrinxindo dito homomorfismo a G temos un homomorfiso de monoides nas condicións de 1.2, que denominaremos ρ. □

Nota 1.13. Pola demostración previa temos que dado un $K[G]$-módulo V, a representación correspondente, ρ, queda definida para cada $g \in G$ como $\rho(g)(v) = gv$, para cada $v \in V$, onde $\rho(g) \in GL(V)$. Reciprocamente, se $\rho\colon G \longrightarrow GL(V)$ é unha representación de G, a estrutura de $K[G]$-módulo en V determínase construíndo un homomorfismo como o $\tilde{\rho}$ da demostración e definindo $\alpha v = \tilde{\rho}(\alpha)(v)$ para $\alpha \in K[G]$ e $v \in V$.

Exemplos 1.14.

1. Retomemos o exemplo do grupo diedral D_8 explicado en 3 de 1.8 cuxa representación ρ construiamola establecendo a imaxe dos xeradores do grupo:

$$\rho(s) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \text{ e } \rho(t) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

   Sabemos que os elementos de D_8, xerados por s e t, forman unha base de $\mathbb{C}[D_8]$. Por outra banda, se V é un espazo vectorial con base $B = \{v_1, v_2\}$ e interpretamos ρ como unha representación lineal, $\rho\colon G \longrightarrow GL(V)$, dito V presentará unha estrutura de $\mathbb{C}[D_8]$-módulo como a descrita na demostración de 1.12:

$$\begin{aligned} sv_1 &= \tilde{\rho}(s)(v_1) = \rho(s)(v_1) = -v_2 \\ tv_1 &= \tilde{\rho}(t)(v_1) = \rho(t)(v_1) = v_1 \\ sv_2 &= \tilde{\rho}(s)(v_2) = \rho(s)(v_2) = v_1 \\ tv_2 &= \tilde{\rho}(t)(v_2) = \rho(t)(v_2) = -v_2 \end{aligned}$$

2. Sexa o grupo de permutacións S_n e a súa representación ρ, descritos en 4 de 1.8. Entón, basándonos na demostración de 1.12 a estrutura de $K[S_n]$-módulo do V, en cuxo grupo de automorfismos está a imaxe de ρ, queda determinada, para cada $i \in \{1, \dots, n\}$ e cada $\sigma \in S_n$, do seguinte xeito: $\sigma v_i = \rho(\sigma)(v_i) = v_{\sigma(i)}$.

   Particularizando en S_3, posto que é coñecido que dito grupo queda xerado por $\{(12), (123)\}$ a estrutura de $K[S_3]$-módulo de V queda definida por:

$$\begin{aligned} (12)v_1 &= \rho((12))(v_1) = v_2 & \quad (123)v_1 &= \rho((123))(v_1) = v_2 \\ (12)v_2 &= \rho((12))(v_2) = v_1 & \quad (123)v_2 &= \rho((123))(v_2) = v_3 \\ (12)v_3 &= \rho((12))(v_3) = v_3 & \quad (123)v_3 &= \rho((123))(v_3) = v_1 \end{aligned}$$

3. Tomemos un grupo de orde finita G e a súa representación regular nun K-espazo vectorial V descritos en 5 de 1.8. Sabemos que V ten dimensión igual á orde de G, entón calquera V nestas condicións será isomorfo como K-espazo vectorial a $K[G]$, polo que en particular podemos supor que $V = K[G]$. Definamos agora en $K[G]$ unha estrutura de $K[G]$-módulo basándonos en 1.12. Xa vimos que $B = \{1 \cdot g_1, \dots, 1 \cdot g_n\}$

constitúe unha base de $K[G]$; entón, como dado un $g \in G$ arbitrario para cada $i \in \{1, ..., n\}$ existe un único $j \in \{1, ..., n\}$ tal que $gg_i = g_j$, con $g_i, g_j \in G$, a estrutura de $K[G]$-módulo de $K[G]$ queda determinada por $g(1 \cdot g_i) = \rho_{reg}(g)(1 \cdot g_i) = 1 \cdot g_j$. Nótese que este exemplo ilustra que a representación regular dun determinado grupo G ten asociada o $K[G]$-módulo $K[G]$, polo que $\boldsymbol{K[G]}$ recibe o nome de **$\boldsymbol{K[G]}$-módulo regular**.

Teorema 1.15. *Dúas representacións, ρ_1, ρ_2 dun grupo G sobre un corpo K son equivalentes se, e só se, os $K[G]$-módulos correspondentes son isomorfos.*

Demostración. Supoñamos que $\rho_1 : G \longrightarrow GL(V_1)$ e $\rho_2 : G \longrightarrow GL(V_2)$ son dúas representacións equivalentes. Logo, existe un isomorfismo $f : V_1 \longrightarrow V_2$ tal que $\rho_2(g) = f\rho_1(g)f^{-1}$ para todo $g \in G$.

Vexamos que f é un $K[G]$-isomorfismo. Sexan $\alpha = \sum \alpha_i g_i \in K[G]$, $v_1 \in V_1$ arbitrarios e $\tilde{\rho_1}$, $\tilde{\rho_2}$ homomorfismos de aneis análogos ó $\tilde{\rho}$ empregado na demostración de 1.12. Vexamos que $f(\alpha v_1) = \alpha f(v_1)$:

$$f(\alpha v_1) = f(\tilde{\rho_1}(\alpha)(v_1)) = f(\tilde{\rho_1}(\sum \alpha_i g_i)(v_1)) = f(\sum \alpha_i \rho_1(g_i)(v_1)) = \sum \alpha_i f(\rho_1(g_i)(v_1)) = \sum \alpha_i \rho_2(g_i)(f(v_1)) = \tilde{\rho_2}(\sum \alpha_i g_i)(f(v_1)) = \tilde{\rho_2}(\alpha)(f(v_1)) = \alpha f(v_1).$$

Reciprocamente, supoñamos $f : V_1 \longrightarrow V_2$ homomorfismo de $K[G]$-módulos. Sexan ρ_1 e ρ_2 as representacións asociadas ós $K[G]$-módulos V_1 e V_2, respectivamente, tales que

$$\rho_1(g)(v_1) = gv_1, \text{ para } g \in G \text{ e } v_1 \in V_1 \text{ e}$$
$$\rho_2(g)(v_2) = gv_2, \text{ para } g \in G \text{ e } v_2 \in V_2.$$

Por ser f isomorfismo de $K[G]$-módulos temos que $f(gv_1) = gf(v_1)$, para $g \in G$ e $v_1 \in V_1$. Así por ser o diagrama

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

conmutativo para todo $g \in G$ e por f ser isomorfismo de K-espazos vectoriais, concluímos que ρ_1 e ρ_2 son representacións equivalentes. □

Co seguinte exemplo ilustraremos o enunciado no teorema previo:

Exemplo 1.16. Retomemos o C_3 de 1.8. Denotemos simplemente como ρ a representación ρ_3 alí tratada, que quedará definida do seguinte modo:

$$\rho(1) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \ \rho(g) = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix} \text{ e } \rho(g^2) = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}.$$

Sexa V o $\mathbb{C}$-espazo vectorial, con base $B = \{v_1, v_2\}$, de tal maneira que ρ interpretada como representación lineal é un homomorfismo de C_3 en $GL(V)$. Entón V ten estrutura de $\mathbb{C}[C_3]$-módulo que, como $\{1, g, g^2\}$ constitúe unha base de $\mathbb{C}[C_3]$, queda determinada por:

$$\begin{aligned} 1v_1 &= \rho(1)(v_1) = v_1 & 1v_2 &= \rho(1)(v_2) = v_2 \\ gv_1 &= \rho(g)(v_1) = v_2 & gv_2 &= \rho(g)(v_2) = -v_1 - v_2 \\ g^2v_1 &= \rho(g^2)(v_1) = -v_1 - v_2 & g^2v_2 &= \rho(g^2)(v_2) = v_1 \end{aligned}$$

Agora, sexa W outro $\mathbb{C}$-espazo vectorial con base $B' = \{w_1, w_2\}$, isomorfo a V vía $f : V \longrightarrow W$. Dito isomorfismo danos en W outra base, que pode ser por exemplo $B'' = \{f(v_1) = w_1, f(v_2) = -w_1 + w_2\}$. Logo W terá a estrutura de $\mathbb{C}[C_3]$-módulo descrita polo diagrama recollido na demostración de 1.15:

$$\begin{aligned} 1w_1 &= f \circ \rho(1) \circ f^{-1}(w_1) = w_1 & 1w_2 &= f \circ \rho(1) \circ f^{-1}(w_2) = w_2 \\ gw_1 &= f \circ \rho(g) \circ f^{-1}(w_1) = -w_1 + w_2 & gw_2 &= f \circ \rho(g) \circ f^{-1}(w_2) = -w_1 \\ g^2w_1 &= f \circ \rho(g^2) \circ f^{-1}(w_1) = -w_2 & g^2w_2 &= f \circ \rho(g^2) \circ f^{-1}(w_2) = w_1 - w_2 \end{aligned}$$

Entón obtemos outra representación de C_3 sobre $\mathbb{C}$, que denominaremos $\tilde{\rho}$ e que é equivalente a ρ pois $\tilde{\rho}(g) = f \circ \rho(g) \circ f^{-1}$ para todo $g \in C_3$.

1.3. Suma e subrepresentacións.

Nesta derradeira sección do capítulo introduciremos as sumas de representacións, subrepresentacións e representacións cocientes, que serán unha ferramenta útil nos capítulos posteriores.

Definición 1.17. Sexan G un grupo, K un corpo e ρ_1 e ρ_2 dúas representacións de G sobre K, $\rho_1 \colon G \longrightarrow GL(m, K)$ e $\rho_2 \colon G \longrightarrow GL(n, K)$. A **suma das representacións** previas:

$$\rho_1 \bigoplus \rho_2 \colon G \longrightarrow GL(m+n, K)$$

defínese como

$$(\rho_1 \bigoplus \rho_2)(g)(i,j) = \begin{cases} \rho_1(g)(i,j) & \text{se } i,j \in \{1, \dots, m\} \\ \rho_2(g)(i,j) & \text{se } i,j \in \{m+1, \dots, m+n\} \\ 0 & \text{noutros casos,} \end{cases}$$

é dicir:

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

Nota 1.18. Debido á correspondencia entre representacións dun grupo G sobre un corpo K e os $K[G]$-módulos, podemos dicir que a suma de representacións é a representación asociada á suma directa dos $K[G]$-módulos correspondentes a cada unha das representacións sumadas.

Tomemos agora $\rho : G \longrightarrow GL(V)$ unha representación do grupo G sobre un corpo K con $K[G]$-módulo asociado V. Dado $U \subset V$ $K[G]$-submódulo de V, temos que para todo $g \in G$, $\rho(g)(U) \subset U$ e que $U \subset V$ é K-espazo vectorial.

Definición 1.19. Denomínase por **subrepresentación de ρ** á seguinte representación:

$$\begin{aligned} \rho|U \colon G &\longrightarrow GL(U) \\ g &\longmapsto \rho(g)_{/U}. \end{aligned}$$

Unha representación cuxa imaxe veña dada para todo elemento do grupo por unha matriz da forma

$$\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}$$

é suma de subrepresentacións.

Do mesmo xeito, dado o $K[G]$-submódulo de V, U, tamén podemos definir o $K[G]$-módulo V/U que será, de igual modo, K-espazo vectorial.

Definición 1.20. Definiremos **representación cociente de ρ** como a seguinte representación:

$$\begin{aligned} \rho|V/U \colon G &\longrightarrow GL(V/U) \\ g &\longmapsto \rho_|V/U(g) \end{aligned}$$

onde $\rho_|V/U(g)(v+U) = \rho(g)(v) + U$.

Así, se tomamos unha base de V, $B_V = \{v_1, \dots, v_t, v_{t+1}, \dots, v_m\}$, tal que $B_U = \{v_1, \dots, v_t\}$ é unha base de U e $B_{V/U} = \{v_{t+1} + U, \dots, v_m + U\}$ é unha base de V/U, a imaxe da representación ρ correspóndese, para todo $g \in G$, cunha matriz da forma:

$$\rho(g) = \begin{pmatrix} \rho_|U(g) & C \\ 0 & \rho|V/U(g) \end{pmatrix}$$

onde

$$C = \begin{pmatrix} a_{1,t+1} & \dots & a_{1,m} \\ \dots & \dots & \dots \\ a_{t,t+1} & \dots & a_{t,m} \end{pmatrix}$$

é a matriz asociada ó seguinte homomorfismo:

$$\langle\{v_{t+1},\dots,v_m\}\rangle \longrightarrow V \xrightarrow{\rho(g)} V \xrightarrow{\pi} U.$$

Capítulo 2

Representacións irreducibles.

Neste capítulo introduciranse as representacións irreducibles e veremos a súa correspondencia con certo tipo de módulos, os módulos simples. Daremos unha demostración do *Teorema de Maschke* e probaremos, baixo certa hipótese, que todo $K[G]$-módulo é semisimple. Posteriormente restrinxirémonos ó corpo dos complexos, $\mathbb{C}$, para introducir unha proba do *Lema de Schur* e estudaremos como acotar o número máximo de representacións irreducibles non equivalentes dun grupo. A bibliografía empregada neste capítulo é principalmente o texto de James [12], aínda que tamén se fixo uso dos de Sancho [15] e Jacobson [11]. No referente á notación empregada, cabe destacar que por G denotaremos un grupo finito de orde n, como viñamos facendo na última parte do primeiro capítulo.

2.1. Módulos simples e semisimples.

Comezaremos introducindo os conceptos de módulo simple e semisimple así como os de representación irreducibe e reducible e as relacións entre eles:

Definición 2.1. Dise que un módulo V é **simple** se non é nulo e non ten submódulos propios. Se V é suma directa de módulos simples entón diremos que é un módulo **semisimple**.

Definición 2.2. Unha representación ρ de G, dirase **irreducible** se non ten subrepresentacións propias, noutro caso dirase **reducible**. Ademais, se ρ é suma de subrepresentacións irreducibles diremos que é **completamente reducible**.

Equivalentemente, se denotamos por V o $K[G]$-módulo asociado a ρ, podemos dicir por 1.12, que ρ é irreducible se, e só se, V é simple, que é completamente reducible se, e só se, V é semisimple e que é reducible se, e só se, V ten algún $K[G]$-submódulo propio.

Nótese que, polo visto no capítulo previo sobre representacións cocientes, ρ é unha representación reducible con $K[G]$-módulo asociado V e U un $K[G]$-submódulo, se, e só se, podemos expresar a imaxe de ρ para todo $g \in G$ como:

$$\rho(g) = \begin{pmatrix} \rho|U(g) & C \\ 0 & \rho|V/U(g) \end{pmatrix}.$$

Exemplos 2.3.

1. Toda representación de grao 1 é irreducible.

2. A representación dun grupo cíclico G recollida en 2 de 1.8 é completamente reducible pois, polo feito na última sección do capítulo anterior, podemos concluír que unha representación cuxa imaxe é unha matriz diagonal para todo elemento do grupo é suma de representacións de grao 1 e polo tanto irreducibles.

2.2. Teorema de Maschke.

Nesta sección introduciremos dous resultados vertebrais en vindeiros enunciados por sentar as bases para a descomposición de calquera representación dun grupo. O primeiro deles é o *Teorema de Maschke* (aínda que o segundo pode aparecer tamén nomeado como tal en certos textos):

Teorema 2.4 (Teorema de Maschke)**.** *Sexa U un $K[G]$-submódulo de V. Entón, se a característica de K non divide á orde do grupo, hai un $K[G]$-submódulo W de V tal que*

$$V = U \bigoplus W,$$

como suma directa de $K[G]$-módulos.

Demostración. Dado U un $K[G]$-submódulo de V, sabemos que podemos tomar un subespazo vectorial W_0 de V, suplementario de U, de xeito que $V = U \bigoplus W_0$.

Nesta situación, é coñecido que cada $v \in V$ pode escribirse de forma única como suma dun $u \in U$ e un $w_0 \in W_0$. Entón existe un endomorfismo

$$\begin{array}{rccc} \pi\colon & V & \longrightarrow & V \\ & v & \longmapsto & u \end{array}$$

con núcleo W_0 e imaxe U.

Agora, coa finalidade de conseguir un W nas condicións de W_0 que ademais sexa $K[G]$-submódulo, modificaremos π para obter un $K[G]$-homomorfismo cuxo núcleo será o W desexado. Para isto definimos

$$\begin{array}{rcl} \theta\colon V & \longrightarrow & V \\ v & \longmapsto & \frac{1}{n}\sum_{g\in G} g^{-1}\pi(gv) \end{array}$$

que é claramente un homomorfismo de espazos vectoriais con imaxe contida en U. Ademais, está ben definido pois n non divide á característica de K.

Vexamos agora que θ é un $K[G]$-homomorfismo. Como é un homomorfismo de espazos vectoriais bastará ver que para todo $g' \in G$ se verifica que $\theta(g'v) = g'\theta(v)$. Posto que na definición de θ, g percorre tódolos elementos do grupo G, temos que

$$\theta(g'v) = \frac{1}{n}\sum_{g\in G} g^{-1}\pi(gg'v) = g'(\frac{1}{n}\sum_{g\in G} g'^{-1}g^{-1}\pi(gg'v)) =$$

$$g'(\frac{1}{n}\sum_{g\in G}(gg')^{-1}\pi(gg'v)) = g'(\frac{1}{n}\sum_{g\in G} g^{-1}\pi(gv)) = g'\theta(v),$$

xa que para un $g' \in G$ arbitrario gg' percorre G ó igual que fai g. Así temos que θ é un $K[G]$-homomorfismo. Falta comprobar que a imaxe de θ é U, para isto tomamos $v \in V$ cuxa imaxe viña dada por:

$$\theta(v) = \frac{1}{n}\sum_{g\in G} g^{-1}\pi(gv).$$

$\pi(gv) \in U$ e $\pi(gu) = gu$ para todo $v \in V$, $u \in U \subset V$ e $g \in G$. Polo tanto $\theta(u) = u$ para todo $u \in U$ e xa que U é $K[G]$-submódulo de V, temos que efectivamente a imaxe de θ é U. Agora, denominando W ó núcleo de θ, obtense que $V = U \bigoplus W$ onde W é tamén un $K[G]$-submódulo de V. □

Nótese que en termos de representacións o *Teorema de Maschke* pódese enunciar da seguinte forma:

Dada ρ unha representación reducible dun grupo G, $\rho\colon G \longrightarrow GL(m, K)$, é equivalente a unha representación $\tilde{\rho}$ da forma

$$\tilde{\rho}(g) = \begin{pmatrix} \tilde{\rho}|U(g) & 0 \\ 0 & \tilde{\rho}|W(g) \end{pmatrix}$$

para todo $g \in G$.

Cabe destacar tamén que a condición de que a característica de K non divida á orde do grupo é necesaria para que se verifique o *Teorema de Maschke*. Isto queda reflexado no caso dun grupo cíclico, C_p, xerado por un elemento g e de orde un número primo p. Se V é un espazo vectorial sobre o corpo $\mathbb{Z}_p$ con base $B = \{v_1, v_2\}$, por 1.8 sabemos que para $j \in \{0, 1, \ldots, p-1\}$, a aplicación $\rho\colon C_p \longrightarrow GL(2, \mathbb{Z}_p)$, definida por

$$\rho(g^j) = \begin{pmatrix} 1 & 0 \\ j & 1 \end{pmatrix}$$

é unha representación de C_p sobre $\mathbb{Z}_p$, xa que $\rho(g)^2 = I$.

O $\mathbb{Z}_p[C_p]$-módulo correspondente á representación ρ será aquel cuxa estrutura queda determinada por $g^j v_1 = \rho(g^j)v_1 = v_1 + jv_2$ e por $g^j v_2 = \rho(g^j)v_2 = v_2$. Con dita estrutura de $\mathbb{Z}_p[C_p]$-módulo de V é claro que $U = \langle v_2 \rangle$ é un $\mathbb{Z}_p[C_p]$-submódulo de dimensión 1. Porén, non podemos chegar á conclusión do *Teorema de Maschke*, pois U é o único $\mathbb{Z}_p[C_p]$-submódulo de dimensión 1. En caso contrario, supoñamos que existise outro $\mathbb{Z}_p[C_p]$-submódulo W de tal dimensión. Este sería da forma $W = \langle \alpha v_1 + \beta v_2 \rangle$ con $\alpha, \beta \in \mathbb{Z}_p$ e, para todo $g \in C_p$ e $j \in \{0, \dots, p-1\}$, teríase que $g^j(\alpha v_1 + \beta v_2) \in W$. Entón obteriamos o seguinte:

$$\alpha v_1 + (\alpha j + \beta)v_2 = \lambda(\alpha v_1 + \beta v_2), \lambda \in \mathbb{Z}_p \Longrightarrow \left\{ \begin{array}{r} \alpha = \lambda\alpha \\ \alpha j + \beta = \lambda\beta \end{array} \right. \Longrightarrow \alpha = 0 \Longrightarrow W = U.$$

Exemplo 2.5. Consideramos o grupo simétrico S_3 e V o $K[S_3]$-módulo coa estrutura descrita en 2 de 1.14 onde imos supor $K = \mathbb{C}$. Sexa U o subespazo vectorial de V xerado por $u = v_1 + v_2 + v_3$ que é tamén $\mathbb{C}[S_3]$-submódulo pois verifica:

$$(12)u = \rho((12))(u) = \sum_{i=1}^{3} \rho((12))(v_i) = u,$$

$$(123)u = \rho((123))(u) = \sum_{i=1}^{3} \rho((123))(v_i) = u.$$

Nesta situación seguiremos a demostración do *Teorema de Maschke* para conseguir un $\mathbb{C}[S_n]$-submódulo W de V tal que $V = U \bigoplus W$. Así, W_0 podería ser o subespazo vectorial de V xerado por v_1 e v_2. Agora definimos o endomorfismo π como

$$\begin{array}{rccl} \pi\colon V & \longrightarrow & V & \\ v_1 & \longmapsto & 0 & \\ v_2 & \longmapsto & 0 & \\ v_3 & \longmapsto & u & = v_1 + v_2 + v_3. \end{array}$$

Continuando os pasos da demostración do teorema para $i \in \{1, 2, 3\}$ temos

$$\begin{array}{rccl} \theta\colon V & \longrightarrow & V & \\ v_i & \longmapsto & \frac{1}{3}u & \end{array}$$

cuxo núcleo é o seguinte:

$$Ker(\theta) = \{v = \sum_{i=1}^{3} \lambda_i v_i \in V \mid \theta(v) = \sum_{i=1}^{3} \lambda_i \frac{1}{3} u = 0\} =$$

$$\{v = \sum_{i=1}^{3} \lambda_i v_i \in V | \sum_{i=1}^{3} \lambda_i = 0\} = \langle v_1 - v_2, v_2 - v_3 \rangle .$$

Así, $Ker(\theta)$ é o W requerido.

En termos de representacións, o que acabamos de facer é pasar da representación ρ, de S_3 en V, tomando como base de V $B_1 = \{v_1 + v_2 + v_3, v_1, v_2\}$ e tal que a matriz ligada a imaxe de ρ para cada $\sigma \in S_3$ é unha matriz como a seguinte:

$$(\rho(\sigma))_{B_1} = \begin{pmatrix} \rho|U(\sigma) & C \\ 0 & \rho|V/U(\sigma) \end{pmatrix} = \begin{pmatrix} ... & ... & ... \\ 0 & ... & ... \\ 0 & ... & ... \end{pmatrix}$$

a ρ de S_3 en V, pero tomando neste caso como base de V $B_2 = \{v_1+v_2+v_3, v_1-v_2, v_2-v_3\}$ para todo $\sigma \in S_3$. Deste xeito a matriz ligada a imaxe vén dada por unha matriz como a que segue:

$$(\rho(\sigma))_{B_2} = \begin{pmatrix} \rho|U(\sigma) & 0 \\ 0 & \rho|W(\sigma) \end{pmatrix} = \begin{pmatrix} ... & 0 & 0 \\ 0 & ... & ... \\ 0 & ... & ... \end{pmatrix} .$$

A continuación enunciamos o derradeiro resultado clave da sección, que tamén se debe a Maschke:

Teorema 2.6. *Se K é un corpo e a súa característica non divide á orde de G, todo $K[G]$-módulo é semisimple.*

Demostración. Sexa V un $K[G]$-módulo. Supoñamos que $dim(V) > 1$ e que V non é simple, pois se V ten dimensión 1 ou é simple o resultado é trivial.

Nestas hipóteses sempre poderemos atopar un $K[G]$-submódulo propio de V. Entón, chamando U a dito $K[G]$-submódulo de V e aplicando o *Teorema de Maschke*, obtemos un W, $K[G]$-submódulo de V, de tal modo que $V = U \bigoplus W$.

Agora repetiremos o proceso iterativamente con U e W ata ter as descomposicións: $U = U_1 \bigoplus \cdots \bigoplus U_t$ e $W = W_1 \bigoplus \cdots \bigoplus W_r$, onde os U_i, con $i \in \{1, ..., t\}$, e os W_j, con $j \in \{1, ..., r\}$, son $K[G]$-submódulos irreducibles de U e W respectivamente e en consecuencia tamén de V, polo que poderemos expresar V como $V = U_1 \bigoplus \cdots \bigoplus U_t \bigoplus W_1 \bigoplus \cdots \bigoplus W_r$. □

En termos de representacións, o teorema previo supón que toda representación dun grupo G sobre un corpo K, cuxa característica non divide a orde de G, é completamente reducible. É dicir, dada unha representación, en particular ρ, é da forma $\rho = \rho_1 \bigoplus \cdots \bigoplus \rho_t \bigoplus \rho_{t+1} \bigoplus \cdots \bigoplus \rho_{t+r}$, onde ρ é a representación asociada ó $K[G]$-módulo V

e cada ρ_i correspóndese co $K[G]$-submódulo simple U_i para $i \in \{1, \dots, t\}$ ou co W_i para $i \in \{t+1, \dots, t+r\}$, da demostración previa.

Exemplo 2.7. Un caso sinxelo do enunciado do teorema previo é o exemplo 2.5. Nel escribiamos o $\mathbb{C}[S_3]$-módulo V como suma directa dos $\mathbb{C}[S_3]$-submódulos U e W. Xa sabemos que U era $\mathbb{C}[S_3]$-submódulo irreducible, se agora demostramos que W tamén o é, teremos que este exemplo ilustra o teorema previo e a súa demostración. Recordemos que $W = \langle v_1 - v_2, v_2 - v_3 \rangle$ e supoñamos que W ten un $\mathbb{C}[S_3]$-submódulo, $\tilde{W}$, non trivial, que sexa de dimensión 1 e da forma $\tilde{W} = \langle \tilde{w} \rangle$, con $\tilde{w} = \lambda(v_1 - v_2) + \mu(v_2 - v_3)$, onde $\lambda, \mu \in \mathbb{C}$. Isto suporía que $(12)\lambda(v_1 - v_2) + \mu(v_2 - v_3) = \lambda(v_2 - v_1) + \mu(v_1 - v_3)$. Polo tanto, para que se cumpra a igualdade $(12)\tilde{w} = \alpha\tilde{w}$, con $\alpha \in \mathbb{C}$ distinto de 0, $\mu = 0$; entón $\tilde{w}$ será da forma $\lambda(v_1 - v_2)$. Así $(123)\lambda(v_1 - v_2) = \lambda(v_2 - v_3)$, o que constitúe unha contradición, polo que W ten que ser irreducible.

2.3. Lema de Schur.

A partir de agora, ademais de considerar G un grupo finito de orde n, traballaremos co corpo $\mathbb{C}$, garantindo así que a característica do corpo non divida á orde do grupo. Ademais isto conlevará que as representacións coas que traballemos estean definidas tamén sobre $\mathbb{C}$ o que nos permitirá aproveitar propiedades de dito corpo. A continuación, probaremos o lema que dá nome á sección e que terá unha salientable utilidade para demostrar posteriores resultados:

Lema 2.8 (Lema de Schur)**.** *Sexan V e W dous $\mathbb{C}[G]$-módulos simples.*

1. *Se $\theta : V \longrightarrow W$ é un $\mathbb{C}[G]$-homomorfismo, verifícase que θ é un $\mathbb{C}[G]$-isomorfismo ou que $\theta(v) = 0$ para todo $v \in V$.*

2. *Se $\theta : V \longrightarrow V$ é un $\mathbb{C}[G]$-isomorfismo, θ é un múltiplo do $\mathbb{C}[G]$-isomorfismo identidade.*

Demostración.

1. Supoñamos que $\theta(v) \neq 0$ para algún $v \in V$, entón $Im(\theta) \neq \{0\}$. Como a imaxe de θ é un $\mathbb{C}[G]$-submódulo de W e W é simple, tense que $Im(\theta) = W$. Por outra parte, o núcleo de θ é á súa vez $\mathbb{C}[G]$-submódulo de V; como V é simple e $Ker(\theta) \neq V$, teremos que $Ker(\theta) = 0$. Así, se existe algún $v \in V$ para o cal $\theta(v) \neq 0$, θ será isomorfismo.

2. Sábese que θ ten que ter un autovalor $\lambda \in \mathbb{C}$ polo que $Ker(\theta - \lambda Id) \neq 0$. Posto que $\theta - \lambda Id$ é un endomorfismo de módulos, $Ker(\theta - \lambda Id)$ é un $\mathbb{C}[G]$-submódulo de V e por ser V simple tense que $Ker(\theta - \lambda Id) = V$ concluíndo que $(\theta - \lambda Id)(v) = 0$ para todo $v \in V$ e consecuentemente $\theta = \lambda Id$.

□

Proposición 2.9. *Sexa V un $\mathbb{C}[G]$-módulo non nulo tal que todo $\mathbb{C}[G]$-endomomorfismo de V é múltiplo da identidade. Entón V é simple.*

Demostración. Supoñamos que V non é simple. Entón, V terá algún $\mathbb{C}[G]$-submódulo propio, U, e polo *Teorema de Maschke*, 2.4, existirá outro $\mathbb{C}[G]$-submódulo de V, W, tal que $V = U \bigoplus W$. Tomando agora π o $\mathbb{C}[G]$-homomorfismo definido por $\pi(u+w) = u$ para todo $u \in U$ e $w \in W$, empregado na demostración de 2.4, obtemos que π non é múltiplo da identidade, chegando a unha contradición. Así, podemos concluír que V é simple. □

Corolario 2.10. *Sexa $\rho : G \longrightarrow GL(m, \mathbb{C})$ unha representación de G. Entón ρ é irreducible se, e só se, toda matriz A, $m \times m$, verificando*

$$\rho(g)A = A\rho(g) \text{ para todo } g \in G$$

é da forma

$$A = \lambda I_m \text{ con } \lambda \in \mathbb{C}.$$

Demostración. Sexa A unha matriz $m \times m$ con entradas en $\mathbb{C}$. O endomorfismo

$$\begin{array}{ccc} \mathbb{C}^n & \longrightarrow & \mathbb{C}^n \\ v & \longmapsto & Av \end{array}$$

é $\mathbb{C}[G]$-homomorfismo se, e só se, $A(gv) = g(Av)$ para todo $v \in \mathbb{C}$ e $g \in G$ ou equivalentemente se, e só se, $\rho(g)A = A\rho(g)$ para todo $g \in G$. Agora por 2.8 e 2.9 tense o resultado. □

Exemplo 2.11. Retomemos a representación de C_3 descrita en 2 de 1.8 que viña dada por

$$\rho(g) = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$$

posto que a matriz anterior conmuta coa imaxe por ρ de tódolos elementos de C_3, polo corolario previo, temos que ρ é completamente reducible pois $\rho(g)$ non é múltiplo da identidade.

Proposición 2.12. *Supoñamos que G é un grupo abeliano. Entón, todo $\mathbb{C}[G]$-módulo simple, V, ten dimensión* 1.

Demostración. Por ser G abeliano temos que dado $h \in G$ cúmprese que $hgv = ghv$ para todo $g \in G$ e todo $v \in V$. En consecuencia, temos que o endomorfismo

$$\begin{array}{ccc} V & \longrightarrow & V \\ v & \longmapsto & hv \end{array}$$

é $\mathbb{C}[G]$-isomorfismo. Logo polo *Lema de Schur*, 2.8, temos que dito $\mathbb{C}[G]$-isomorfismo é múltiplo do $\mathbb{C}[G]$-isomorfismo identidade, polo que todo subespazo de V é tammén $\mathbb{C}[G]$-submódulo. Como V é simple, necesariamente terá dimensión 1. □

Proposición 2.13. *Sexa ρ unha representación de G en V. Dado $g \in G$ de orde r, existe unha base B de V tal que $(\rho(g))_B$ é diagonal. Ademais, os coeficientes non nulos de $(\rho(g))_B$ son raíces r-ésimas da unidade.*

Demostración. Sexa $H = \langle g \rangle$. Entón V terá estrutura de $\mathbb{C}[H]$-módulo pois, se denotamos por i o homomorfismo inclusión de H en G, é sinxelo ver que $\rho \circ i$ é unha representación de H cuxo $\mathbb{C}[H]$-módulo asociado é V. Así, en base a 2.6, $V = U_1 \bigoplus \cdots \bigoplus U_t$ onde os U_i con $i \in \{1, \ldots, t\}$ son $\mathbb{C}[H]$-submódulos simples de V. Posto que todo grupo cíclico é abeliano, por 2.12 sabemos que cada U_i ten dimensión 1. Logo, tomando para cada i un u_i que xere U_i e denotando por $\omega_1, \ldots, \omega_r$ as raíces r-ésimas da unidade, obtemos por 2 de 1.8 que, para toda representación ρ de G en V, $gu_i = \rho(g)(u_i) = \omega_i u_i$, con $\omega_i \in \{\omega_1, \ldots, \omega_r\}$. En consecuencia, se tomamos $B = \{u_1, \ldots, u_t\}$ como base de V temos que

$$(\rho(g))_B = \begin{pmatrix} \omega_1 & \ldots & 0 \\ \ldots & \ldots & \ldots \\ 0 & \ldots & \omega_t \end{pmatrix}.$$

□

2.4. Número de representacións irreducibles.

Esta sección será a principal do capítulo, pois nela introduciranse os resultados precisos para saber cantas representacións irreducibles non equivalentes ten un determinado grupo. En primeiro lugar veranse unha serie de enunciados que permitirán establecer unha cota superior para dita cantidade de representacións irreducibles.

Proposición 2.14. *Sexa V un $\mathbb{C}[G]$-módulo e supoñamos que*

$$V = U_1 \bigoplus \cdots \bigoplus U_t,$$

onde cada U_i é un $\mathbb{C}[G]$-submódulo simple de V. Se U é un $\mathbb{C}[G]$-submódulo simple de V, entón é isomorfo a algún U_i, con $i \in \{1, \dots, t\}$.

Demostración. Sexa $u \in U$ non nulo. Por hipótese, sabemos que u pode ser escrito de forma única como $u = u_1 + \cdots + u_t$ con $u_i \in U_i$ para cada $i \in \{1, \dots, t\}$. Para probar que U é isomorfo a algún U_i, consideremos $i \in \{1, \dots, t\}$ tal que $u_i \neq 0$ e definimos $\pi_i \colon U \longrightarrow U_i$ por $\pi_i(u) = u_i$. Esta aplicación é trivialmente un $\mathbb{C}[G]$-homomorfismo de módulos. Por outra parte, como U e U_i son simples e $\pi_i \neq 0$, o *Lema de Schur*, 2.8, dános que π_i é un $\mathbb{C}[G]$-isomorfismo e, en consecuencia, U e U_i son $\mathbb{C}[G]$-módulos isomorfos. □

Proposición 2.15. *Sexan V e W dous $\mathbb{C}[G]$-módulos e $\theta \colon V \longrightarrow W$ un $\mathbb{C}[G]$-homomorfismo. Entón existe un $\mathbb{C}[G]$-submódulo de V, U, tal que*

$$V = Ker(\theta) \bigoplus U \quad e \quad U \cong Im(\theta).$$

Demostración. É sabido que $Ker(\theta)$ é un $\mathbb{C}[G]$-submódulo de V; así, polo *Teorema de Maschke*, 2.4, existe outro $\mathbb{C}[G]$-submódulo de V, U, tal que $V = Ker(\theta) \bigoplus U$. Definimos agora o seguinte $\mathbb{C}[G]$-homomorfismo:

$$\begin{array}{rcl} \tilde{\theta} \colon U & \longrightarrow & Im(\theta) \\ u & \longmapsto & \theta(u). \end{array}$$

Posto que, por hipótese, θ é $\mathbb{C}[G]$-homomorfismo, é claro que $\tilde{\theta}$ tamén o é. Vexamos agora que ademais $\tilde{\theta}$ é $\mathbb{C}[G]$-isomorfismo. Se $u \in Ker(\tilde{\theta})$, $u \in Ker(\theta) \cap U = 0$, logo $Ker(\tilde{\theta}) = 0$. Falta probar que $\tilde{\theta}$ é sobrexectivo, para isto sexa $w \in Im(\theta)$ tal que $w = \theta(v)$ para algún $v \in V$. Posto que $V = Ker(\theta) \bigoplus U$, podemos escribir $v = u_0 + u$ con $u_0 \in Ker(\theta)$ e $u \in U$. Entón temos que $w = \theta(v) = \theta(u_0) + \theta(u) = \theta(u) = \tilde{\theta}(u)$ e, polo tanto, $Im(\theta) = Im(\tilde{\theta})$. Así, temos probado que $\tilde{\theta}$ é $\mathbb{C}[G]$-isomorfismo e que $U \cong Im(\theta)$.

□

Teorema 2.16. *Sexa $\mathbb{C}[G]$ o $\mathbb{C}[G]$-módulo regular. Supoñamos*

$$\mathbb{C}[G] = U_1 \bigoplus \cdots \bigoplus U_t$$

onde cada U_i é un $\mathbb{C}[G]$-submódulo simple de $\mathbb{C}[G]$. Se W é un $\mathbb{C}[G]$-módulo simple, entón é isomorfo a algún U_i, con $i \in \{1, \dots, t\}$.

Demostración. Sexa W un $\mathbb{C}[G]$-módulo simple e sexa $w \in W$ un vector non nulo. É claro que $\{\alpha w \mid \alpha \in \mathbb{C}[G]\}$ é un $\mathbb{C}[G]$-submódulo non trivial de W, pero como W é simple tense que $W = \{\alpha w \mid \alpha \in \mathbb{C}[G]\}$. Definimos agora

$$\begin{array}{rcl} \theta \colon \mathbb{C}[G] & \longrightarrow & W \\ \alpha & \longmapsto & \alpha w \end{array}$$

que é $\mathbb{C}[G]$-homomorfismo por verificar que $\theta(\alpha+\alpha') = (\alpha+\alpha')w = \alpha w+\alpha' w = \theta(\alpha)+\theta(\alpha')$ e que $\theta(\alpha\alpha') = (\alpha\alpha')w = t(\alpha' w) = r\theta(\alpha')$, con $\alpha, \alpha' \in \mathbb{C}[G]$. Ademais é claro que $W = Im(\theta)$, é dicir que θ é un $\mathbb{C}[G]$-epimorfismo. Por outra parte, por 2.15, sabemos que existe un $\mathbb{C}[G]$-submódulo de $\mathbb{C}[G]$, U, tal que $\mathbb{C}[G] = Ker(\theta) \bigoplus U$ e $U \cong Im(\theta) = W$. Como W é simple, U tamén o será, e por 2.14, obtemos que $U \cong U_i$ para algún $i \in \{1, \dots, t\}$ polo que $W \cong U_i$. □

Nótese que do anterior teorema extraemos que para atopar os $\mathbb{C}[G]$-módulos simples necesitamos descompor o $\mathbb{C}[G]$-módulo regular, $\mathbb{C}[G]$, en suma directa de $\mathbb{C}[G]$-submódulos simples e que o número de $\mathbb{C}[G]$-módulos simples non isomorfos, é como moito t, onde t é o número de $\mathbb{C}[G]$-submódulos simples que forman parte da suma directa á que é igual $\mathbb{C}[G]$.

En termos de representacións, podemos expresar ρ_{reg} como $\rho_{reg} = \rho_1 \bigoplus \cdots \bigoplus \rho_t$. Nesta situación, dedúcese facilmente que o número de representacións irreducibles non equivalentes dun grupo finito G é como moito t.

A continuación ilustraremos isto cun par de exemplos, pero en xeral non é un método práctico para estudar os $\mathbb{C}[G]$-módulos simples:

Exemplos 2.17.

1. Sexa o grupo $C_3 = \langle g \mid g^3 = 1 \rangle$ e sexa $\omega = e^{2\pi i/3}$. Retomemos a representación regular dun grupo cíclico xenérico descrita en 5 de 1.8 e particularicémola para C_3 sobre o corpo $\mathbb{C}$. Por ser a representación regular terá asociada o $\mathbb{C}[C_3]$-módulo regular, $\mathbb{C}[C_3]$. Sexa entón a representación $\rho_{reg}\colon C_3 \longrightarrow GL(3,\mathbb{C})$, definida por

$$\rho_{reg}(g) = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

   É sinxelo ver que os autovalores de $\rho_{reg}(g)$ son $1, \omega$ e ω^2, as raíces cúbicas da unidade, e que os autovectores asociados son:

$$\begin{aligned} u_0 &= 1 + g + g^2, \\ u_1 &= 1 + \omega^2 g + \omega g^2, \\ u_2 &= 1 + \omega g + \omega^2 g^2. \end{aligned}$$

   Posto que u_0, u_1, u_2 son autovectores asociados a autovalores distintos, son linealmente independentes. Como ademais $\mathbb{C}[C_3]$ ten dimensión 3, $B = \{u_0, u_1, u_2\}$ constitúe unha base de dito espazo vectorial.

En relación á estrutura de $\mathbb{C}[C_3]$-módulo de $\mathbb{C}[C_3]$, esta queda determinada para cada $i \in \{0,1,2\}$ por $gu_i = \rho_{reg}(g)u_i = \omega^i u_i$. Así, deducimos que os $U_i = \langle u_i \rangle$ para $i \in \{0,1,2\}$ son $\mathbb{C}[C_3]$-submódulos simples de $\mathbb{C}[C_3]$ tales que $\mathbb{C}[C_3] = U_0 \bigoplus U_1 \bigoplus U_2$ e que as representacións irreducibles asociadas a cada U_i, en base a 1.12, son aquelas que cumpren que $\rho_i(g^j) = w^{ij}$ con $i,j \in \{0,1,2\}$. Polo tanto, empregando o teorema previo temos que todo $\mathbb{C}[C_3]$-módulo simple, U, é isomorfo a un U_i e, consecuentemente, o número máximo de representacións irreducibles non equivalentes de C_3 é tres.

2. Sexa o grupo $D_6 = \langle s,t : s^3 = t^2 = 1, t^{-1}st = s^{-1} \rangle$. É coñecido que dito grupo é isomorfo ó grupo simétrico S_3, por elo será sinxelo establecer a representación regular de D_6 a partir da representación regular de S_3 construída en 5 de 1.8. Así, dita representación quedará determinada polas imaxes dos xeradores de D_6, t e s:

$$\rho_{reg}(t) = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix} \text{ e } \rho_{reg}(s) = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

Nótese que, por ser a representación regular, o $\mathbb{C}[D_6]$-módulo correspondente será o propio $\mathbb{C}[D_6]$ ó cal asociamos a base $B = \{1, t, st, s^2t, s, s^2\}$. Nesta situación é fácil comprobar que $\rho_{reg}(s)$ ten tres autovalores dobres, 1, ω e ω^2 con autovectores asociados

$$\begin{array}{rclrcl} u_0 &=& 1 + s + s^2 & w_0 &=& t + st + s^2t \\ u_1 &=& 1 + \omega^2 s + \omega s^2 & w_1 &=& t + \omega^2 st + \omega s^2 t \\ u_2 &=& 1 + \omega s + \omega^2 s^2 & w_2 &=& t + \omega st + \omega^2 s^2 t \end{array}$$

que son linealmente independentes. Así os autovectores forman outra base de $\mathbb{C}[D_6]$ e a estrutura de $\mathbb{C}[D_6]$-módulo queda determinada do seguinte xeito:

$$su_i = \omega^i u_i \text{ e } sw_i = \omega^i w_i \text{ con } i \in \{0,1,2\}$$

$$\begin{array}{ll} tu_0 = w_0 & tw_0 = u_0 \\ tu_1 = w_2 & tw_1 = u_2 \\ tu_2 = w_1 & tw_2 = u_1. \end{array}$$

Por tanto, podemos concluír que $\langle u_0, w_0 \rangle$, $\langle u_1, w_2 \rangle$ e $\langle u_2, w_1 \rangle$ son $\mathbb{C}[D_6]$-submódulos. Ademais $\langle u_1, w_2 \rangle$ e $\langle u_2, w_1 \rangle$ son simples, o que se pode comprobar seguindo un proceso análogo ó feito en 2.7. Porén, $\langle u_0, w_0 \rangle$ non o é xa que podemos comprobar que

$\langle u_0 + w_0\rangle$ e $\langle u_0 - w_0\rangle$ son $\mathbb{C}[D_6]$-submódulos simples de $\langle u_0, w_0\rangle$. Así temos a seguinte suma directa de $\mathbb{C}[D_6]$-submódulos simples: $\mathbb{C}[D_6] = U_1 \bigoplus U_2 \bigoplus U_3 \bigoplus U_4$, onde $U_1 = \langle u_0 + w_0\rangle, U_2 = \langle u_0 - w_0\rangle, U_3 = \langle u_1, w_2\rangle$ e $U_4 = \langle u_2, w_1\rangle$. Do anterior e en base a 1.12 tamén se extrae, coma no caso previo, que as representacións irreducibles de D_6 asociadas ós U_i con $i \in \{1,2,3,4\}$, ρ_i, quedan determinadas da seguinte forma:

$$\begin{aligned} \rho_1(s) &= 1, \quad & \rho_1(t) &= \quad 1, \\ \rho_2(s) &= 1, \quad & \rho_2(t) &= -1, \end{aligned}$$

$$\rho_3(s) = \begin{pmatrix} \omega & 0 \\ 0 & \omega^2 \end{pmatrix}, \quad \rho_3(t) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

$$\rho_4(s) = \begin{pmatrix} \omega^2 & 0 \\ 0 & \omega \end{pmatrix} \text{ e } \quad \rho_4(t) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Ademais, polo teorema previo temos que todo $\mathbb{C}[D_6]$-módulo simple, U, é isomorfo a un U_i con $i \in \{1,2,3,4\}$ e, consecuentemente, o número máximo $\mathbb{C}[D_6]$-módulos simples non isomorfos é 4.

A continuación, introduciremos os elementos precisos para poder determinar a cantidade de representacións irreducibles non equivalentes dun grupo G.

Se V e W son dous $\mathbb{C}[G]$-módulos denotaremos por $Hom_{\mathbb{C}[G]}(V,W)$ ó $\mathbb{C}$-espazo vectorial dos $\mathbb{C}[G]$-homomorfismos de V en W.

Proposición 2.18. *Supoñamos que V e W son $\mathbb{C}[G]$-módulos simples. Entón*

$$dim(Hom_{\mathbb{C}[G]}(V,W)) = \begin{cases} 1 & \text{se } V \cong W, \\ 0 & \text{se } V \ncong W. \end{cases}$$

Demostración. Se $V \ncong W$ tense o requerido polo *Lema de Schur*(2.8).

Se $V \cong W$, sexa un $\mathbb{C}[G]$-isomorfismo $\theta : V \longrightarrow W$. Tomando $\phi \in Hom_{\mathbb{C}[G]}(V,W)$, obtemos que $\phi^{-1} \circ \theta$ é un $\mathbb{C}[G]$-isomorfismo de V en V. Logo, polo *Lema de Schur*(2.8), existirá un $\lambda \in \mathbb{C}$ tal que $\phi^{-1} \circ \theta = \lambda Id_V$. Polo tanto $\theta = \lambda\phi$ e, como consecuencia, $dim(Hom_{\mathbb{C}[G]}(V,W)) = 1$. □

Proposición 2.19. *Sexan V, V_1, V_2 e W, W_1 e W_2 $\mathbb{C}[G]$-módulos. Logo:*

1. $dim(Hom_{\mathbb{C}[G]}(V, W_1 \bigoplus W_2)) = dim(Hom_{\mathbb{C}[G]}(V,W_1)) + dim(Hom_{\mathbb{C}[G]}(V,W_2))$.
2. $dim(Hom_{\mathbb{C}[G]}(V_1 \bigoplus V_2, W)) = dim(Hom_{\mathbb{C}[G]}(V_1,W)) + dim(Hom_{\mathbb{C}[G]}(V_2,W))$.

Demostración.

1. Consideremos as aplicacións

$$\begin{array}{rccc} \pi_1\colon & W_1 \bigoplus W_2 & \longrightarrow & W_1 \\ & w_1 + w_2 & \longmapsto & w_1 \end{array} \qquad \begin{array}{rccc} \pi_2\colon & W_1 \bigoplus W_2 & \longrightarrow & W_2 \\ & w_1 + w_2 & \longmapsto & w_2. \end{array}$$

Podemos ver facilmente que estas aplicacións son $\mathbb{C}[G]$-homomorfismos. Se agora tomamos $\theta \in Hom_{\mathbb{C}[G]}(V, W_1 \bigoplus W_2)$, teremos que $\pi_1 \circ \theta \in Hom_{\mathbb{C}[G]}(V, W_1)$ e $\pi_2 \circ \theta \in Hom_{\mathbb{C}[G]}(V, W_2)$. Nesta situación definimos:

$$\begin{array}{rccc} f\colon & Hom_{\mathbb{C}[G]}(V, W_1 \bigoplus W_2) & \longrightarrow & Hom_{\mathbb{C}[G]}(V, W_1) \bigoplus Hom_{\mathbb{C}[G]}(V, W_2) \\ & \theta & \longmapsto & (\pi_1 \circ \theta, \pi_2 \circ \theta). \end{array}$$

Se agora comprobamos que f é un isomorfismo de espazos vectoriais teremos o desexado. Que f é unha aplicación lineal é claro. Verifiquemos agora que f é sobrexectiva, para iso tomemos $\phi_1 \in Hom_{\mathbb{C}[G]}(V, W_1)$ e $\phi_2 \in Hom_{\mathbb{C}[G]}(V, W_2)$. Entón podemos definir unha aplicación $\phi \in Hom_{\mathbb{C}[G]}(V, W_1 \bigoplus W_2)$ tal que $\phi(v) = \phi_1(v) + \phi_2(v)$ para todo $v \in V$. Así temos que dados ϕ_1 e ϕ_2 arbitrarios atopamos un ϕ tal que $f(\phi) = (\phi_1, \phi_2)$ polo que f é sobrexectiva. Tomemos agora un elemento $\theta \in Ker(f)$, logo $\pi_1 \circ \theta(v) = 0$ e $\pi_2 \circ \theta(v) = 0$ para todo $v \in V$ e xa que $\theta(v) = (\pi_1 + \pi_2)(\theta(v))$ temos que $\theta = 0$ e polo tanto f inxectiva.

2. Sexa agora $\theta \in Hom_{\mathbb{C}[G]}(V_1 \bigoplus V_2, W)$. Considerando as restricións de θ a V_1 e V_2 definimos

$$\begin{array}{rccc} h\colon & Hom_{\mathbb{C}[G]}(V_1 \bigoplus V_2, W) & \longrightarrow & Hom_{\mathbb{C}[G]}(V_1, W) \bigoplus Hom_{\mathbb{C}[G]}(V_2, W) \\ & \theta & \longmapsto & (\theta_{/V_1}, \theta_{/V_2}) \end{array}$$

que é un monomorfismo. Sexan agora $\phi_1 \in Hom_{\mathbb{C}[G]}(V_1, W)$ e $\phi_2 \in Hom_{\mathbb{C}[G]}(V_2, W)$. Entón podemos definir unha aplicación $\phi \in Hom_{\mathbb{C}[G]}(V_1 \bigoplus V_2, W)$ tal que $\phi(v_1 + v_2) = \phi_1(v_1) + \phi_2(v_2)$ para todo $v_1 \in V_1$ e $v_2 \in V_2$. Así temos que dados ϕ_1 e ϕ_2 arbitrarios, atopamos un ϕ tal que $h(\phi) = (\phi_1, \phi_2)$, polo que h é tamén sobrexectiva.

□

Corolario 2.20. *Nas hipóteses da proposición anterior:*

$$dim(Hom_{\mathbb{C}[G]}(V_1 \bigoplus \cdots \bigoplus V_t, W_1 \bigoplus \cdots \bigoplus W_r)) = \sum_{i=1}^{t} \sum_{j=1}^{r} dim(Hom_{\mathbb{C}[G]}(V_i, W_j)).$$

Corolario 2.21. *Sexa V un $\mathbb{C}[G]$-módulo e supoñamos que*

$$V = U_1 \bigoplus \cdots \bigoplus U_t,$$

onde cada U_i é un $\mathbb{C}[G]$-módulo simple.

Se W é un $\mathbb{C}[G]$-módulo simple, as dimensións de $Hom_{\mathbb{C}[G]}(V,W)$ e $Hom_{\mathbb{C}[G]}(W,V)$ son iguais ó número de $\mathbb{C}[G]$-módulos U_i, con $i \in \{1,\dots,t\}$, isomorfos a W.

Demostración. Polo corolario previo, 2.20, sabemos que

$$dim(Hom_{\mathbb{C}[G]}(V,W)) = \sum_{i=1}^{t} dim(Hom_{\mathbb{C}[G]}(U_i,W))$$

$$dim(Hom_{\mathbb{C}[G]}(W,V)) = \sum_{i=1}^{t} dim(Hom_{\mathbb{C}[G]}(W,U_i)).$$

Ademais, pola proposición 2.18,

$$dim(Hom_{\mathbb{C}[G]}(U_i,W)) = dim(Hom_{\mathbb{C}[G]}(W,U_i)) = \begin{cases} 1 & \text{se } U_i \cong W, \\ 0 & \text{se } U_i \ncong W. \end{cases}$$

Agora, se denotamos por k o número de $\mathbb{C}[G]$-módulos U_i, con $i \in \{1,\dots,t\}$, isomorfos a W, conclúese facilmente que $dim(Hom_{\mathbb{C}[G]}(V,W)) = k = dim(Hom_{\mathbb{C}[G]}(W,V))$. □

Proposición 2.22. *Se U é un $\mathbb{C}[G]$-módulo,*

$$dim(Hom_{\mathbb{C}[G]}(\mathbb{C}[G],U)) = dim(U).$$

Demostración. Sexa $d = dim(U)$. Tomemos unha base de U, $B_U = \{u_1,\dots,u_d\}$. Definamos para cada $i \in \{1,\dots,d\}$ o seguinte homomorfismo de $\mathbb{C}[G]$-módulos:

$$\begin{array}{rccc} \phi_i\colon \mathbb{C}[G] & \longrightarrow & U \\ \alpha & \longmapsto & \alpha u_i. \end{array}$$

$\phi_i \in Hom_{\mathbb{C}[G]}(\mathbb{C}[G],U)$ xa que para todo $\alpha,\alpha' \in \mathbb{C}[G]$ verifícase que $\phi_i(\alpha\alpha') = (\alpha\alpha')u_i = \alpha(\alpha' u_i) = \alpha\phi_i(\alpha')$. Procedemos agora a probar que $\phi_1,\dots,\phi_d$ constitúen unha base de $Hom_{\mathbb{C}[G]}(\mathbb{C}[G],U)$. Para isto tomamos $\phi \in Hom_{\mathbb{C}[G]}(\mathbb{C}[G],U)$ arbitrario. Logo, para $\lambda_i \in \mathbb{C}$, $\phi(1) = \lambda_1 u_1 + \cdots + \lambda_d u_d$. Posto que $\phi \in Hom_{\mathbb{C}[G]}(\mathbb{C}[G],U)$ tense que $\phi(\alpha) = \alpha\phi(1) = \alpha\lambda_1 u_1 + \cdots + r\lambda_d u_d = \alpha(\lambda_1\phi_1 + \cdots + \lambda_d\phi_d)$ para todo $\alpha \in \mathbb{C}[G]$. Así, $\phi = \lambda_1\phi_1 + \cdots + \lambda_d\phi_d$, polo que $\{\phi_1,\dots,\phi_d\}$ é un conxunto de xeradores de $Hom_{\mathbb{C}[G]}(\mathbb{C}[G],U)$. A continuación, imos ver que é un conxunto linealmente independente, para isto consideramos unha combinación lineal $\lambda_1\phi_1 + \cdots + \lambda_d\phi_d = 0$ cos $\lambda_i \in \mathbb{C}$ e, evaluando en 1, obtemos que $0 = \lambda_1 u_1 + \cdots + \lambda_d u_d$, polo que para todo i, $\lambda_i = 0$. Así chegamos a que $\phi_1,\dots,\phi_d$ son linealmente independentes, e como xa sabiamos que eran un conxunto de xeradores de $Hom_{\mathbb{C}[G]}(\mathbb{C}[G],U)$, podemos dicir que constitúen unha base. Concluímos por tanto que $dim(Hom_{\mathbb{C}[G]}(\mathbb{C}[G],U)) = dim(U)$. □

Tomemos o $\mathbb{C}[G]$-módulo $\mathbb{C}[G]$ e supoñamos que $\mathbb{C}[G] = U_1 \bigoplus \cdots \bigoplus U_t$, onde U_i é un $\mathbb{C}[G]$-módulo simple para todo $i \in \{1, \dots, t\}$. Entón verifícase:

Corolario 2.23. *Dado calquera $\mathbb{C}[G]$-módulo simple U, o número de $\mathbb{C}[G]$-módulos U_i isomorfos a U é igual a $dim(U)$.*

Demostración. Pola proposición previa, 2.22, temos que

$$dim(U) = dim(Hom_{\mathbb{C}[G]}(\mathbb{C}[G], U)).$$

Agora, polo corolario 2.21, o anterior é igual ó número de U_i isomorfos a U. □

Nótese que, polos resultados anteriores, temos que da expresión como suma directa dun número finito de $\mathbb{C}[G]$-submódulos simples do $\mathbb{C}[G]$-módulo regular, $\mathbb{C}[G] = U_1 \bigoplus \cdots \bigoplus U_t$, podemos extraer un subconxunto maximal de $\{U_1, \dots, U_t\}$, $\{U_1, \dots, U_s\}$ con $s \leq t$, que sexa un conxunto maximal de $\mathbb{C}[G]$-módulos simples non isomorfos. Teremos entón o seguinte corolario:

Corolario 2.24. *Dado $\{U_1, \dots, U_s\}$ un conxunto maximal de $\mathbb{C}[G]$-módulos simples non isomorfos, todo $\mathbb{C}[G]$-módulo V pode expresarse como*

$$V \cong (U_1 \bigoplus \cdots \bigoplus U_1) \bigoplus \cdots \bigoplus (U_s \bigoplus \cdots \bigoplus U_s).$$

Demostración. A proba séguese directamente de 2.6, 2.16 e 2.23. □

En termos de representacións, exportando o obtido para $\mathbb{C}[G]$-módulos, conclúese que dada a representación regular do grupo G, $\rho_{reg} = \rho_1 \bigoplus \cdots \bigoplus \rho_t$, podemos tomar un subconxunto maximal de $\{\rho_1, \dots, \rho_t\}$, $\{\rho_1, \cdots, \rho_s\}$ con $s \leq r$, que sexa un conxunto maximal de representacións irreducibles non equivalentes de G e, analogamente ó caso previo, podemos concluír que dado $\{\rho_1, \dots, \rho_s\}$ un conxunto maximal de representacións irreducibles non equivalentes de G temos que toda representación de G, ρ, é equivalente a unha da forma

$$(\rho_1 \bigoplus \cdots \bigoplus \rho_1) \bigoplus \cdots \bigoplus (\rho_s \bigoplus \cdots \bigoplus \rho_s).$$

Exemplos 2.25. Retomemos os exemplos de 2.17.

1. Do primeiro exemplo obtiñamos que $\mathbb{C}[C_3] = U_1 \bigoplus U_2 \bigoplus U_3$. Agora podemos dicir en base ó corolario previo, que posto que tódolos U_i con $i \in \{1, 2, 3\}$ teñen dimensión 1, non son isomorfos. Así, existen exactamente tres representacións irreducibles non equivalentes de C_3, unha asociada a cada U_i que son as descritas en 2.17.

2. Respecto ó segundo exemplo, concluiamos que $\mathbb{C}[D_6] = U_1 \bigoplus U_2 \bigoplus U_3 \bigoplus U_4$. Porén, novamente en base ó corolario previo, como U_3 e U_4 teñen ambos dimensión 2 mentres U_1 e U_2 teñen dimensión 1, necesariamente U_3 e U_4 son $\mathbb{C}[D_6]$-submódulos de $\mathbb{C}[D_6]$ isomorfos, polo que haberá tres $\mathbb{C}[D_6]$-submódulos non isomorfos. Logo hai exactamente tres representacións irreducibles non equivalentes de D_6, ρ_1, ρ_2 e ρ_3 ou ρ_4, que son equivalentes.

Para concluír o capítulo introducimos un resultado que relaciona o grao das representacións irreducibles dun grupo G coa orde de dito grupo e que terá especial interese no seguinte capítulo para a elaboración de táboas de caracteres.

Proposición 2.26. *Sexa $\rho_1, \dots, \rho_s$ un conxunto maximal de representacións irreducibles non equivalentes dun grupo G, cuxos graos son respectivamente $m_1, \dots, m_s$. Entón tense que*

$$|G| = \sum_{i=1}^{s} m_i^2.$$

Demostración. Sexa ρ_{reg} a representación regular de G de grao a orde do grupo, n, que podemos expresar como $\rho_{reg} = \tilde{\rho}_1 \bigoplus \cdots \bigoplus \tilde{\rho}_t$, onde as representacións $\tilde{\rho}_1, \dots, \tilde{\rho}_t$ son representacións irreducibles de G con graos $\tilde{m}_1, \dots, \tilde{m}_t$. Agora, en base a 2.23, temos que o número de $\tilde{\rho}_j$ con $j \in \{1, \dots, t\}$ equivalentes a unha determinada ρ_i, con $i \in \{1, \dots, s\}$, é m_i. En consecuencia

$$n = \sum_{j=1}^{t} \tilde{m}_j = \sum_{i=1}^{s} m_i^2.$$

Como $|G| = n$, tense o resultado. □

Capítulo 3

Caracteres de representacións.

Neste capítulo farase un estudo dos caracteres das representacións dun grupo G, así como das súas propiedades. Para iso, consideraremos a relación de equivalencia definida polas clases de conxugación de G e construímos a partir de ditas clases unha base de $Z(\mathbb{C}[G])$. Introducirase tamén o concepto de carácter dunha representación e certas propiedades dos mesmos, como que todo carácter é unha función de clase ou as relacións de ortogonalidade. Ademais, probaremos que os caracteres de representacións irreducibles (caracteres irreducibles), constitúen unha base ortonormal para o espazo de funcións de clase e deduciremos que o número de caracteres irreducibles é igual ó número de clases de conxugación. Finalmente, definiremos o concepto de táboa de caracteres dun grupo e ilustrarémolo con algúns exemplos. No que respecta á bibliografía, ó longo do capítulo empregáronse os textos de James [12], Ivorra [10] e tamén Rotman [14], Curtis [5] ou Jacobson [11].

3.1. Clases de conxugación.

Comezaremos comentando o que supón que dous elementos dun grupo G sexan conxugados e definiremos o subgrupo centralizador dun elemento de G no grupo. Tamén relacionaremos os cardinais da clase de conxugación dun elemento do grupo e do seu centralizador en G e determinaremos as clases de conxugación de certos grupos de interese:

Definición 3.1. Dados $g, g' \in G$, diremos que son **conxugados** se existe $h \in G$ tal que $g' = h^{-1}gh$. Esta relación, pola que g é conxugado con g', é de equivalencia; o conxunto dos elementos conxugados de g denotarase por g^G e recibe o nome de **clase de conxugación de g**. Así, todo grupo pode expresarse como unión disxunta de clases de conxugación.

Exemplos 3.2.

1. $1^G = \{1\}$ para todo grupo G.

2. Se o grupo é abeliano as clases de conxugación son unitarias. En particular, para un grupo cíclico tamén o son.

3. Sexa o grupo $D_6 = \langle s, t : s^3 = t^2 = 1, t^{-1}st = s^{-1} \rangle$, con elementos $\{1, s, s^2, t, st, s^2t\}$. Por 1 sabemos que $1^{D_6} = \{1\}$. Por outra banda, é claro que para todo $h \in D_6$ cúmprese que $h^{-1}sh = s$ ou $h^{-1}sh = s^2$ e, posto que $t^{-1}st = s^2$, tense que $s^{D_6} = \{s, s^2\}$. Por último, para $i \in \{1, 2\}$ verifícase que $s^{-i}ts^i = s^it$ polo que $t^{D_6} = \{t, st, s^2t\}$. En consecuencia, $1^{D_6}, s^{D_6}$ e t^{D_6} son as clases de conxugación de D_6.

   Nótese que, por ser D_6 e S_3 isomorfos, podemos deducir que as clases de conxugación de S_3 son $1^{S_3} = \{1\}, (123)^{S_3} = \{(123), (132)\}$ e $(12)^{S_3} = \{(12), (13), (23)\}$.

4. Sexa $D_8 = \langle s, t : s^4 = t^2 = 1, t^{-1}st = s^{-1} \rangle$ con elementos $\{1, s, s^2, s^3, t, st, s^2t, s^3t\}$. Por 1 sabemos que $1^{D_8} = \{1\}$. Ademais, tense que para todo $h \in D_8$ cúmprese que $h^{-1}sh = s$ ou $h^{-1}sh = s^3$ e como $t^{-1}st = s^3$ obtemos que $s^{D_8} = \{s, s^3\}$. Do mesmo xeito compróbase que $h^{-1}s^2h = s^2$ para todo $h \in D_8$ polo que $s^{2^{D_8}} = \{s^2\}$. Por outra banda, tense que $h^{-1}th \neq st$ para cada $h \in D_8$ polo que $t^{D_8} \neq st^{D_8}$. Entón, como $s^3ts = s^2t$ e $t^{-1}st^2 = s^3t$, concluímos que $t^{D_8} = \{t, s^2t\}$ e $st^{D_8} = \{st, s^3t\}$. Así, as clases de conxugación de D_8 son $1^{D_8}, s^{D_8}, s^{2^{D_8}}, t^{D_8}$ e st^{D_8}.

5. Sexa $Q = \langle s, t : s^4 = 1, s^2 = t^2, t^{-1}st = s^{-1} \rangle$ o grupo dos cuaternios, con elementos $\{1, s, s^2, s^3, t, st, s^2t, s^3t\}$. Por un razoamento análogo ó feito en 4 chegamos á conclusión de que as súas clases de conxugación son $1^Q = \{1\}, s^Q = \{s, s^3\}, s^{2^Q} = \{s^2\}, t^Q = \{t, s^2t\}$ e $st^Q = \{st, s^3t\}$.

Definición 3.3. Dado $g \in G$ defínese **centralizador de g en G** como o subgrupo de G

$$C_G(g) = \{g' \in G \mid gg' = g'g\}.$$

Teorema 3.4. *Dado $g \in G$, o número de elementos conxugados de g é igual ó índice do seu centralizador:*

$$|g^G| = (G : C_G(g)).$$

Ademais, este número é divisor de $|G|$ se G é finito:

$$(G : C_G(g)) = \frac{|G|}{|C_G(g)|}.$$

Demostración. É coñecido que dada unha actuación dun grupo G sobre un conxunto X, o cardinal da órbita de calquera elemento $x \in X$ coincide co índice do seu subgrupo de isotropía. Se en particular consideramos a actuación conxugación de G sobre si mesmo, é sinxelo ver que g^G é a órbita de g respecto á dita acción e que o centralizador de g, $C_G(g)$

é o subgrupo de isotropía. Polo tanto $|g^G| = (G : C_G(g))$. Ademais, se G finito, aplicando o *Teorema de Lagrange* ó subgrupo de isotropía, tense que $(G : C_G(g)) = \frac{|G|}{|C_G(g)|}$. □

Nesta situación podemos establecer de modo xenérico as clases de conxugación dos grupos D_{2n} e S_n para todo $n \in \mathbb{N}$.

No que respecta ós grupos diedrais, $D_{2n} = \langle s, t \mid s^n = t^2 = 1, t^{-1}st = s^{-1} \rangle$, cómpre discernir entre valores pares e impares de n para determinar as súas clases de conxugación:

Sexa o caso no que n é par e tomemos $n = 2m$. Posto que $t^{-1}s^m t = s^{-m} = s^m$, tense que $C_{D_{2n}}(s^m) = D_{2n}$ e, en consecuencia, $s^{m^{D_{2n}}} = \{s^m\}$. Sexa agora s^i con $i \in \{1, \dots, m-1\}$; entón $(D_{2n} : C_{D_{2n}}(s^i)) \leq (D_{2n} : \langle s \rangle) = 2$, xa que $\langle s \rangle \subset C_{D_{2n}}(s^i)$. Como ademais $t^{-1}s^i t = s^{-i}$, obtense que $\{s^i, s^{-i}\} \subset s^{i^{D_{2n}}}$. Pero $s^i \neq s^{-i}$, pois en caso contrario $s^{2i} = s^i s^{-i} = 1$, contradecindo a definición de D_{2n} ó ser $2i < n$; así, podemos afirmar que $|s^{i^{D_{2n}}}| \geq 2$ e en base a 3.4, $2 \leq |s^{i^{D_{2n}}}| = (D_{2n} : C_{D_{2n}}(s^i)) \leq 2$, do que deducimos que $C_{D_{2n}}(s^i) = \langle s \rangle$ e que $s^{i^{D_{2n}}} = \{s^i, s^{-i}\}$. Por outra banda, $s^i t s^{-i} = s^{2i}t, s^i(st)s^{-i} = s^{2i+1}t$, para todo enteiro i, do que se segue que $t^{D_{2n}} = \{s^{2i}t \mid i \in \{0, \dots, m-1\}\}$ e que $(st)^{D_{2n}} = \{s^{2i+1}t \mid i \in \{0, \dots, m-1\}\}$. Polo tanto, neste caso as clases de conxugación son $1^{D_{2n}}$, $s^{D_{2n}}$, ..., $s^{(m-1)^{D_{2n}}}$, $s^{m^{D_{2n}}}$, $t^{D_{2n}}$ e $st^{D_{2n}}$, como se pode ver no exemplo de D_8 feito en 3.2.

Sexa agora o caso no que n é impar, e tomemos s^i con $i \in \{1, \dots, n-1\}$. De xeito análogo ó feito no caso previo, podemos concluír que $C_{D_{2n}}(s^i) = \langle s \rangle$ e que $s^{i^{D_{2n}}} = \{s^i, s^{-i}\}$, pois $s^i \neq s^{-i}$ xa que do contrario $s^{2i} = s^i s^{-i} = 1$, chegando a unha contradición coa natureza impar de n. Pola súa parte, $\{1, t\} \subset C_{D_{2n}}(t)$ e como $t^{-1}s^i t = s^{-i}$, ningún elemento da forma s^i ou $s^i t$ conmuta con t por ser n impar. Logo, $C_{D_{2n}}(t) \subset \{1, t\}$ e por 3.4, $|t^{D_{2n}}| = n$. Nesta situación, xa que as clases de conxugación de tódolos elementos da forma s^i están definidas, é sinxelo ver que $t^{D_{2n}} = \{t, st, \dots, s^{n-1}t\}$. En conclusión, temos visto que os grupos diedrais D_{2n} con n impar teñen exactamente $\frac{n+3}{2}$ clases de conxugación: $1^{D_{2n}}$, $s^{D_{2n}}$, ..., $s^{\frac{n-1}{2}^{D_{2n}}}$ e $t^{D_{2n}}$, como se pode apreciar no caso particular de D_6 realizado en 3.2.

En relación ós grupos simétricos, S_n, cabe recordar en primeiro lugar, que toda permutación pode ser completamente factorizada nun produto de ciclos actuando sobre conxuntos disxuntos. Así, diremos que dúas permutacións $\sigma, \gamma \in S_n$ teñen a mesma estrutura de ciclos se, e só se, as súas factorizacións coinciden no número de ciclos que teñen de cada orde.

A continuación intoduciremos un resultado que nos permitirá establecer as clases de conxugación dos grupos simétricos, S_n:

Teorema 3.5. *Dúas permutacións $\sigma, \gamma \in S_n$ son conxugadas se, e só se, teñen a mesma estrutura de ciclos.*

Demostración. Vexamos en primeiro lugar que dúas permutacións conxugadas teñen a mesma estrutura de ciclos. Supoñamos que $\sigma, \gamma \in S_n$ son permutacións conxugadas, entón

existe $\alpha \in S_n$ tal que $\sigma = \alpha\gamma\alpha^{-1}$. Se γ deixa fixo un elemento $i \in \{1, \dots, n\}$, σ deixa fixo $\alpha(i)$, xa que $\sigma(\alpha(i)) = \alpha\gamma\alpha^{-1}(\alpha(i)) = \alpha(\gamma(i)) = \alpha(i)$. Se pola contra para $i, j \in \{1, \dots, n\}$ distintos, $\gamma(i) = j$, σ levará $\alpha(i)$ a $\alpha(j)$, pois $\sigma(\alpha(i)) = \alpha\gamma\alpha^{-1}(\alpha(i)) = \alpha(\gamma(i)) = \alpha(j)$. Así, posto que α é bixectiva, é claro que σ e γ teñen a mesma estrutura de ciclos.

Reciprocamente, sexan σ e γ dúas permutacións de S_n coa mesma estrutura de ciclos que factorizan como $\gamma = \delta_1 \cdots \delta_t$ e $\sigma = \beta_1 \cdots \beta_t$ respectivamente. Se tomamos $\alpha \in S_n$ que asocie os ciclos das mesmas ordes da primeira factorización cos da segunda podemos concluír que $\sigma = \alpha\gamma\alpha^{-1}$, polo que σ e γ son permutacións conxugadas. □

Nesta situación podemos concluír que, para todo $\sigma \in S_n$, a súa clase de conxugación, σ^{S_n}, consiste nas permutacións de S_n coa mesma estrutura de ciclo que σ, como se pode apreciar no caso particular de S_3 visto en 3.2.

A continuación inclúese o concepto de centro de $\mathbb{C}[G]$, $Z(\mathbb{C}[G])$, e un resultado que o relacionará coas clases de conxugación do grupo:

Definición 3.6. Definiremos **centro de $\mathbb{C}[G]$** como:

$$Z(\mathbb{C}[G]) = \{\beta \in \mathbb{C}[G] \mid \beta\alpha = \alpha\beta \text{ para todo } \alpha \in \mathbb{C}[G]\}.$$

Proposición 3.7. *Sexa $G = C_1 \cup \dots \cup C_s$ a descomposición de G nas súas clases de conxugación. Se*

$$c_i = \sum_{g_i \in C_i} g_i \in \mathbb{C}[G],$$

$\{c_1, \dots, c_s\}$ é unha base de $Z(\mathbb{C}[G])$.

Demostración. Comezaremos probando que cada $c_i \in Z(\mathbb{C}[G])$. C_i está integrada polas distintas conxugacións posibles dun elemento $g \in G$, $g_1'^{-1}gg_1', \dots, g_n'^{-1}gg_n'$. Así temos:

$$c_i = \sum_{j=1}^{n} g_j'^{-1}gg_j'.$$

Vexamos agora que para todo $h \in G$ $c_ih = hc_i$. Do anterior deducimos que

$$h^{-1}c_ih = \sum_{j=1}^{n} h^{-1}g_j'^{-1}gg_j'h,$$

pero os $h^{-1}g_j'^{-1}gg_j'h \in C_i$. Logo $h^{-1}g_j'^{-1}gg_j'h = h^{-1}g_k'^{-1}gg_k'h \Leftrightarrow g_j'^{-1}gg_j' = g_k'^{-1}gg_k'$. Así:

$$h^{-1}c_ih = \sum_{j=1}^{n} h^{-1}g_j'^{-1}gg_j'h = c_i.$$

Polo que $c_i \in Z(\mathbb{C}[G])$.

Vexamos agora que efectivamente $\{c_1, \dots, c_s\}$ forman unha base de $Z(\mathbb{C}[G])$. En primeiro lugar comprobemos que se trata dun conxunto linealmente independente. É dicir, se $\sum_{i=1}^{s} \lambda_i c_i = 0$, $\lambda_i = 0$ para todo $i \in \{1, \dots, s\}$, o que se ten por ser as clases de conxugacións disxuntas.

Por último probemos que se trata dun conxunto de xeradores de $Z(\mathbb{C}[G])$. Tomemos $\gamma = \sum_{g \in G} \lambda_g g \in Z(\mathbb{C}[G])$. Para todo $h \in G$ temos que $\gamma h = h\gamma$ ou equivalentemente $h^{-1}\gamma h = \gamma$. Entón

$$\sum_{g \in G} \lambda_g h^{-1} g h = \sum_{g \in G} \lambda_g g.$$

Disto extraemos que o coeficiente λ_g é o mesmo para tódolos elementos g da mesma clase de conxugación. Así, $\gamma = \sum_{i=1}^{s} \lambda_i c_i$, onde λ_i é o coeficiente λ_g para algún $g \in c_i$. □

Corolario 3.8. *A dimensión de $Z(\mathbb{C}[G])$ é o número de clases de conxugación de G.*

3.2. Caracteres e as súas propiedades.

Neste epígrafe introduciranse os caracteres e as súas propiedades principais, ilustradas en certos casos particulares, que serán unha ferramenta útil para coñecer propiedades dos grupos dos que proceden, así como para demostrar resultados de maior complexidade.

Antes de definir o concepto de carácter dunha representación necesitamos introducir un resultado previo de trazas de matrices. Como é sabido, a traza dunha matriz $A = (a_{ij})$ de orde m vén dada por $tr(A) = \sum_{i=1}^{m} a_{ii}$. Entón verifícase:

Lema 3.9. *Dadas dúas matrices $m \times m$, A e B verifícase que $tr(AB) = tr(BA)$.*

Demostración. Sexan $A = (a_{ij})$ e $B = (b_{ij})$. Entón, $tr(AB) = \sum_{i=1}^{m} \sum_{j=1}^{m} a_{ij} b_{ji} = \sum_{j=1}^{m} \sum_{i=1}^{m} b_{ji} a_{ij} = tr(BA)$. □

Corolario 3.10. *Se T é unha matriz $m \times m$ invertible tense que $tr(TAT^{-1}) = tr(A)$.*

Demostración. $tr(TAT^{-1}) = tr((TA)T^{-1}) = tr(T^{-1}(TA)) = tr(A)$, onde a segunda igualdade débese ó lema previo. □

Procedamos agora a definir o concepto de carácter:

Definición 3.11. Sexa ρ unha representación de G, $\rho\colon G \longrightarrow Gl(m, \mathbb{C})$. Defínese o **carácter da representación $\boldsymbol{\rho}$** como a aplicación $\chi\colon G \longrightarrow \mathbb{C}$ que asocia a cada $g \in G$ con $tr(\rho(g))$, onde $tr(\rho(g))$ denota a traza da matriz $\rho(g)$.

Nótese que, se $\rho\colon G \longrightarrow Gl(V)$ é a nosa representación e B e B' son bases de V, as matrices $(\rho(g))_B$ e $(\rho(g))_{B'}$ son semellantes e polo corolario previo podemos afirmar que teñen a mesma traza. En consecuencia, o concepto de carácter está ben definido.

Ademais, dado un $\mathbb{C}[G]$-módulo V, en base a 1.13, existe unha representación ρ tal que, para cada $g \in G$, verifica que $\rho(g)(v) = gv$ para todo $v \in V$. Así, o **carácter do $\mathbb{C}[G]$-módulo V** definirase do mesmo xeito que o carácter da representación ρ asociada.

Os caracteres asociados ás representacións de G ou a $\mathbb{C}[G]$-módulos denomínanse en xeral **caracteres de G**. Ademais, nun determinado carácter asociado a unha representación ou a un $\mathbb{C}[G]$-módulo defínese o **grao** como o grao da representación ou como a dimensión do $\mathbb{C}[G]$-módulo citados. Dirase que un carácter é **irreducible** se está asociado a unha representación irreducible ou equivalentemente a un $\mathbb{C}[G]$-módulo simple.

Deseguido probaremos as principais propiedades dos caracteres:

Proposición 3.12.

1. *$\mathbb{C}[G]$-módulos isomorfos teñen o mesmo carácter.*
2. *Os caracteres son constantes sobre clases de conxugación de G.*
3. *O carácter asociado a unha suma directa finita de $\mathbb{C}[G]$-módulos é a suma dos caracteres de cada un dos $\mathbb{C}[G]$-módulos sumados.*

Demostración.

1. Sexan V_1 e V_2 dous $\mathbb{C}[G]$-módulos isomorfos e ρ_1, ρ_2 as súas representacións asociadas, que son equivalentes. Logo, existe unha matriz invertible T tal que para todo $g \in G$, $T\rho_1(g)T^{-1} = \rho_2(g)$. Así, para todo $g \in G$ temos que $\chi_2(g) = tr(\rho_2(g)) = tr(T\rho_1(g)T^{-1}) = tr(\rho_1(g)) = \chi_1(g)$, onde a terceira igualdade débese a 3.10.

2. Sexan g e g' elementos conxugados de G, $g' = hgh^{-1}$ para certo $h \in G$. Logo, dado χ un carácter arbitrario de G, temos que $\chi(g') = \chi(hgh^{-1}) = tr(\rho(hgh^{-1})) = tr(\rho(h)\rho(g)\rho(h)^{-1}) = tr(\rho(g)) = \chi(g)$, onde a cuarta igualdade débese a 3.10.

3. Farémolo para o caso da suma directa de dous $\mathbb{C}[G]$-módulos, $V = V_1 \bigoplus V_2$. Para un maior número de sumandos bastaría aplicar indución. Por 1.18 a representación asociada a V será da forma $\rho = \rho_1 \bigoplus \rho_2$. Así, tense que, para todo $g \in G$

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

de onde extraemos facilmente que, se χ, χ_1, χ_2 son os caracteres asociados a ρ, ρ_1, ρ_2 respectivamente, $\chi(g) = \chi_1(g) + \chi_2(g)$ para todo $g \in G$.

□

Nota 3.13. En termos de representacións, na proposición previa teriamos, por 1, que representacións equivalentes teñen o mesmo carácter asociado e por 3 que o carácter asociado á suma finita de representacións é a suma dos caracteres de cada unha das representacións sumadas.

Proposición 3.14. *Sexa χ un carácter unidimensional. Entón, χ é un homomorfismo de grupos.*

Demostración. Tomemos $g, g' \in G$ e vexamos que $\chi(gg') = \chi(g)\chi(g')$, pero isto é sinxelo porque ó ter χ grao 1 tense que $tr(\rho(g)) = \rho(g)$ para todo $g \in G$. Así, $\chi(gg') = \rho(gg') = \rho(g)\rho(g') = \chi(g)\chi(g')$. □

Proposición 3.15. *Sexa χ o carácter dunha representación $\rho\colon G \longrightarrow GL(m, \mathbb{C})$, V o $\mathbb{C}[G]$-módulo asociado a ρ e g un elemento de G de orde r. Entón verifícanse:*

1. *$\chi(e) = dim(V) = m$.*
2. *$\chi(g)$ é suma de m raíces r-ésimas da unidade.*
3. *$\chi(g^{-1}) = \overline{\chi(g)}$.*
4. *$\chi(g)$ é un número real se g é conxugado de g^{-1}.*

Demostración.

1. Sexa $m = dimV$. Tense que: $\chi(e) = tr(\rho(e)) = tr(I_m) = m$.
2. Por 2.13 existe unha base B de V tal que $(\rho(g))_B$ é unha matriz diagonal cuxos coeficientes non nulos son m raíces r-ésimas da unidade que denotaremos $\omega_1, \dots, \omega_m$. Consecuentemente, $\chi(g) = \omega_1 + \cdots + \omega_m$.
3. Do anterior deducimos que os coeficientes non nulos de $(\rho(g)^{-1})_B$ son $\omega_1^{-1}, \dots, \omega_m^{-1}$, polo que $\chi(g^{-1}) = \omega_1^{-1} + \cdots + \omega_m^{-1}$. Posto que para toda raíz r-ésima da unidade ω tense que $\bar{\omega} = \omega^{-1}$, podemos concluír que $\chi(g^{-1}) = \overline{\omega_1} + \cdots + \overline{\omega_m} = \overline{\chi(g)}$.
4. Se g é conxugado de g^{-1}, por 3.10, tense que $\chi(g) = \chi(g^{-1})$ e, polo anterior, $\overline{\chi(g)} = \chi(g^{-1})$. Disto extraemos que $\chi(g) = \overline{\chi(g)}$ e, polo tanto, $\chi(g)$ é un número real.

□

Definición 3.16. Se χ é un carácter de G definimos o seu **núcleo** como:

$$Ker(\chi) = \{g \in G \mid \chi(g) = \chi(e)\}.$$

Teorema 3.17. *Sexa unha representación $\rho\colon G \longrightarrow GL(m,\mathbb{C})$ con carácter asociado χ. Entón:*

1. *Para todo $g \in G$ tense que $|\chi(g)| \leq m$ e ademais $|\chi(g)| = m$ se, e só se, $\rho(g) = \lambda I_m$.*
2. *$Ker(\chi) = Ker(\rho)$.*

Demostración.

1. Por 3.15, sabemos que, dado $g \in G$ de orde r e arbitrario, $\chi(g) = \omega_1 + \cdots + \omega_m$, onde os ω_i con $i \in \{1, \ldots, m\}$ son raíces r-ésimas da unidade. En consecuencia, $|\chi(g)| = |\omega_1 + \cdots + \omega_m| \leq |\omega_1| + \cdots + |\omega_m| = m$ e a igualdade só se dá se os argumentos das m raíces r-ésimas son iguais, polo que sempre se ten que $|\chi(g)| \leq m$ e ademais se $|\chi(g)| = m$ necesariamente $\rho(g) = \lambda I_m$, con λ unha raíz r-ésima da unidade.

   Reciprocamente, se tomamos $g \in G$ de orde r e $\rho(g) = \lambda I_m$ con $\lambda \in \mathbb{C}$, dedúcese que λ é unha raíz r-ésima da unidade, xa que $\chi(g) = m\lambda$ e por 3.15 $\chi(g)$ é suma de m raíces r-ésimas da unidade. Entón, concluímos que $|\chi(g)| = m$.

2. Se $g \in Ker(\rho)$, $\rho(g) = I_m$ polo que $\chi(g) = m = \chi(e)$ e $g \in Ker(\chi)$.

   Reciprocamente, supoñamos que $g \in Ker(\chi)$, polo que $\chi(g) = \chi(e) = m$. Así, do apartado anterior deduciriamos que $\rho(g) = \lambda I_m$ para algún $\lambda \in \mathbb{C}$. Pero entón $\chi(g) = \lambda\chi(e)$, polo que necesariamente $\lambda = 1$, $\rho(g) = I_m$ e $g \in Ker(\rho)$.

□

Exemplos 3.18.

1. Tomemos a representación de C_n, ρ, recollida en 2 de 1.8, particularizada en C_3 e determinada por:

$$\rho(1) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \rho(g) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \omega & 0 \\ 0 & 0 & \omega^2 \end{pmatrix} \text{ e } \rho(g^2) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \omega^2 & 0 \\ 0 & 0 & \omega \end{pmatrix}.$$

   Temos que o carácter asociado χ verifica que $\chi(1) = 3$, $\chi(g) = 0$ e $\chi(g^2) = 0$. Polo tanto $Ker(\chi) = \{1\}$.

2. Sexa S_3 coa representación 4 de 1.8. Pola definición de carácter temos que $\chi(1) = 3$, $\chi((12)) = 1$, $\chi((13)) = 1$, $\chi((23)) = 1$, $\chi((123)) = 0$ e $\chi((132)) = 0$. Como consecuencia $Ker(\chi) = \{1\}$. Neste exemplo, ilústrase tamén a coincidencia da imaxe do carácter en elementos conxugados (3 de 3.2). Do mesmo xeito, por ser S_3 isomorfo

a D_6, este carácter está ligado a unha representación de D_6. É dicir, existe unha representación de D_6 cuxo carácter é χ, de modo que se verifica que $\chi(1) = 3$, $\chi(t) = 1$, $\chi(st) = 1$, $\chi(s^2t) = 1$, $\chi(s) = 0$ e $\chi(s^2) = 0$.

3. Sexa D_8 coa representación 3 de 1.8. Entón o carácter asociado verifica $\chi(e) = 2$, $\chi(s) = 0$, $\chi(s^2) = -2$, $\chi(s^3) = 0$, $\chi(t) = 0$, $\chi(st) = 0$, $\chi(s^2t) = 0$, $\chi(s^3t) = 0$, e polo tanto $Ker(\chi) = \{1\}$. Neste exemplo ilústrase, como no anterior, a coincidencia da imaxe do carácter en elementos conxugados (3 de 3.2), pero tamén constitúe un contraexemplo da falsedade do recíproco.

Sabemos, polo visto no capítulo previo, que toda representación irreducible dun grupo é equivalente a unha subrepresentación da representación regular. Así, é interesante destacar entre os caracteres asociados a dita representación o seguinte:

Definición 3.19. Definimos **carácter regular**, $\boldsymbol{\chi_{reg}}$ como o carácter da representación regular dun grupo ou equivalentemente como o carácter do $\mathbb{C}[G]$-módulo regular $\mathbb{C}[G]$.

Proposición 3.20. *Se χ_{reg} é o carácter regular de G, temos que*

1. $\chi_{reg}(e) = |G|$.
2. $\chi_{reg}(g) = 0$ *se* $g \neq e$.

Demostración.

1. Sexan $g_1, \dots, g_n$ os elementos de G. É coñecido que ditos elementos forman unha base B de $\mathbb{C}[G]$. Logo, por 3.15 temos que $\chi_{reg}(e) = dim(\mathbb{C}[G]) = |G|$.
2. Sexa agora $g \in G$, $g \neq e$. É coñecido que $gg_i = g_j$ con $i, j \in \{1, \dots, n\}$ distintos. Logo temos que os elementos da diagonal de $(\rho_{reg}(g))_B$ son nulos polo que $\chi_{reg}(g) = 0$.

□

Exemplos 3.21. Retomemos os exemplos vistos en 2.17 e 2.25:

1. Dado C_3 coa súa representación regular, vemos que o carácter asociado cumpre 3.20 pois $\chi_{reg}(1) = 3$, $\chi_{reg}(g) = 0$, $\chi_{reg}(g^2) = 0$, polo que $Ker(\chi_{reg}) = \{1\}$. Por outra banda, en relación coas tres representacións irreducibles obtidas anteriormente, temos que os caracteres irreducibles asociados cumpren

$$\chi_1(1) = 1,\ \chi_1(g) = 1,\ \chi_1(g^2) = 1,$$

$$\chi_2(1) = 1,\ \chi_2(g) = \omega,\ \chi_2(g^2) = \omega^2,$$

$$\chi_3(1) = 1,\ \chi_3(g) = \omega^2,\ \chi_3(g^2) = \omega.$$

Así, este exemplo ilustra que o carácter asociado a unha suma de representacións é a suma dos caracteres asociados a cada sumando, pois para todo $g' \in C_3$ tense que $\chi_{reg}(g') = \chi_1(g') + \chi_2(g') + \chi_3(g')$.

2. O carácter regular de D_6 tamén verifica 3.20: $\chi_{reg}(1) = 6$, $\chi_{reg}(s) = 0$, $\chi_{reg}(s^2) = 0$, $\chi_{reg}(t) = 0$, $\chi_{reg}(st) = 0$, $\chi_{reg}(s^2t) = 0$, polo que $Ker(\chi_{reg}) = \{1\}$. No referente ás representacións irreducibles cuxa suma é igual á regular, obtidas previamente, temos que os caracteres irreducibles asociados cumpren

$$\chi_1(1) = 1,\ \chi_1(s) = 1,\ \chi_1(s^2) = 1,\ \chi_1(t) = 1,\ \chi_1(st) = 1,\ \chi_1(s^2t) = 1,$$

$$\chi_2(1) = 1,\ \chi_2(s) = 1,\ \chi_2(s^2) = 1,\ \chi_2(t) = -1,\ \chi_2(st) = -1,\ \chi_2(s^2t) = -1,$$

$$\chi_3(1) = 2,\ \chi_3(s) = -1,\ \chi_3(s^2) = -1,\ \chi_3(t) = 0,\ \chi_3(st) = 0,\ \chi_3(s^2t) = 0,$$

$$\chi_4(1) = 2,\ \chi_4(s) = -1,\ \chi_4(s^2) = -1,\ \chi_4(t) = 0,\ \chi_4(st) = 0,\ \chi_4(s^2t) = 0.$$

Cabe destacar a coincidencia dos caracteres χ_3 e χ_4 por provir das representacións equivalentes ρ_3 e ρ_4, respectivamente. Do mesmo xeito, nos distintos caracteres de D_6 apréciase a súa coincidencia en elementos da mesma clase de conxugación.

Ademais, este exemplo, como o anterior, ilustra que o carácter asociado a unha suma de representacións é a suma dos caracteres asociados a cada sumando, pois para todo $g \in D_6$ tense que $\chi_{reg}(g) = \chi_1(g) + \chi_2(g) + \chi_3(g) + \chi_4(g)$.

3.3. Relacións de ortogonalidade.

Veremos nesta sección que no $\mathbb{C}$-espazo vectorial $\mathbb{C}^G$, do conxunto de funcións de G en $\mathbb{C}$, pódese definir un produto interior, polo que en particular os caracteres, ó herdar dito produto, presentan unha serie de características vinculadas ó mesmo, as relacións de ortogonalidade, que constituirán un potente recurso para traballar con eles.

En $\mathbb{C}^G$ podemos definir para calquera dous elementos $\theta, \phi \in \mathbb{C}^G$, o seguinte produto:

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

Que é produto interior é claro pois verifícase:

1. $\langle \theta, \phi \rangle = \overline{\langle \phi, \theta \rangle}$ para todo $\theta, \phi \in \mathbb{C}^G$.

2. $\langle \lambda_1\theta_1 + \lambda_2\theta_2, \phi \rangle = \lambda_1 \langle \theta_1, \phi \rangle + \lambda_2 \langle \theta_2, \phi \rangle$ para todo $\theta_1, \theta_2, \phi \in \mathbb{C}^G$ e todo $\lambda_1, \lambda_2 \in \mathbb{C}$.

3. $\langle\theta,\theta\rangle \geq 0$. A igualdade só se dá se $\theta = 0$.

A partir de agora traballaremos co produto interior definido, tomando en particular $\chi, \gamma \in \mathbb{C}^G$ que ademais sexan caracteres, o que nos permitirá empregar propiedades dos mesmos para simplificar o cálculo do produto interior previo para este caso.

Proposición 3.22. *Supoñamos que G ten s clases de conxugación con representantes $g_1, \dots, g_s$ e sexan χ, γ caracteres en G. Entón verifícase:*

1. $\langle\chi,\gamma\rangle = \langle\gamma,\chi\rangle = \frac{1}{|G|}\sum_{g\in G}\chi(g)\gamma(g^{-1})$ *e é un número real.*
2. $\langle\chi,\gamma\rangle = \sum_{i=1}^{s}\frac{\chi(g_i)\overline{\gamma(g_i)}}{|C_G(g_i)|}$.

Demostración.

1. Por 3.15 sabemos que $\gamma(g^{-1}) = \overline{\gamma(g)}$ para todo $g \in G$. En consecuencia,

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

   Posto que podemos expresar G como $G = \{g^{-1} \mid g \in G\}$ temos que

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

   Así, como ademais $\overline{\langle\chi,\gamma\rangle} = \langle\gamma,\chi\rangle$, obtemos que $\langle\chi,\gamma\rangle$ é real.

2. Xa que os caracteres son constantes en clases de conxugación por 3.12, para todo g_i^G,

$$\sum_{g\in g_i^G}\chi(g)\overline{\gamma(g)} = |g_i^G|\chi(g_i)\overline{\gamma(g_i)}.$$

   Logo, por 3.4 e 3.7 temos que:

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

$$\sum_{i=1}^{s}\frac{|g_i|^G}{|G|}\chi(g_i)\overline{\gamma(g_i)} = \sum_{i=1}^{s}\frac{\chi(g_i)\overline{\gamma(g_i)}}{|C_G(g_i)|}.$$

□

A continuación, veremos a relación existente entre as propiedades das representacións e as relacións de ortogonalidade dos seus correspondentes caracteres:

Teorema 3.23 (Relacións de ortogonalidade). *Sexan ρ_1 e ρ_2 dúas representacións arbitrarias, irreducibles e non equivalentes do grupo G e χ_1 e χ_2 os seus caracteres asociados. Entón,*

$$\langle \chi_1, \chi_1 \rangle = 1,$$
$$\langle \chi_1, \chi_2 \rangle = 0.$$

Demostración. Sexan $\rho_i \colon G \longrightarrow GL(V_i)$ con $i \in \{1,2\}$, f unha aplicación lineal arbitraria entre os $\mathbb{C}[G]$-módulos V_1 e V_2, de dimensións m_1 e m_2 respectivamente, e $\bar{f}$ a aplicación lineal

$$\begin{array}{rccc} \bar{f}\colon & V_1 & \longrightarrow & V_2 \\ & v & \longrightarrow & \frac{1}{|G|}\sum_{g\in G} g^{-1} f(gv) \end{array}$$

que ademais é homomorfismo de $\mathbb{C}[G]$-módulos:

$$\bar{f}(g'v) = \frac{1}{|G|}\sum_{g\in G} g^{-1} f(gg'v) = g'(\frac{1}{|G|}\sum_{g\in G}(gg')^{-1} f(gg'v)) = g'\bar{f}(v).$$

Tomemos B_1 e B_2 bases de V_1 e V_2 respectivamente, e denotemos por $\rho_i(g)$ a $(\rho_i(g))_{B_i}$, con $i \in \{1,2\}$ e por A e $\bar{A}$ as matrices asociadas a f e $\bar{f}$ respecto das bases B_1 e B_2. Así

$$\bar{A}_{ij} = \frac{1}{|G|}\sum_{g\in G}\sum_{k=1}^{m_1}\sum_{l=1}^{m_2} \rho_1(g)_{ik} A_{kl} \rho_2(g^{-1})_{lj}.$$

Posto que ρ_1 e ρ_2 non son equivalentes, o *Lema de Schur*, 2.8, conclúe que $\bar{f} = 0$ independentemente da f escollida, polo que $\bar{A} = 0$ e, en particular, supondo que $A_{ij} = 1$ e $A_{kl} = 0$ cando $(i,j) \neq (k,l)$, temos que

$$0 = \frac{1}{|G|}\sum_{g\in G} \rho_1(g)_{ii}\rho_2(g^{-1})_{jj}.$$

En consecuencia,

$$\langle \chi_1, \chi_2 \rangle = \frac{1}{|G|}\sum_{g\in G} \chi_1(g)\chi_2(g^{-1}) = 0.$$

Por outra banda é obvio que ρ_1 é equivalente a si mesma, se tomamos $\rho_2 = \rho_1$, en base a 1.15 e polo *Lema de Schur*, 2.8, $\bar{f}(v) = \lambda v$ para certo $\lambda \in \mathbb{C}$. O valor de λ depende de f e podemos calculalo. En primeiro lugar, obtemos que

$$m_1\lambda = tr(\bar{f}) = \frac{1}{|G|}\sum_{g\in G} tr(\rho_1(g^{-1}) \circ f \circ \rho_1(g)) = \frac{1}{|G|}\sum_{g\in G} tr(f) = tr(f),$$

polo que $\lambda = \frac{tr(f)}{m_1}$. No caso $i \neq j$, tomando $A_{ij} = 1$ e $A_{kl} = 0$ cando $(i,j) \neq (k,l)$, obtemos

$$0 = \frac{1}{|G|}\sum_{g\in G} \rho_1(g^{-1})_{ii}\rho_1(g)_{jj}.$$

Porén, con $i = j$ e as restantes condicións invariantes, $tr(f) = 1$ polo que

$$\frac{1}{m_1} = \frac{1}{|G|} \sum_{g \in G} (\rho_1(g^{-1}))_{ii} (\rho_1(g))_{ii},$$

do que se deduce que

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

□

Nota 3.24. En termos de $\mathbb{C}[G]$-módulos o anterior teorema poderíase expresar tomando como hipótese V_1 e V_2 dous $\mathbb{C}[G]$-módulos arbitrarios, simples e non isomorfos, en lugar de ρ_1 e ρ_2. Ademais, a demostración sería análoga tomando as representacións asociadas a V_1 e V_2.

Corolario 3.25. *Dado un conxunto maximal de representacións irreducibles non equivalentes $\rho_1, \dots, \rho_s$ con caracteres asociados $\{\chi_1, \dots, \chi_s\}$, podemos expresar as relacións de ortogonalidade xenericamente do seguinte modo:*

$$\langle \chi_i, \chi_j \rangle = \delta_{ij} \text{ para todo } i, j \in \{1, \dots, s\}.$$

Para concluír esta sección introducimos as funcións de clase, que nos permitirán asociar o número de caracteres e representacións irreducibles dun grupo co seu número de clases de conxugación, o que tamén nos deixerá expresar as relacións de ortogonalidade de xeito máis manexable:

Definición 3.26. Unha **función de clase en G** é unha función $\theta\colon G \longrightarrow \mathbb{C}$ constante nas clases de conxugación do grupo; é dicir, se $g_1, g_2 \in g^G$ verifícase que $\theta(g_1) = \theta(g_2)$.

Nota 3.27. As funcións de clase en G constitúen un subespazo de $\mathbb{C}^G$ que denotaremos $F(G)$. Unha posible base de dito subespazo é o conxunto de funcións de clase $\{\theta_1, \dots, \theta_s\}$ tal que para $i, j \in \{1, \dots, s\}$ $\theta_i(g_i') = 1$ con $g_i' \in g_i^G$ e $\theta_i(g_j') = 0$ para $i \neq j$ e $g_j' \in g_j^G$. Así, o número de clases de conxugación de G e a dimensión de $F(G)$ serán iguais a s.

A proposición 3.12 permítenos afirmar que os caracteres constitúen un caso particular de funcións de clase en G.

A continuación imos probar un lema que empregaremos para demostrar que o conxunto dos caracteres irreducibles constitúe unha base ortonormal do espazo $F(G)$. Para isto, introduciremos en primeiro lugar o seguinte concepto:

Definición 3.28. Sexa χ un carácter dunha determinada representación. Defínese o **carácter conxugado de χ**, $\bar{\chi}$, por $\bar{\chi}(g) = \overline{\chi(g)}$, para todo $g \in G$.

Lema 3.29. *Sexa $\rho\colon G \longrightarrow GL(V)$ unha representación irreducible de grao m con carácter asociado χ. Se θ é unha función de clase non nula, á cal asociamos o elemento $\alpha = \sum_{g\in G}\theta(g)g \in Z(\mathbb{C}[G])$, verifícase que para todo $v \in V$*

$$\alpha v = \frac{|G|}{m}\langle\theta, \bar{\chi}\rangle\, v,$$

onde $\bar{\chi}$ é o carácter conxugado de χ.

Demostración. Pola demostración de 1.12, dada unha representación $\rho\colon G \longrightarrow GL(V)$ a estrutura de $\mathbb{C}[G]$-módulo de V proporciónanos que $\beta v = \tilde{\rho}(\beta)(v)$ para todo $\beta = \sum_{h\in G}\alpha_h h \in \mathbb{C}[G]$ e todo $v \in V$. En particular, para α obtense a aplicación

$$\begin{array}{rccc} \tilde{\rho}(\alpha)\colon & V & \longrightarrow & V \\ & v & \longrightarrow & \alpha v \end{array}$$

que é homomorfismo de $\mathbb{C}[G]$-módulos. Así, en base ó *Lema de Schur*, 2.8, existe $\lambda \in \mathbb{C}$ tal que $\tilde{\rho}(\alpha)(v) = \lambda v$ para todo $v \in V$. Este λ calcularémolo empregando a linealidade da traza e o produto interior en $\mathbb{C}^{\mathbb{G}}$:

$$m\lambda = tr(\tilde{\rho}(\alpha)) = \sum_{g\in G}\theta(g)\chi(g) = |G|\,\langle\theta, \bar{\chi}\rangle\,.$$

□

Teorema 3.30. *Os caracteres irreducibles de G constitúen unha base ortonormal do subespazo $F(G)$ de $\mathbb{C}^G$, integrado polas funcións de clase.*

Demostración. En primeiro lugar, vexamos que o conxunto $\{\chi_1, \dots, \chi_s\}$ dos caracteres irreducibles de G é linealmente independente. Para iso supoñamos que $\lambda_1\chi_1 + \cdots + \lambda_s\chi_s = 0$, con $\lambda_i \in \mathbb{C}$ para todo $i \in \mathbb{C}$; por 3.25, $0 = \langle\lambda_1\chi_1 + \cdots + \lambda_s\chi_s, \chi_i\rangle = \lambda_i$. Así, concluímos que efectivamente $\chi_1, \dots, \chi_s$ son linealmente independentes.

Falta ver que $\{\chi_1, \dots, \chi_s\}$ é un conxunto de xeradores de $F(G)$. Isto será consecuencia de que $dim(F(G)) = s$, pois xa sabemos que $\chi_1, \dots, \chi_s$ son linealmente independentes. Para comprobar que $dim(F(G)) = s$ veremos que $\{\bar{\chi}_1, \dots, \bar{\chi}_s\}$ é un conxunto de xeradores de $F(G)$. Para elo, sexa θ unha función de clase. Definimos ϕ como $\phi = \theta - \sum_{i=1}^{s}\langle\theta, \bar{\chi}_i\rangle\,\bar{\chi}_i$, verificando que $\langle\phi, \bar{\chi}_i\rangle = 0$ para todo $i \in \{1, \dots, s\}$. Vexamos que disto podemos extraer que $\phi = 0$. Con este fin, tomamos $\alpha = \sum_{g\in G}\phi(g)g \in Z(\mathbb{C}[G])$ e consideramos unha representación $\rho\colon G \longrightarrow GL(V)$. Se ρ é irreducible estamos nas hipóteses do lema previo 3.29 para ϕ, do que extraemos que $\alpha v = 0$ para todo $v \in V$. Se ρ fose reducible, expresariamola como suma de subrepresentacións irreducibles e aplicariamos a cada unha delas 3.29, podendo concluír tamén que $\alpha v = 0$ para todo $v \in V$.

Facendo o anterior para o caso no que $V = \mathbb{C}[G]$ ou, equivalentemente, $\rho = \rho_{reg}$ e $v = 1$, teríase que

$$0 = \alpha 1 = \sum_{g \in G} \phi(g) g,$$

polo que $\phi = 0$.

Falta demostrar que $\{\chi_1, \dots, \chi_s\}$ é unha base ortonormal, pero isto dedúcese de 3.25. □

Corolario 3.31. *O número de clases de conxugación dun grupo coincide co número de caracteres irreducibles e, en consecuencia, co número de representacións irreducibles non equivalentes de dito grupo.*

Cabe destacar que este último resultado xogará un importante papel no cálculo da táboa de caracteres dun grupo que levaremos a cabo no seguinte epígrafe.

Exemplos 3.32. Retomemos os exemplos de 3.21:

1. Sabemos que ρ_1, ρ_2 e ρ_3 constitúen un conxunto maximal de representacións irreducibles non equivalentes de C_3. Así, χ_1, χ_2, χ_3 son tódolos caracteres irreducibles distintos de dito grupo, polo que forman unha base de $F(C_3)$. Nesta situación, por 3.22, podemos concluír que $\langle \chi_{reg}, \chi_i \rangle = \frac{1}{|C_3|} \sum_{g' \in C_3} \chi_{reg}(g') \chi_i(g'^{-1}) = 1$ para cada $i \in \{1, 2, 3\}$. Ademais, polas relacións de ortogonalidade, como $\chi_{reg} = \chi_1 + \chi_2 + \chi_3$, conclúese tamén que $\langle \chi_{reg}, \chi_i \rangle = 1$ para cada $i \in \{1, 2, 3\}$. En definitiva, o que nos proporciona $\langle \chi_{reg}, \chi_i \rangle$ para cada $i \in \{1, 2, 3\}$ é o número de veces que aparece o sumando χ_i en χ_{reg}.

2. Analogamente, para D_6 (ou equivalentemente S_3), sabemos que os $\mathbb{C}[D_6]$-módulos simples asociados a ρ_1, ρ_2 e ρ_3 forman un conxunto maximal de $\mathbb{C}[D_6]$-módulos simples non isomorfos. En consecuencia, χ_1, χ_2, χ_3 son tódolos caracteres irreducibles distintos de D_6, polo que integran unha base de $F(D_6)$. Así, por 3.22, podemos concluír que $\langle \chi_{reg}, \chi_i \rangle = \frac{1}{|D_6|} \sum_{g \in D_6} \chi_{reg}(g) \chi_i(g^{-1}) = 1$ para cada $i \in \{1, 2\}$ e $\langle \chi_{reg}, \chi_3 \rangle = \frac{1}{|D_6|} \sum_{g \in D_6} \chi_{reg}(g) \chi_3(g^{-1}) = 2$.

   Polas relacións de ortogonalidade, como $\chi_{reg} = \chi_1 + \chi_2 + \chi_3 + \chi_4 = \chi_1 + \chi_2 + 2\chi_3$ obtense tamén que $\langle \chi_{reg}, \chi_1 \rangle = 1$, $\langle \chi_{reg}, \chi_2 \rangle = 1$, e $\langle \chi, \chi_3 \rangle = 2$. En conclusión, coma no exemplo previo, o que nos proporciona $\langle \chi_{reg}, \chi_i \rangle$ para cada $i \in \{1, 2, 3\}$ é o número de veces que aparece o sumando χ_i en χ_{reg}.

Isto último é certo en xeral. É dicir, se $\{\chi_1, \dots, \chi_s\}$ é o coxunto de caracteres irreducibles dun grupo G e χ é un caracter de G que polo teorema 3.30 verifica $\chi = \lambda_1 \chi_1 + \cdots + \lambda_s \chi_s$, os escalares λ_i con $i \in \{1, \dots, s\}$ cumpren $\lambda_i = \langle \chi, \chi_i \rangle$.

Imos proceder agora a reescribir as relacións de ortogonalidade a partir das clases de conxugación do grupo:

Teorema 3.33. *Sexan $\{\chi_1, \dots, \chi_s\}$ o conxunto dos caracteres irreducibles de G e $g_1, \dots, g_s$ representantes das clases de conxugación de dito grupo. Entón, para todo $r, t \in \{1, \dots, s\}$ podemos expresar as relacións de ortogonalidade dos seguintes modos:*

1. $\langle \chi_r, \chi_t \rangle = \sum_{i=1}^{s} \frac{\chi_r(g_i)\overline{\chi_t(g_i)}}{|C_G(g_i)|} = \delta_{rt}$.
2. $\langle \chi_r, \chi_t \rangle = \frac{1}{|C_G(g_r)|} \sum_{i=1}^{s} \chi_i(g_r)\overline{\chi_i(g_t)} = \delta_{rt}$.

Demostración.

1. É consecuencia directa de 3.22, 3.25 e 3.31.

2. Tomemos para $t \in \{1, \dots, s\}$ unha función de clase θ_t tal que $\theta_t(g_r) = \delta_{rt}$ para $r \in \{1, \dots, s\}$. Por 3.30 podemos expresar θ_t como

$$\theta_t = \sum_{i=1}^{s} \lambda_i \chi_i.$$

   Ademais, como por 3.25 $\langle \chi_i, \chi_j \rangle = \delta_{ij}$, tense que

$$\lambda_i = \langle \theta_t, \chi_i \rangle = \frac{1}{|G|} \sum_{g \in G} \theta_t(g)\overline{\chi_i(g)}.$$

   Por outra banda, sabemos que $\theta_t(g) = 1$ se $g \in g_t^G$ e anúlase noutro caso. Ademais, por 3.4 sabemos que $|g_t^G| = \frac{|G|}{|C_G(g_t)|}$, polo tanto:

$$\lambda_i = \frac{1}{|G|} \sum_{g \in g_t^G} \theta_t(g)\overline{\chi_i(g)} = \frac{\overline{\chi_i(g_t)}}{|C_G(g_t)|}.$$

   En consecuencia,

$$\delta_{rt} = \theta_t(g_r) = \sum_{i=1}^{s} \lambda_i \chi_i(g_r) = \sum_{i=1}^{s} \frac{\chi_i(g_r)\overline{\chi_i(g_t)}}{|C_G(g_t)|},$$

   do que se obtén que

$$\langle \chi_r, \chi_t \rangle = \frac{1}{|C_G(g_r)|} \sum_{i=1}^{s} \chi_i(g_r)\overline{\chi_i(g_t)} = \delta_{rt}.$$

□

3.4. Táboas de caracteres.

Neste derradeiro epígrafe do capítulo incluímos un método para representar a información do grupo proporcionada polos caracteres irreducibles e as clases de conxugación do mesmo: as táboas de caracteres.

Definición 3.34. Sexan $\chi_1, \dots, \chi_s$ os caracteres irreducibles de G e $g_1, \dots, g_s$ representantes das distintas clases de conxugación de dito grupo. Entón, a matriz $s \times s$ cuxa entrada na fila i-ésima e columna j-ésima é $\chi_i(g_j)$ denomínase **táboa de caracteres de G**.

Proposición 3.35. *A táboa de caracteres de G é unha matriz invertible.*

Demostración. Supoñamos que a táboa de caracteres de G non fose invertible. Entón habería unha fila combinación lineal das outras. Porén, os caracteres irreducibles son linealmente independentes por 3.30, chegando a unha contradición. □

Nota 3.36. En 3.33 os sumandos da primeira forma na que se expresan as relacións de ortogonalidade percorren as filas da táboa de caracteres de G, e os da segunda percorren as columnas. En consecuencia, estas dúas maneiras de expresar as relacións de ortogonalidade denomínanse relacións de ortogonalidade por filas e relacións de ortogonalidade por columnas, respectivamente.

Exemplos 3.37. Retomemos os grupos C_3 e D_6. En 3.21 obtivemos os seus caracteres irreducibles e en 3.2 as súas clases de conxugación. A continuación, procederemos a analizar as súas táboas de caracteres:

1. Dado C_3 cos seus caracteres irreducibles, χ_1, χ_2, χ_3, posto que cada elemento determina unha clase de conxugación, a táboa de caracteres de C_3 é

	1	g	g^2
χ_1	1	1	1
χ_2	1	ω	ω^2
χ_3	1	ω^2	ω

   Notemos que por 3.4 obtemos que $|C_{C_3}(1)| = 3$, $|C_{C_3}(g)| = 3$, $|C_{C_3}(g^2)| = 3$. Nestas condicións, pódese comprobar que se verifican as relacións de ortogonalidade por filas e por columnas recollidas en 3.33:

   a) Comecemos polas relacións por filas:

      1) Para $r = t$, por exemplo $r = t = 1$:

$$\frac{\chi_1(1)\chi_(1)}{|C_{C_3}(1)|} + \frac{\chi_1(g)\chi_1(g^2)}{|C_{C_3}(g)|} + \frac{\chi_1(g^2)\chi_1(g)}{|C_{C_3}(g^2)|} = \frac{1}{3} + \frac{1}{3} + \frac{1}{3} = 1.$$

2) Para $r \neq t$, por exemplo $r = 2, t = 1$:

$$\frac{\chi_2(1)\chi_1(1)}{|C_{C_3}(1)|} + \frac{\chi_2(g)\chi_1(g^2)}{|C_{C_3}(g)|} + \frac{\chi_2(g^2)\chi_1(g)}{|C_{C_3}(g^2)|} = \frac{1}{3} + \frac{\omega}{3} + \frac{\omega^2}{3} = 0.$$

b) Para as relacións por columnas:

1) Cando $r = t$, por exemplo $r = t = 2$:

$$\frac{1}{|C_{C_3}(g)|}(\chi_1(g)\chi_1(g^2) + \chi_2(g)\chi_2(g^2) + \chi_3(g)\chi_3(g^2)) = \frac{1}{3}(1 + 1 + 1) = 1.$$

2) Para $r \neq t$, por exemplo $r = 2, t = 3$:

$$\frac{1}{C_{C_3}(g)|}(\chi_1(g)\chi_1(g) + \chi_2(g)\chi_2(g) + \chi_3(g)\chi_3(g)) = \frac{1}{3}(1 + \omega^2 + \omega) = 0.$$

2. No referente a D_6 ou analogamente S_3, dados $1, s, t$, representantes das distintas clases de conxugación do grupo, e χ_1, χ_2, χ_3, os seus caracteres irreducibles, a táboa de caracteres de D_6 é:

	1	s	t
χ_1	1	1	1
χ_2	1	1	-1
χ_3	2	-1	0

Notemos que por 3.4 obtemos que $|C_{D_6}(1)| = 6$, $|C_{D_6}(s)| = 3$, $|C_{D_6}(t)| = 2$. Así, podemos comprobar que se verifican as relacións de ortogonalidade por filas e por columnas recollidas en 3.33:

a) Nas relacións por filas temos:

1) Para $r = t$, por exemplo $r = t = 3$:

$$\frac{\chi_3(1)\chi_3(1)}{|C_{D_6}(1)|} + \frac{\chi_3(s)\chi_3(s^2)}{|C_{D_6}(s)|} + \frac{\chi_3(t)\chi_3(t)}{|C_{D_6}(t)|} = \frac{2}{3} + \frac{1}{3} + 0 = 1.$$

2) Para $r \neq t$, por exemplo $r = 1, t = 3$:

$$\frac{\chi_1(1)\chi_3(1)}{|C_{D_6}(1)|} + \frac{\chi_1(s)\chi_3(s^2)}{|C_{D_6}(s)|} + \frac{\chi_1(t)\chi_3(t)}{|C_{D_6}(t)|} = \frac{1}{3} + \frac{-1}{3} + 0 = 0.$$

b) Para as relacións por columnas:

1) Cando $r = t$, por exemplo $r = t = 2$:

$$\frac{1}{|C_{D_6}(s)|}(\chi_1(s)\chi_1(s^2) + \chi_2(s)\chi_2(s^2) + \chi_3(s)\chi_3(s^2)) = \frac{1}{3}(1 + 1 + 1) = 1.$$

2) Para $r \neq t$, por exemplo $r = 2, t = 3$:

$$\frac{1}{|C_{D_6}(s)|}(\chi_1(s)\chi_1(t) + \chi_2(s)\chi_2(t) + \chi_3(s)\chi_3(t)) = \frac{1}{3}(1 - 1 + 0) = 0.$$

Ademais, é sinxelo ver que $Ker(\chi_2) = \{1, s, s^2\}$ é un subgrupo normal propio de orde 3. Así, podemos afirmar que tanto D_6 como S_3 non son grupos simples.

O cálculo da táboa de caracteres dun grupo G non é en xeral tan doado coma nos dous exemplos previos, xa que non se adoita partir do $\mathbb{C}[G]$-módulo regular expresado en forma de suma directa de $\mathbb{C}[G]$-módulos simples. Deseguido determinaremos as táboas de caracteres dos grupos D_8 e Q dende outro punto de partida.

En relación a D_8, sabemos que ten oito elementos e cinco clases de conxugación, como vimos en 3.2, das que podemos tomar como representantes $1, s^2, s, t$ e st. Ademais, por 3.31, podemos afirmar que presentará cinco representacións irreducibles, $\rho_1, \dots, \rho_5$ cos seus correspondentes caracteres irreducibles, $\chi_1, \dots, \chi_5$ e por 2.26 obtemos que dados $\{m_1, \dots, m_5\}$ os graos das representacións irreducibles, $\sum_{i=1}^{5} m_i^2 = 8$. Así, deducimos facilmente que tódalas representacións irreducibles son de grao 1 agás unha, que ten grao 2, que suporemos que é ρ_5 sen perda de xeneralidade. Por outra banda, en base a 3.14, sabemos que os caracteres unidimensionais son homomorfismos de grupos. Entón, para $i \in \{1, 2, 3, 4\}$, temos que $\chi_i(t^2) = \chi_i(t)^2 = 1$ polo que $\chi_i(t) = \pm 1$; ademais, como s^2t e t están na mesma clase de conxugación, $\pm 1 = \chi_i(t) = \chi_i(s^2t) = \chi_i(s^2)\chi_i(t) = \pm\chi_i(s)^2$ e, en consecuencia, $\chi_i(s) = \pm 1$. Entón a táboa de caracteres de D_8 será da seguinte forma:

	1	s	s^2	t	st
χ_1	1	1	1	1	1
χ_2	1	1	1	-1	-1
χ_3	1	-1	1	1	-1
χ_4	1	-1	1	-1	1
χ_5	2	x_1	x_2	x_3	x_4

Nesta situación, falta calcular a fila da táboa, correspondente a χ_5, para elo empregaremos as relacións de ortogonalidade por columnas vistas en 3.33. Supoñamos en primeiro lugar que $g_r = 1$ e $g_t = s$; entón $1{\cdot}1+1{\cdot}1+1{\cdot}(-1)+1{\cdot}(-1)+2x_1 = 0$, polo que $x_1 = 0$. Se $g_r = 1$ e $g_t = s^2$, temos que $1{\cdot}1+1{\cdot}1+1{\cdot}1+1{\cdot}1+2x_2 = 0$, e consecuentemente $x_2 = -2$. Se tomamos $g_r = 1$ e $g_t = t$, concluímos que $1 \cdot 1 + 1 \cdot (-1) + 1 \cdot 1 + 1 \cdot (-1) + 2x_3 = 0$, o que conleva que $x_3 = 0$. Por último, se $g_r = 1$ e $g_t = st$, temos que $1 \cdot 1 + 1 \cdot (-1) + 1 \cdot (-1) + 1 \cdot 1 + 2x_4 = 0$ e polo tanto $x_4 = 0$.

Ademais, unha vez construída a táboa de caracteres podemos dicir que $Ker(\chi_2) = \{1, s, s^2, s^3\}$, $Ker(\chi_3) = \{1, s^2, t, s^2t\}$ e $Ker(\chi_4) = \{1, s^2, st, s^3t\}$ son subgrupos normais propios de orde 4 de D_8, polo que D_8 non é simple.

No que respecta a Q sabemos, por 3.2, que ten oito elementos e cinco clases de conxugación, das que podemos tomar como representantes $1, s^2, s, t$ e st. Logo, por 3.31, podemos afirmar que presentará cinco representacións irreducibles, $\rho_1, \ldots, \rho_5$ cos seus correspondentes caracteres irreducibles, $\chi_1, \ldots, \chi_5$. Nesta situación, de xeito análogo ó feito para D_8, podemos concluír que tódalas representacións son de grao 1 agás unha, que ten grao 2 e que suporemos que é ρ_5 sen perda de xeneralidade. Entón, por analoxía con D_8, a táboa de caracteres de Q será:

	1	s	s^2	t	st
χ_1	1	1	1	1	1
χ_2	1	1	1	-1	-1
χ_3	1	-1	1	1	-1
χ_4	1	-1	1	-1	1
χ_5	2	0	-2	0	0

De igual modo que nos casos previos a partir da táboa de caracteres podemos dicir que $Ker(\chi_2) = \{1, s, s^2, s^3\}$, $Ker(\chi_3) = \{1, s^2, t, s^2t\}$ e $Ker(\chi_4) = \{1, s^2, st, s^3t\}$ son subgrupos normais propios de orde 4 de Q, polo que Q non é simple.

Nota 3.38. As táboas de caracteres de D_8 e Q son iguais pese a tratarse de grupos non isomorfos.

Obsérvese que nos exemplos anteriores obtivemos, a partir da táboa de caracteres, algúns subgrupos normais do mesmo: os núcleos dos caracteres irreducibles.

En xeral, a táboa de caracteres dun grupo G proporciona información importante sobre o mesmo. Os núcleos dos caracteres irreducibles son subgrupos normais e polo tanto tamén o son as súas posibles interseccióńs, pero ademais verifícase que todo subgrupo normal é intersección de núcleos de caracteres irreducibles [Isaacs, p.23]. Como consecuencia pódese deducir a simplicidade ou non de G. Tamén é posible determinar tódalas series normais do grupo e os términos involucrados e polo tanto saber se o grupo ten ou non unha serie normal de cocientes abelianos; en definitiva determinar se o grupo é ou non resoluble.

Outras informacións que nos proporciona a táboa de caracteres son o subgrupo conmutador, $G' = \cap\{Ker(\chi_i) \mid \chi_i(e) = 1\}$ [Isaacs, p.25] e o centro do grupo $Z(G) = \cap Z(\chi_i)$ [Isaacs, p.27], onde se χ é un carácter de G, $Z(\chi) = \{g \in G \mid |\chi(g)| = \chi(e)\}$, e en consecuencia pódese determinar se o grupo é ou non nilpotente.

Capítulo 4

Teorema de Burnside.

O cuarto e último capítulo do traballo está dedicado a demostrar o *Teorema p^aq^b de Burnside*. En concreto próbase que os grupos de orde p^aq^b, onde p e q son primos e a e b enteiros positivos, son resolubles. Ademais tamén se probará unha xeneralización de dito teorema, o *Teorema de Hall*, que garante a resolubilidade dunha serie de grupos supondo certas hipóteses sobre o seu cardinal e os seus subgrupos. Para todo isto empregaranse constantemente as propiedades dos caracteres dun grupo. No que respecta ás referencias utilizadas neste capítulo destacan Jacobson [11] e Dummit [6], así como tamén James [12] e Isaacs [9].

4.1. Enteiros alxebraicos.

Nesta primeira sección do capítulo, recordaremos a definición de enteiros alxebraicos e algúns resultados coñecidos sobre os mesmos, que empregamos para obter propiedades dos caracteres.

Definición 4.1. Diremos que un elemento $\lambda \in \mathbb{C}$ é un **enteiro alxebraico** se, e só se, é raíz dun polinomio mónico con coeficientes enteiros.

Proposición 4.2. *Un número complexo $\lambda \in \mathbb{C}$ é un enteiro alxebraico se, e só se, é autovalor dunha matriz con coeficientes enteiros.*

Demostración. Supoñamos que λ é un enteiro alxebraico, é dicir que λ é raíz dun polinomio mónico con coeficientes enteiros, $p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$. Tomemos entón a seguinte

matriz $n \times n$:

$$A = \begin{pmatrix} 0 & 1 & 0 & ... & ... & 0 \\ 0 & 0 & 1 & ... & ... & 0 \\ 0 & 0 & 0 & ... & ... & 0 \\ ... & ... & ... & ... & ... & ... \\ 0 & 0 & 0 & ... & ... & 1 \\ -a_0 & -a_1 & -a_2 & ... & ... & -a_{n-1} \end{pmatrix}.$$

Pódese comprobar de xeito sinxelo que $det(xI - A) = p(x)$, obtendo que λ é autovalor de A.

Reciprocamente, sexa λ un autovalor dunha matriz A de orde $n \times n$ con coeficientes enteiros. Entón, $det(A - \lambda I) = 0$ polo que λ é raíz do polinomio mónico con coeficientes enteiros $det(xI - A)$ e como consecuencia, λ é un enteiro alxebraico. □

A importancia dos enteiros alxebraicos na teoría de representacións de grupos finitos queda establecida polo seguinte feito:

Proposición 4.3. *Dado un carácter dun grupo G, χ, tense que $\chi(g)$ é un enteiro alxebraico para todo $g \in G$.*

Demostración. Sabemos por 3.15 que $\chi(e)$ é igual ó grao da representación á que está asociado. Supoñamos que este grao é m. Ademais, tamén por 3.15, temos que se g é un elemento de orde r de G, $\chi(g)$ é suma de m raíces r-ésimas da unidade. Posto que é coñecido que o conxunto de enteiros alxebraicos de $\mathbb{C}$ sobre $\mathbb{Z}$ é un anel e cada raíz r-ésima da unidade é un enteiro alxebraico, xa que é raíz do polinomio $p(x) = x^r - 1$, podemos concluír que $\chi(g)$ é un enteiro alxebraico para todo $g \in G$. □

Deseguido introduciremos un resultado que nos permitirá concluír que os graos dos caracteres irreducibles dun grupo dividen á orde do mesmo, pero antes incluiremos o seguinte resultado previo:

Lema 4.4. *Sexa V un $\mathbb{C}[G]$-módulo simple e $\alpha \in Z(\mathbb{C}[G])$. Entón existe $\lambda \in \mathbb{C}$ tal que $\alpha v = \lambda v$ para todo $v \in V$.*

Demostración. Posto que $\alpha \in Z(\mathbb{C}[G])$ temos que o endomorfismo

$$\begin{array}{ccc} V & \longrightarrow & V \\ v & \longmapsto & \alpha v \end{array}$$

é $\mathbb{C}[G]$-isomorfismo. Así, en base ó *Lema de Schur*, 2.8, dito $\mathbb{C}[G]$-isomorfismo é múltiplo da identidade. □

Proposición 4.5. *Sexan $C_1, \dots, C_s$ as clases de conxugación dun grupo G con representantes $g_1, \dots, g_s$ e $\chi_1, \dots, \chi_s$ os seus caracteres irreducibles, con graos $m_1, \dots, m_s$ respectivamente. Entón, os números*

$$\frac{|C_j|\chi_i(g_j)}{m_i},$$

con $i, j \in \{1, \dots, s\}$, son enteiros alxebraicos.

Demostración. Sexan $c_1, \dots, c_s$ as sumas de clase asociadas ás clases de conxugación $C_1, \dots, C_s$. Se $g_1, \dots, g_n$ son os elementos que forman G, tense que para calquera $c_j \in \{c_1, \dots, c_s\}$

$$c_j g_l = (\textstyle\sum_{g \in C_j} g) g_l = \sum_{k=1}^{n} a_{kl} g_k, \text{ con } l, k \in \{1, \dots, n\}.$$

Nótese que o coeficiente a_{kl} de $g_k = g g_l$ toma os valores 0 e 1 e soamente vale 1 se $g \in C_j$. Nesta situación, se $A = (a_{kl})$, obtense facilmente que para todo $u \in \mathbb{C}[G]$ non nulo, $Au = c_j u$

Sexa $u = \sum_{l=1}^{n} \alpha_l g_l$ arbitrario. Entón

$$c_j u = (\sum_{g \in C_j} g)(\sum_{l=1}^{n} \alpha_l g_l) = \sum_{l=1}^{n} \sum_{k=1}^{n} a_{kl} \alpha_l g_k = \sum_{k=1}^{n} (\sum_{l=1}^{n} a_{kl} \alpha_l) g_k$$

e

$$Au = A \sum_{l=1}^{n} \alpha_l g_l = \sum_{k=1}^{n} (\sum_{l=1}^{n} a_{kl} \alpha_l) g_k,$$

polo que $Au = c_j u$.

Sexan agora $U_1, \dots, U_s$ os $\mathbb{C}[G]$-módulos simples asociados a $\chi_1, \dots, \chi_s$. Vexamos que para cada $u_i \in U_i$

$$c_j u_i = \frac{|C_j|\chi_i(g_j)}{m_i} u_i,$$

con $i, j \in \{1, \dots, s\}$. Para isto, como sabemos que $c_j \in Z[\mathbb{C}[G]]$, podemos afirmar en base a 4.4 que existe $\lambda \in \mathbb{C}$ tal que $c_j u_i = (\sum_{g \in C_j} g) u_i = \lambda u_i$ para todo $u_i \in U_i$. Deseguido imos identificar o valor deste λ, para iso escollemos unha base B_i de U_i e por 1.12 tense que

$$\textstyle\sum_{g \in C_j} (\rho_i(g))_{B_i} = \lambda I,$$

onde ρ_i e a representación asociada a U_i. Agora, tomando as trazas na anterior igualdade de matrices obtemos que

$$\sum_{g \in C_j} \chi_i(g) = \lambda m_i,$$

e, xa que $\chi_i(g)$ é constante para todo $g \in C_j$, tomando un representante g_j de C_j, chégase a que

$$\lambda = \frac{|C_j|\chi_i(g_j)}{m_i}.$$

Polo tanto, para todo $u_i \in U_i$ con $i \in \{1, \dots, s\}$ temos que

$$Au_i = \frac{|C_j|\chi_i(g)}{m_i} u_i.$$

Como A ten coeficientes enteiros, obtemos que os números λ son enteiros alxebraicos para todo $i, j \in \{1, \dots, s\}$. □

Corolario 4.6. *Nas hipóteses de 4.5, m_i divide a $|G|$ para todo $i \in \{1, \dots, s\}$.*

Demostración. Por 3.4 sabemos que $|C_G(g_k)| = \frac{|G|}{|C_k|}$ para todo $k \in \{1, \dots, s\}$, isto xunto coas relacións de ortogonalidade por filas dános que $\frac{1}{|G|} \sum_{i=1}^{k} |C_k|\chi_i(g_k)\overline{\chi_j(g_k)} = \delta_{ij}$ para todo $i, j, k \in \{1, \dots, s\}$. Así, tomando $i = j$ e dividindo na expresión das relacións de ortogonalidade entre m_i obtemos que

$$\sum_{i=1}^{k} \frac{|C_k|\chi_i(g_k)}{m_i} \overline{\chi_i(g_k)} = \frac{|G|}{m_i}.$$

Como cada número da forma $\frac{|C_k|\chi_i(g_k)}{m_i}$ é enteiro alxebraico, por 4.5, os $\overline{\chi_i(g_k)}$ tamén o son, por 4.3, e o conxunto de enteiros alxebraicos de $\mathbb{C}$ sobre $\mathbb{Z}$ ten estrutura de anel, concluímos que $\frac{|G|}{m_i}$ é un enteiro alxebraico. Porén, sabemos que todo enteiro alxebraico racional é necesariamente enteiro polo que m_i terá que dividir a $|G|$. □

Cabe destacar que este último corolario é especialmente útil para a elaboración de táboas de caracteres como as vistas no capítulo previo, xa que proporciona un recurso máis para determinar os posibles graos das representacións irreducibles dun determinado grupo.

4.2. Teorema de Burnside.

A continuación introduciremos unha serie de lemas previos que nos darán as condicións precisas para demostrar o *Teorema $p^a q^b$ de Burnside*:

Lema 4.7. *Sexa χ un carácter irreducible de grao m dun grupo G. Supoñamos que existe unha clase de conxugación de G, C, tal que $mcd(|C|, m) = 1$. Entón, para todo $g \in C$ verifícase $\chi(g) = 0$ ou $|\chi(g)| = m$.*

Demostración. Sabemos, por 4.5, que $\frac{|C|\chi(g)}{m}$ é un enteiro alxebraico. Xa que $mcd(|C|, m) = 1$, podemos tomar $s, t \in \mathbb{Z}$ tales que $s|C| + tm = 1$. Así, para todo $g \in C$, temos:

$$\frac{s|C|\chi(g)}{m} + \frac{tm\chi(g)}{m} = \frac{\chi(g)}{m},$$

entón,

$$\frac{s|C|\chi(g)}{m} + t\chi(g) = \frac{\chi(g)}{m}.$$

É sinxelo ver que $\frac{s|C|\chi(g)}{m}$ e $t\chi(g)$ son enteiros alxebraicos. Como a súa suma tamén o é, temos que

$$\alpha = \frac{\chi(g)}{m}$$

é un enteiro alxebraico.

Supoñamos que $|\chi(g)| \neq m$. Teremos que comprobar que $\chi(g) = 0$. Por 3.17 se $|\chi(g)| \neq m$ tense que $|\chi(g)| < m$ e, en consecuencia, $|\alpha| < 1$.

Asumamos que g ten orde $r \leq n$ como elemento de G. Entón, en base a 3.15, podemos escribir:

$$\chi(g) = \underbrace{\omega_1 + \cdots + \omega_r}_{m},$$

onde cada ω_i con $i \in \{1, \ldots, r\}$ é unha raíz r-ésima da unidade. Así, é claro que α pertence ó corpo de escisión de $p(x) = x^r - 1$ sobre $\mathbb{Q}$ en $\mathbb{C}$, que denotaremos por E.

Tomemos agora $H = Gal(E : K)$. Dado $\sigma \in H$ arbitrario, é coñecido que $\sigma(\omega_j) = \omega_k$, sendo ω_j e ω_k raíces r-ésimas da unidade para todo $j, k \in \{1, \ldots, r\}$. Consecuentemente, $\sigma(\chi(g))$ é suma de m raíces r-ésimas da unidade. Polo tanto, para todo $\sigma \in H$, temos:

$$|\sigma(\chi(g))| \leq m \Rightarrow |\frac{\sigma(\chi(g))}{m}| \leq 1 \Rightarrow |\sigma(\frac{\chi(g)}{m})| \leq 1 \Rightarrow |\sigma(\alpha)| \leq 1$$

e disto dedúcese que

$$\prod_{\sigma \in H} |\sigma(\alpha)| < 1 \Rightarrow |\prod_{\sigma \in H} \sigma(\alpha)| < 1.$$

Por outra banda, tense que $\beta = \prod_{\sigma \in H} \sigma(\alpha)$ queda fixo por todo $\sigma \in H$, polo que $\beta \in \mathbb{Q}$. Ademais, para todo $\sigma \in H$, verifícase que $\sigma(\alpha)$ é raíz dos mesmos polinomios que α, e como α é enteiro alxebraico, os $\sigma(\alpha)$ e consecuentemente β, tamén o son. Así, β é un número racional que é enteiro alxebraico, polo que necesariamente é enteiro.

Como β é un enteiro con valor absoluto menor que 1, obtemos que $\beta = 0$. Entón, temos que $0 = \beta = \prod_{\sigma \in H} \sigma(\alpha)$, co que $\sigma(\alpha) = 0$ para algún $\sigma \in H$, polo tanto $\alpha = 0$ e podemos concluír que $\chi(g) = 0$.

□

Lema 4.8. *Sexa G un grupo simple e non abeliano. Entón, dada unha clase de conxugación de G arbitraria, C, tense que*

$$|C| \neq p^a,$$

con p primo e $a > 0$.

Demostración. Sexan $\rho_1, \dots, \rho_s$ as representacións irreducibles de G e $\chi_1, \dots, \chi_s$ os caracteres irreducibles correspondentes, cuxos graos son $m_1, \dots, m_s$, respectivamente, e supoñamos que existe unha clase de conxugación de G, C, tal que $|C| = p^a$ con p primo e $a > 0$. Sen perda de xeneralidade, podemos asumir que ρ_1 é a representación trivial de grao 1.

Por 4.7, se p non divide a ningún dos $m_1, \dots, m_s$, temos que ou $\chi_i(g) = 0$ ou $|\chi_i(g)| = m_i$, para todo $i \in \{1, \dots, s\}$ e todo $g \in C$. Nótese que se $|\chi_i(g)| = m_i$, por 3.17 conclúese que $\rho_i(g) = \lambda I$ con $\lambda \in \mathbb{C}$.

Entón, fixado un $i \in \{2, \dots, s\}$, se existe algún $g \in C$, $g \neq e$, tal que $\chi_i(g) \neq 0$ temos que $\rho_i(g) = \lambda I$. Como G é simple $Ker(\rho_i) = \{e\}$, pois $Ker(\rho_i) \lhd G$. Así, ρ_i é unha representación fiel, e posto que $\rho_i(g)$ conmuta con $\rho_i(g')$ para todo $g' \in G$ teremos que $g \in Z(G)$. Vexámolo:

En primeiro lugar nótese que

$$\rho_i(gg') = \rho_i(g)\rho_i(g') = \lambda\rho_i(g') = \rho_i(g')\lambda = \rho_i(g')\rho_i(g) = \rho_i(g'g).$$

Agora, xa que ρ_i é fiel, obtemos que $gg' = g'g$ para todo $g' \in G$ e, en consecuencia, $g \in Z(G)$. Como sabemos que $Z(G) \lhd G$ e $Z(G) \neq \{e\}$, dedúcese que G non será simple se $Z(G) \neq G$, ou será abeliano se $Z(G) = G$, contradecindo as hipóteses sobre G.

No anterior comprobamos que se p non divide a ningún dos $m_1, \dots, m_s$, a posibilidade de que para algún $g \in C$ $|\chi_i(g)| = m_i$, non cumpre as hipóteses sobre G para todo $i \in \{2, \dots, s\}$. Vexamos se a posibilidade de que $\chi_i(g) = 0$ para $g \in C$, $g \neq e$ e $i \in \{2, \dots, s\}$ concorda con ditas hipóteses:

Das relacións de ortogonalidade por columnas extraemos que para todo $g \in C$ con $g \neq e$

$$\sum_{i=1}^{s} \chi_i(g)\overline{\chi(e)} = \sum_{i=1}^{s} m_i\chi_i(g) = 0.$$

Como $m_1 = 1$, $\chi_1(g) = 1$ e $\chi_i(g) = 0$ para $i \in \{2, \dots, s\}$, chegariamos a que $1 = 0$, o que claramente é un absurdo.

Entón, necesariamente p divide a algún dos $m_1, \dots, m_s$. Supoñamos ordenados os $m_1, \dots, m_s$ de modo que os m_i, con $i \in \{2, \dots, s\}$, divisibles por p sexan o subconxunto $\{m_2, \dots, m_t\}$ de $\{m_1, \dots, m_s\}$, onde $t \leq s$. Logo, polo obtido anteriormente a partir das relacións de ortogonalidade por columnas, temos que para todo $g \in C$ tal que $g \neq e$:

$$1 + \sum_{i=2}^{t} m_i\chi_i(g) = 0.$$

Posto que p divide a m_i con $i \in \{2, \dots, t\}$, podemos escribir ditos m_i como $m_i = p\alpha_i$. Entón

$$1 + \sum_{i=2}^{t} p\alpha_i\chi_i(g) = 0$$

e polo tanto

$$\frac{1}{p} + \sum_{i=2}^{t} \alpha_i \chi_i(g) = 0.$$

Como, por 4.3, temos que os $\chi_i(g)$ son enteiros alxebraicos, chegariamos a que $\frac{1}{p}$ é un enteiro alxebraico. Pero é coñecido que os enteiros alxebraicos que son tamén números racionais, son números enteiros, polo que obteriamos unha contradición.

En consecuencia, ningunha das clases de equivalencia de G ten como cardinal unha potencia dun número primo p.

□

Do resultado que acabamos de probar pódese deducir o seguinte:

Corolario 4.9. *Un grupo simple e non abeliano, G, non pode ter un subgrupo abeliano de índice primo.*

Demostración. Supoñamos que existe un subgrupo abeliano de G, H, tal que $(G : H) = p^r$, onde p é un número primo e r un número enteiro. Se $H = \{e\}$, tense polo *Teorema de Lagrange* que $|G| = p^r$. Entón, toda clase de conxugación de G, C, verificaría que $|C| = p^a$, con $a \leq r$, por 3.4. Nesta situación, por 4.8, teríase que non se verifican as hipóteses sobre G. Así, $H \neq \{e\}$, polo que podemos tomar $h \in H$ tal que $h \neq e$. Neste caso $H < C_G(h)$, por ser H abeliano, logo 3.4 dános que $|C| = (G : C_G(h)) = p^b$, con $b \leq r$ e onde C é a clase de conxugación de G que contén a h. Así, se $|C| = 1$, $\langle h \rangle \lhd G$, polo que G non sería simple. Se $|C| > 1$, G tampouco sería simple en base a 4.8. □

Procedemos agora a enunciar e probar o resultado esencial desta sección, que garante a resolubilidade dun grupo baixo certas hipóteses na súa orde.

Teorema 4.10 (Teorema $p^a q^b$ de Burnside.)**.** *Se G ten orde $p^a q^b$, con p e q primos e a e b enteiros non negativos, G é un grupo resoluble.*

Demostración. Supoñamos que G non é abeliano, xa que en caso contrario é coñecido que G é resoluble. Tomemos P un p-Sylow de G, polo que $|P| = p^a$. Por ser P un p-grupo non trivial, sabemos que $Z(P)$ tampouco é trivial. Se tomamos $g \in Z(P)$, $g \neq e$, é claro que $P \subset C_G(g)$, polo que $|P| = p^a$ divide a $|C_G(g)|$. Así, en base ó *Teorema de Lagrange*, obtemos que $(G : C_G(g)) = q^c$, onde c é un enteiro tal que $c \leq b$.

Por 3.4, se denotamos por C a clase de conxugación de G tal que $g \in C$ temos que $|C| = (G : C_G(g))$. Logo hai dous casos posibles:

1. Se $|C| > 1$, concluímos, por 4.8, que G non é simple ademais de non ser abeliano.

2. Se $|C| = 1$, temos que $C_G(g) = G$ e, polo tanto, $g \in Z(G)$. Así $Z(G) \neq e$ e G non é simple xa que $Z(G) \lhd G$, pois G é non abeliano por hipótese.

Entón, dado G non abeliano nas hipóteses do teorema, este ten que ter un subgrupo normal propio H. Se facemos indución na orde de G, teremos que G é resoluble por selo H e G/H. □

Cabe destacar que se G é un grupo simple e non abeliano con orde menor que 80, necesariamente $|G| = 60$. Vexámolo:

Do Teorema de Burnside deducimos que $|G|$ será divisible como mínimo por tres números primos. Como ademais $3 \cdot 5 \cdot 7 > 80$ tense que $|G|$ será divisible por 2. Para saber cal é exactamente a orde de G, veremos que todo grupo de orde $2k$ con k impar ten un subgrupo normal. Para isto tomamos a representación regular, ρ_{reg} de dito grupo. Como G ten orde par, tomando subconxuntos da forma $\{g, g^{-1}\}$, concluímos que existe $g \neq e$ en G tal que $g = g^{-1}$, polo que g ten orde 2. Nesta situación, é posible tomar unha base B de $\mathbb{C}[G]$ tal que

$$(\rho_{reg}(g))_B = \begin{pmatrix} 0 & 1 & 0 & 0 & ... & 0 & 0 \\ 1 & 0 & 0 & 0 & ... & 0 & 0 \\ 0 & 0 & 0 & 1 & ... & 0 & 0 \\ 0 & 0 & 1 & 0 & ... & 0 & 0 \\ ... & ... & ... & ... & ... & ... & ... \\ 0 & 0 & 0 & 0 & ... & 0 & 1 \\ 0 & 0 & 0 & 0 & ... & 1 & 0 \end{pmatrix}.$$

É claro que a matriz anterior está constituída por k bloques

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

polo que $det((\rho_{reg}(g))_B) = -1$, xa que k é impar. Polas propiedades dos determinantes conclúese que dados $g', g'' \in G$ arbitrarios, $det(\rho_{reg}(gg'')) = det(\rho_{reg}(g'))det(\rho_{reg}(g''))$. Entón, podemos definir un homomorfismo de grupos, $\tilde{\rho}$, que asocie g' con $det(\rho_{reg}(g'))$ e que sexa en consecuencia, unha representación de G de grao 1, coincidindo co seu carácter asociado, $\tilde{\chi}$. Ademais é claro que $Im(\tilde{\chi})$ é un subgrupo finito de $\mathbb{C}^*$, que ten que ser cíclico pois se $Im(\tilde{\chi})$ ten orde r, polo *Teorema de Lagrange* $h^r = e$ para todo $h \in Im(\tilde{\chi})$. Polo tanto

$$Im(\tilde{\chi}) < \{g' \in G \mid g'^r = e\} = \left\langle e^{\frac{2\pi i}{r}} \right\rangle.$$

Como $|Im(\tilde{\chi})| = |\left\langle e^{\frac{2\pi i}{r}} \right\rangle| = r$, temos que $Im(\tilde{\chi}) = \left\langle e^{\frac{2\pi i}{r}} \right\rangle$, polo que é cíclico.

O feito anteriormente permítenos deducir que $-1 \in Im(\tilde{\chi})$ e como -1 ten orde 2, necesariamente $Im(\tilde{\chi})$ ten orde par; é dicir $r = 2t$. Así, por ser $Im(\tilde{\chi})$ cíclico, contén un subgrupo H de orde t tal que $(Im(\tilde{\chi}) : H) = 2$ e polo tanto normal. Nesta situación é claro que $\{g' \in G \text{ tal que } \tilde{\chi}(g') \in H\}$ tamén é un subgrupo de G de índice 2 e consecuentemente tamén normal.

Así, temos comprobado que se $|G| = 2k$ con k impar, G non é simple, polo que $|G|$ ten que ser múltiplo de 4 para verificar as hipóteses. Como $4 \cdot 3 \cdot 7 > 80$ tense que $|G| = 4 \cdot 3 \cdot 5 = 60$.

4.3. Teorema de Hall.

Neste derradeiro epígrafe probarase o *Teorema de Hall*, que tamén permite concluír que certos grupos son resolubles. Para a súa demostración emprégase o *Teorema de Burnside* e algúns resultados que se inclúen seguidamente:

Definición 4.11. Dado un subgrupo H de G, se existe outro subgrupo de G, K tal que $G = HK$ e $H \cap K = 1$, dise que K é un **complemento** de H en G.

Lema 4.12. *Se G é un grupo resoluble de orde $n > 1$, existe un p-grupo P tal que $P \lhd G$.*

Demostración. Sabemos que dado G de orde $n > 1$ é resoluble se, e só se, existe $r > 0$ tal que $G^{(r)} = \{e\}$, sendo $G^{(0)} > G^{(1)} > \cdots > G^{(r-1)} > G^{(r)}$ a serie derivada de G. En particular, $G^{(r-1)}$ non é o grupo trivial, polo que se pode deducir que existe un p-Sylow P de $G^{(r-1)}$, para algún primo p. Ademais, dito subgrupo P será normal en $G^{(r-1)}$ xa que este é abeliano. □

Lema 4.13. *Sexan $|G| = p_1^{a_1} p_2^{a_2} \cdots p_t^{a_t}$, onde $p_1, \ldots, p_t$ son primos distintos e H e K subgrupos de G de tal xeito que para todo $i \in \{1, \ldots, t\}$, $p_i^{a_i}$ divide a $|H|$ ou a $|K|$. Entón $G = HK$ e $|H \cap K| = (|H|, |K|)$.*

Demostración. É claro que HK pode interpretarse como a unión disxunta das clases de equivalencia de H pola dereita, que teñen cardinal $|H|$, ou das clases de equivalencia de K pola esquerda, cuxo cardinal é $|K|$. Así, debido a que $p_i^{a_i}$ divide a $|H|$ ou a $|K|$ por hipótese, tense que tamén dividirá a $|HK|$ e, como i foi tomado arbitrariamente, dedúcese que $|G|$ divide a $|HK|$, polo que necesariamente $G = HK$. Ademais, xa que

$$|HK| = \frac{|H||K|}{|H \cap K|}$$

obtense tamén que $|H \cap K| = (|H|, |K|)$. □

Teorema 4.14 (Teorema de Hall). *Se* $|G| = p_1^{a_1} p_2^{a_2} \cdots p_t^{a_t}$, *onde* $p_1, \ldots, p_t$ *son primos distintos e para cada* $i \in \{1, \ldots, t\}$ *existe un subgrupo* H_i *de* G *tal que* $(G : H_i) = p_i^{a_i}$, *entón* G *é resoluble.*

Demostración. Empregaremos a indución na orde de G, asumindo que temos o resultado para $t-1$ e comprobando que se dá para t. Se $t \leq 2$ o resultado verifícase, pois estamos nas hipóteses do *Teorema de Burnside*. Supoñamos $t \geq 3$ e tomemos $i \in \{1, \ldots, t\}$ arbitrario. Entón, por 4.13, para todo $j \in \{1, \ldots, t\}$, $j \neq i$, $(H_i : H_i \cap H_j) = p_j^{a_j}$. Así, para calquera p_j-Sylow de H_i, $H_i \cap H_j$ é o seu complemento en H_i. Por outra banda, asumiremos que H_i é resoluble pola hipótese de indución.

Nesta situación, poderiamos tomar, por 4.12, $P \lhd H_1$ con $|P| = p_i^a > 1$ para algún $i \in \{2, \ldots, t\}$. Xa que $t \geq 3$, existe $j \in \{1, \ldots, t\}$ tal que $j \neq \{1, i\}$ e por 4.13 $|H_1 \cap H_j| = p_2^{a_2} \cdots p_{j-1}^{a_{j-1}} p_{j+1}^{a_{j+1}} \cdots p_t^{a_t}$. Entón, $H_1 \cap H_j$ contén un p_i-Sylow de H_1. Posto que $P \lhd H_1$, P está contido en todo p_i-Sylow de H_1 e, en consecuencia, $P < H_1 \cap H_j$. Por 4.13, $G = H_1 H_j$, polo que todo $g \in G$ pode ser escrito como $g = h_1 h_j$ para certos $h_1 \in H_1$ e $h_j \in H_j$. Así, $gH_j g^{-1} = (h_1 h_j) H_j (h_1 h_j)^{-1} = h_1 H_j h_1^{-1}$ e polo tanto $\cap_{g \in G} g H_j g^{-1} = \cap_{h_1 \in H_1} h_1 H_j h_1^{-1}$. Como $P < H_j$ e $h_1 P h_1^{-1} = P$ para todo $h_1 \in H_1$ tense que $e \neq P < \cap_{h_1 \in H_1} h_1 H_j h_1^{-1} = \cap_{g \in G} g H_j g^{-1} = N$. Así N é un subgrupo normal, propio e non trivial de G. Entón, posto que N e G/N satisfán as hipóteses do teorema, son resolubles pola hipótese de indución, polo que G é tamén resoluble.

□

Bibliografía

[1] Bender, H. A group-theoretic proof of Burnside's p^aq^b-theorem. *Math. Z.* (126) (1972), 327-338.

[2] Burnside, W. On groups of order p^aq^b. *Proc. London Math. Soc.***(2)** (1904), 388-392.

[3] Cárdenas, H e E. Lluis. *Módulos semisimples y representación de grupos.* F. Trillas, Méjico, 1970.

[4] Corrádi, K. e E. Horváth. Steps towards and elementary proof of Frobenius' Theorem. *Comm. in Algebra* 24 (1996), 2285-2292.

[5] Curtis, C. W. e I. Reiner. *Representation Theory of Finite Groups and Associative Algebras.* Wiley and Sons, New York, 1988.

[6] Dummit, D.S. e R.M. Foote. *Abstract Algebra.* Wiley and Sons, New York, 2004.

[7] Flavell, P. A Note on Frobenius Groups. *Journal of Algebra* 228 (2000), 367-376.

[8] Goldschmidt, D. A group-theoretic proof of the p^aq^b-theorem for odd primes. *Math. Z.* 113 (1970), 373-375.

[9] Isaacs, I. M. *Character Theory of finite groups.* Academic Press, New York, 1976.

[10] Ivorra Castillo, C. *Representaciones de grupos finitos* [2008]. Recuperado de https://www.uv.es/ivorra/Libros/Representaciones.pdf o $26-01-2019$.

[11] Jacobson, N. *Basic Algebra II.* W. H.Freeman and Company, San Francisco, 1980.

[12] James, G e M. Liebeck. *Representations and Characters of Groups.* Cambridge University Press, Cambridge, 1993.

[13] Matsuyama, H. Solvabililty of groups of order 2^ap^b. *Osaka J. Math.* **10** (1973), 375-378.

[14] Rotman, J. J. *An Introduction to the Theory of Groups.* Fourth Edition. Springer-Verlag, New York, 1995.

[15] Sancho, P. *Representaciones de grupos finitos* [2003]. Recuperado de http://matematicas.unex.es/∼ sancho/Apuntes/Rep0.pdf o $23 - 01 - 2019$