Representaciones lineales de grupos finitos (introducción al álgebra)

19 – 23 de diciembre de 2016

> Álgebra.
> 1. Parte de las matemáticas en la cual las operaciones aritméticas son generalizadas empleando números, letras y signos.
> 2. Arte de restituir a su lugar los huesos dislocados.
>
> El Diccionario de la Real Academia Española

Estos apuntes acompañan un breve curso en la Universidad de El Salvador para los estudiantes del primer año. Nuestro objetivo es ver algunos resultados básicos sobre las representaciones lineales de grupos finitos sobre $\mathbb{C}$. Las primeras dos lecciones están dedicadas a las definiciones necesarias de la teoría de grupos y el álgebra lineal. Luego se definen las representaciones de grupos y sus caracteres. Muchos ejemplos están presentados en forma de ejercicios. El lector tiene que por lo menos intentar de resolverlos todos y la colaboración con compañeros de clase es bienvenida.

Para todo tipo de preguntas, pueden contactarme por correo cadadr@gmail.com.

Agradecimientos

Le doy gracias a Gabriel Chicas Reyes por su asistencia con organización del curso y la revisión de estos apuntes. También agradezco a todos mis alumnos: Teresa Elena Beltrán Morales, Martha Beatriz Bran Hernández, Raúl Valentín Cortez Ares, Susana Isabel Escobar Mejía, Marvin Alberto Ferman Bell, Jony Manuel Hernández Marquez, Ernesto Ariel Hidalgo Mayén, José Wilfredo Iraheta Martínez, David Ernesto Martínez Alvarado, Rodrigo Daniel Meléndez Mayén, Karen Rosibel Navas Cornejo, Javier Alexander Pleités Crespín, Madeline Patricia Sibrián Morales.

Índice

Literatura

Una pregunta popular es la literatura sugerida. Esta teoría combina teoría de grupos con álgebra lineal; entonces puede ser útil cualquier libro de texto sobre estos temas.

Personalmente, recomiendo el libro de texto estándar estadounidense *Abstract Algebra* de Dummit y Foote, que ocupa más de 900 páginas y contiene casi todo lo que un estudiante de licenciatura debe aprender de álgebra.

Otro buen libro, más breve, es *A Course in Algebra* de Vinberg, escrito para los estudiantes de Moscú y luego traducido del ruso (nos interesan los capítulos 1, 2, 4, 5).

Las representaciones de grupos aparecen en ambos libros, pero también recomiendo el libro *Representation Theory of Finite Groups: An Introductory Approach* de Steinberg. Allí nos sirven los primeros 4 capítulos.

Primer día: Permutaciones

1. Ejemplo primordial: permutaciones

Antes de estudiar grupos, sería instructivo analizar un caso particular que son los grupos de permutaciones (también conocidos como grupos simétricos).

1.1. Notación. Si $f\colon X \to Y$ e $g\colon Y \to Z$ son aplicaciones entre conjuntos, su composición se denota por

$$g \circ f\colon X \to Z,$$

y es definida por

$$(g \circ f)(x) = g(f(x)) \quad \text{para todo } x \in X.$$

Note que "$g \circ f$" significa que primero se aplica f y luego g. La composición es **asociativa**: para todo $f\colon X \to Y$, $g\colon Y \to Z$, $h\colon Z \to W$ tenemos

$$h \circ (g \circ f) = (h \circ g) \circ f.$$

Ejercicio I.1. *1) Sea $f\colon X \to Y$ una aplicación. Entonces las siguientes condiciones son equivalentes:*

- *Existe una aplicación $f^{-1}\colon Y \to X$ tal que $f^{-1} \circ f = \mathrm{id}_X$ y $f \circ f^{-1} = \mathrm{id}_Y$, es decir,*

$$(f^{-1} \circ f)(x) = x, \quad (f \circ f^{-1})(y) = y \quad \textit{para todo } x \in X,\ y \in Y.$$

- *f es inyectiva y sobreyectiva.*

*Estas condiciones equivalentes significan que f es una **biyección**.*
2) Demuestre que la composición de aplicaciones inyectivas (resp. sobreyectivas, biyectivas) es también inyectiva (resp. sobreyectiva, biyectiva).

1.2. Definición. Sea X un conjunto. Una **permutación** de los elementos de X es una **biyección** entre X y sí mismo; es decir, es una aplicación $\sigma\colon X \to X$ tal que existe $\sigma^{-1}\colon X \to X$ tal que

$$\sigma^{-1}(\sigma(x)) = \sigma(\sigma^{-1}(x)) = x \quad \text{para todo } x \in X.$$

1.3. Observación. *Las permutaciones de los elementos de X tienen las siguientes propiedades:*

1) si σ y τ son permutaciones, entonces $\tau \circ \sigma$ es también una permutación;

*2) la composición es **asociativa**:*

$$\rho \circ (\tau \circ \sigma) = (\rho \circ \tau) \circ \sigma.$$

*3) existe una biyección especial, la **aplicación identidad** id_X,*

$$\mathrm{id}_X(x) = x \quad \textit{para todo } x \in X,$$

para la cual se cumple

$$\sigma \circ \mathrm{id}_X = \mathrm{id}_X \circ \sigma = \sigma;$$

*4) por definición, para toda biyección σ tenemos su **aplicación inversa** σ^{-1} tal que*

$$\sigma^{-1} \circ \sigma = \sigma \circ \sigma^{-1} = \mathrm{id}_X.$$

1.4. Notación. El conjunto de permutaciones de los elementos de X se denota por $\mathrm{Sym}(X)$. Si X es un conjunto finito de n elementos, podemos suponer que

$$X = \{1, 2, \ldots, n\},$$

y en este caso se usa la notación

$$S_n := \mathrm{Sym}(\{1, 2, \ldots, n\}).$$

Una permutación puede ser escrita como

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix},$$

donde $\sigma(1), \sigma(2), \ldots, \sigma(n)$ es una sucesión de elementos de X sin repeticiones (así que $i \mapsto \sigma(i)$ es una biyección).

Ejercicio I.2. *Demuestre que* $|S_n| = n!$
(Indicación: use inducción sobre $|X|$*. La base de inducción: el caso* $X = \emptyset$*, o* $|X| = 1$*, si le teme a los conjuntos vacíos; el paso de inducción:* $|S_n| = n \cdot |S_{n-1}|$*.)*

Por ejemplo, si $X = \{1, 2, 3\}$, tenemos

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \quad \text{y} \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}. \tag{1}$$

Note en particular que el resultado de composición depende del orden de permutaciones: en general $\tau \circ \sigma \neq \sigma \circ \tau$.

1.5. Notación. Sea i_1 algún elemento de $X = \{1, \ldots, n\}$ y σ una permutación de X definida por

$$\begin{aligned} \sigma(i_1) &= i_2, \\ \sigma(i_2) &= i_3, \\ &\vdots \\ \sigma(i_k) &= i_1, \end{aligned}$$

donde $i_1, \ldots, i_k$ son elementos distintos de X, y $\sigma(j) = j$ para $j \notin \{i_1, \ldots, i_k\}$. En este caso se dice que σ es una **permutación cíclica de orden** k y se escribe

$$\sigma = (i_1\ i_2\ \cdots\ i_k).$$

(Obviamente, los índices pueden ser *permutados cíclicamente*: $(i_1\ i_2\ \cdots\ i_k) = (i_2\ i_3\ \cdots\ i_k\ i_1) = (i_k\ i_1\ \cdots\ i_{k-1}) = \cdots$, pero normalmente en esta notación se empieza por el índice mínimo i_1.)

Por ejemplo, la formula (1) puede ser escrita como

$$(2\ 3) \circ (1\ 2) = (1\ 3\ 2) \quad \text{y} \quad (1\ 2) \circ (2\ 3) = (1\ 2\ 3). \tag{2}$$

La permutación identidad es un caso trivial de permutaciones cíclicas. Vamos a denotarla por $(\ )$.

1.6. Observación. *Si* $(i_1\ i_2\ \cdots\ i_k)$ *es una permutación cíclica, entonces*

$$(i_1\ i_2\ \cdots\ i_k)^{-1} = (i_k\ i_{k-1}\ \cdots i_1) = (i_1\ i_k\ i_{k-1}\ \cdots i_2).$$

Ejercicio I.3. *Todas las permutaciones en S_3 son cíclicas:*

$$S_3 = \{(\,),\ (1\,2),\ (1\,3),\ (2\,3),\ (1\,2\,3),\ (1\,3\,2)\}.$$

Escriba la tabla de composición de permutaciones:

$\circ$	$\cdots$	τ	$\cdots$
$\vdots$		$\vdots$	
σ	$\cdots$	$\sigma \circ \tau$	$\cdots$
$\vdots$		$\vdots$	

Ya hemos calculado (2):

$\circ$	$(\,)$	$(1\,2)$	$(1\,3)$	$(2\,3)$	$(1\,2\,3)$	$(1\,3\,2)$
$(\,)$	$(\,)$	$(1\,2)$	$(1\,3)$	$(2\,3)$	$(1\,2\,3)$	$(1\,3\,2)$
$(1\,2)$	$(1\,2)$			$(1\,2\,3)$		
$(1\,3)$	$(1\,3)$					
$(2\,3)$	$(2\,3)$	$(1\,3\,2)$				
$(1\,2\,3)$	$(1\,2\,3)$					
$(1\,3\,2)$	$(1\,3\,2)$					

Note que toda permutación cíclica puede ser escrita como un producto de permutaciones de orden 2 *que se llaman* ***transposiciones****:*

$$(i_1\ i_2\ \cdots\ i_k) = (i_1\ i_2) \circ (i_2\ i_3) \circ (i_3\ i_4) \cdots (i_{k-1}\ i_k).$$

Ejercicio I.4. *En general, no todas las permutaciones son cíclicas. Por ejemplo, en S_4 tenemos*

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = (1\,2) \circ (3\,4).$$

Demuestre que en general en S_n toda permutación puede ser representada como una composición de permutaciones cíclicas ***disjuntas*** *(sin repeticiones de índices). Por ejemplo, en S_4 tenemos las siguientes* 24 *permutaciones:*

$$\begin{gathered}
(\,), \\
(1\,2),\ (1\,3),\ (1\,4),\ (2\,3),\ (2\,4),\ (3\,4), \\
(1\,2\,3),\ (1\,2\,4),\ (1\,3\,2),\ (1\,3\,4),\ (1\,4\,2),\ (1\,4\,3),\ (2\,3\,4),\ (2\,4\,3), \\
(1\,2\,3\,4),\ (1\,2\,4\,3),\ (1\,3\,2\,4),\ (1\,3\,4\,2),\ (1\,4\,2\,3),\ (1\,4\,3\,2), \\
(1\,2) \circ (3\,4),\ (1\,3) \circ (2\,4),\ (1\,4) \circ (2\,3).
\end{gathered}$$

Note que las permutaciones cíclicas disjuntas ***conmutan*** *(su composición no depende del orden), por ejemplo* $(1\,2) \circ (3\,4) = (3\,4) \circ (1\,2)$.

Segundo día: Grupos

Los grupos son unos de los objetos más importantes en matemáticas. Estos apuntes no están dedicados a la teoría de grupos per se, pero vamos a ver algunas definiciones y ejemplos básicos, sin entrar en detalles (que harían parte de un curso separado).

2. Definición de grupo

Las propiedades de permutaciones de 1.3 motivan la siguiente

2.1. Definición. Un **grupo** G es un conjunto con operación

$$(x, y) \mapsto x \star y$$

que satisface las siguientes propiedades:

1) si $x, y \in G$, entonces $x \star y \in G$;
2) la operación $\star$ es **asociativa**:
$$x \star (y \star z) = (x \star y) \star z.$$
3) existe un elemento **neutro** $e \in G$ que satisface
$$e \star x = x \star e = x;$$
4) para todo $x \in G$ tenemos el elemento **inverso** x^{-1} tal que
$$x^{-1} \star x = x \star x^{-1} = e.$$

2.2. Definición. Si además para todo $x, y \in G$ se cumple

$$x \star y = y \star x,$$

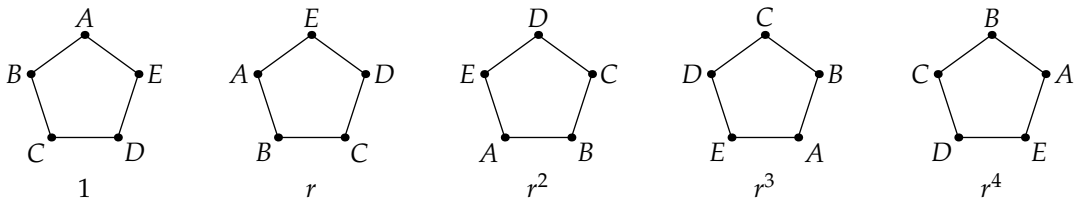
se dice que G es un grupo **abeliano**[*] o **conmutativo**.

2.3. Ejemplo.

1) El conjunto S_n de la sección precedente forma un grupo, conocido como el **grupo simétrico**. No es abeliano para $n \geq 3$.
2) Los números racionales $\mathbb{Q}$, reales $\mathbb{R}$, complejos $\mathbb{C}$, etc. forman grupos abelianos respecto la adición $+$ con elemento neutro 0. Los conjuntos $\mathbb{Q} \setminus \{0\}$, $\mathbb{R} \setminus \{0\}$, $\mathbb{C} \setminus \{0\}$ forman grupos abelianos respecto la multiplicación $\cdot$ con elemento neutro 1.

   (Estos ejemplos son muy especiales porque $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ forman estructuras más sofisticadas, **cuerpos**.)
3) El **grupo cíclico finito** C_n tiene varias encarnaciones. Por ejemplo, es el grupo de rotaciones del n-gono regular. Si r es la rotación por $360/n$ grados, este grupo tiene n elementos $1, r, \ldots, r^{n-1}$, que son las potencias de r (de allí viene el nombre "cíclico").

[*] Niels Henrik Abel (1802–1829), un matemático noruego.



Rotaciones del pentágono regular

Es la misma cosa que $\mathbb{Z}/n\mathbb{Z}$, el grupo de números enteros módulo n respecto la adición.

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

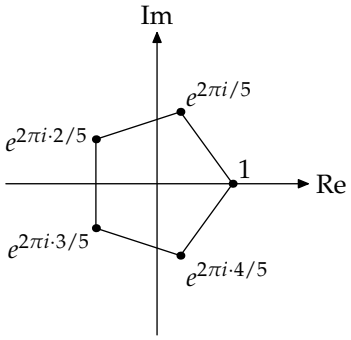
Adición módulo 5

(Los elementos de $\mathbb{Z}/n\mathbb{Z}$ no son números enteros $m \in \mathbb{Z}$, sino las clases de equivalencia $[m]$ respecto la relación "$m_1 \sim m_2 \iff m_1 - m_2$ es divisible por n", pero a veces los corchetes no se escriben.)
Los elementos de $\mathbb{Z}/n\mathbb{Z}$ son $1,\ 1+1,\ 1+1+1,\ \ldots,\ \underbrace{1+\cdots+1}_{n-1},\ \underbrace{1+\cdots+1}_{n} = 0$.

También el grupo cíclico es la misma cosa que las n-ésimas raíces de la unidad respecto la multiplicación en $\mathbb{C}^\times$:

$$\mu_n = \{e^{2\pi ik/n} \mid k = 0, \ldots, n-1\}.$$

Note que en el plano complejo las n-ésimas raíces de la unidad son vértices de un n-ágono regular.



Las raíces de la unidad de quinto grado en el plano complejo

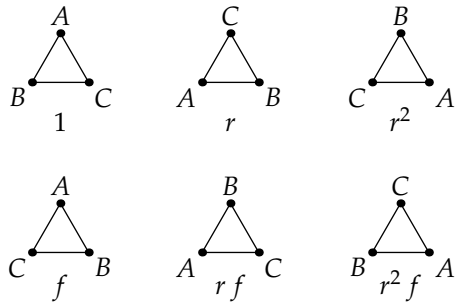
Note que aunque es esencialmente el mismo grupo, la operación en $\mathbb{Z}/n\mathbb{Z}$ es aditiva y la operación en μ_n es multiplicativa.

4) Los números enteros $\mathbb{Z}$ forman un grupo respecto la adición $+$. El elemento neutro es 0.
Todo elemento de $\mathbb{Z}$ es de la forma $\pm\underbrace{(1+\cdots+1)}_{n}$, y por esto $\mathbb{Z}$ recibe el nombre de **grupo cíclico infinito**.

5) μ_n está en un grupo infinito que es el **grupo del círculo**:

$$\mathbb{S}^1 := \{z \in \mathbb{C} \mid |z| = 1\}.$$

6) El **grupo diédrico** D_n es el grupo de rotaciones y reflexiones del n-gono regular. Se puede ver que D_n tiene $2n$ elementos. A saber, sea f una de las reflexiones y r la rotación por $360/n$ grados. Todo elemento de D_n es un producto de f y r, y tenemos relaciones $f^2 = 1$, $r^n = 1$, $frf = r^{-1}$ (reflexión seguida por una rotación y otra reflexión es rotación en el sentido contrario). D_n no es conmutativo para $n \geq 3$.



Las rotaciones y reflexiones del triángulo

Notemos que cuando $n = 3$, el grupo D_3 corresponde a las seis permutaciones de los vértices del triángulo. En este sentido, D_3 puede ser identificado con S_3.

▲

A partir de la definición se puede deducir varias propiedades e identidades básicas.

2.4. Observación. $(x \star y)^{-1} = y^{-1} \star x^{-1}$.

(Note el orden de elementos. Por ejemplo, para vestirse, primero se pone traje y luego abrigo; luego, primero se quita el abrigo y luego el traje :-)

Demostración.

$$\begin{aligned}(y^{-1} \star x^{-1}) \star (x \star y) &= y^{-1} \star (x^{-1} \star x) \star y \\ &= y^{-1} \star e \star y \\ &= y^{-1} \star y \\ &= e;\end{aligned}$$

$$\begin{aligned}(x \star y) \star (y^{-1} \star x^{-1}) &= x \star (y \star y^{-1}) \star x^{-1} \\ &= x \star e \star x^{-1} \\ &= x \star x^{-1} \\ &= e;\end{aligned}$$

■

2.5. Observación. *Tenemos la* ***ley de cancelación***

$$x \star y = x \star z \Rightarrow y = z$$

y

$$y \star x = z \star x \Rightarrow y = z.$$

Demostración. Por ejemplo, en el primer caso,

$$\begin{aligned} x \star y = x \star z &\Rightarrow x^{-1} \star (x \star y) = x^{-1} \star (x \star z) \\ &\Rightarrow (x^{-1} \star x) \star y = (x^{-1} \star x) \star z \\ &\Rightarrow e \star y = e \star z \\ &\Rightarrow y = z. \end{aligned}$$

■

2.6. Observación. *El elemento neutro $e \in G$ es único.*

Demostración. Si tenemos dos elementos neutros $e, e' \in G$, entonces

$$e = e \star e' = e'.$$

■

2.7. Observación. *Para todo $x \in G$ el elemento inverso $x^{-1} \in G$ es único.*

Demostración. Sean y, z dos elementos tales que

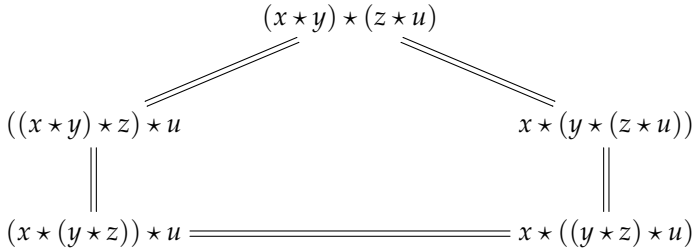
$$y \star x = x \star y = e, \quad z \star x = x \star z = e.$$

Entonces

$$y = y \star e = y \star (x \star z) = (y \star x) \star z = e \star z = z.$$

■

Ejercicio II.1. *Si la operación $\star$ es asociativa, es decir $(x \star y) \star z = x \star (y \star z)$, entonces en general, por inducción tenemos la "asociatividad generalizada": en cualquier expresión $x_1 \star \cdots \star x_n$ el resultado es el mismo para cualquier orden de operaciones (para cualquier modo de poner los paréntesis). Por ejemplo, para cuatro variables tenemos*



Ejercicio II.2 (Para los amantes de la combinatoria)**.** *Hay dos diferentes modos de poner los paréntesis en la expresión $x \star y \star z$:*

$$(x \star y) \star z, \ x \star (y \star z).$$

Para cuatro variables, hay 5 *opciones:*

$$(x\star y)\star(z\star u),\ ((x\star y)\star z)\star u,\ x\star(y\star(z\star u)),\ (x\star(y\star z))\star u,\ x\star((y\star z)\star u).$$

Para cinco variables, hay 14 *posibilidades*

$$\begin{gathered}(((x\star y)\star z)\star u)\star v,\ ((x\star(y\star z))\star u)\star v,\ ((x\star y)\star(z\star u))\star v,\\ (x\star((y\star z)\star u))\star v,\ (x\star(y\star(z\star u)))\star v,\ ((x\star y)\star z)\star(u\star v),\\ (x\star(y\star z))\star(u\star v),\ (x\star y)\star((z\star u)\star v),\ (x\star y)\star(z\star(u\star v)),\\ x\star(((y\star z)\star u)\star v),\ x\star((y\star(z\star u))\star v),\ x\star((y\star z)\star(u\star v)),\\ x\star(y\star((z\star u)\star v)),\ x\star(y\star(z\star(u\star v))).\end{gathered}$$

En general, para n variables, hay

$$C_n=\frac{1}{n+1}\binom{2n}{n}=\binom{2n}{n}-\binom{2n}{n+1}$$

posibilidades. Estos números se conocen como los ***números de Catalan*** *(OEIS A000108).*

n:	3	4	5	6	7	8	9	10	11	12	$\cdots$
C_n:	2	5	14	42	132	429	1430	4862	16796	58786	$\cdots$

2.8. Definición. Se dice que dos elementos $x, y \in G$ son **conjugados** (por z) si

$$y = z\star x\star z^{-1}$$

para algún $z \in G$.

2.9. Ejemplo. Si G es abeliano, tenemos $z\star x\star z^{-1} = x\star z\star z^{-1} = x$, así que todos los elementos de G son conjugados entre sí. ▲

2.10. Observación. *La relación "x está conjugado con y" es una relación de equivalencia.*

Demostración. La relación es reflexiva, ya que $x = e\star x\star e^{-1}$.
Es simétrica: si $y = z\star x\star z^{-1}$, entonces $x = z^{-1}\star y\star z$.
Por fin, si tenemos $x_2 = z_1\star x_1\star z_1^{-1}$ y $x_3 = z_2\star x_2\star z_2^{-1}$, entonces

$$x_3 = z_2\star(z_1\star x_1\star z_1^{-1})\star z_2^{-1} = (z_2\star z_1)\star x_1\star(z_1^{-1}\star z_2^{-1}) = (z_2\star z_1)\star x_1\star(z_2\star z_1)^{-1}.$$

■

Para todo x, su clase de equivalencia se llama la **clase de conjugación**:

$$\{z\star x\star z^{-1} \mid z\in G\}.$$

En general, $x \in G$ no tiene por qué estar conjugado con su inverso x^{-1}.

Ejercicio II.3. *Verifique que en S_3 hay tres diferentes clases de conjugación:*

$$\begin{gathered}(\ ),\\ (1\,2),\ (1\,3),\ (2\,3),\\ (1\,2\,3),\ (1\,3\,2).\end{gathered}$$

Ejercicio II.4. *Recordemos que en S_n toda permutación puede ser escrita como un producto de permutaciones cíclicas disjuntas. Se dice que dos permutaciones tienen el mismo* ***tipo de ciclo*** *si en sus descomposiciones las permutaciones cíclicas del mismo orden aparecen la misma cantidad de veces. Por ejemplo, los tipos de ciclo posibles en S_4 están representados por las siguientes permutaciones:*

$$(\,),\ (1\,2),\ (1\,2\,3),\ (1\,2\,3\,4),\ (1\,2)\circ(3\,4).$$

Demuestre que dos permutaciones son conjugadas en S_n si y solamente si tienen el mismo tipo de ciclo. Por ejemplo, en S_3 tenemos

$$(1\,2\,3) = (2\,3)\circ(1\,3\,2)\circ(2\,3)^{-1}.$$

Indicación:

- *Para ver que permutaciones conjugadas tienen el mismo tipo de ciclo, note que para todo $\sigma \in S_n$ se tiene*

$$\sigma \circ \begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix} \circ \sigma^{-1} = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(i_1) & \sigma(i_2) & \cdots & \sigma(i_n) \end{pmatrix},$$

  así que la conjugación por σ corresponde a una reenumeración de $\{1,\dots,n\}$ y por lo tanto no afecta el tipo cíclico.

- *Si dos permutaciones tienen el mismo tipo de ciclo, se puede considerar una biyección entre ciclos del mismo orden y para pares de ciclos correspondientes*

$$(i_0\ \cdots\ i_k) \leftrightarrow (j_1\ \cdots\ j_k)$$

  definir una permutación $\sigma\colon i_\ell \mapsto j_\ell$. Entonces la conjugación por σ identifica nuestras dos permutaciones.

3. Subgrupos y morfismos

3.1. Definición. Un **homomorfismo** de grupos $f\colon G \to H$ es una aplicación tal que

$$f(x \star y) = f(x) \star f(y) \quad \text{para todo } x, y \in G.$$

3.2. Ejemplo. La aplicación identidad $\mathrm{id}_G\colon G \to G$ es obviamente un homomorfismo. ▲

3.3. Ejemplo. La aplicación

$$\begin{aligned} \mathbb{Z} &\to \mathbb{Z}/n\mathbb{Z}, \\ x &\mapsto x \pmod n \end{aligned}$$

es un homomorfismo. ▲

Ejercicio II.5. *Sea $(i_1, i_2, \dots, i_n)$ una sucesión de números entre 1 y n sin repeticiones. Se dice que hay una* ***inversión*** *si $i_k > i_\ell$ para $k < \ell$. El* ***signo*** *de tal sucesión es entonces*

$$\operatorname{sgn}(i_1, i_2, \dots, i_n) := \begin{cases} +1, \text{ el número de inversiones es par,} \\ -1, \text{ el número de inversiones es impar.} \end{cases}$$

Para una permutación su signo es

$$\operatorname{sgn}\begin{pmatrix} i_1 & i_2 & \cdots & i_n \\ \sigma(i_1) & \sigma(i_2) & \cdots & \sigma(i_n) \end{pmatrix} := \operatorname{sgn}(i_1, i_2, \dots, i_n) \cdot \operatorname{sgn}(\sigma(i_1), \sigma(i_2), \dots, \sigma(i_n)). \tag{3}$$

(Normalmente para escribir una permutación, ponemos en la primera fila $(i_1, i_2, \dots, i_n) = (1, 2, \dots, n)$, donde no hay inversiones.) Por ejemplo, he aquí los signos de las permutaciones de tres elementos:

$$\begin{aligned}
\operatorname{sgn}(\ ) &= \operatorname{sgn}\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix} = +1\colon && \textit{no hay inversiones}\\
\operatorname{sgn}(1\ 2) &= \operatorname{sgn}\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix} = -1\colon && \textit{una inversión } 2>1\\
\operatorname{sgn}(1\ 3) &= \operatorname{sgn}\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix} = -1\colon && \textit{tres inversiones } 3>2,\ 3>1,\ 2>1\\
\operatorname{sgn}(2\ 3) &= \operatorname{sgn}\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix} = -1\colon && \textit{una inversión } 3>2\\
\operatorname{sgn}(1\ 2\ 3) &= \operatorname{sgn}\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} = +1\colon && \textit{dos inversiones } 2>1,\ 3>1\\
\operatorname{sgn}(1\ 3\ 2) &= \operatorname{sgn}\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix} = +1\colon && \textit{dos inversiones } 3>1,\ 3>2
\end{aligned}$$

1) *Si en una sucesión*
$$(i_1,\dots,i_k,\dots,i_\ell,\dots,i_n)$$
se intercambian dos números:
$$(i_1,\dots,i_\ell,\dots,i_k,\dots,i_n),$$
(es decir, se aplica una transposición), entonces el signo cambia al opuesto.

2) *Demuestre que la expresión (3) no depende de la representación particular de* $\sigma = \begin{pmatrix} i_1 & i_2 & \cdots & i_n \\ \sigma(i_1) & \sigma(i_2) & \cdots & \sigma(i_n)\end{pmatrix}$*:*
las permutaciones de columnas no afectan el signo.
(Indicación: toda permutación de columnas puede ser representada por una sucesión de transposiciones; el cambio del signo de la primera fila se recompensa por el cambio del signo de la segunda fila.)

3) *Demuestre que* $\operatorname{sgn}(\tau\circ\sigma) = \operatorname{sgn}\tau\cdot\operatorname{sgn}\sigma$*, es decir, el signo es un homomorfismo de grupos*
$$\operatorname{sgn}\colon S_n \to \{\pm 1\}.$$

4) *Demuestre que para una transposición* $(i_1\ i_2)$ *se tiene* $\operatorname{sgn}(i_1\ i_2) = -1$.

5) *Para una permutación cíclica se tiene*
$$\operatorname{sgn}(i_1\ i_2\ \cdots\ i_k) = (-1)^{k-1}.$$

6) *El signo de una permutación es la paridad del número de las transposiciones que aparecen en su descomposición. Por ejemplo,*
$$\operatorname{sgn}(1\ 2\ 3) = \operatorname{sgn}(1\ 2)\circ(2\ 3) = \operatorname{sgn}(1\ 2)\cdot\operatorname{sgn}(2\ 3) = (-1)\cdot(-1) = +1.$$

3.4. Observación. *Todo homomorfismo preserva la identidad:*
$$f(e_G) = e_H$$
y los elementos inversos:
$$f(x^{-1}) = f(x)^{-1}.$$

Demostración. En efecto, tenemos
$$f(e_G) = f(e_G\star e_G) = f(e_G)\star f(e_G),$$

y entonces $f(e_G) = e_H$ por cancelación. Luego, para $x \in G$ tenemos

$$f(x) \star f(x^{-1}) = f(x \star x^{-1}) = f(e_G) = e_H$$

y

$$f(x^{-1}) \star f(x) = f(x^{-1} \star x) = f(e_G) = e_H.$$

■

La palabra "homomorfismo" viene de las raíces griegas ὁμός, "mismo" y μορφή, "forma". A veces se dice simplemente "morfismo". También es útil conocer otras raíces griegas: mono-, epi-, iso-.

3.5. "Definición". Un homomorfismo de grupos $f\colon G \to H$

- es un **monomorfismo** si y solamente si es **inyectivo** ($f(x) = f(y)$ si y solamente si $x = y$);
- es un **epimorfismo** si y solamente si es **sobreyectivo** (para todo $y \in H$ existe $x \in G$ tal que $f(x) = y$);
- es un **isomorfismo** si y solamente si es **biyectivo** (inyectivo y sobreyectivo).

En particular, un isomorfismo de grupos es la misma cosa que un mono- y epimorfismo al mismo tiempo. Cuando entre G y H existe un isomorfismo, se escribe $G \cong H$.

(He puesto "definición" entre comillas y he escrito las palabras "si y solamente si" porque en realidad, las definiciones correctas de mono-, epi-, iso- son diferentes, pero en el caso de grupos son equivalentes a las de arriba.)

3.6. Ejemplo. Entre el grupo aditivo $(\mathbb{R}, +)$ y el grupo multiplicativo $(\mathbb{R}_{>0}, \cdot)$ hay un isomorfismo definido por la función exponencial $\exp\colon \mathbb{R} \to \mathbb{R}_{>0}$ y el logaritmo $\log\colon \mathbb{R}_{>0} \to \mathbb{R}$.

$$e^{x+y} = e^x \cdot e^y, \quad \log(x \cdot y) = \log x \cdot \log y, \quad \log e^x = x, \quad e^{\log x} = x.$$

▲

3.7. Ejemplo. Una biyección entre conjuntos $X \cong Y$ induce un isomorfismo $\mathrm{Sym}(X) \cong \mathrm{Sym}(Y)$. ▲

3.8. Definición. Si G es un grupo, entonces $H \subset G$ es un **subgrupo** si $e \in H$ y para todo $x, y \in H$ también $x^{-1} \in H$ y $x \star y \in H$. En otras palabras, H es un subconjunto que es un grupo respecto a la misma operación.

Ejercicio II.6. *Si $H_1 \subset G$ y $H_2 \subset G$ son subgrupos de G, entonces $H_1 \cap H_2$ es también un subgrupo. Note que $H_1 \cup H_2$ no tiene por qué ser un subgrupo (por ejemplo, para $\mu_n \subset \mathbb{S}^1$ y $\mu_m \subset \mathbb{S}^1$ analice $\mu_n \cap \mu_m$ y $\mu_n \cup \mu_m$).*

3.9. Ejemplo. Como hemos notado en 2.3, μ_n es un subgrupo de $\mathbb{S}^1$. ▲

3.10. Ejemplo. La inclusión $\{1, \dots, n-1\} \hookrightarrow \{1, \dots, n\}$ induce una inclusión de subgrupos $S_{n-1} \subset S_n$. ▲

3.11. Ejemplo. Para un elemento fijo $x \in G$ el **subgrupo cíclico generado por** x es

$$\langle x \rangle := \{x^n \mid n \in \mathbb{Z}\},$$

donde

$$x^n := \begin{cases} \underbrace{x \star \cdots \star x}_{n}, & n > 0, \\ e, & n = 0, \\ (\underbrace{x \star \cdots \star x}_{n})^{-1}, & n < 0. \end{cases}$$

Este grupo puede ser o bien infinito (cuando G es infinito), y en este caso es isomorfo a $\mathbb{Z}$; o bien finito, y en este caso es isomorfo a C_n. El isomorfismo es dado por

$$x^n \mapsto n.$$

▲

En breve vamos a ver que todo grupo finito es isomorfo a un subgrupo de S_n para algún n.

Ejercicio II.7. *Determine todos los subgrupos de S_3.*

3.12. Observación. *Sea $f\colon G \to H$ un homomorfismo de grupos. Entonces su **imagen***

$$\operatorname{im} f := \{f(x) \mid x \in G\} \subseteq H$$

es un subgrupo de H.

Demostración. Primero, $e_H = f(e_G) \in \operatorname{im} f$. Luego, si $f(x), f(y) \in \operatorname{im} f$, entonces $f(x) \star f(y) = f(x \star y) \in \operatorname{im} f$. Si $f(x) \in \operatorname{im} f$, entonces $f(x)^{-1} = f(x^{-1}) \in \operatorname{im} f$. ■

3.13. Observación. *Si $f\colon G \to H$ es un monomorfismo, entonces*

$$G \cong \operatorname{im} f.$$

Demostración. f es inyectivo por nuestra hipótesis, y la aplicación correspondiente $G \to \operatorname{im} f$ es sobreyectiva por la definición de $\operatorname{im} f$. ■

3.14. Teorema (Cayley). *Todo grupo finito de n elementos es isomorfo a un subgrupo de S_n.*

Demostración. Para todo elemento fijo $x \in G$ podemos considerar la siguiente aplicación:

$$\begin{aligned} \phi_x\colon G &\to G, \\ z &\mapsto x \star z. \end{aligned}$$

ϕ_x no es un homomorfismo, pero es una biyección (es decir, una permutación de los elementos de G). En efecto, notemos que

$$\phi_{x\star y}(z) = (x \star y) \star z = x \star (y \star z) = \phi_x(\phi_y(z)) = (\phi_x \circ \phi_y)(z).$$

Esto implica que la aplicación inversa para ϕ_x es $\phi_{x^{-1}}$ y que tenemos un homomorfismo de grupos

$$\begin{aligned} \phi\colon G &\to \operatorname{Sym}(G), \\ x &\mapsto \phi_x. \end{aligned}$$

Este homomorfismo es visiblemente inyectivo: si $x \neq y$, entonces $\phi_x \neq \phi_y$ (por ejemplo, $x = \phi_x(e) \neq \phi_y(e) = y$). Se concluye que

$$G \cong \operatorname{im} \phi \subset \operatorname{Sym}(G) \cong S_n.$$

■

Los fundadores de la teoría de grupos estudiaban solamente los grupos de permutación finitos S_n y sus subgrupos. En efecto, el término "grupo" viene del "grupo de permutaciones".

Ejercicio II.8. *Analice el teorema de arriba en el caso $G = C_3$. ¿Cuál subgrupo de S_3 es isomorfo a G?*

Tercer y cuarto día: Álgebra lineal

Aunque un típico curso malo de álgebra lineal de primer semestre se dedica al cálculo de determinantes de matrices de 5×5 y otras cosas inútiles y fastidiosas, en realidad álgebra lineal estudia **espacios vectoriales** y **aplicaciones lineales** entre ellos.

A partir de ahora k denota un **cuerpo**. El lector que todavía no conoce esta noción puede pensar en $k = \mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, etcétera.

4. Espacios vectoriales

4.1. Definición. Un **espacio vectorial** sobre k es un conjunto V junto con dos operaciones: la adición de vectores

$$\begin{aligned} +\colon V \times V &\to V, \\ (u, v) &\mapsto u + v, \end{aligned}$$

y la multiplicación de vectores por los elementos de k:

$$\begin{aligned} k \times V &\to V, \\ (\lambda, v) &\mapsto \lambda \cdot v. \end{aligned}$$

Se piden los siguientes axiomas:

1) V es un grupo abeliano respecto a la adición $+$. Esto quiere decir que la adición es conmutativa ($u + v = v + u$), asociativa ($u + (v + w) = (u + v) + w$), posee el elemento neutro $0 \in V$ (el vector nulo) tal que $0 + v = v + 0 = v$, y para todo vector $v \in V$ existe el vector opuesto $-v$ tal que $v + (-v) = (-v) + v = 0$.

2) Para cualesquiera $\lambda \in k$ y $u, v \in V$ se tiene

$$\lambda \cdot (u + v) = \lambda \cdot u + \lambda \cdot v.$$

3) Para cualesquiera $\lambda, \mu \in k$ y $u \in V$ se tiene

$$(\lambda\mu) \cdot u = \lambda \cdot (\mu \cdot u).$$

4) Para cualesquiera $\lambda, \mu \in k$ y $u \in V$ se tiene

$$(\lambda + \mu) \cdot u = \lambda \cdot u + \mu \cdot u.$$

5) Para todo $u \in V$ se tiene

$$1 \cdot u = u.$$

Los elementos de V se llaman **vectores** y los elementos de k a veces se llaman **escalares**.

4.2. Ejemplo. $\mathbb{R}^n$ es un espacio vectorial sobre $\mathbb{R}$, con la adición de vectores y multiplicación por escalares habitual. En general, para cualquier k se tiene un espacio vectorial

$$k^n := \{(x_1, \ldots, x_n) \mid x_i \in k\},$$

con adición

$$(x_1, \ldots, x_n) + (y_1, \ldots, y_n) := (x_1 + y_1, \ldots, x_n + y_n)$$

y multiplicación escalar

$$\lambda \cdot (x_1, \ldots, x_n) := (\lambda\, x_1, \ldots, \lambda\, x_n).$$

▲

4.3. Ejemplo. Es fácil verificar que $\mathbb{C}$ es un espacio vectorial sobre $\mathbb{R}$ y $\mathbb{R}$ es un espacio vectorial sobre $\mathbb{Q}$ respecto la adición y multiplicación habitual. ▲

Las siguientes propiedades se siguen de los axiomas:

4.4. Observación. *Sea V un espacio vectorial.*

1) $\lambda \cdot 0 = 0$ *para todo* $\lambda \in k$ *y el vector nulo* $0 \in V$.
2) $0 \cdot v = 0$ *para todo* $v \in V$ *(la notación es un poco ambigua: aquí a la izquierda tenemos el escalar nulo y a la derecha el vector nulo).*
3) $\lambda \cdot (-v) = -(\lambda \cdot v)$ *para todo* $\lambda \in k$, $v \in V$.
4) $\lambda \cdot (u - v) = \lambda \cdot u - \lambda \cdot v$ *para todo* $\lambda \in k$, $u, v \in V$.
5) $(-1) \cdot v = -v$ *para todo* $v \in V$.
6) $(\lambda - \mu) \cdot v = \lambda \cdot v - \mu \cdot v$ *para todo* $\lambda, \mu \in k$, $v \in V$.

Demostración.

1) Tenemos $\lambda \cdot 0 = \lambda \cdot (0 + 0) = \lambda \cdot 0 + \lambda \cdot 0$, y por cancelación se concluye que $\lambda \cdot 0 = 0$.
2) De modo similar, $0 \cdot v = (0 + 0) \cdot v = 0 \cdot v + 0 \cdot v$, y por lo tanto $0 \cdot v = 0$.
3) Notamos que $\lambda \cdot v + \lambda \cdot (-v) = \lambda \cdot (v - v) = \lambda \cdot 0 = 0$.
4) Sigue de 3): $\lambda \cdot (u - v) = \lambda \cdot (u + (-v)) = \lambda \cdot u + \lambda \cdot (-v) = \lambda \cdot u - \lambda \cdot v$.
5) Tenemos $v + (-1) \cdot v = 1 \cdot v + (-1) \cdot v = (1 - 1) \cdot v = 0 \cdot v = 0$.
6) $(\lambda - \mu) \cdot v = (\lambda + (-1) \cdot \mu) \cdot v = \lambda \cdot v + (-1) \cdot (\mu \cdot v) = \lambda \cdot v - \mu \cdot v$.

■

4.5. Definición. Sea V un espacio vectorial. Se dice que $U \subseteq V$ es su **subespacio** si

1) U es un subgrupo de V respecto la adición de vectores ($0 \in U$, $u + v \in V$ para todo $u, v \in V$, $-v \in U$ para todo $v \in V$)
2) $\lambda \cdot v \in U$ para todo $v \in U$ y $\lambda \in k$ (note que esta condición in particular implica $-v = (-1) \cdot v \in U$ para todo $v \in U$).

4.6. Ejemplo. V siempre tiene dos subespacios triviales: todo V y el subespacio 0 formado por el vector nulo. ▲

4.7. Ejemplo. En $\mathbb{R}^3$ los vectores paralelos a una recta o plano fijo forma un subespacio vectorial. ▲

Ejercicio III.1. *Si $U \subset V$ y $W \subset V$ son dos subespacios en V, entonces $U \cap W$ es también un subespacio.*

5. Bases y dimensión

5.1. Definición. Una expresión de la forma

$$u = \lambda_1 \cdot v_1 + \cdots + \lambda_n \cdot v_n$$

para $u, v_1, \ldots, v_n \in V$, $\lambda \in k$ se llama una **combinación lineal**. Se dice que **no es trivial** si $(\lambda_1, \ldots, \lambda_n) \neq (0, \ldots, 0)$.

Se dice que los vectores $v_1, \ldots, v_n$ son **linealmente dependientes** si existe alguna combinación no trivial

$$0 = \lambda_1 \cdot v_1 + \cdots + \lambda_n \cdot v_n;$$

cuando ninguna combinación no trivial de $v_1, \ldots, v_n$ es nula, se dice que $v_1, \ldots, v_n$ son **linealmente independientes**.

5.2. Ejemplo. Dos vectores en $\mathbb{R}^2$ son linealmente dependientes si y solamente si son colineales. Tres vectores en $\mathbb{R}^3$ son linealmente dependientes si y solamente si son coplanares. ▲

Ejercicio III.2. *Sea X un conjunto de vectores de V. Entonces todas las combinaciones lineales de elementos de X:*

$$\langle X \rangle := \{\textit{sumas (finitas)} \sum_{v \in X} \lambda_v \cdot v\}$$

*forman un subespacio $\langle X \rangle \subset V$, que es el subespacio mínimo que contiene a todos los vectores de X. Este subespacio se llama la **envolvente lineal** de X. También se dice que V es **generado** por X.*

5.3. Definición. Se dice que V es un espacio **de dimensión finita** si $V = \langle X \rangle$ para un conjunto finito X.

5.4. Observación.

1) *Los vectores $v_1, \ldots, v_n$ (para $n > 1$) son linealmente dependientes si y solamente si alguno de ellos puede ser expresado como una combinación lineal de los otros.*

2) *Sean $v_1, \ldots, v_n$ vectores linealmente independientes. Entonces $v_1, \ldots, v_n, u$ son linealmente dependientes si y solamente si u puede ser expresado como una combinación lineal de $v_1, \ldots, v_n$.*

3) *Si u es una combinación lineal de $v_1, \ldots, v_n$:*

$$u = \lambda_1 \cdot v_1 + \cdots + \lambda_n \cdot v_n,$$

entonces esta expresión es única si y solamente si $v_1, \ldots, v_n$ son linealmente independientes.

Demostración. En la parte 1) En una dirección, si tenemos

$$v_1 = \lambda_2 \cdot v_2 + \cdots + \lambda_n \cdot v_n,$$

entonces

$$v_1 - \lambda_2 \cdot v_2 - \cdots - \lambda_n \cdot v_n = 0.$$

En la otra dirección, si tenemos una combinación lineal no trivial

$$0 = \lambda_1 \cdot v_1 + \cdots + \lambda_n \cdot v_n,$$

sin pérdida de generalidad, $\lambda_1 \neq 0$, y luego

$$v_1 = -\frac{\lambda_2}{\lambda_1} \cdot v_2 - \cdots - \frac{\lambda_n}{\lambda_1} \cdot v_n.$$

En la parte 2), si u es una combinación lineal de $v_1, \ldots, v_n$, entonces $v_1, \ldots, v_n, u$ son linealmente dependientes como acabamos de ver. En la otra dirección, si tenemos

$$0 = \lambda_1 \cdot v_1 + \cdots + \lambda_n \cdot v_n + \mu \cdot u,$$

donde $(\lambda_1, \ldots, \lambda_n, \mu) \neq (0, \ldots, 0, 0)$, entonces $\mu \neq 0$ (en el caso contrario, $v_1, \ldots, v_n$ serían linealmente dependientes) y podemos escribir

$$u = -\frac{\lambda_1}{\mu} \cdot v_1 - \cdots - \frac{\lambda_n}{\mu} \cdot v_n.$$

En la parte 3), notamos que si u posee dos expresiones lineales

$$u = \lambda_1 \cdot v_1 + \cdots + \lambda_n \cdot v_n = \lambda'_1 \cdot v_1 + \cdots + \lambda'_n \cdot v_n,$$

entonces $v_1, \ldots, v_n$ son linealmente dependientes:

$$0 = (\lambda_1 - \lambda'_1) \cdot v_1 + \cdots + (\lambda_n - \lambda'_n) \cdot v_n.$$

En la otra dirección, si tenemos una dependencia lineal entre $v_1, \ldots, v_n$:

$$0 = \mu_1 \cdot v_1 + \cdots + \mu_n \cdot v_n,$$

entonces podemos escribir

$$u = (\lambda_1 + \mu_1) \cdot v_1 + \cdots + (\lambda_n + \mu_n) \cdot v_n.$$

■

5.5. Definición. Una **base** de V es una colección de vectores linealmente independientes X tal que $V = \langle X \rangle$.

5.6. Ejemplo. En $\mathbb{R}^2$ dos vectores no colineales forman una base. En $\mathbb{R}^3$ tres vectores no coplanares forman una base. ▲

5.7. Ejemplo. Todo número complejo puede ser representado de modo único como $z = x + i\,y$ donde $x, y \in \mathbb{R}$, y se tiene

$$(x_1 + i\,y_1) + (x_2 + i\,y_2) = (x_1 + x_2) + i\,(y_1 + y_2), \quad \lambda\,(x + i\,y) = (\lambda\,x) + i\,(\lambda\,y).$$

$\mathbb{R}$ como un espacio vectorial sobre $\mathbb{Q}$ no posee una base finita. Su base infinita se conoce como **base de Hamel** y su existencia no puede ser justificada sin el **axioma de la elección** (estas cosas se estudian detalladamente en el curso de lógica; son un mal necesario para demostrar muchos resultados en álgebra). ▲

5.8. Ejemplo. Los espacios vectoriales como $\mathbb{R}^n$ o k^n en general poseen una **base** especial: tenemos los vectores

$$e_1 := (1, 0, \ldots, 0),\ e_2 := (0, 1, 0, \ldots, 0),\ \ldots,\ e_n := (0, 0, \ldots, 0, 1)$$

tales que todo vector de k^n se expresa como una combinación lineal de $e_1, \ldots, e_n$. En un espacio vectorial abstracto no hay ninguna base preferida. ▲

5.9. Proposición.

1) Todo espacio vectorial de dimensión finita posee una base. Específicamente, si X es un conjunto finito tal que $V = \langle X \rangle$, entonces se pueden escoger algunos elementos de X que forman una base.

2) *Si V es un espacio vectorial de dimensión finita, toda base de V tiene el mismo número de vectores, que se llama la* ***dimensión de*** *V y se denota por* $\dim V$.

Demostración. En 1), si $V = \langle X \rangle$ y X no es una base, esto significa precisamente que algún elemento $v \in X$ puede ser expresado como una combinación lineal de los otros. Podemos quitarlo entonces y considerar $X \setminus \{v\}$, etcétera. Así quitando uno por uno los vectores redundantes, eventualmente se termina con un conjunto linealmente independiente, que es una base.

En 2), supongamos que hay dos bases

$$(v_1, \ldots, v_n) \quad \text{y} \quad (u_1, \ldots, u_m).$$

Sin pérdida de generalidad, $m \geq n$. Podemos expresar los vectores u_i como combinaciones lineales de los v_i:

$$\begin{aligned} u_1 &= \mu_{11} \cdot v_1 + \mu_{12} \cdot v_2 + \cdots + \mu_{1n} \cdot v_n, \\ u_2 &= \mu_{21} \cdot v_1 + \mu_{22} \cdot v_2 + \cdots + \mu_{2n} \cdot v_n, \\ &\vdots \\ u_m &= \mu_{m1} \cdot v_1 + \mu_{m2} \cdot v_2 + \cdots + \mu_{mn} \cdot v_n. \end{aligned}$$

Luego, una combinación lineal de los u_i puede ser escrita como

$$\begin{aligned} \lambda_1 u_1 + \lambda_2 u_2 + \cdots + \lambda_m u_m = {} & (\lambda_1 \mu_{11} + \lambda_2 \mu_{21} + \cdots + \lambda_m \mu_{m1}) \cdot v_1 + \\ & (\lambda_1 \mu_{12} + \lambda_2 \mu_{22} + \cdots + \lambda_m \mu_{m2}) \cdot v_2 + \\ & \cdots + \\ & (\lambda_1 \mu_{1n} + \lambda_2 \mu_{2n} + \cdots + \lambda_m \mu_{mn}) \cdot v_n. \end{aligned}$$

Ahora si $m > n$, entonces el sistema de ecuaciones lineales

$$\left\{ \begin{array}{rcl} \lambda_1 \mu_{11} + \lambda_2 \mu_{21} + \cdots + \lambda_m \mu_{m1} &=& 0, \\ \lambda_1 \mu_{12} + \lambda_2 \mu_{22} + \cdots + \lambda_m \mu_{m2} &=& 0, \\ & \vdots & \\ \lambda_1 \mu_{1n} + \lambda_2 \mu_{2n} + \cdots + \lambda_m \mu_{mn} &=& 0 \end{array} \right.$$

tiene una solución no trivial $(\lambda_1, \ldots, \lambda_m) \neq (0, \ldots, 0)$. Pero tal solución nos daría una dependencia lineal

$$\lambda_1 u_1 + \lambda_2 u_2 + \cdots + \lambda_m u_m = 0,$$

que es imposible ya que u_i forman una base. Entonces $m = n$. ■

5.10. Definición. Una **aplicación lineal** entre espacios vectoriales

$$f \colon U \to V$$

es una aplicación que satisface

$$f(u + v) = f(u) + f(v), \quad f(\lambda \cdot v) = \lambda \cdot f(v)$$

para cualesquierq $u, v \in V$, $\lambda \in k$.

Recordemos que una **matriz** es un modo de especificar una aplicación lineal $f\colon k^n \to k^m$. A saber, es una tabla A de $m \times n$ (a saber, m filas y n columnas) donde a_{ij} es la i-ésima coordenada de $f(e_j)$.

Ejercicio III.3. *Comprobar que la multiplicación de matrices corresponde a la composición de aplicaciones lineales. La matriz identidad corresponde a la aplicación identidad.*

5.11. Definición. Una aplicación lineal $f\colon U \to V$ se llama **invertible** si existe una aplicación lineal $f^{-1}\colon V \to U$ tal que $f^{-1} \circ f = \mathrm{id}_U$ y $f \circ f^{-1} = \mathrm{id}_V$. También se dice que f es un **isomorfismo** de espacios vectoriales y se escribe $U \cong V$.

Para matrices, recordemos que una matriz A de $n \times n$ es **invertible** si existe A^{-1} tal que $A \cdot A^{-1} = A^{-1} \cdot A = \mathrm{Id}$.

Ejercicio III.4. *Una aplicación lineal $f\colon U \to V$ es invertible si y solamente si es biyectiva.*

5.12. Observación. *Todo espacio vectorial que posee una base finita de n vectores es isomorfo a k^n. Es decir, si $\dim V = n$, entonces hay un isomorfismo $V \cong k^n$ (que no es canónico y depende de la elección de la base).*

Demostración. Si $e_1, \dots, e_n$ es una base, todo vector de V es de la forma

$$\lambda_1 e_1 + \cdots + \lambda_n e_n,$$

y la aplicación

$$\begin{aligned} f\colon V &\to k^n, \\ \lambda_1 e_1 + \cdots + \lambda_n e_n &\mapsto (\lambda_1, \dots, \lambda_n) \end{aligned}$$

es lineal y biyectiva. ■

5.13. Ejemplo. $\mathbb{C}$ es isomorfo a $\mathbb{R}^2$ como un espacio vectorial sobre $\mathbb{R}$. ▲

5.14. Definición. Para un espacio vectorial V, el **grupo lineal general** $\mathrm{GL}(V)$ es el grupo de aplicaciones lineales invertibles $V \to V$ respecto la composición.

Para matrices, el grupo $\mathrm{GL}_n(k)$ es el grupo de matrices invertibles de $n \times n$ con elementos en k.

5.15. Ejemplo. $\mathrm{GL}_1(k) \cong k^\times := k \setminus \{0\}$. ▲

Todo espacio vectorial V de dimensión n es isomorfo a k^n, y las aplicaciones lineales (invertibles) $k^n \to k^n$ son precisamente las matrices (invertibles) de $n \times n$. Esto nos da un isomorfismo de grupos (no canónico)

$$\mathrm{GL}(V) \cong \mathrm{GL}_n(k).$$

Recordemos que el grupo $\mathrm{GL}(V)$ no es abeliano. Para matrices esto significa que en general $A \cdot B \neq B \cdot A$.

Ejercicio III.5. *Encontrar dos aplicaciones lineales (o matrices) que no conmutan.*

El grupo de aplicaciones lineales invertibles $\mathrm{GL}(V)$ es un análogo lineal del grupo de permutaciones $\mathrm{Sym}(X)$.

En la última lección vamos a necesitar otra definición de álgebra lineal: la **traza**. Recordemos que la traza de una matriz es la suma de sus coeficientes diagonales:

$$\mathrm{tr} \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix} := a_{11} + a_{22} + \cdots + a_{nn}.$$

Ejercicio III.6. $\mathrm{tr}(A \cdot B) = \mathrm{tr}(B \cdot A)$.

Ahora si $f\colon V \to V$ es una aplicación lineal, podemos escoger una base de V y considerar la matriz correspondiente A. Diferentes bases dan diferentes matrices, y en otra base la matriz tiene la forma TAT^{-1}, donde T es alguna matriz invertible (el cambio de base). Ya que

$$\mathrm{tr}(TAT^{-1}) = \mathrm{tr}(AT^{-1}T) = \mathrm{tr}(A \cdot \mathrm{Id}) = \mathrm{tr}(A),$$

la traza no depende de una base particular y no es un invariante de matrices, sino de aplicaciones lineales. (En efecto, hay otra definición de la traza, más correcta, pero no tengo tiempo para entrar en detalles.)

Quinto día: Representaciones

Una representación de un grupo G sobre un espacio vectorial V es un modo de asociar a los elementos de G transformaciones lineales invertibles $V \to V$. Por lo menos cuando se trabaja con los espacios sobre $\mathbb{C}$, hay una teoría elegante que clasifica todas las representaciones de un grupo finito fijo.

6. Representaciones de grupos

6.1. Definición. Sea G un grupo y V un espacio vectorial. Una **representación** de G es un homomorfismo

$$\phi\colon G \to \mathrm{GL}(V).$$

Para nosotros, la dimensión de V siempre va a ser finita. También se dice que $\dim V$ es el **grado** de la representación ($\deg \phi$). La definición significa que para todo elemento $x \in G$ se especifica una aplicación lineal invertible

$$\phi_x\colon V \to V,$$

de manera compatible con la multiplicación en G:

$$\phi_{x\star y} = \phi_x \circ \phi_y.$$

Cuando $V = k^n$, vamos a usar la identificación $\mathrm{GL}(k^n) \cong \mathrm{GL}_n(k)$. En este caso, a todo elemento de G se asocia una matriz de $n \times n$, de tal modo que la multiplicación en G corresponde a la multiplicación de matrices.

6.2. Ejemplo. Todo grupo posee una representación trivial de grado 1 definida por

$$\begin{aligned} \phi\colon G &\to \mathbb{C}^\times, \\ x &\mapsto 1. \end{aligned}$$

▲

6.3. Ejemplo. Para el grupo $\mathbb{Z}/n\mathbb{Z}$ tenemos la siguiente representación (que es simplemente la visualización del grupo cíclico como el grupo de las raíces n-ésimas de la unidad):

$$\begin{aligned} \phi\colon \mathbb{Z}/n\mathbb{Z} &\to \mathbb{C}^\times, \\ m \pmod n &\mapsto e^{2\pi i m/n}. \end{aligned}$$

▲

6.4. Ejemplo (Representación estándar de S_n). El grupo simétrico S_n tiene la representación estándar $\phi\colon S_n \to \mathrm{GL}_n(\mathbb{C})$ que simplemente permuta los vectores de la base:

$$\phi_\sigma(e_i) := e_{\sigma(i)}.$$

En términos de matrices, ϕ_σ es la matriz identidad con sus filas permutadas por σ:

$$\phi_{(1\ 2)} = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \phi_{(1\ 2\ 3)} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

▲

Ejercicio V.1. *Completar la descripción de* $S_3 \to \mathrm{GL}_3(\mathbb{C})$.

Notemos que en el último ejemplo, $\phi\colon S_n \to \mathrm{GL}_n(\mathbb{C})$ es un monomorfismo: diferentes elementos de S_n nos dan diferentes aplicaciones lineales $\phi_n\colon \mathbb{C}^n \to \mathbb{C}^n$. Esto significa que hemos realizado (representado) S_n como un subgrupo de $\mathrm{GL}_n(\mathbb{C})$.

6.5. Definición. Si $\phi\colon G \to \mathrm{GL}(V)$ es un monomorfismo, se dice que la representación es **fiel**.

El teorema de Cayley nos dice que para todo grupo finito G hay un monomorfismo $G \to S_n$ (donde $n = |G|$). Considerando la composición con la representación estándar de S_n:

$$G \to S_n \to \mathrm{GL}_n(k)$$

se obtiene la siguiente

6.6. Observación. *Todo grupo finito posee una representación fiel. Es decir, todo grupo puede ser visto como un subgrupo de aplicaciones lineales (o matrices).*

Podemos revisar la demostración del teorema de Cayley para describir explícitamente la representación fiel de arriba:

6.7. Ejemplo (Representación regular). Sea $V \cong \mathbb{C}^n$ el espacio vectorial generado por los elementos de G; es decir, equipado con una base e_z para $z \in G$. Para $x \in G$ sea $\rho_x\colon V \to V$ la aplicación definida por

$$e_z \mapsto e_{x\star z}.$$

Es invertible, su aplicación inversa siendo $\rho_{x^{-1}}$, y $x \mapsto \rho_x$ define un monomomorfismo de grupos $G \to \mathrm{GL}(V)$ (diferentes $x \in G$ dan diferentes aplicaciones ρ_x).

Toda aplicación ρ_x permuta los vectores de la base $\{e_z\}$, y en esta base puede ser representada como una **matriz de permutación** (donde todos los coeficientes son nulos, excepto un coeficiente $= 1$ en cada fila y cada columna).

Esta representación se llama la **representación regular** de G y tiene rol muy importante. ▲

Ejercicio V.2. *Describir explícitamente la representación regular* $\mathbb{Z}/3\mathbb{Z} \to \mathrm{GL}_3(\mathbb{C})$.

Otro fenomeno curioso que se ve en el ejemplo con la representación estándar de S_n: para toda permutación σ se tiene

$$e_{\sigma(1)} + e_{\sigma(2)} + \cdots + e_{\sigma(n)} = e_1 + e_2 + \cdots + e_n,$$

y entonces el subespacio de $\mathbb{C}^n$ generado por el vector $e_1 + e_2 + \cdots + e_n$ se queda fijo bajo la acción de S_n.

6.8. Definición. Para una representación $\phi\colon G \to \mathrm{GL}(V)$ se dice que $U \subset V$ es un **subespacio G-invariante** si para todo $x \in G$ y $u \in U$ se tiene $\phi_x(u) \in U$.

6.9. Ejemplo. Siempre hay dos subespacios G-invariantes triviales: todo V y el subespacio nulo 0. ▲

Si $U \subset V$ es un subespacio G-invariante para una representación $\phi\colon G \to \mathrm{GL}(V)$, entonces se puede considerar la "restricción" $\phi|_U : G \to \mathrm{GL}(U)$.

6.10. Definición. Se dice que una representación $G \to \mathrm{GL}(V)$ es **irreducible**[*] si V no tiene subespacios G-invariantes no triviales.

6.11. Ejemplo. Toda representación $G \to \mathbb{C}^\times$ de grado 1 es irreducible, ya que $\mathbb{C}$ no tiene subespacios no triviales. ▲

Nuestro objetivo es ver que todas las representaciones en algún sentido se construyen a partir de representaciones irreducibles.

[*]El diccionario de la RAE ofrece dos variantes: "irreducible" e "irreductible"

7. Isomorfismos y sumas directas de representaciones

Normalmente, los espacios vectoriales nos interesan módulo isomorfismo, y nos gustaría identificar representaciones sobre espacios isomorfos. El isomorfismo de espacios en este caso tiene que ser compatible con las representaciones:

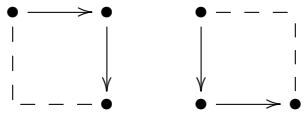
7.1. Definición. Sean $\phi\colon G \to \mathrm{GL}(U)$ y $\psi\colon G \to \mathrm{GL}(V)$ dos representaciones de G. Se dice que son **isomorfas** (o **equivalentes**) si existe un isomorfismo de espacios vectoriales $f\colon U \xrightarrow{\cong} V$ tal que para todo $x \in G$ se tiene

$$f \circ \phi_x = \psi_x \circ f.$$

Ya que f es invertible, la condición de arriba puede ser escrita como $\phi_x = f^{-1} \circ \psi_x \circ f$. También se puede dibujar un diagrama

$$\begin{array}{ccc} U & \xrightarrow{\phi_x} & U \\ {\scriptstyle f}\downarrow{\scriptstyle \cong} & & {\scriptstyle \cong}\downarrow{\scriptstyle f} \\ V & \xrightarrow[\psi_x]{} & V \end{array}$$

Se dice que este diagrama es **conmutativo**: los dos caminos son iguales:



Ejercicio V.3. *Sea* $\phi\colon \mathbb{Z}/n\mathbb{Z} \to \mathrm{GL}_2(\mathbb{C})$ *la representación que a todo número* m *módulo* n *asocia la rotación por* $2\pi m/n$*:*

$$\phi_{[m]} := \begin{pmatrix} \cos(2\pi m)/n & -\sin(2\pi m)/n \\ \sin(2\pi m)/n & \cos(2\pi m)/n \end{pmatrix}.$$

Sea $\psi\colon \mathbb{Z}/n\mathbb{Z} \to \mathrm{GL}_2(\mathbb{C})$ *la representación definida por*

$$\psi_{[m]} := \begin{pmatrix} e^{2\pi i m/n} & 0 \\ 0 & e^{-2\pi i m/n} \end{pmatrix}.$$

Demostrar que son isomorfas.

(Indicación: considerar la aplicación $\mathbb{C}^2 \to \mathbb{C}^2$ *definida por* $A := \begin{pmatrix} i & -i \\ 1 & 1 \end{pmatrix}$*.)*

Si V_1 y V_2 son dos espacios vectoriales, entonces su **suma directa** $V_1 \oplus V_2$ es el espacio vectorial que como conjunto corresponde al producto cartesiano $V_1 \times V_2$, y tiene adición de vectores y multiplicación por escalares definidos por

$$\begin{aligned} (v_1, v_2) + (v_1', v_2') &:= (v_1 + v_1', v_2 + v_2'), \\ \lambda \cdot (v_1, v_2) &:= (\lambda \cdot v_1, \lambda \cdot v_2). \end{aligned}$$

7.2. Ejemplo. El espacio $\mathbb{C}^m \oplus \mathbb{C}^n$ es isomorfo a $\mathbb{C}^{m+n}$ ▲

7.3. Definición. Sean $\phi\colon G \to \mathrm{GL}(V_1)$ y $\psi\colon G \to \mathrm{GL}(V_2)$ dos representaciones. Su **suma directa** es la representación $\phi \oplus \psi\colon G \to \mathrm{GL}(V_1 \oplus V_2)$ definida por

$$(\phi \oplus \psi)_x(v_1, v_2) := (\phi_x(v_1), \psi_x(v_2)).$$

En términos de matrices, para $\phi\colon G \to \mathrm{GL}_m(\mathbb{C})$ y $\psi\colon G \to \mathrm{GL}_n(\mathbb{C})$ la representación

$$\phi \oplus \psi\colon G \to \mathrm{GL}_{m+n}(\mathbb{C})$$

es definida por

$$(\phi \oplus \psi)_x = \begin{pmatrix} \phi_x & 0 \\ 0 & \psi_x \end{pmatrix}$$

7.4. Ejemplo. La representación $G \to \mathrm{GL}_n(\mathbb{C})$ que a todo $g \in G$ asocia la matriz identidad $\mathrm{Id} \in \mathrm{GL}_n(\mathbb{C})$ es isomorfa a la suma directa de n copias de la representación trivial $G \to \mathbb{C}^\times$. ▲

El primer resultado no trivial (aunque bastante fácil) en teoría de la representación es el siguiente:

7.5. Teorema (Maschke). *Toda representación de un grupo finito $\phi\colon G \to \mathrm{GL}(V)$ es isomorfa a una suma directa*

$$\phi_1 \oplus \cdots \oplus \phi_s,$$

donde ϕ_i son irreducibles.

En otras palabras, $V \cong V_1 \oplus \cdots V_s$, donde los V_i son espacios G-invariantes y las restricciones correspondientes $\phi|_{V_i}$ son irreducibles.

(La demostración del teorema de Maschke no es complicada, pero vamos a omitirla. Una nota técnica para el lector que conoce un poco más de álgebra de lo que hemos revisado: en el teorema el cuerpo de base k puede ser arbitrario de característica 0, o de característica p tal que $p \nmid |G|$.)

Este teorema dice que toda representación puede ser descompuesta en algunos bloques elementales que son representaciones irreducibles. Resulta que, por lo menos en el caso $k = \mathbb{C}$, hay una teoría elegante que permite clasificar las posibles representaciones irreducibles.

8. Caracteres

A partir de ahora vamos a suponer que $k = \mathbb{C}$.

8.1. Definición. Si $\phi\colon G \to \mathrm{GL}(V)$ es una representación, entonces su **carácter** $\chi_\phi\colon G \to \mathbb{C}$ está definido por

$$\chi_\phi(x) := \mathrm{tr}(\phi_x).$$

Para calcular la traza, normalmente se fija una base de V y se trabaja con las representaciones $G \to \mathrm{GL}_n(\mathbb{C})$.

8.2. Ejemplo. Si $\phi\colon G \to \mathbb{C}^\times$ es una representación de grado 1, entonces $\chi_\phi = \phi$. ▲

8.3. Ejemplo. La representación regular $\rho\colon G \to \mathrm{GL}_n(\mathbb{C})$ está definida por $x \mapsto \phi_x$, donde $\phi_x\colon e_z \mapsto e_{x\star z}$. La matriz que corresponde a ϕ_x es una matriz de permutación que tiene todos los coeficientes nulos, excepto un coeficiente $= 1$ en cada fila y cada columna.

Tenemos

$$\chi_\rho(x) := \mathrm{tr}(\phi_x) = \#\{z \in G \mid x \star z = z\} = \begin{cases} |G|, & x = e, \\ 0, & x \neq e. \end{cases}$$

▲

8.4. Observación. *Para una representación $\phi\colon G \to \mathrm{GL}(V)$ se tiene $\chi_\phi(e) = \deg \phi$.*

Demostración.

$$\chi_\phi(e) = \mathrm{tr}(\phi_e) = \mathrm{tr}(\mathrm{Id}) = \dim V = \deg \phi.$$

■

8.5. Observación. *Si ϕ y ψ son dos representaciones isomorfas, entonces $\chi_\phi = \chi_\psi$.*

Demostración. Isomorfismo de representaciones $G \to \mathrm{GL}_n(\mathbb{C})$ quiere decir que para todo $x \in G$ existe $T \in \mathrm{GL}_n(\mathbb{C})$ tal que $\phi_x = T \circ \psi_x \circ T^{-1}$. Luego,

$$\mathrm{tr}(\phi_x) = \mathrm{tr}(T \circ \psi_x \circ T^{-1}) = \mathrm{tr}(\psi_x \circ T^{-1} \circ T) = \mathrm{tr}(\psi_x).$$

■

La misma propiedad de la traza puede ser usada para obtener la siguiente

8.6. Observación. *Si x e y son elementos conjugados de G (es decir, $y = z \star x \star z^{-1}$ para algún $z \in G$), entonces $\chi_\phi(x) = \chi_\phi(y)$.*

Demostración.

$$\chi_\phi(x) = \mathrm{tr}(\phi_x) = \mathrm{tr}(\phi_{z\star y\star z^{-1}}) = \mathrm{tr}(\phi_z \circ \phi_y \circ \phi_z^{-1}) = \mathrm{tr}(\phi_y \circ \phi_z^{-1} \circ \phi_z) = \mathrm{tr}(\phi_y) = \chi_\phi(y).$$

■

Entonces los caracteres pueden ser vistos como funciones $f\colon \mathrm{Cl}(G) \to \mathbb{C}$ sobre *las clases de conjugación* de G con valores en $\mathbb{C}$. Tales funciones forman un espacio vectorial con la adición y multiplicación por escalares "punto a punto"

$$(f+g)(x) := f(x) + g(x), \quad (\lambda \cdot f)(x) := \lambda \cdot (f(x)).$$

Además, este espacio tiene una estructura adicional: un producto definido por

$$\langle f, g\rangle := \frac{1}{|G|} \sum_{x\in G} f(x)\,\overline{g(x)}.$$

(La división por $|G|$ es nada más que una especie de "normalización"; véase abajo las relaciones de ortogonalidad.) Es un **producto prehilbertiano**, lo que significa que se cumplen los siguientes axiomas:

1) es **hermitiano**: $\langle f, g\rangle = \overline{\langle g, f\rangle}$ (no confundir con *ermitaño* :-)
2) es **sesquilineal** (del latin *sesqui*, uno y medio): $\langle \lambda \cdot f, g\rangle = \lambda \cdot \langle f, g\rangle$ y $\langle f + f', g\rangle = \langle f, g\rangle + \langle f', g\rangle$; note que esto junto con 1) implica que en la segunda variable, se tiene $\langle f, \lambda \cdot g\rangle = \overline{\lambda} \cdot \langle f, g\rangle$ y $\langle f, g + g'\rangle = \langle f, g\rangle + \langle f, g'\rangle$.
3) es **definido positivo**: $\langle f, f\rangle \geq 0$ para todo f y $\langle f, f\rangle = 0$ si y solamente si $f = 0$.

El espacio vectorial de funciones $\mathrm{Cl}(G) \to \mathbb{C}$ tiene dimensión $|\mathrm{Cl}(G)|$. A saber, para toda clase de conjugación $C \subset G$ se puede definir

$$\delta_C(x) := \begin{cases} 1, & x \in C, \\ 0, & x \notin C. \end{cases}$$

Las combinaciones lineales de estas funciones generan todo el espacio, ya que para toda aplicación f constante sobre las clases de conjugación

$$f = \sum_{C\in \mathrm{Cl}(G)} f(C) \cdot \delta_C.$$

Para ver que las δ_C son linealmente independientes, se verifica que son **ortogonales** respecto al producto $\langle \cdot, \cdot \rangle$:

$$\langle \delta_C, \delta_{C'}\rangle = \begin{cases} |C|/|G|, & C = C', \\ 0, & C \neq C'. \end{cases}$$

Sumas directas de representaciones corresponden a sumas de caracteres:

8.7. Observación. $\chi_{\phi\oplus\psi} = \chi_\phi + \chi_\psi$.

Demostración. Si $\phi\colon G \to \mathrm{GL}_m(\mathbb{C})$ y $\psi\colon G \to \mathrm{GL}_n(\mathbb{C})$, entonces $\phi \oplus \psi\colon G \to \mathrm{GL}_{m+n}(\mathbb{C})$ es dada por

$$(\phi \oplus \psi)_x = \begin{pmatrix} \phi_x & 0 \\ 0 & \psi_x \end{pmatrix},$$

y tenemos

$$\operatorname{tr}\begin{pmatrix} \phi_x & 0 \\ 0 & \psi_x \end{pmatrix} = \operatorname{tr}\phi_x + \operatorname{tr}\psi_x.$$

■

El segundo resultado no trivial en teoría de la representación (después del teorema de Maschke) es el siguiente:

8.8. Teorema (Las relaciones de ortogonalidad). *Si ϕ y ψ son representaciones irreducibles, entonces*

$$\langle \chi_\phi, \chi_\psi \rangle = \begin{cases} 1, & \phi \cong \psi, \\ 0, & \phi \ncong \psi. \end{cases}$$

En particular, diferentes representaciones irreducibles son ortogonales y por lo tanto linealmente independientes.

En efecto, se puede ver que χ_i forman una base del espacio de aplicaciones constantes en clases de conjugación, y entonces hay precisamente $|\operatorname{Cl}(G)|$ diferentes representaciones irreducibles.

La demostración de las relaciones de ortogonalidad requiere un par de lecciones extra que lamentablemente no tenemos. Solo notamos que para este resultado es importante que las representaciones sean sobre los espacios vectoriales complejos (el teorema de Maschke es válido en muchas otras situaciones, y es más sencillo).

Usando las relaciones de ortogonalidad, se puede deducir muchas propiedades importantes. Por ejemplo, según el teorema de Maschke, toda representación ϕ es una suma directa de representaciones irreducibles, entonces tenemos

$$\phi \cong m_1\phi_1 \oplus \cdots \oplus m_s\phi_s,$$

donde ϕ_i son irreducibles, y el múltiplo m_i significa que se toma la suma directa de m_i copias de ϕ_i. Los números m_i se llaman las **multiplicidades** de representaciones irreducibles en una representación ϕ.

8.9. Teorema. *En la descomposición*

$$\phi \cong m_1\phi_1 \oplus \cdots \oplus m_s\phi_s$$

se tiene $m_i = \langle \chi_\phi, \chi_{\phi_i} \rangle$.

Demostración. La descomposición de arriba nos da al nivel de caracteres

$$\chi_\phi = m_1\chi_{\phi_1} + \cdots + m_s\chi_{\phi_s}.$$

Luego,

$$\langle \chi_\phi, \chi_{\phi_i} \rangle = m_1 \langle \chi_{\phi_1}, \chi_{\phi_i} \rangle + \cdots + m_n \langle \chi_{\phi_s}, \chi_{\phi_i} \rangle = m_i.$$

■

8.10. Corolario. *La descomposición de ϕ en representaciones irreducibles es única.*

8.11. Corolario. *ϕ está determinado por su carácter χ_ϕ.*

8.12. Corolario. *ϕ es irreducible si y solamente si $\langle \chi_\phi, \chi_\phi \rangle = 1$.*

Demostración. Por las relaciones de ortogonalidad, se calcula $\langle \chi_\phi, \chi_\phi \rangle = m_1^2 + \cdots + m_s^2$. Los m_i son números enteros no negativos. ■

Podemos calcular las multiplicidades m_i para la representación regular $\rho\colon G \to \mathrm{GL}_n(\mathbb{C})$. Ya que

$$\chi_\rho(x) = \begin{cases} |G|, & x = e, \\ 0, & x \neq e, \end{cases}$$

se ve que

$$\langle \rho, \chi_i \rangle := \frac{1}{|G|} \sum_{x \in G} \chi_\rho(x)\, \overline{\chi_i(x)} = \frac{1}{|G|}\, |G|, \overline{\chi_i(e)} = \deg \phi_i.$$

Tenemos entonces para la representación regular

$$\chi_\rho = d_1\, \chi_1 + \cdots + d_s\, \chi_s,$$

donde χ_i son los caracteres de todas las representaciones irreducibles de G y d_i son sus grados correspondientes. Ya que $\chi_i(e) = \deg \phi_i =: d_i$ y $\chi_\rho(e) = |G|$, evaluando la expresión de arriba, se obtiene

$$|G| = d_1^2 + \cdots + d_s^2.$$

8.13. Ejemplo. Como hemos mencionado, $s = |\mathrm{Cl}(G)|$. Si G es un grupo abeliano, tenemos $|\mathrm{Cl}(G)| = |G|$ y la única posibilidad para que se cumpla $|G| = d_1^2 + \cdots + d_s^2$ es $d_1 = \cdots = d_s = 1$. Todas las representaciones irreducibles de un grupo abeliano son de grado 1. ▲

8.14. Ejemplo. El grupo S_3 tiene 3 clases de conjugación (representados por permutaciones $(\,)$, $(1\ 2)$, $(1\ 2\ 3)$), y entonces tres representaciones irreducibles. Sus grados tienen que cumplir la identidad $6 = d_1^2 + d_2^2 + d_3^2$. La única posibilidad (módulo numeración de representaciones) es $d_1 = d_2 = 1$ y $d_3 = 2$.

Una representación irreducible evidente es la representación trivial $\phi_1\colon S_3 \to \mathbb{C}^\times$ definida por $\sigma \mapsto 1$ para todo $\sigma \in S_3$. Otra representación irreducible de grado 1 corresponde a otro homomorfismo $S_3 \to \mathbb{C}^\times$ que ya conocimos... el signo:

$$\mathrm{sgn}\colon S_3 \to \{\pm 1\} \subset \mathbb{C}^\times.$$

Hay una representación más de orden 2. Sea $\chi_?$ su carácter. La tabla de caracteres de S_3 es entonces dada por

	$(\,)$	$(1\ 2)$	$(1\ 2\ 3)$
χ_1	1	1	1
χ_{sgn}	1	-1	1
$\chi_?$	2	???	???

Ya sabemos que $\chi_?((\,)) = 2$ es el grado, y nos faltan dos valores $\chi_?((1\ 2))$ y $\chi_?((1\ 2\ 3))$. Es posible encontrarlos usando las relaciones de ortogonalidad:

$$\begin{aligned} \langle \chi_?, \chi_1 \rangle = 0 \quad &\Rightarrow \quad \chi_?((\,)) + 3 \cdot \chi_?((1\ 2)) + 2 \cdot \chi_?((1\ 2\ 3)) = 0, \\ \langle \chi_?, \chi_{\mathrm{sgn}} \rangle = 0 \quad &\Rightarrow \quad \chi_?((\,)) - 3 \cdot \chi_?((1\ 2)) + 2 \cdot \chi_?((1\ 2\ 3)) = 0, \end{aligned}$$

y por lo tanto $\chi_?((1\ 2)) = 0$ y $\chi_?((1\ 2\ 3)) = -1$. ▲