1. Introducción.

Estas son las notas del curso "Matrices Gruperas: una introducción a la Teoría de Representaciones de Grupos", impartido por Luis Valero Elizondo en la I Escuela de Algebra del CIMAT, del 24 al 30 de abril del 2005. Aquí aparecen todas las definiciones que se verán en el curso, así como algunos resultados fundamentales de teoría de grupos y álgebra lineal. Algunos de estos resultados son relativamente sencillos de demostrar, y decidí mejor llamarles "ejercicios", para que el lector interesado en los retos tenga algo en qué pensar. Para comodidad de los participantes incluyo al final un índice analítico. Cabe observar que este material es sólo la mitad de lo que haremos en el curso. La otra mitad consta de varias actividades que haremos durante las sesiones, en donde demostraremos algunos teoremas básicos de la teoría de representaciones de grupos.

En la Sección 2 están los prerrequisitos, que son conocimientos básicos de la teoría de grupos (ver [2]) y un primer curso de álgebra lineal (ver [3]). No es estrictamente necesario haber llevado estas materias, pues el material que se necesita está completamente incluido en esta sección, pero ayuda mucho tener cierta destreza en el manejo de estos conceptos.

En la Seccion 3 están algunos de los conceptos fundamentales de la teoría de representaciones de grupos finitos, tanto clásicas (teoría de caracteres complejos, ver [4]) como modulares (en característica $p > 0$, ver [1]). Es posible dar muchas clases avanzadas en estos temas, por lo que este curso muestra sólo una pequeña parte de la punta del iceberg de la teoría de representaciones. Aún así, espero que los participantes se lleven al menos algunas de las ideas que se manejan en esta fascinante rama de las matemáticas.

2. Prerrequisitos.

2.1. Teoría de grupos.

Definición 1. Sea G un conjunto no vacío. Una **operación binaria** en G es una función $* : G \times G \longrightarrow G$.

Notación 2. Usualmente escribiremos ab en lugar de $*(a, b)$, tanto si se trata de una operación binaria $*$ en un conjunto, o simplemente de una función $* : A \times B \longrightarrow C$ con A, B, C conjuntos. La única excepción a esta convención es cuando tengamos una operación binaria denotada $+$ en un

conjunto; usualmente escribiremos $a+b$ en lugar de $+(a,b)$ o ab. La expresión $\sum_{i=1}^{s} a_i$ significa $a_1 + a_2 + \cdots + a_s$.

Definición 3. Un **grupo** es un conjunto G junto con una operación binaria $*$ que satisface las siguientes tres propiedades:

(i) Para cualesquiera elementos a, b, c en G se tiene que $a(bc) = (ab)c$. En este caso, se dice que la operación binaria $*$ es **asociativa**.

(ii) Existe un elemento e en G tal que $ea = a = ae$ para todo a en G. El elemento e se llama la **identidad** del grupo G.

(iii) Para todo a en G, existe un elemento b en G tal que $ba = e = ab$. El elemento b se llama el **inverso** del elemento a, y usualmente se denota a^{-1}.

Definición 4. Sea G un grupo. El **orden** de G es el número de elementos de G, y se denota $|G|$.

Definición 5. Sean p un número primo, y G un grupo finito. Decimos que G es un **p-grupo** si el orden de G es una potencia de p.

Definición 6. Sea G un grupo. Decimos que G es **abeliano** si la operación es **conmutativa**, es decir, si para todos a, b en G se tiene que $ab = ba$. Muchas veces uno denota la operación en un grupo abeliano por $+$, al elemento identidad por 0, al inverso de a por $-a$, y uno escribe $a - b$ en lugar de $a + (-b)$.

Definición 7. Sea G un grupo. Decimos que G es un grupo **cíclico** si existe un elemento x en G tal que todo elemento de G distinto de la identidad se puede expresar como un producto de la forma $xxx\ldots x$, o de la forma $x^{-1}x^{-1}\ldots x^{-1}$. En este caso decimos que x es un **generador** del grupo G, y lo denotamos $G =< x >$.

Definición 8. Sea G un grupo. Un **G-conjunto** es un conjunto X en el que el grupo G **actúa**, es decir, existe una función $\cdot : G \times X \longrightarrow X$, para la cuál usamos la notación gx en lugar de $\cdot(g, x)$, y que cumple lo siguiente:

(i) Para todo x en X se tiene que $ex = x$, donde e denota la identidad del grupo G;

(ii) Para todos g, h en G y para todo x en X, se tiene que $(gh)x = g(hx)$.

Definición 9. Sean G un grupo y X un G-conjunto. Los **puntos fijos** de X bajo la acción de G son los elementos x de X que cumplen $gx = x$ para toda g en G. El conjunto de todos los puntos fijos de X bajo la acción de G se denota X^G.

Definición 10. Sean G un grupo y X un G-conjunto no vacío. Decimos que X es un G-conjunto **transitivo** si para todos x, y en X existe g en G tal que $y = gx$.

Ejercicio 11. Sean G un grupo y X un G-conjunto transitivo. Demuestre que las siguientes condiciones son equivalentes:

(i) X tiene al menos un punto fijo bajo G.
(ii) Todos los puntos de X están fijos bajo la acción de G.
(iii) X tiene cardinalidad uno.

Teorema 12. *Sean G un grupo finito y X un G-conjunto transitivo. Entonces X es finito, y su cardinalidad es un divisor del orden de G.*

Definición 13. Sean G un grupo, X un G-conjunto y Y un subconjunto de X. Decimos que Y es un **G-subconjunto** de X si Y es **cerrado** bajo la acción de G, es decir, si para toda g en G y para toda y en Y tenemos que gy está en Y. En este caso, Y se puede considerar a su vez como un G-conjunto con la acción de G que Y hereda de X.

Teorema 14. *Sean G un grupo y X un G-conjunto no vacío. Entonces X se parte de manera única como la unión disjunta de G-subconjuntos transitivos, que se llaman las **órbitas** de G en X.*

Ejercicio 15. Sean p un número primo, G un p-grupo finito y X un G-conjunto finito. Si la cardinalidad de X no es un múltiplo de p, entonces X tiene al menos un punto fijo bajo la acción de G. (Sugerencia: demuestre por contradicción que al menos una de las órbitas de X tiene tamaño uno.)

Definición 16. Sea G un grupo, y sean X y Y G-conjuntos. Una función $f : X \longrightarrow Y$ es un **homomorfismo de G-conjuntos** si cumple que $f(gx) = gf(x)$ para toda g en G y para toda x en X.

2.2. Álgebra lineal.

Definición 17. Un **campo** (también llamado **cuerpo**) es un conjunto k junto con dos operaciones binarias $+$ y $*$ en k, llamadas **suma** y **producto** respectivamente, que tienen las siguientes propiedades:

(i) Ambas operaciones son asociativas.
(ii) Ambas operaciones son conmutativas.

(iii) Existen elementos distintos 0 y 1 en k tales que para toda a en k se tiene $a + 0 = a = a1$. Note la convención que usamos en el apartado 2.

(iv) Para todo elemento a en k existe un elemento denotado $-a$ tal que $a + (-a) = 0$.

(v) Para todo elemento a en k con $a \neq 0$, existe un elemento denotado a^{-1} tal que $aa^{-1} = 1$.

(vi) Para todos a, b, c en k se tiene que $a(b + c) = (ab) + (ac)$, llamada propiedad **distributiva**.

Definición 18. Sea k un campo. Si existe un número n tal que el 1 de k sumado n veces da 0 y n es el menor entero positivo con esa propiedad, decimos que k tiene **característica** n. Si no existe tal n, decimos que el campo k tiene característica 0.

Teorema 19. *Sea p un número primo. Entonces existe un campo con exactamente p elementos, cuya característica es p. (Nota: se puede construir este campo tomando a los enteros módulo p.)*

Definición 20. Sea k un campo. Un **k-espacio vectorial** (también llamado un **espacio vectorial** sobre k) es un conjunto V junto con dos operaciones $+$ y $\cdot$, llamadas la **suma vectorial** y **multiplicación escalar** respectivamente, las cuáles cumplen las siguientes propiedades:

(i) $+$ es una operación binaria en V, y V con $+$ es un grupo abeliano. El elemento identidad de este grupo abeliano se denota 0, y se le llama el **vector cero** de V. A los elementos de V se les suele llamar **vectores**.

(ii) $\cdot$ es una función de $k \times V$ en V.

(iii) Para cualesquiera s, t en k y para todo v en V, se tiene que $(s+t)v = (sv) + (tv)$ y $(st)v = s(tv)$.

(iv) Para todo v en V se tiene que $1v = v$.

(v) Para todo s en k y para cualesquiera v, u en V se tiene que $s(v+u) = (sv) + (su)$.

Definición 21. Sea k un campo, y sea V un k-espacio vectorial. Una sucesión ordenada de vectores $v_1, \ldots, v_s$ en V es una **base** de V sobre k si para todo vector u en V existen escalares únicos $a_1, \ldots, a_s$ en k tales que $u = \sum_{i=1}^{s} a_i v_i$. Si V tiene una base con s elementos, decimos que V tiene **dimensión** s sobre k, y en particular que la dimensión de V sobre k es finita.

Teorema 22. *Sean k un campo finito con p elementos y V un k-espacio vectorial de dimensión finita. Entonces la cardinalidad de V es una potencia de p.*

Definición 23. Sea k un campo, y sean V y W k-espacios vectoriales. Una función $f : V \longrightarrow W$ es una **transformación lineal** si cumple las condiciones siguientes:

(i) $f(u+v) = f(u) + f(v)$ para cualesquiera u, v en V.

(ii) $f(av) = af(v)$ para toda a en k y para toda v en V.

Notación 24. Sea k un campo, y sea V un k-espacio vectorial. Denotamos por $\mathbf{End}_k(V)$ al conjunto de todas las transformaciones lineales de V en sí mismo. El subconjunto de $\mathrm{End}_k(V)$ que consta de las transformaciones lineales biyectivas se denota $\boldsymbol{GL}(V)$.

Definición 25. Sea k un campo, y sea V un k-espacio vectorial de dimensión finita con base $v_1, \ldots, v_s$. Sea f una transformación lineal de V en sí mismo. Para cada básico v_i, escriba $f(v_i) = \sum_{j=1}^{s} a_{i,j} v_i$, donde cada $a_{i,j}$ es un escalar en el campo k. La **traza** de la transformación lineal f, denotada $Tr(f)$, es el escalar del campo dado por $\sum_{i=1}^{s} a_{i,i}$. Este escalar no depende de la base de V que se tome.

Definición 26. Sean k un campo, V un k-espacio vectorial y W un subconjunto no vacío de V. Decimos que W es un **k-subespacio vectorial** de V si W es cerrado bajo las operaciones de V, es decir, si se cumplen las siguientes condiciones:

(i) Para cualesquiera v, u en W se tiene que $u + v$ está en W.

(ii) Para todo v en W y para todo a en k se tiene que av está en W.

Teorema 27. *Sean k un campo, V y W k-espacios vectoriales, y $f : V \longrightarrow W$ una transformación lineal. El conjunto $\{v \in V \mid f(v) = 0\}$ es un k-subespacio vectorial de V, llamado el **núcleo** (o **kernel**) de la transformación lineal f.*

Teorema 28. *Sean k un campo, V un k-espacio vectorial y W un k-subespacio vectorial de V. Entonces existe una transformación lineal $f : V \longrightarrow W$ tal que $f(w) = w$ para toda w en W. Esta transformación lineal se llama una **proyección** de V sobre W, y en general no es única.*

Definición 29. Sean k un campo y V un k-espacio vectorial cualquiera. El conjunto $\{0\}$ forma un k-subespacio vectorial de V, llamado el **subespacio cero**, y denotado 0.

Definición 30. Sean k un campo, V un k-espacio vectorial y $U_1, \ldots, U_s$ k-subespacios vectoriales de V. Decimos que V es la **suma directa** de los subespacios $U_1, \ldots, U_s$, y lo denotamos $V = U_1 \oplus U_2 \oplus \cdots \oplus U_s$ (o también $V = \oplus_{i=1}^{s} U_i$) si para todo v en V existen vectores únicos u_1 en U_1, u_2 en U_2, $\ldots$, u_s en U_s tales que $v = u_1 + u_2 + \cdots + u_s$.

Ejercicio 31. Sean k un campo, V un k-espacio vectorial, y sean W y U k-subespacios vectoriales de V. Entonces $V = W \oplus U$ si y sólo si se cumplen las siguientes dos condiciones:

(i) Para todo v en V existen w en W y u en U tales que $v = w + u$.

(ii) $W \cap U = 0$.

Ejercicio 32. Sean k un campo, V un k-espacio vectorial, W un k-subespacio vectorial de V y $f : V \longrightarrow W$ una proyección de V sobre W. Entonces tenemos que $V = W \oplus \mathrm{Ker}(f)$.

3. kG-módulos.

Definición 33. Sean G un grupo finito y k un campo. Un conjunto M es un kG-**módulo** (también llamado **módulo** sobre kG) si es un k-espacio vectorial que a la vez es un G-conjunto, donde las dos estructuras satisfacen las siguientes condiciones de compatibilidad:

(i) Para toda g en G y para cualesquiera v, u en M se tiene que $g(v+u) = (gv) + (gu)$.

(ii) Para toda g en G, para toda v en M y para toda a en k se tiene que $g(av) = a(gv)$.

Definición 34. Sean G un grupo finito, k un campo y M un kG-módulo. Para cada g en G, denote por $\rho_M(g)$ la transformación lineal de M en sí mismo que manda a cada vector v en gv. De hecho, $\rho_M(g)$ es una transformación lineal biyectiva (con inverso $\rho_M(g^{-1})$). La función $\rho_M : G \longrightarrow GL(M)$ se llama la **representación** asociada al kG-módulo M.

Definición 35. Sean G un grupo, k un campo, M un kG-módulo y N un subconjunto de M. Decimos que N es un kG-**submódulo** de M si N es a la vez un k-subespacio vectorial y un G-subconjunto de M.

Ejercicio 36. Sean G un grupo, k un campo, M un kG-módulo y N un kG-submódulo de M. Defina una relación $\sim$ en M por $v \sim u$ si y sólo si

$v - u \in N$. Demuestre que $\sim$ es una relación de equivalencia, y que $\sim$ es "compatible" con la estructura de módulo de M, es decir, si $v \sim u$ y $w \sim x$, entonces

(i) $v + w \sim u + x$ (compatibilidad con la suma vectorial);

(ii) $av \sim au$ para todo a en k (compatibilidad con la multiplicación escalar);

(iii) $gv \sim gu$ para todo g en G (compatibilidad con la acción del grupo G).

Ejercicio 37. Sean k un campo, G un grupo y M un kG-módulo. Entonces el conjunto $\{0\}$ (que usualmente se denota 0) es una órbita de M como G-conjunto. En particular, 0 es un kG-submódulo de M.

Ejercicio 38. Sean k un campo, G un grupo y M un kG-módulo. Sea M^G el conjunto de los puntos fijos de M bajo la acción de G (ver Definición 9). Demuestre que M^G es un kG-submódulo de M.

Definición 39. Sean G un grupo, k un campo y M un kG-módulo. Decimos que M es un kG-módulo **simple** (también llamado **irreducible**) si M tiene exactamente dos kG-submódulos, a saber, 0 y M mismo.

Definición 40. Sean k un campo, G un grupo, M un kG-módulo y $N_1, \ldots, N_s$ kG-submódulos de M. Decimos que el kG-módulo M es la **suma directa** de los submódulos $N_1, \ldots, N_s$, y lo denotamos $M = N_1 \oplus \cdots \oplus N_s$ (o también $M = \oplus_{i=1}^{s} N_i$), si M es la suma directa de los $N_1, \ldots, N_s$ como k-espacios vectoriales.

Definición 41. Sean k un campo, G un grupo y M un kG-módulo. Decimos que M es un kG-módulo **inescindible** si no existen submódulos N y P de M diferentes de 0 tales que $M = N \oplus P$.

Definición 42. Sean k un campo, G un grupo y M un kG-módulo. Decimos que M es un kG-módulo **semisimple** si existen submódulos simples de M tales que M es su suma directa.

Definición 43. Sea $\mathbb{C}$ el campo de los números complejos, sea G un grupo finito, M un $\mathbb{C}G$-módulo y ρ_M la representación asociada a M. Para cada g en G, sea $\chi_M(g)$ la traza de la transformación lineal $\rho_M(g)$. La función $\chi_M : G \longrightarrow \mathbb{C}$ se llama el **carácter** asociado al $\mathbb{C}G$-módulo M.

Referencias

[1] J. L. Alperin. *Local Representation Theory.* Cambridge studies in advanced mathematics. Cambridge University Press, Cambridge; New York, 1986.

[2] I. N. Herstein. *Álgebra moderna: grupos, anillos, campos, teoría de Galois.* Editorial Trillas, 1970.

[3] Kenneth Hoffman, Ray Kunze. *Álgebra lineal.* Prentice Hall, 1973.

[4] Gordon Douglas James and Martin Liebeck. *Representations and characters of groups.* Cambridge Mathematical Textbooks. Cambridge University Press, 1993.

Actividad: Problema. Sean k un campo, G un grupo, M y N kG-módulos, y $\phi : M \longrightarrow N$ una función. Defina lo que significa que ϕ sea un **homomorfismo de kG-módulos**. También defina **isomorfismo** de kG-módulos.

Notación 44. Sean k un campo, G un grupo, M y N kG-módulos. Al conjunto de transformaciones lineales de M a N lo denotamos $\mathrm{Hom}_k(M, N)$; al conjunto de homomorfismos de kG-módulos de M a N lo denotamos $\mathrm{Hom}_{kG}(M, N)$.

Actividad: Problema. Sean k un campo, G un grupo, M y N kG-módulos.

(i) Demuestre que $\mathrm{Hom}_k(M, N)$ es un k-espacio vectorial con suma $(f + g)(v) = f(v) + g(v)$ y multiplicación escalar $(af)(v) = af(v)$.

(ii) Demuestre que $\mathrm{Hom}_k(M, N)$ es un kG-módulo, donde G actúa por medio de $(gf)(v) = gf(g^{-1}v)$.

(iii) Demuestre que $(\mathrm{Hom}_k(M, N))^G = \mathrm{Hom}_{kG}(M, N)$.

Actividad: Problema. Sean k un campo, G un grupo, M y N kG-módulos, y $\phi : M \longrightarrow N$ un homomorfismo de kG-módulos.

1. Demuestre que $\mathrm{Ker}(\phi) = \{v \in M \mid \phi(v) = 0\}$ es un submódulo de M.
2. Demuestre que $\mathrm{Im}(\phi) = \{\phi(v) \mid v \in M\}$ es un submódulo de N.
3. Demuestre que ϕ es inyectiva si y sólo si $\mathrm{Ker}(\phi) = \{0\}$.
4. Demuestre que ϕ es suprayectiva si y sólo si $\mathrm{Im}(\phi) = N$.
5. Demuestre que si M es simple, entonces o ϕ es inyectiva o $\phi(v) \equiv 0$ (es decir, $\phi(v) = 0$ para todo $v \in M$).
6. Demuestre que si N es simple, entonces o ϕ es suprayectiva o $\phi \equiv 0$.
7. Demuestre que si tanto M como N son simples, entonces o ϕ es un isomorfismo o $\phi \equiv 0$.

Actividad: Problema. Sean G un grupo finito, M un $\mathbb{C}G$-módulo simple y $\phi : M \longrightarrow M$ un homomorfismo de kG-módulos. Entonces existe un escalar $a \in \mathbb{C}$ tal que $\phi(v) = av$ para todo $v \in M$. (Sugerencia: use el hecho

de que existen $a \in \mathbb{C}$ y $0 \neq v \in M$ tales que $\phi(v) = av$; considere la función $\psi(v) = \phi(v) - av$.)

Actividad: Problema. (Lema de Schur) Sean k un campo, G un grupo, M y N kG-módulos simples. Entonces la dimensión de $\mathrm{Hom}_{\mathbb{C}G}(M, N)$ sobre $\mathbb{C}$ es 1 si M y N son kG-módulos isomorfos, y 0 si no lo son.

Ejercicio 45. Sean k un campo, G un grupo, M un kG-módulo y N un kG-submódulo de M. Defina la relación de equivalencia $\sim$ en M por $v \sim u$ si y sólo si $v - u \in N$ (véase el apartado 36). Demuestre que las clases de equivalencia de esta relación forman un kG-módulo, llamado el módulo **cociente** de M entre N.

Actividad: Juego de maratón. Divídanse en cuatro equipos, y decidan el orden en que jugarán los equipos.

1. (UN PUNTO) Notación hasta la pregunta 18: Sean k el campo con dos elementos y sea $G =< x >$ el grupo de orden 2. Escriba la tabla de la operación de G.
2. Escriba la tabla de la suma de k.
3. Escriba la tabla de la multiplicación de k.
4. Calcule la dimensión de kG sobre k.
5. (DOS PUNTOS) Diga cuántos elementos hay en kG y lístelos todos.
6. Calcule gv para todo g en G y un vector v en kG (4 preguntas).
7. Encuentre todos los puntos fijos de kG bajo la acción del grupo G.
8. Demuestre que cualquier submódulo propio no trivial de kG tiene dimensión uno sobre k.
9. Sea $S = \{0, v\}$ un submódulo propio no cero de kG. Demuestre que v es un punto fijo de G.
10. (CINCO PUNTOS) Encuentre un submódulo propio no trivial de kG.
11. Encuentre todos los submódulos propios no triviales de kG.
12. ¿Es kG un kG-módulo inescindible?
13. Demueste que kG es un kG-módulo inescindible.
14. ¿Es kG un kG-módulo simple?
15. Demuestre que kG no es un kG-módulo simple.
16. ¿Es kG un kG-módulo semisimple?
17. Demuestre que kG no es un kG-módulo semisimple.
18. (DIEZ PUNTOS) Exhiba un kG-módulo semisimple que no sea simple.

19. Sean p un número primo, k el campo con p elementos, G un grupo finito y $M \neq 0$ un kG-módulo de dimensión finita sobre k. Demuestre que la cardinalidad de M es un múltiplo de p.

20. Sean k un campo, G un grupo, M un kG-módulo y $X = M - \{0\}$. Demuestre que el conjunto X es un G-subconjunto de M.

21. Sean p un número primo, k el campo con p elementos, G un grupo finito, M un kG-módulo diferente de 0 de dimensión finita sobre k y $X = M - \{0\}$. Demuestre que la cardinalidad de X no es un múltiplo de p.

22. EL PRIMERO QUE ADIVINE CONTESTA: (QUINCE PUNTOS) Sean p un número primo, k el campo con p elementos, G un p-grupo finito y $M \neq 0$ un kG-módulo de dimensión finita sobre k. Demuestre que $M^G \neq 0$.

23. (VEINTE PUNTOS) Sean p un número primo, k el campo con p elementos, G un p-grupo finito y $M \neq 0$ un kG-módulo simple de dimensión finita sobre k. Demuestre que G actúa trivialmente sobre M, es decir, que $M^G = M$.

24. (CUARENTA PUNTOS) Sean p un número primo, k el campo con p elementos, G un p-grupo finito y $M \neq 0$ un kG-módulo simple de dimensión finita sobre k. Demuestre que M tiene dimensión uno sobre k.

Actividad: Espacios. Complete cada uno de los espacios con una o varias palabras o símbolos apropiados.

Teorema 46. *(Maschke) Sean k un campo, G un grupo finito, M un kG-módulo y N un kG-submódulo de M. Si $|G|$ es invertible en k, entonces existe un kG-submódulo P de M tal que $M = N \oplus P$.*

Demostración. Considerando a M y N como k-espacios _____ , existe una proyección $f : M \longrightarrow N$. Considere la función $\phi : M \longrightarrow N$ dada por

$$\phi(v) = \frac{1}{|G|} \sum_{g \in G} gf(g^{-1}v)$$

para toda _____ en M. Note que esta función está bien _____ , pues _____ es un kG-submódulo de M y $\frac{1}{|G|}$ es un escalar bien definido en _____ por hipótesis. Afirmamos que ϕ es una _____ lineal. En efecto, tenemos que _____ v y u en M

$$\begin{aligned}
\phi(v+u) &= \frac{1}{|G|} \sum_{g \in G} gf(g^{-1}(\text{_____})) = \frac{1}{|G|} \sum_{g \in G} gf(g^{-1}v + g^{-1}u) \\
&= \frac{1}{|G|} \sum_{g \in G} g(\text{_____} + f(g^{-1}u)) \\
&= \frac{1}{|G|} \sum_{g \in G} gf(g^{-1}v) + \text{_____} \\
&= \frac{1}{|G|} \sum_{g \in G} gf(g^{-1}v) + \frac{1}{|G|} \sum_{g \in G} gf(g^{-1}u) \\
&= \text{_____} + \phi(u).
\end{aligned}$$

Además, para cualquier escalar _____ en k tenemos

$$\begin{aligned}
\phi(\text{_____}) &= \frac{1}{|G|} \sum_{g \in G} gf(\text{_____}) = \frac{1}{|G|} \sum_{g \in G} gf(a(g^{-1}v)) \\
&= \frac{1}{|G|} \sum_{g \in G} g(af(\text{_____})) = \frac{1}{|G|} \sum_{g \in G} agf(g^{-1}v) \\
&= \text{_____} \sum_{g \in G} g(f(g^{-1}v)) \\
&= a\phi(v),
\end{aligned}$$

por lo que _____ es una transformación lineal.

Más aún, ϕ es una _____ de M sobre N, pues si v está en N, entonces para _____ g en G tenemos que $g^{-1}v$ también está en _____ (pues N es _____ bajo la acción del grupo G), y por lo tanto $f(g^{-1}v) =$ _____, y se sigue que

$$\begin{aligned} \text{\_\_\_\_} &= \frac{1}{|G|}\sum_{g\in G} gf(g^{-1}v) = \frac{1}{|G|}\sum_{g\in G} g(\text{\_\_\_\_}) \\ &= \frac{1}{|G|}\sum_{g\in G} (\text{\_\_\_\_})v = \frac{1}{|G|}\sum_{g\in G} ev \\ &= \frac{1}{|G|}\sum_{g\in G} \text{\_\_\_\_} = \text{\_\_\_\_}|G|v \\ &= v \end{aligned}$$

Como ϕ es una proyección sobre N, tenemos que

$$\text{\_\_\_\_} = N \oplus \mathrm{Ker}(\phi)$$

donde ésta es una descomposición como _____ directa de espacios vectoriales. Resta demostrar que _____ es en realidad un kG-submódulo de M, es decir, que $\mathrm{Ker}(\phi)$ es cerrado bajo la acción del _____ . Sean $v \in \mathrm{Ker}(\phi)$ y $h \in G$. Queremos demostrar que $hv \in$ _____. Evaluando obtenemos

$$\phi(hv) = \frac{1}{|G|}\sum_{g\in G} gf(g^{-1}(\text{\_\_\_\_})) = \frac{1}{|G|}\sum_{g\in G} gf((\text{\_\_\_\_})v).$$

Haciendo un cambio de variable $x = h^{-1}g$ (por lo que $x^{-1} =$ _____ y también $g =$ _____) y notando que g recorre _____ los elementos de G si y sólo si x también recorre todos los elementos de _____ , tenemos

$$\phi(hv) = \frac{1}{|G|}\sum_{x\in G} (\text{\_\_\_\_})f(x^{-1}v) = \frac{1}{|G|}h\sum_{x\in G} xf(x^{-1}v) = \text{\_\_\_\_}\phi(v) = h0 = 0,$$

por lo que $hv \in$ _____ , lo que concluye la demostración. □

Ejercicio 47. Sean k un campo y G un grupo finito. Demuestre que si la característica del campo k no divide al orden del grupo G, entonces todo kG-módulo M de dimensión finita puede escribirse como suma directa de submódulos simples.

Actividad: Rompecabezas. Ordene los pasos en la siguiente demostración.

Teorema 48. *(Relaciones de ortogonalidad para los caracteres complejos) Sea G un grupo finito, y sean χ y ψ caracteres de dos kG-módulos simples M y N respectivamente. Tenemos que el producto interior $<\chi, \psi>$ es igual a uno si M y N son isomorfos como kG-módulos, y cero si no lo son.*

Demostración. Demostraremos ambas afirmaciones a la vez.

Paso D: Comenzaremos citando un lema anterior, que afirma que la traza del elemento

Paso I:

$$\frac{1}{|G|}\sum_{g\in G} g$$

Paso A: en su acción sobre $\mathrm{Hom}_{\mathbb{C}}(M, N)$ es igual a la dimensión del espacio de puntos fijos, es decir,

Paso F:

$$\dim_{\mathbb{C}}(\mathrm{Hom}_{\mathbb{C}}(M, N))^G = tr\left(\frac{1}{|G|}\sum_{g\in G} g\right) \qquad (*)$$

Paso K: en su acción sobre $\mathrm{Hom}_{\mathbb{C}}(M, N)$.

Paso H: Considere el lado izquierdo de esta igualdad. Por un ejercicio anterior, sabemos que

Paso G:

$$(\mathrm{Hom}_{\mathbb{C}}(M,N))^G = \mathrm{Hom}_{\mathbb{C}G}(M,N),$$

Paso J: y por el Lema de Schur, la dimensión de este espacio es uno si M es isomorfo a N como $\mathbb{C}G$-módulos, o cero si no.

Paso C: Ahora considere el lado derecho de la fórmula (*). Por un resultado sobre caracteres, la traza de un elemento g de G en el módulo $\mathrm{Hom}_{\mathbb{C}}(M,N)$ es $\chi(g^{-1})\psi(g)$, por lo que

Paso E:

$$tr\left(\frac{1}{|G|}\sum_{g\in G} g\right) = \frac{1}{|G|}\sum_{g\in G}\chi(g^{-1})\psi(g) =< \chi, \psi >,$$

Paso B: donde la última igualdad es simplemente la definición del producto interior de caracteres. Esto termina la demostración.

□