Pedro Montero
con la colaboración de Juan Fuenzalida & Fabián Levican

ÁLGEBRA ABSTRACTA

Pedro Montero*, con la colaboración de Juan* Fuenzalida *& Fabián* Levican

ÁLGEBRA ABSTRACTA

Pedro MONTERO

con la colaboración de Juan FUENZALIDA & Fabián LEVICAN

CONTENIDOS

Agradecimientos 7

1. Prerrequisitos 9
1.1. Relaciones de equivalencia y cocientes 9
1.2. Permutaciones 12

2. Grupos 17
2.1. Generalidades sobre los grupos 17
2.1.1. Definiciones 17
2.1.2. Sub-grupos y generadores 19
2.1.3. Morfismos de grupos 21
2.1.4. Clases laterales 22
2.1.5. Sub-grupos normales 23
2.1.6. Cocientes 24
2.1.7. Cocientes de espacios vectoriales 29
2.2. Acciones de grupos 30
2.2.1. Acción de un grupo sobre un conjunto 30
2.2.2. Órbitas 31
2.2.3. Conjugación 34
2.2.4. Fórmula de clases y p-grupos 35
2.3. Teoremas de Sylow 37
2.4. Grupos abelianos finitamente generados 41
2.4.1. Teorema chino del resto y grupos abelianos de tipo finito 41
2.4.2. Grupos abelianos libres finitamente generados 43
2.5. Grupos simples y series de composición 48

3. Representaciones de grupos finitos ... 55
3.1. Representaciones lineales ... 55
3.2. Sub-representaciones y morfismos ... 57
3.3. Representaciones irreducibles ... 59
3.4. Producto tensorial de espacios vectoriales ... 60
3.5. Caracteres ... 65
3.6. Lema de Schur ... 69
3.7. Ortogonalidad de caracteres ... 71
3.8. Caracteres y funciones centrales ... 74
3.9. Tablas de caracteres ... 78

4. Anillos y módulos ... 81
4.1. Anillos e ideales ... 81
4.1.1. Primeras definiciones ... 81
4.1.2. Ideales ... 83
4.1.3. Anillos reducidos y anillos noetherianos ... 88
4.1.4. Algunos teoremas de Hilbert ... 90
4.1.5. Topología de Zariski y geometría ... 94
4.1.6. Geometría de ideales ... 99
4.1.7. Morfismos entre cocientes y teorema chino del resto ... 101
4.2. Módulos sobre un anillo ... 103
4.2.1. Primeras definiciones ... 103
4.2.2. Módulos cocientes ... 106
4.2.3. Operaciones sobre sub-módulos ... 107
4.2.4. Módulos finitamente generados y módulos libres ... 109
4.2.5. Teorema de Cayley-Hamilton y Lema de Nakayama ... 112
4.2.6. Sucesiones exactas y complejos ... 116
4.2.7. Módulos proyectivos e inyectivos ... 122
4.2.8. Lema de la serpiente ... 125
4.2.9. Producto tensorial de módulos ... 127

Comentarios finales ... 131

Índice ... 133

Bibliografia ... 137

AGRADECIMIENTOS

El presente texto tiene como principal objetivo complementar el curso de *Estructuras Algebraicas* en la Universidad Técnica Federico Santa María.

El Capítulo 1 recuerda nociones y resultados básicos sobre relaciones de equivalencia y permutaciones, que serán requeridos a lo largo del texto. El Capítulo 2 es una introducción a la teoría de grupos, mientras que el Capítulo 3 tiene por objetivo estudiar representaciones de grupos finitos. Finalmente, el Capítulo 4 es una introducción a la teoría de anillos y módulos, con un énfasis en el punto de vista geométrico inspirado por la geometría algebraica.

Quisiera expresar mi gratitud a Fabián Levicán y Juan Fuenzalida por su ayuda en traspasar pacientemente a LaTeX parte de mis apuntes escritos a mano, así como por sus comentarios y observaciones a versiones previas de este texto.

Durante la escritura de este texto, he sido parcialmente financiado por el proyecto Fondecyt Iniciación 11190323.

Agradezco de antemano por cualquier tipo de comentario, sugerencia o corrección, para lo cual pueden comunicarse directamente conmigo al correo electrónico `pedro.montero@usm.cl`.

Pedro Montero
Departamento de Matemática
Universidad Técnica Federico Santa María
Valparaíso, Diciembre 2019

CAPÍTULO 1

PRERREQUISITOS

Durante todo el texto denotaremos por $\mathbb{N} = \{0, 1, 2, \ldots\}$ el conjunto de los números naturales, $\mathbb{Z}$ el anillo de números enteros, y por $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ los cuerpos de los números racionales, reales y complejos. De manera similar, $\mathbb{N}^{\geq 1} = \{1, 2, 3, \ldots\}$, $\mathbb{R}^{>0} = \{x \in \mathbb{R} \mid x > 0\}$, etc. Dado $x \in \mathbb{C}$ denotamos por $x\mathbb{Z} = \{nx,\ n \in \mathbb{Z}\}$ al conjunto de múltiplos enteros de x. Además, usaremos las siguientes abreviaciones:

- c.f. (*confer*): "comparar con".
- e.g. (*exempli gratia*): "por ejemplo".
- i.e. (*id est*): "es decir".

La notacion $f : A \hookrightarrow B$ (resp. $f : A \twoheadrightarrow B$) indica que f es una función inyectiva (resp. sobreyectiva).

Si V es un espacio vectorial sobre un cuerpo k y $S \subseteq V$ un sub-conjunto, denotamos por $\mathrm{Vect}_k(S)$ al k-sub-espacio vectorial generado por S.

1.1. Relaciones de equivalencia y cocientes

***Definición 1.1.1* (relación de equivalencia).** — Sea A un conjunto y sea $\mathscr{R}$ una relación en A (es decir, un subconjunto $\mathscr{R} \subseteq A \times A$). Si para todo $(a, b) \in A \times A$ tal que $(a, b) \in \mathscr{R}$ escribimos $a \sim b$, entonces decimos que $\mathscr{R}$ es una **relación de equivalencia** si es:

1. **reflexiva:** $a \sim a$ para todo $a \in A$,
2. **simétrica:** $a \sim b$ si y sólo si $b \sim a$ para todos $a, b \in A$,
3. **transitiva:** si $a \sim b$ y $b \sim c$ entonces $a \sim c$, para todos $a, b, c \in A$.

***Definición 1.1.2* (clase de equivalencia).** — Sea $\mathscr{R}$ una relación de equivalencia en A. Para todo $a \in A$ diremos que el conjunto

$$[a]_{\mathscr{R}} = \{b \in A \mid a \sim b\} = \{b \in A \mid b \sim a\}$$

es la **clase de equivalencia** de $a \in A$ respecto a $\mathscr{R}$, el cual es también denotado $a \mod \mathscr{R}$. En caso que la relación $\mathscr{R}$ sea clara en el contexto, escribiremos simplemente $[a]$ o bien $\overline{a}$.

***Definición 1.1.3* (cociente).** — Sea $\mathscr{R}$ una relación de equivalencia en A. El conjunto cuyos elementos son todas las clases de equivalencia es llamado **conjunto cociente** de A por $\mathscr{R}$, y será denotado $A/\mathscr{R}$ (o simplemente $A/\sim$ si la relación $\mathscr{R}$ es clara en el contexto). Explícitamente,

$$A/\mathscr{R} = \{[a]_{\mathscr{R}},\ a \in A\}.$$

Las relaciones de equivalencia satisfacen las siguientes propiedades.

Proposición 1.1.4. — *Sea $\mathscr{R}$ una relación de equivalencia en A. Entonces:*

1. *Para todo $a \in A, a \in [a]_{\mathscr{R}}$. En particular, $[a]_{\mathscr{R}} \neq \emptyset$.*
2. *Si $b \in [a]_{\mathscr{R}}$ entonces $a \in [b]_{\mathscr{R}}$. Además, en este caso tenemos que $[a]_{\mathscr{R}} = [b]_{\mathscr{R}}$.*
3. *Para todos $a, b \in A$ ya sea $[a]_{\mathscr{R}} = [b]_{\mathscr{R}}$ o bien $[a]_{\mathscr{R}} \cap [b]_{\mathscr{R}} = \emptyset$. En particular, A es la unión disjunta de las clases $[a]_{\mathscr{R}}$.*

Demostración. — Ejercicio al lector. □

Uno de los principales ejemplos de relación de equivalencia es la **congruencia módulo** $n \in \mathbb{N}^{\geq 1}$.

Ejemplo 1.1.5. — Sea $n \in \mathbb{N}^{\geq 1}$. Consideremos la relacion en $\mathbb{Z}$ dada por

$$\begin{aligned} a \sim b &\Leftrightarrow n \text{ divide } a - b \\ &\Leftrightarrow \exists k \in \mathbb{Z} \text{ tal que } a - b = nk. \end{aligned}$$

No es difícil verificar que la relación anterior es en efecto una relación de equivalencia. Utilizaremos la siguiente notación en lo que sigue:

- Si $a \sim b$, escribimos $a \equiv b \pmod{n}$ y diremos que "a es congruente con b módulo n".
- La clase de equivalencia de a módulo n está dada por

$$[a]_n = \{b \in \mathbb{Z} \mid a \equiv b \pmod{n}\}.$$

- El conjunto de clases de equivalencia, "$\mathbb{Z}$ módulo $n\mathbb{Z}$", es denotado por

$$\mathbb{Z}/n\mathbb{Z} = \{[a]_n,\ a \in \mathbb{Z}\}.$$

Por ejemplo, si $n = 2$ entonces observamos que

$$[0]_2 = \{a \in \mathbb{Z} \mid a \equiv 0 \pmod 2\} = \{a \in \mathbb{Z} \mid \exists k \in \mathbb{Z},\ a = 2k\}$$

es el conjunto de enteros pares. De manera similar, $[1]_2$ es el conjunto de enteros impares. Luego, el cociente $\mathbb{Z}/2\mathbb{Z} = \{[0]_2, [1]_2\}$ es un conjunto con 2 elementos.

***Recuerdo 1.1.6* (division euclideana).** — Sean $a, b \in \mathbb{Z}$ con $b \neq 0$. Entonces existen únicos enteros $q, r \in \mathbb{Z}$ tales que $a = bq + r$ y $0 \leq r < |b|$.

Ejercicio 1.1.7. —

a) Utilizando la división euclideana en $\mathbb{Z}$, demostrar que

$$\mathbb{Z}/n\mathbb{Z} = \{[0]_n, [1]_n, \ldots, [n-1]_n\}.$$

b) Demostrar que para todo $a, b \in \mathbb{Z}$ se tiene que $[a+b]_n$ y $[ab]_n$ dependen sólamente de $[a]_n$ y $[b]_n$, es decir, si $a \equiv a' \pmod n$ y $b \equiv b' \pmod n$ entonces $[a+b]_n = [a'+b']_n$ y $[ab]_n = [a'b']_n$. En particular, la suma $[a]_n + [b]_n := [a+b]_n$ y el producto $[a]_n \cdot [b]_n := [ab]_n$ de clases de equivalencias están bien definidos.

***Lema 1.1.8* (Bézout).** — *Sean $a, b \in \mathbb{Z}$ no nulos. Entonces existen $x, y \in \mathbb{Z}$ tales que $ax + by = \mathrm{mcd}(a, b)$.*

Demostración. — Sea $S = \{ax + by \mid x, y \in \mathbb{Z}\}$ y sea d el menor elemento en $S \cap \mathbb{N}^{\geq 1}$. Observemos que d divide a a. En efecto, la división euclidiana permite escribir:

$$a = qd + r, \quad \text{con } q, r \in \mathbb{Z}, 0 \leq r < d$$

Dado que $a, d \in S$, tenemos que $r = a - qd \in S$. Por otro lado, como d es el mínimo de $S \cap \mathbb{N}^{\geq 1}$ tenemos necesariamente que $r = 0$ (de lo contrario, se obtiene una contradicción con la minimalidad de d). Por lo tanto, $d \mid a$ ("d divide a a"). Análogamente, $d \mid b$.

Finalmente, si d' un divisor en común de a y de b entonces d' divide a todos los elementos de S. En particular, $d' \mid d$ y luego $d' \leq d$. Se concluye de esta manera que $d = \mathrm{mcd}(a, b) = ax_0 + by_0$ para ciertos $x_0, y_0 \in \mathbb{Z}$. □

Corolario 1.1.9. — *Sea p un número primo. Entonces para todo $a \in \mathbb{Z}$ tal que $p \nmid a$, existe $b \in \mathbb{Z}$ tal que $p \nmid b$ tal que $ab \equiv 1 \pmod p$.*

Demostración. — Dado que p no divide a $a \in \mathbb{Z}$ se tiene que $\mathrm{mcd}(a,p) = 1$, pues p es primo. Entonces, el lema de Bézout implica que existen $x, y \in \mathbb{Z}$ tales que $ax + py = 1$. Equivalentemente,

$$ax - 1 = p(-y)$$

Si definimos $b = x$, entonces $ab \equiv 1 \pmod{p}$. □

Una consecuencia del corolario anterior es que para todo número primo p, el conjunto

$$\mathbb{Z}/p\mathbb{Z} = \{[0]_p, [1]_p, ..., [p-1]_p\}$$

es un **cuerpo** (ver Definición 2.1.3). En efecto, para todo $[a]_p \neq [0]_p$ existe $[a]_p^{-1}$ tal que $[a]_p \cdot [a]_p^{-1} = [1]_p$.

Notación 1.1.10. — Sea p un número primo. Denotaremos por $\mathbb{F}_p$ al **cuerpo de p elementos** $(\mathbb{Z}/p\mathbb{Z}, +, \cdot)$.

Ejercicio 1.1.11. — Calcular las tablas de suma y multiplicación en $\mathbb{F}_3$.

Ejercicio 1.1.12. — Sea p un número primo.

a) Sea $k \in \{1, \ldots, p-1\}$. Probar que p divide a $\binom{p}{k} = \frac{p!}{k!(p-k)!}$.
b) Probar que para todos $x, y \in \mathbb{F}_p$ se tiene $(x+y)^p = x^p + y^p$.

1.2. Permutaciones

***Definición 1.2.1* (permutación).** — Sea $n \in \mathbb{N}^{\geq 1}$. Una **permutación** del conjunto $\{1, 2, \ldots, n\}$ es una función biyectiva

$$\sigma : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$$

La denotaremos mediante

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

ó simplemente

$$\sigma = (\sigma(1), \sigma(2), \ldots, \sigma(n)).$$

Ejemplo 1.2.2. — La permutación $\sigma = (2, 3, 4, 1)$ corresponde a la biyección

$$\sigma : \begin{cases} 1 \mapsto 2 \\ 2 \mapsto 3 \\ 3 \mapsto 4 \\ 4 \mapsto 1 \end{cases}$$

Notación 1.2.3. — El conjunto de todas las permutaciones de $\{1,\dots,n\}$ será denotado $\mathfrak{S}_n$. Además, si $\sigma,\tau\in\mathfrak{S}_n$, entonces denotamos $\sigma\tau := \sigma\circ\tau$ (composición de funciones) y como σ^{-1} a la función inversa de σ.

Ejemplo 1.2.4. —

1. Si $\sigma=(2,3,4,1)$ y $\tau=(2,1,4,3)$, entonces $\tau\sigma=(1,4,3,2)$ y $\sigma\tau=(3,2,1,4)$. Además, la inversa de σ se calcula gráficamente como a continuación:
$$\sigma:\begin{cases}1\mapsto 2\\ 2\mapsto 3\\ 3\mapsto 4\\ 4\mapsto 1\end{cases}\implies \sigma^{-1}:\begin{cases}1\mapsto 4\\ 2\mapsto 1\\ 3\mapsto 2\\ 4\mapsto 3\end{cases}$$
2. $\mathfrak{S}_3=\{(1,2,3),(2,1,3),(3,2,1),(1,3,2),(2,3,1),(3,1,2)\}$

Proposición 1.2.5. — *El cardinal de $\mathfrak{S}_n$ es $n!=1\cdot 2\cdots n$.*

Demostración. — Por inducción en $n\in\mathbb{N}^{\geq 1}$. Si $n=1$, entonces $S_1=\{(1)\}$. Supongamos que $|\mathfrak{S}_n|=n!$ para algún n, y consideremos $\mathfrak{S}_{n+1}$. Para $k\in\mathbb{N}^{\geq 1}$ tal que $1\leq k\leq n+1$, consideremos A_k como el número de $\sigma\in\mathfrak{S}_{n+1}$ tales que $\sigma=(a_1,a_2,\dots,a_{n+1})$, con $a_k=n+1$. Dada una permutación tal, definimos $(a_1,a_2,...,a_{k-1},a_{k+1},...,a_{n+1})\in\mathfrak{S}_n$. Recíprocamente, dada $(b_1,b_2,...,b_n)\in\mathfrak{S}_n$, definimos $\sigma=(b_1,b_2,...,b_{k-1},n+1,b_k,...,b_n)$ (permutación de la forma anterior). Luego, $A_k=|\mathfrak{S}_n|=n!$. Finalmente, $|\mathfrak{S}_{n+1}|=\sum_{k=1}^{n+1}A_k=\sum_{k=1}^{n+1}n!=(n+1)!$. □

Definición 1.2.6 **(transposición).** — Una permutación $\tau\in\mathfrak{S}_n$ que sólo cambia dos elementos de $\{1,\dots,n\}$ es llamada una **transposición**.

Notación 1.2.7. — Sea $n\geq 2$. Para todos $i,j\in\{1,\dots,n\}$ tales que $i\neq j$, denotamos por $\tau=(i,j)$ a la transposición tal que $\tau(i)=j$, $\tau(j)=i$ y $\tau(k)=k$ para todo k distinto de i y de j.

Observación 1.2.8. — Notar que $(i,j)=(j,i)=(i,j)^{-1}$.

Ejemplo 1.2.9. — Siguiendo la Notacion 1.2.7, se tiene que
$$\mathfrak{S}_3=\{\mathrm{id},(1,2),(2,3),(1,3),(2,3,1),(3,1,2)\}.$$

Definición 1.2.10 **(inversión).** — Sea $\sigma\in\mathfrak{S}_n$ y sean $i,j\in\mathbb{N}^{\geq 1}$ tales que $1\leq i<j\leq n$. Decimos que σ **invierte** i y j si $\sigma(i)>\sigma(j)$.

Ejemplo 1.2.11. — 1. La identidad $\mathrm{id}=(1,2,\dots,n)$ no tiene inversiones.

2. La transposición $(1,2) \in \mathfrak{S}_n$ tiene 1 inversión.
3. $(2,3,1)$ y $(3,1,2)$ en $\mathfrak{S}_3$ tienen 2 inversiones.

Ejercicio 1.2.12. — Demostrar que la transposición $(i,j) \in \mathfrak{S}_n$ tiene $2|i-j|-1$ inversiones.

***Definición 1.2.13* (signatura).** — Sea $\sigma \in \mathfrak{S}_n$. Llamaremos al número

$$\varepsilon(\sigma) := (-1)^{\text{número de inversiones de } \sigma}$$

la **signatura** de σ. Decimos que σ es **par** (resp. **impar**) si $\varepsilon(\sigma) = 1$ (resp. $\varepsilon(\sigma) = -1$).

Ejemplo 1.2.14. — 1. La identidad es par, pues $\varepsilon(\mathrm{id}) = (-1)^0 = 1$.
2. $\varepsilon((i,j)) = -1$, es decir, toda transposición es impar.
3. En $\mathfrak{S}_3$ hay 3 permutaciones pares y 3 permutaciones impares.

Lema 1.2.15. — *Sea $\sigma \in \mathfrak{S}_n$. Entonces,*

$$\varepsilon(\sigma) = \prod_{1 \le i < j \le n} \frac{\sigma(j) - \sigma(i)}{j - i}.$$

Demostración. — Claramente, la cantidad

$$\prod_{i<j} \frac{\sigma(j) - \sigma(i)}{j - i}$$

tiene el mismo signo que $\varepsilon(\sigma)$. Además,

$$\left(\prod_{i<j} \frac{\sigma(j) - \sigma(i)}{j - i} \right)^2 = \prod_{i<j} \left(\frac{\sigma(j) - \sigma(i)}{j - i} \right)^2 = \frac{\prod_{i \neq j} (\sigma(j) - \sigma(i))}{\prod_{i \neq j} (j - i)} = 1$$

Para obtener la última igualdad, nótese que los términos en el numerador y denominador son los mismos, pues σ es una biyección. □

Proposición 1.2.16. — *La signatura $\varepsilon : \mathfrak{S}_n \to \{-1, 1\}$ satisface*

$$\varepsilon(\sigma\tau) = \varepsilon(\sigma)\varepsilon(\tau)$$

para todos $\sigma, \tau \in \mathfrak{S}_n$.

Demostración. — Sean $\sigma, \tau \in \mathfrak{S}_n$. Como

$$\frac{\sigma(j) - \sigma(i)}{j - i} = \frac{\sigma(i) - \sigma(j)}{i - j},$$

esta cantidad no depende del orden de i y j. Luego,

$$\varepsilon(\sigma) = \prod_{i<j} \frac{\sigma(\tau(j)) - \sigma(\tau(i))}{\tau(j) - \tau(i)},$$

lo que implica que

$$\begin{aligned}\varepsilon(\sigma\tau) &= \prod_{i<j} \frac{\sigma(\tau(j)) - \sigma(\tau(i))}{j - i} \\ &= \prod_{i<j} \frac{\sigma(\tau(j)) - \sigma(\tau(i))}{\tau(j) - \tau(i)} \cdot \prod_{i<j} \frac{\tau(j) - \tau(i)}{j - i} \\ &= \varepsilon(\sigma)\varepsilon(\tau),\end{aligned}$$

de donde se obtiene el resultado. □

Observemos que los elementos de $\mathfrak{S}_3 = \{\mathrm{id}, (1,2), (2,3), (1,3), (2,3,1), (3,1,2)\}$ pueden ser escritos como productos de transposiciones. En efecto, $\mathrm{id} = (1,2)(1,2)$, $(2,3,1) = (1,3)(1,2)$ y $(3,1,2) = (1,2)(1,3)$. Además, dicha escritura no es única pues $(3,1,2) = (1,2)(1,3) = (1,3)(2,3)$. La proposición siguiente generaliza esta situación.

Proposición 1.2.17. — *Toda permutación se escribe como producto de transposiciones. Dicha escritura no es única, pero toda descomposición de una permutación par (resp. impar) tiene un número par (resp. impar) de factores.*

Idea de la demostración. — La demostración es algorítmica. La idea es, dada $\sigma \in \mathfrak{S}_n$, multiplicar transposiciones por su izquierda para ir obteniendo cada vez más elementos fijos. Supongamos por ejemplo que

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 1 & 5 & 3 \end{pmatrix}.$$

Como $1 \mapsto 2$ via σ, componemos con $(1,2)$:

$$(1,2)\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 2 & 5 & 3 \end{pmatrix}$$

Como $2 \mapsto 4$ via la permutación anterior, componemos con $(2,4)$:

$$(2,4)(1,2)\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 4 & 5 & 3 \end{pmatrix}$$

Como $3 \mapsto 4$ via la permutación anterior, componemos con $(3,4)$:

$$(3,4)(2,4)(1,2)\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 5 & 4 \end{pmatrix} = (4,5)$$

Así, se obtiene por ejemplo que $(2,4)(1,2)\sigma = (3,4)^{-1}(4,5) = (3,4)(4,5)$ (c.f. Observación 1.2.8), y luego $\sigma = (1,2)(2,4)(3,4)(4,5)$.

Tal como notamos anteriormente, la escritura no es única. Sin embargo, si $\sigma = \tau_1\tau_2\cdots\tau_r$, donde cada τ_i es una transposición, entonces

$$\varepsilon(\sigma) = \varepsilon(\tau_1)\varepsilon(\tau_2)\cdots\varepsilon(\tau_r) = (-1)^r$$

Luego r y σ poseen la misma paridad. □

CAPÍTULO 2

GRUPOS

2.1. Generalidades sobre los grupos

2.1.1. Definiciones. —

Definición 2.1.1. — Un **grupo** es un conjunto no vacío G dotado de una ley de composición interna

$$G \times G \longrightarrow G$$
$$(g_1, g_2) \longmapsto g_1 g_2$$

que satisface las siguientes condiciones:

1. **asociatividad:** para todos $g_1, g_2, g_3 \in G$ tenemos que
$$(g_1 g_2) g_3 = g_1 (g_2 g_3);$$
2. **elemento neutro:** existe un elemento $e \in G$ (necesariamente único) tal que para todo $g \in G$ tenemos que
$$ge = eg = g;$$
3. **inverso:** para todo $g \in G$ existe un elemento $g^{-1} \in G$ (necesariamente único) tal que
$$gg^{-1} = g^{-1}g = e.$$

Observación 2.1.2. — Un conjunto no vacío S dotado de una ley de composición interna asociativa (i.e., que verifica la condición (1)) es llamado un **semi-grupo**. Por otro lado, si S además posee un elemento neutro (i.e., verifica las condiciones (1) y (2)) es llamado un **monoide** .

Denotamos frecuentemente por 1 el elemento neutro de un grupo. Para todo elemento g de un grupo G y todo entero $n \in \mathbb{Z}$, denotamos

$$g^n = \begin{cases} \overbrace{g \cdots g}^{n \text{ veces}} & \text{si } n > 0; \\ e & \text{si } n = 0; \\ \overbrace{g^{-1} \cdots g^{-1}}^{-n \text{ veces}} & \text{si } n < 0 \end{cases}$$

En particular, si $n, m \in \mathbb{Z}$ entonces

$$g^{m+n} = g^m g^n.$$

Decimos que el grupo G es **abeliano** (o conmutativo) si para todos $g_1, g_2 \in G$ tenemos que $g_1 g_2 = g_2 g_1$. En cuyo caso, la ley de composición interna es generalmente escrita de forma aditiva $g_1 + g_2$, el elemento neutro es denotado 0, y el inverso de g es llamado el elemento **opuesto**, el cual es denotado $-g$.

***Definición 2.1.3* (anillo y cuerpo).** — Sea $(A, +, \cdot)$ un conjunto no-vacío con dos leyes de composición interna. Se dice que A es un **anillo** si:

1. $(A, +)$ es un grupo abeliano.
2. $(A, \cdot)$ es un monoide.
3. Para todos $a, b, c \in A$ se tiene que $a(b+c) = ab+ac$ y $(b+c)a = ba+ca$.

Además, se dice que A es un **anillo abeliano** si $ab = ba$ para todos $a, b \in A$. Finalmente, diremos que un anillo abeliano k es un **cuerpo** si $k \neq \{0\}$ y si $(k \setminus \{0\}, \cdot)$ es un grupo.

Decimos que el grupo G es **finito** si el conjunto subyacente es finito. En cuyo caso, su cardinal es llamado su **orden**, el cual es denotado $|G|$.

Si G y G' son grupos podemos formar el grupo $G \times G'$, llamado **producto directo**, dotando al conjunto producto de la ley de composición interna $(g_1, g_1')(g_2, g_2') = (g_1 g_2, g_1' g_2')$.

Ejemplo 2.1.4. —

1. Los enteros con la suma $(\mathbb{Z}, +)$ forman un grupo abeliano.
2. Si k es un cuerpo (como $\mathbb{Q}, \mathbb{R}$ o $\mathbb{C}$), $(k, +)$ y $(k \setminus \{0\}, \cdot)$ son grupos abelianos. Más generalmente, para un anillo A tenemos el grupo abeliano $(A, +)$ y el grupo multiplicativo $(A^\times, \cdot)$ de **unidades** de A (los elementos de A que son inversibles respecto a la multiplicación). En particular, si k es un cuerpo entonces $k^\times = k \setminus \{0\}$.
3. Para todo entero $n \in \mathbb{N}^*$, el par $(\mathbb{Z}/n\mathbb{Z}, +)$ es un grupo finito de orden n. Estos grupos son llamados **cíclicos**.

4. Si X es un conjunto, el conjunto $\mathrm{Biy}(X)$ de biyecciones de X en X, dotado de la composición de funciones, es un grupo. En particular, el **grupo simétrico** $\mathfrak{S}_n$ de biyecciones del conjunto $\{1, \ldots, n\}$ es un grupo finito de orden $n!$, no abeliano para $n \geq 3$.
5. Si k es un cuerpo, las matrices inversibles de tamaño $n \times n$ con coeficientes en k forman el **grupo general lineal** $\mathrm{GL}_n(k)$. Si V es un k-espacio vectorial, las aplicaciones lineales biyectivas de V en V forman un grupo $\mathrm{GL}(V)$. Si V es de dimensión finita n, la elección de una base de V provee un isomorfismo entre $\mathrm{GL}(V)$ y $\mathrm{GL}_n(k)$. Las aplicaciones afines biyectivas de V en V (es decir, las aplicaciones de la forma $x \mapsto u(x) + b$, donde $u \in \mathrm{GL}(V)$ y $b \in V$) forman también un grupo, llamado el **grupo general afín**, denotado $\mathrm{GA}(V)$.
6. Más generalmente, si A es un anillo conmutativo, podemos formar el grupo $\mathrm{GL}_n(A)$ de matrices inversibles de tamaño $n \times n$ con coeficientes en A, el cual está formado[(1)] por las matrices cuyo determinante pertenece a $A^\times$. Por ejemplo, el grupo $\mathrm{GL}_n(\mathbb{Z})$ está constituído por matrices de tamaño $n \times n$ con coeficientes enteros y determinante ± 1.

Ejercicio 2.1.5. — Sea G un grupo tal que $g^2 = e$ para todo $g \in G$. Mostrar que G es abeliano.

Ejercicio 2.1.6. — Mostrar que $\mathrm{GL}_n(\mathbb{Q})$ es denso en $\mathrm{GL}_n(\mathbb{R})$.

2.1.2. Sub-grupos y generadores. — Un subconjunto H de un grupo G es llamado un **sub-grupo**, en cuyo caso escribiremos $H \leq G$ (y $H < G$ o bien $H \lneq G$ si además $H \neq G$), si la ley de composición interna de G se restringe a H dotándolo de estructura de grupo, lo que equivale a las siguientes propiedades:

1. $e \in H$;
2. para todos $h_1, h_2 \in H$, tenemos que $h_1 h_2 \in H$;
3. para todo $h \in H$, tenemos que $h^{-1} \in H$.

Ejemplo 2.1.7. —

1. La intersección de una familia arbitraria de sub-grupos de un grupo G es un sub-grupo de G.

(1) Si una matriz M admite una inversa M^{-1} con coeficientes en A, al tomar determinantes en la fórmula $M \cdot M^{-1} = I_n$, la relación $\det(M)\det(M^{-1}) = 1$ implica que $\det(M)$ es invertible en A. Recíprocamente, si $\det(M)$ es invertible en A, la fórmula $M \cdot {}^{\mathrm{t}}\mathrm{com}(M) = \det(M) I_n$ implica que M admite una inversa con coeficientes en A.

2. Los sub-grupos de $\mathbb{Z}$ son de la forma $n\mathbb{Z}$ para $n \in \mathbb{Z}$.
3. El **grupo ortogonal** $O_n(\mathbb{R})$ de matrices M de tamaño $n \times n$ reales ortogonales (es decir, que satisfacen $M\,{}^{\mathrm{t}}M = I_n$ es un sub-grupo de $\mathrm{GL}_n(\mathbb{R})$.
4. Sea n un entero ≥ 2. El **grupo diedral** D_n de transformaciones ortogonales de $\mathbb{R}^2$ preservando los vértices de un polígono regular de n lados centrado en el origen es un sub-grupo de orden $2n$ de $O_2(\mathbb{R})$. En efecto, si r es la rotación de ángulo $\frac{2\pi}{n}$ y s es la simetría respecto a una recta pasando por el origen y uno de los vértices, entonces
$$D_n = \{e = \mathrm{I}_2, r, \ldots, r^{n-1}, s, rs, \ldots, r^{n-1}s\},$$
donde $rsrs = e$. Podemos ver también D_n como un sub-grupo del grupo $\mathfrak{S}_n$ ya que sus elementos permutan los n vértices del polígono.
5. El **centro**
$$Z(G) = \{h \in G \mid \forall g \in G,\ gh = hg\}$$
de un grupo G es un sub-grupo de G. Un grupo G es abeliano si y solamente si $Z(G) = G$. Por ejemplo, se puede probar que el centro de $\mathrm{GL}_n(k)$ está formado por homotecias, es decir, matrices de la forma $\lambda\,\mathrm{I}_n$ para cierto $\lambda \in k^\times$.

Ejercicio 2.1.8. — Calcular el centro del grupo diedral D_n.

Ejercicio 2.1.9. — Calcular el centro del grupo simétrico $\mathfrak{S}_n$.

Proposición 2.1.10. — *Sea A un sub-conjunto de un grupo G. Entonces, existe un sub-grupo de G conteniendo a A el cual es minimal respecto a la inclusión (es decir, el más pequeño posible). Dicho sub-grupo es llamado el* **sub-grupo generado por** *A y lo denotamos por $\langle A \rangle$.*

Demostración. — Una forma de definir $\langle A \rangle$ es via la intersección de todos los sub-grupos conteniendo A:
$$\langle A \rangle = \bigcap_{A \subset H} H$$
donde el índice H recorre todos los sub-grupos de G (usar el Ejemplo 2.1.7 (1) para verificar que $\langle A \rangle$ es efectivamente un sub-grupo). De manera equivalente, podemos construir $\langle A \rangle$ explícitamente como
$$\langle A \rangle = \{x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_n^{\varepsilon_n} \mid n \in \mathbb{N}, x_i \in A, \varepsilon \in \{-1, 1\}\}.$$
□

Un sub-conjunto A de un grupo G es un **conjunto generador** de G (o bien, **genera** G; o bien, es un **conjunto de generadores** de G) si $\langle A \rangle = G$. Diremos que G es **de tipo finito** (o **finitamente generado**) si admite un conjunto de generadores finito. Todo grupo finito es obviamente un grupo de tipo finito.

¡Atención! — Un sub-grupo de un grupo de tipo finito no es necesariamente de tipo finito (ver Ejercicio 2.1.14).

Ejemplo 2.1.11. —

1. Sea $n \in \mathbb{N}^{\geq 1}$. El grupo $\mathbb{Z}/n\mathbb{Z}$ es generado por la clase de equivalencia de cualquier entero relativamente primo a n.
2. Los siguientes tres conjuntos generan al grupo simétrico $\mathfrak{S}_n$:
   - todas las transposiciones;
   - las transposiciones $(1,2), (2,3), \ldots, ((n-1), n)$;
   - la transposición $(1,2)$ y el ciclo $(2,3,\ldots,n,1)$.
3. Con las notaciones precedentes, el grupo diedral D_n es generado por la rotación r y la simetría s.

Ejercicio 2.1.12. — Demostrar que un grupo de tipo finito es numerable.

Ejercicio 2.1.13. — Demostrar que el grupo $(\mathbb{Q}, +)$ no es de tipo finito.

Ejercicio 2.1.14. — Sea G el grupo (de tipo finito) de $\mathrm{GL}_2(\mathbb{Q})$ generado por las matrices

$$\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \text{ y } \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Demostrar que el sub-grupo de G formado por los elementos de G cuyos coeficientes en la diagonal son todos iguales a 1 no es de tipo finito.

2.1.3. Morfismos de grupos. — Un **morfismo de grupos** (u **homomorfismo**) es una aplicación $f : G \to G'$ entre grupos, tal que

$$\forall g_1, g_2 \in G \quad f(g_1 g_2) = f(g_1) f(g_2).$$

Si f es biyectiva, se deja como ejercicio al lector verificar que la función inversa f^{-1} también es un morfismo de grupos, en cuyo caso decimos que f es un **isomorfismo**. Si $G = G'$ entonces un morfismo $f : G \to G$ es llamado un **endomorfismo** y un isomorfismo $f : G \to G$ es llamado un **automorfismo**.

Si $f : G \to G'$ es un morfismo de grupos, el **kernel** y la **imagen** de f

$$\ker(f) = \{g \in G \mid f(g) = e\}, \quad \mathrm{Im}(f) = \{f(g) \mid g \in G\}$$

son sub-grupos de G y G', respectivamente.

Ejercicio 2.1.15. — Sea $f : G \to G$ un morfismo de grupos. Demostrar que la imagen inversa por f de todo sub-grupo de G' es un sub-grupo de G, y la imagen por f de todo sub-grupo de G es un sub-grupo de G'.

Un morfismo f es injectivo si y solamente si $\ker(f) = \{e\}$; el es sobreyectivo si y solamente si $\mathrm{Im}(f) = G'$.

Ejemplo 2.1.16. —

1. Sea $n \in \mathbb{N}^{\geq 1}$. La proyección canónica $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ es un morfismo sobreyectivo. Su kernel es el sub-grupo $n\mathbb{Z}$.
2. La signatura $\varepsilon : \mathfrak{S}_n \to \{\pm 1\}$ es un morfismo de grupos, sobreyectivo cuando $n \geq 2$. El kernel de dicho morfismo es llamado el **grupo alternante** $\mathfrak{A}_n$. No es difícil verificar (c.f. Teorema 2.5.5) que $\mathfrak{A}_n$ está generado por los 3-ciclos (a, b, c) ya que $(a, b)(a, c) = (a, c, b)$ y $(a, b)(c, d) = (a, c, b)(a, c, d)$.
3. La función exponencial $\exp : (\mathbb{C}, +) \to (\mathbb{C}^\times, \times)$ es un morfismo sobreyectivo. Su kernel es el sub-grupo $2\pi i\mathbb{Z}$ de $\mathbb{C}$.
4. Sea k un cuerpo. El determinante $\det : \mathrm{GL}_n(k) \to k^\times$ es un morfismo sobreyectivo. Su kernel es el **grupo especial lineal** de matrices de determinante 1; es denotado $\mathrm{SL}_n(k)$.
5. El conjunto formado por todos los automorfimos de un grupo, dotado de la ley de composición de funciones, es un grupo que denotamos $\mathrm{Aut}(G)$. Dado $g \in G$, la aplicación
$$\begin{aligned} \iota_g : G &\longrightarrow G \\ x &\longmapsto gxg^{-1} \end{aligned}$$
es un automorfismo de G. Un automorfismo de G de dicha forma es llamado un **automorfismo interno** de G, y $\iota : G \to \mathrm{Aut}(G)$, dado por $g \mapsto \iota_g$, es un morfimo de grupos cuyo núcleo es el centro $Z(G)$.

2.1.4. Clases laterales. — Sea H un sub-grupo de un grupo G. Definimos sobre G la relación de equivalencia $\mathscr{R}$ de la forma siguiente:
$$g_1 \mathscr{R} g_2 \Leftrightarrow \exists h \in H,\ g_2 = g_1 h.$$
Podemos verificar facilmente que $\mathscr{R}$ es efectivamente una relación de equivalencia (es decir, es reflexiva, simétrica y transitiva). La clase de equivalencia de un elemento $g \in G$ está dada por $gH := \{gh \mid h \in H\}$. Los sub-conjuntos gH (para $g \in G$) son llamados **clases laterales izquierdas** de G, y el conjunto

cociente de G por $\mathscr{R}$ (es decir, el conjunto cuyos elementos son las clases laterales izquierda) es denotado G/H. El cardinal del conjunto G/H es denotado $[G : H]$ y es llamado el **índice** de H en G.

Podemos definir también las **clases laterales derechas** $Hg := \{hg \mid h \in H\}$ para $g \in G$, y el respectivo conjunto cociente (es decir, el conjunto cuyos elementos son las clases laterales derechas) es denotado $H\backslash G$.

Es importante remarcar que, afortunadamente, es indiferente de trabajar con clases laterales izquierdas o derechas. En efecto, la aplicación inversa $\Phi : G \to G$, $g \mapsto g^{-1}$ envía gH en Hg^{-1}. Por ende, induce una biyección

$$G/H \longrightarrow H\backslash G.$$

Además, dado $g \in G$ la aplicación $H \to G$ dada por $h \mapsto gh$ induce una biyección

$$H \longrightarrow gH.$$

En particular, si H es finito, el cardinal de una clase lateral izquierda gH es igual al orden de H. Las clases laterales izquierdas forman por ende una partición del conjunto G, todas del mismo cardinal $|H|$. Dado que el cardinal del conjunto de clases laterales es por definición $[G : H]$, podemos deducir fácilmente el siguiente resultado.

***Teorema 2.1.17* (Teorema de Lagrange).** — *Sea H un sub-grupo de un grupo finito G. Entonces*

$$|G| = |H|[G : H].$$

En particular, el orden de un sub-grupo de G divide el orden de G.

Ejercicio 2.1.18. — Sea G un grupo de tipo finito y sea H un sub-grupo de índice finito de G. Demostrar que H es de tipo finito.
Indicación: Si $a_1, \ldots, a_m$ generan G, y si $g_1H, \ldots, g_nH$ son todas las clases laterales izquierdas, donde $g_1 = e$, demostrar que el conjunto finito $H \cap \{g_i^{-1}a_k g_j \mid 1 \leq k \leq m, 1 \leq i, j \leq n\}$ genera H.

2.1.5. Sub-grupos normales. — Diremos que un sub-grupo H de un grupo G es un **sub-grupo normal**, en cuyo caso denotaremos $H \trianglelefteq G$ (y $H \triangleleft G$ o bien $H \trianglelefteq G$ si además $H \neq G$), si dicho sub-grupo es estable por todos los automorfismos internos de G, es decir, si

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

Para todo grupo G, los sub-grupos $\{e\}$ y G de G son sub-grupos normales. El grupo G es llamado **simple** si G no posee otros sub-grupos normales y si $G \neq \{e\}$.

Si $f : G \to G'$ es un morfismo de grupos entonces $\ker(f) \trianglelefteq G$. Sin embargo, en general la imagen de f no es un sub-grupo normal de G'.

Ejercicio 2.1.19. — Sea $f : G \to G'$ un morfismo de grupos. Probar que si $H' \trianglelefteq G'$ entonces $f^{-1}(H') \trianglelefteq G$.

Es importante remarcar que si H es un sub-grupo normal de G, entonces las clases laterales izquierdas y derechas respecto a H coinciden. En efecto, para todo $g \in G$ tenemos que $gH = Hg$ ya que $gHg^{-1} = H$ y por ende $G/H = H\backslash G$. Dejamos como ejercicio al lector verificar que el recíproco es cierto: si H es un sub-grupo de G tal que $G/H = H\backslash G$, entonces H es un sub-grupo normal de G.

Ejemplo 2.1.20. —

1. Todos los sub-grupos de un grupo abeliano son normales.
2. El grupo alternante $\mathfrak{A}_n$ es normal en el grupo $\mathfrak{S}_n$, ya que es el kernel del morfismo signatura. Por lo tanto, $\mathfrak{S}_n$ no es simple para $n \geq 3$.
3. Si k es un cuerpo, el sub-grupo $\mathrm{SL}_n(k)$ de $\mathrm{GL}_n(k)$ es normal, ya que es el kernel del morfismo determinante.

Ejercicio 2.1.21. — Sea G un grupo y sea H un sub-grupo de G de índice 2. Demostrar que H es normal en G.

Ejercicio 2.1.22. — Sea G un grupo y sea $\{H_i\}_{i\in I}$ una familia arbitraria de sub-grupos normales de G. Probar que la intersección $\cap_{i\in I} H_i$ es un sub-grupo normal de G.

2.1.6. Cocientes. — Sea H un sub-grupo de un grupo G. Nos gustaría dotar al conjunto G/H de una estructura de grupo de tal suerte que la aplicación (sobreyectiva)

$$\begin{aligned} p : G &\longrightarrow G/H \\ g &\longmapsto gH \end{aligned}$$

que envía un elemento g en su clase lateral izquierda gH sea un morfismo de grupos. En este caso, el elemento neutro de G/H tiene que ser necesariamente $p(e) = eH$, y por ende el kernel de p debe estar dado por la clase lateral de e, es decir, H. Concluímos así que $\ker(p) = H$ debe ser normal en G (condición necesaria). El resultado siguiente nos muestra que esta condición es además suficiente.

Teorema 2.1.23. — *Si H es un sub-grupo normal de G, entonces G/H puede ser dotado de una única estructura de grupo de tal suerte que la aplicación sobreyectiva $p : G \to G/H$ sea un morfismo de grupos.*

Demostración. — Para que p sea un morfismo de grupos, es necesario que la ley de composición interna de G/H satisfaga

$$(g_1H)(g_2H) = g_1g_2H.$$

Lo primero que debemos hacer es verificar que la fórmula anterior no depende de la elección de g_1 y g_2 en sus clases laterales: si escribimos $g_1 = g_1'h_1$ y $g_2 = g_2'h_2$, entonces

$$g_1g_2 = g_1'h_1g_2'h_2 = g_1'g_2'(g_2'^{-1}h_1g_2')h_2.$$

Dado que H es un sub-grupo normal en G, tenemos que $g_2'^{-1}h_1g_2' \in H$ y por ende $g_1g_2H = g_1'g_2'H$. La fórmula anterior define por lo tanto una ley de composición interna sobre G/H. Podemos verificar fácilmente que es en efecto una ley de grupo. □

¡Atención! — Sea $H \trianglelefteq G$ sub-grupo normal y sea $p : G \to G/H$ la **proyección canónica**. Podemos verificar que las aplicaciones

$$\begin{aligned} \{\text{sub-grupos de } G/H\} &\longrightarrow \{\text{sub-grupos de } G \text{ que contienen } H\} \\ K' &\longmapsto p^{-1}(K') \\ p(K) &\longmapsto K \end{aligned}$$

son biyecciones y son inversas una de la otra. Además, K' es un sub-grupo normal de G/H si y solamente si $p^{-1}(K')$ es un sub-grupo normal de G.

Ejemplo 2.1.24 **(Grupos abelianos simples).** — El grupo $\mathbb{Z}/n\mathbb{Z}$ es el grupo cociente de $\mathbb{Z}$ por $n\mathbb{Z}$. Podemos deducir por ende los sub-grupos de $\mathbb{Z}/n\mathbb{Z}$ ya que su imagen inversa por la proyección canónica $p : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ es un sub-grupo de $\mathbb{Z}$ que contiene a $n\mathbb{Z}$, es decir, un sub-grupo de la forma $d\mathbb{Z}$ con $d \mid n$. Luego, los sub-grupos de $\mathbb{Z}/n\mathbb{Z}$ son exactamente los sub-grupos cíclicos generados por clases de enteros d tales que $d \mid n$. En particular, el grupo $\mathbb{Z}/n\mathbb{Z}$ es simple si y solamente si n es un número primo.

El siguiente resultado, llamado la **propiedad universal** del cociente, permite caracterizar al cociente y a la proyección canónica.

Teorema 2.1.25 **(Propiedad universal).** — *Sea G un grupo, sea $H \trianglelefteq G$ un sub-grupo normal y sea $f : G \to G'$ un morfismo de grupos. Si $H \subseteq \ker(f)$,*

entonces existe un único morfismo $\widehat{f} : G/H \to G'$ *tal que* $f = \widehat{f} \circ p$*, es decir, tal que el diagrama siguiente es conmutativo*

$$\begin{array}{ccc} G & \xrightarrow{f} & G' \\ {\scriptstyle p}\downarrow & \nearrow_{\exists!\widehat{f}} & \\ G/H & & \end{array}$$

Además, $\ker(\widehat{f}) = \ker(f)/H$ *y* $\mathrm{Im}(\widehat{f}) = \mathrm{Im}(f)$.

Demostración. — Nos gustaría definir $\widehat{f}(gH) := f(g)$. Esta fórmula tiene sentido siempre que $f(gh) = f(g)$ para todo $h \in H$, es decir, $f(h) = e$ para todo $h \in H$. Lo anterior es exactamente la condición $H \subseteq \ker(f)$. La aplicación $\widehat{f} : G/H \to G'$ definida de esta forma es claramente única. Verificamos que es un morfismo de grupos, con las imagenes y kernels mencionados. □

Corolario 2.1.26. — *Si* $f : G \to G'$ *es un morfismo de grupos, entonces* $\widehat{f} : G/\ker(f) \to \mathrm{Im}(f)$ *es un isomorfismo.*

Demostración. — Aplicamos el teorema anterior a $\widetilde{f} : G \to \mathrm{Im}(f)$, la cual coincide con f pero hemos restringido el conjunto de llegada, y al sub-grupo normal $H = \ker(f)$. Obtenemos entonces $\widehat{f} : G/\ker(f) \to \mathrm{Im}(f)$, donde $\ker(\widehat{f}) = \ker(f)/\ker(f) = \{e\}$ y $\mathrm{Im}(\widehat{f}) = \mathrm{Im}(\widetilde{f}) = \mathrm{Im}(f)$. □

Corolario 2.1.27. — *El sub-grupo* $\langle g \rangle$ *generado por un elemento* g *de un grupo* G *es isomorfo a* $\mathbb{Z}$ *si es infinito, o bien a* $\mathbb{Z}/n\mathbb{Z}$ *con* $n \in \mathbb{N}^{\geq 1}$ *si es finito. El entero* n *es llamado el* **orden** *del elemento* g*, y es denotado* $\mathrm{ord}(g)$.

Observación 2.1.28. — El Corolario 2.1.27 y el Teorema de Lagrange, implican que el orden de un elemento de un grupo finito G divide al orden del grupo G, es decir, $\mathrm{ord}(g) \mid |G|$ para todo $g \in G$. En particular, todo grupo de orden un número primo p es necesariamente isomorfo al grupo cíclico $\mathbb{Z}/p\mathbb{Z}$.

Demostración del Corolario 2.1.27. — El morfismo

$$\begin{aligned} \Phi_g : \mathbb{Z} &\longrightarrow G \\ n &\longmapsto g^n \end{aligned}$$

tiene por imagen $\langle g \rangle$. Si Φ_g es inyectivo entonces el induce un isomorfismo sobre su imagen $\mathbb{Z} \xrightarrow{\sim} \langle g \rangle$. Si Φ_g no es inyectivo, su kernel es un sub-grupo $n\mathbb{Z}$ de $\mathbb{Z}$ para cierto $n \in \mathbb{N}^{\geq 1}$, en cuyo caso Φ_g induce, por el corolario anterior, un isomorfismo $\widehat{\Phi}_g : \mathbb{Z}/n\mathbb{Z} \xrightarrow{\sim} \langle g \rangle$. □

Veamos algunos ejemplos explícitos de sub-grupos normales y cocientes.

Ejemplo 2.1.29. —

1. Existe un isomorfismo $\mathfrak{S}_n/\mathfrak{A}_n \cong \mathbb{Z}/2\mathbb{Z}$ inducido por el morfimo signatura (de manera alternativa, podemos observar que este grupo cociente tiene dos elementos y por lo tanto es necesariamente isomorfo a $\mathbb{Z}/2\mathbb{Z}$).
2. La restricción del morfismo determinante al grupo diedral $D_n < O_2(\mathbb{R})$ induce un morfismo sobreyectivo $D_n \to \{\pm 1\}$. El kernel de dicho morfismo es el sub-grupo de D_n generado por la rotación r. Es un sub-grupo de índice 2 y es isomorfo a $\mathbb{Z}/n\mathbb{Z}$.
3. El morfismo $\iota : G \to \mathrm{Aut}(G)$ definido por $\iota(g)(x) = gxg^{-1}$ tiene como kernel al centro $Z(G)$ y como imagen al sub-grupo $\mathrm{Int}(G)$ de automorfismos internos de G, por lo cual $\mathrm{Int}(G) \cong G/Z(G)$.
4. El grupo $\mathrm{Int}(G)$ de automorfismos interiores de G es un sub-grupo normal de $\mathrm{Aut}(G)$. El grupo cociente $\mathrm{Out}(G) := \mathrm{Aut}(G)/\mathrm{Int}(G)$ es llamado el grupo de **automorfismos exteriores** de G.

Proposición 2.1.30. — *Sea G un grupo y sea H un sub-grupo normal de G.*

1. *Si G es de tipo finito, G/H también es de tipo finito*[(2)].
2. *Si H y G/H son de tipo finito, entonces G es de tipo finito.*

Demostración. — Para probar (1) basta notar que la imagen en G/H de un conjunto generador finito de G es un conjunto generador finito de G/H.

Para probar (2) consideramos A un sub-conjunto finito de G de tal suerte que la imagen en G/H genera G/H, y consideramos B un sub-conjunto finito generador de H. Sea $x \in G$. Su clase en G/H se escribe como

$$\overline{x} = \overline{x}_1^{\varepsilon_1} \cdots \overline{x}_m^{\varepsilon_m} = \overline{x_1^{\varepsilon_1} \cdots x_m^{\varepsilon_m}},$$

donde $\varepsilon_1, \ldots, \varepsilon_m \in \{-1, 1\}$ y $x_1, \ldots, x_m \in A$. Por ende,

$$x_m^{-\varepsilon_m} \cdots x_1^{-\varepsilon_1} x \in H.$$

Por otro lado,

$$x_m^{-\varepsilon_m} \cdots x_1^{-\varepsilon_1} x = y_1^{s_1} \cdots y_n^{s_n},$$

donde $s_1, \ldots, s_n \in \{-1, 1\}$ y $y_1, \ldots, y_n \in B$. Deducimos entonces que

$$x = x_1^{\varepsilon_1} \cdots x_m^{\varepsilon_m} y_1^{s_1} \cdots y_n^{s_n},$$

de donde concluimos que $A \cup B$ es un conjunto finito que genera G, de donde obtenemos (2). □

(2) Ya vimos en el Ejercicio 2.1.14 que H no es necesariamente de tipo finito.

Ejercicio 2.1.31. — Sea $\mathbb{F}_q$ un cuerpo finito de q elementos. Demostrar que

$$|\operatorname{GL}_n(\mathbb{F}_q)| = (q^n-1)(q^n-q)\cdots(q^n-q^{n-1}),$$
$$|\operatorname{SL}_n(\mathbb{F}_q)| = (q^n-1)(q^n-q)\cdots(q^n-q^{n-2})q^{n-1}.$$

Ejercicio 2.1.32. — Recordemos que $\operatorname{GL}_n(\mathbb{Z})$ es el grupo de matrices de tamaño $n \times n$ con coeficientes enteros y determinante ± 1.

a) Demostrar que los elementos de $\operatorname{GL}_2(\mathbb{Z})$ de orden finito son de orden $1, 2, 3, 4$ o 6. *Indicación: considerar los valores propios de matrices de orden finito.*

b)* Determinar una función $f : \mathbb{N} \to \mathbb{N}$ de tal suerte que los elementos de $\operatorname{GL}_n(\mathbb{Z})$ de orden finito son de orden $\leq f(n)$.

Ejercicio 2.1.33. — Sean K y H sub-grupos normales de un grupo G de tal suerte que $K \leq H$. Demostrar que el sub-grupo H/K de G/K es normal y que $(G/K)/(H/K) \cong G/H$.

Ejercicio 2.1.34. — Sean H y K sub-grupos de un grupo G de tal suerte que $H \trianglelefteq G$. Demostrar que

$$HK := \{hk \mid h \in H, k \in K\}$$

es un sub-grupo de G, que $HK = KH = HKH$, que $H \cap K$ es un sub-grupo normal de K, y que los grupos HK/H y $K/(H \cap K)$ son isomorfos.

Ejercicio 2.1.35. — Sea k un cuerpo y sea V un k-espacio vectorial. Demostrar que el grupo de traslaciones de V es un sub-grupo normal del grupo afín $\operatorname{GA}(V)$ isomorfo al grupo aditivo (abeliano) $(V, +)$ y que el grupo cociente es isomorfo a $\operatorname{GL}(V)$.

Ejercicio 2.1.36. — El objetivo de este ejercicio es demostrar que todo sub-grupo finito G del grupo multiplicativo de un cuerpo k es cíclico. En particular,

1. El grupo multiplicativo $(k^\times, \cdot)$ de un cuerpo finito k es cíclico. Luego, $\mathbb{F}_p^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$.
2. Todo sub-grupo finito del círculo unitaro $\mathbb{S}^1 = \{z \in \mathbb{C} \mid |z| = 1\}$ (visto como grupo multiplicativo), es cíclico.

La única propiedad que utilizaremos es el hecho que la ecuación $x^n = 1$ tiene a lo más n soluciones en k. Sea g un elemento de G de orden maximal d y sea h un elemento arbitrario de G, de orden e.

a) Supongamos que e *no divide* a d, es decir, $e \nmid d$. Existe por ende un entero positivo $q = p^\alpha$, potencia de un número primo p, que divide a e pero no a d. Sea r el orden del elemento $gh^{e/q}$. Demostrar que q divide al mínimo

común múltiplo $\mathrm{mcm}(d,r)$, que r es divisible por $\mathrm{mcm}(d,r)$, y obtener una contradicción. Para esto último, calcular $(h^{er/q})^{d/\,\mathrm{mcd}(d,r)}$.

b) Tenemos por lo tanto que $e \mid d$. Deducir que g genera G y luego $G \cong \mathbb{Z}/d\mathbb{Z}$.

2.1.7. Cocientes de espacios vectoriales. — Si V es un k-espacio vectorial y $W \subseteq V$ es un sub-espacio vectorial, entonces en particular (gracias a la estructura de grupo abeliano), W es un sub-grupo normal de V y podemos por ende considerar el grupo cociente V/W. En este caso, la estructura de k-espacio vectorial es heredada al cociente: definiendo para $x \in V$ la multiplicación por $\lambda \in k$ como $\lambda(x+W) := (\lambda x)+W$. En efecto, si consideramos otro representante y de la clase de x en V/W entonces $y = x+w$, con $w \in W$, y luego $\lambda y = \lambda x + \lambda w$. Este último elemento representa la clase de $\lambda x + W \in V/W$ ya que $\lambda w \in W$. El morfismo sobreyectivo

$$p : V \longrightarrow V/W$$

es una transformación lineal con kernel W y la propiedad universal del cociente (Teorema 2.1.25) sigue siendo válida al reemplazar morfismos de grupos por transformaciones lineales: si $\phi : V \to V'$ es una transformación lineal tal que $W \subseteq \ker\phi$, ella se factoriza de manera única a través de una transformación lineal $\widehat{\phi} : V/W \to V'$ que satisface $\phi = \widehat{\phi} \circ p$. Al igual que antes, esta propiedad caracteriza al cociente y a la proyección canónica $p : V \longrightarrow V/W$.

Si escogemos un sub-espacio W' de V de tal suerte que $V = W \oplus W'$, la restricción $p|_{W'} : W' \to V/W$ es un isomorfismo lineal. A través de este isomorfismo, la transformación lineal inducida por la propiedad universal, $\widehat{\phi}$, puede ser identificada con la restricción $\phi|_{W'}$. Sin embargo, esto *no es intrínseco*, puesto que el sub-espacio W' no es único.

Vale la pena destacar que esta propiedad es particular a los espacios vectoriales: en el caso de grupos, si $H \trianglelefteq G$, en general no es cierto que G es isomorfo al producto $H \times (G/H)$ (ver Ejemplo 2.1.29 (2)).

2.2. Acciones de grupos

2.2.1. Acción de un grupo sobre un conjunto. — Una **acción** (izquierda[3]) de un grupo G sobre un conjunto X es una aplicación

$$\begin{aligned} G \times X &\longrightarrow X \\ (g, x) &\longmapsto g \cdot x \end{aligned}$$

tal que

1. para todo $x \in X$, tenemos que $e \cdot x = x$;
2. para todos $x \in X$ y $g_1, g_2 \in G$, tenemos que $g_1 \cdot (g_2 \cdot x) = (g_1 g_2) \cdot x$.

Si definimos $\Phi_g(x) = g \cdot x$, entonces la definición anterior implica que

$$\Phi_e = \mathrm{Id}_X, \ \Phi_{g_1} \circ \Phi_{g_2} = \Phi_{g_1 g_2}.$$

Por ende, la acción de un grupo G sobre un conjunto X es exactamente la misma cosa que un morfismo de grupos

$$\begin{aligned} \Phi : G &\longrightarrow \mathrm{Biy}(X) \\ g &\longmapsto \Phi_g \end{aligned}$$

donde $\mathrm{Biy}(X)$ es el grupo de biyecciones de X.

Ejemplo 2.2.1. —

1. Dado un conjunto X, el grupo $\mathrm{Biy}(X)$ actúa sobre X. En particular, el grupo simétrico $\mathfrak{S}_n$ actúa sobre el conjunto $\{1, \ldots, n\}$.
2. Sea k un cuerpo. El grupo $\mathrm{GL}_n(k)$ actúa sobre k^n.
3. El grupo $\mathrm{SL}_2(\mathbb{R})$ actúa sobre el **semi-plano de Poincaré**
$$\mathscr{H} = \{z \in \mathbb{C} \mid \mathrm{Im}(z) > 0\}$$
mediante
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z := \frac{az + b}{cz + d}.$$
4. Si $H \leq G$, entonces G actúa sobre el conjunto de clases laterales izquierdas G/H mediante $g \cdot (xH) = (gx)H$. En el caso particular donde $H = \{e\}$, obtenemos la acción de G sobre si mismo por traslaciones izquierdas.

[3] A veces es útil considerar una **acción derecha**, denotada $(g, x) \mapsto x \cdot g$, la cual satisface la relación $(x \cdot g) \cdot g' = x \cdot (gg')$. Esto no define una acción izquierda, sino que una acción derecha, denotada $\cdot_d$. Uno puede construir una acción izquierda considerando $g \cdot x := x \cdot_d g^{-1}$.

2.2.2. Órbitas. — Sea G un grupo actuando sobre X. Es fácil verificar que la relación

$$x \mathscr{R} y \Leftrightarrow \exists g \in G \text{ tal que } y = g \cdot x$$

es una relación de equivalencia sobre X. La clase de equivalence de un elemento $x \in X$ es llamada su **órbita**

$$Gx := \{g \cdot x \mid g \in G\},$$

de tal suerte que X es la unión disjunta de órbitas bajo la acción de G. El conjunto de órbitas de X bajo G es llamado es **cociente de X por G**, denotado $G\backslash X$[4].

El **estabilizador** o **grupo de isotropía** de x es el sub-grupo de G definido por

$$G_x := \mathrm{Stab}_G(x) := \{g \in G \mid g \cdot x = x\}.$$

La aplicación

$$\begin{aligned} G &\longrightarrow Gx \\ g &\longmapsto g \cdot x \end{aligned}$$

se factoriza en una *biyección*

$$G/G_x \xrightarrow{\sim} Gx \tag{1}$$

entre el conjunto de clases laterales izquierdas de G_x y la órbita de x. En particular, si G es un grupo finito, el Teorema de Lagrange implica que las órbitas son finitas y que su cardinal divide $|G|$.

Los estabilizadores de puntos en una misma órbita son todos conjugados: para todo $x \in X$ y todo $g \in G$ tenemos que

$$G_{g \cdot x} = g G_x g^{-1}.$$

Diremos que la acción de G es **transitiva** si G posee sólo una órbita en X. En ese caso, la acción de G induce una biyección entre G/G_x y X, para todo $x \in X$. En particular, si G es un grupo finito que actúa transitivamente en X, entonces X es un conjunto finito y su cardinal divide $|G|$.

[4] En esta notación, el grupo se ubica a la izquierda si consideramos una acción izquierda. Para una acción derecha, la órbita de x está en biyección con $G_x\backslash G$ y el cociente es denotado X/G.

La acción de G es **fiel** si la aplicación $\Phi : G \to \mathrm{Biy}(X)$ es inyectiva. En general, Φ se factoriza en

$$\begin{array}{ccc} G & \xrightarrow{\Phi} & \mathrm{Biy}(X) \\ \downarrow & \nearrow_{\widehat{\Phi}} & \\ G/\ker\Phi & & \end{array}$$

De donde obtenemos por lo tanto una acción fiel del grupo cociente $G/\ker\Phi$ sobre X. Así, toda acción se factoriza en una acción fiel.

Ejemplo 2.2.2. —

1. Sea k un cuerpo. Para todo $n \geq 1$, la acción de $\mathrm{GL}_n(k)$ sobre k^n es fiel y las órbitas son $k^n \setminus \{0\}$ y $\{0\}$. La acción del grupo afín $\mathrm{GA}_n(k)$ sobre k^n es fiel y transitiva.
2. La acción (fiel) del grupo ortogonal $O_n(\mathbb{R})$ sobre $\mathbb{R}^n$ tiene por órbitas las esferas de radio $r > 0$ y $\{0\}$. El estabilizador de un punto no-nulo es (isomorfo a) $O_{n-1}(\mathbb{R})$ y luego, la biyección (1), permite deducir que $O_n(\mathbb{R})/O_{n-1}(\mathbb{R}) \cong \mathbb{S}^{n-1}$.
3. La acción del grupo $\mathrm{SL}_2(\mathbb{R})$ sobre el semi-plano de Poincaré descrita en Ejemplo 2.2.1 es transitiva. La acción **no** es fiel (su kernel es $\{\pm I_2\}$).
4. Sea k un cuerpo. El grupo $k^\times$ actúa sobre $k^n \setminus \{0\}$ mediante $\lambda \cdot (x_1, \ldots, x_n) = (\lambda x_1, \ldots, \lambda x_n)$, y el cociente es
$$k^\times \backslash (k^n \setminus \{0\}) = \{\text{rectas vectoriales en } k^n\},$$
llamado **espacio proyectivo** sobre k y denotado $\mathbb{P}^{n-1}(k)$.
5. Si $\sigma \in \mathfrak{S}_n$ es una permutación y consideramos la acción del grupo $\langle\sigma\rangle$ sobre el conjunto $\{1, \ldots, n\}$. Entonces $\{1, \ldots, n\}$ es la unión disjunta de órbitas
$$\{1, \ldots, n\} = \bigsqcup_{i=1}^{r} O_i.$$
Podemos definir
$$\sigma_i(x) = \begin{cases} \sigma(x) & \text{si } x \in O_i, \\ x & \text{si } x \notin O_i. \end{cases}$$
Entonces, σ_i es un ciclo de soporte O_i, tenemos que $\sigma_i\sigma_j = \sigma_j\sigma_i$ y
$$\sigma = \sigma_1 \cdots \sigma_r.$$

Hemos demostrado así que toda permutación de descompone (de manera única) como producto de ciclos con soportes disjuntos (y que por ende conmutan).

***Ejemplo 2.2.3* (Teorema de Cayley).** — La acción de G sobre si mismo por traslaciones izquierdas, definida por $g \cdot x := gx$, es una acción fiel. En particular, si G es un grupo finito obtenemos un morfismo inyectivo $G \hookrightarrow \mathfrak{S}_{|G|}$, que depende de la forma en que enumeremos los elementos del conjunto finito G.

Ejercicio 2.2.4. — Sea G un grupo finito de orden n.

a) Demostrar que G es isomorfo a un sub-grupo de $\mathfrak{A}_{2n}$, e inclusive de $\mathfrak{A}_{n+2}$.
b) Sea k un cuerpo. Demostrar que G es isomorfo a un sub-grupo de $\mathrm{GL}_n(k)$ y a un sub-grupo de $\mathrm{SL}_{n+1}(k)$.
c) Demostrar que G es isomorfo a un sub-grupo de $O_{n-1}(\mathbb{R})$.

Ejercicio 2.2.5. — Sea G un grupo finito de orden $2n$, con n impar.

a) Demostrar que G contiene un elemento de orden 2.
Indicación: contar el número de pares (g, g^{-1}).
b) Demostrar que la imagen del morfismo inyectivo $G \hookrightarrow \mathfrak{S}_{2n}$ dado por el teorema de Cayley (Ejemplo 2.2.3) no está contenida en $\mathfrak{A}_{2n}$.
c) Deducir que G contiene un sub-grupo normal de índice 2.

Ejercicio 2.2.6. — Sea G un grupo actuando fiel y transitivamente sobre un conjunto X de cardinal p, donde p es un número primo, y sea $H \trianglelefteq G$ un sub-grupo normal tal que $H \neq \{e\}$. Demostrar que H actúa transitivamente sobre X.

Ejercicio 2.2.7. — Sea G un sub-grupo de $\mathfrak{S}_n$ actuando transitivamente sobre el conjunto $\{1, \ldots, n\}$, conteniendo una transposición y un p-ciclo, donde p es un número primo $> n/2$. El objetivo de este ejercicio es demostrar que $G = \mathfrak{S}_n$.

Si $a, b \in \{1, \ldots, n\}$, escribimos $a \sim b$ si $a = b$ o si $a \neq b$ y la transposición (a, b) está contenida en G.

a) Demostrar que $\sim$ es una relación de equivalencia sobre el conjunto $\{1, \ldots, n\}$.
b) Si $a \sim b$ y $g \in G$, demostrar que $g(a) \sim g(b)$.
c) Demostrar que todas las clases de equivalencia respecto a $\sim$ tienen el mismo cardinal r y que $r \geq 2$.

d) Sea s el número de clases de equivalencia respecto a $\sim$. Demostrar que $n = rs$ y $r \geq p$. Concluir.

2.2.3. Conjugación. — Existe otra acción natural de G sobre sí mismo, dada por el morfismo $G \to \mathrm{Aut}(G)$ definido por $g \cdot x = gxg^{-1}$, llamada la acción por **conjugación**. En este caso, el estabilizador de un elemento $x \in G$ es llamado el **centralizador** de x y es denotado por $C(x)$. Las órbitas son llamadas **clases de conjugación** de G.

En el caso del grupo simétrico tenemos el siguiente resultado.

Proposición 2.2.8. — *Si $\sigma = (a_1 \cdots a_k) \in \mathfrak{S}_n$ es un k-ciclo y $\tau \in \mathfrak{S}_n$, entonces*

$$\tau\sigma\tau^{-1} = (\tau(a_1) \cdots \tau(a_k)). \tag{2}$$

Por ende, todos los k-ciclos son conjugados en $\mathfrak{S}_n$. Más aún, las clases de conjugación de $\mathfrak{S}_n$ están en biyección con las particiones de n:

$$n = k_1 + \cdots + k_r,\ r \in \mathbb{N},\ 1 \leq k_1 \leq \cdots \leq k_r.$$

Demostración. — Si $x \notin \{\tau(a_1), \ldots, \tau(a_k)\}$, entonces $\tau^{-1}(x) \notin \{a_1, \ldots, a_k\}$ y por lo tanto $\tau\sigma\tau^{-1}(x) = x$. Por otro lado, si $x = \tau(a_i)$ entonces $\tau\sigma\tau^{-1}(x) = \tau\sigma(a_i) = \tau(a_{i+1})$. Esto demuestra la primera parte de la proposición.

Para la segunda parte, escribamos $\sigma = \sigma_1 \cdots \sigma_r$ como producto de ciclos con soportes disjuntos de largos $k_1, \ldots, k_r$, los cuales podemos ordenar de tal suerte que $1 \leq k_1 \leq \cdots \leq k_r$. Entonces

$$\tau\sigma\tau^{-1} = (\tau\sigma_1\tau^{-1}) \cdots (\tau\sigma_r\tau^{-1}) \tag{3}$$

es también un producto de ciclos con soportes disjuntos de mismos largos $k_1, \ldots, k_r$, y por ende una clase de conjugación determina una partición de $n = k_1 + \ldots + k_r$. Recíprocamente, dadas las fórmulas (2) y (3), podemos verificar que permutaciones correspondientes a la misma partición son conjugadas. □

Ejemplo 2.2.9. —

1. Las 2 particiones de $n = 2$ son $1 + 1$ y 2. Las clases de conjugación correspondientes en $\mathfrak{S}_2$ son $\{\mathrm{id}\}$ y $\{(1, 2)\}$.
2. Las 3 particiones de $n = 3$ son $1 + 1 + 1$, $1 + 2$ y 3. Las clases de conjugación correspondientes en $\mathfrak{S}_3$ son $\{\mathrm{id}\}$, $\{(1, 2), (1, 3), (2, 3)\}$ y $\{(2, 3, 1), (1, 3, 2)\}$.

3. Las 5 particiones de $n = 4$ son $1+1+1+1$, $1+1+2$, $2+2$, $1+3$ y 4. Las clases de conjugación correspondientes en $\mathfrak{S}_4$ son $\{\mathrm{id}\}$, las 6 transposiciones, las 3 dobles transposiciones (producto de dos transposiciones con soportes disjuntos), los 8 3-ciclos y los 6 4-ciclos.

De manera general, la conjungación preserva las propiedades de una transformación. Por ejemplo, si $\sigma \in O_3(\mathbb{R})$ es una rotación respecto a una recta R y $\tau \in O_3(\mathbb{R})$, entonces $\tau\sigma\tau^{-1}$ es una rotación de mismo ángulo pero respecto a la recta $\tau(R)$.

2.2.4. Fórmula de clases y p-grupos. — La fórmula de clases no es nada más que una reformulación del hecho que un conjunto sobre el cual actúa un gurpo G puede ser escrito como la unión disjunta de órbitas. Su principal interés proviene del hecho que, cuando G es un grupo finito, el cardinal de cada órbita divide $|G|$.

***Proposición 2.2.10* (Fórmula de clases).** — *Sea G un grupo finito actuando sobre un conjunto finito X. Entonces*

$$\mathrm{card}(X) = \sum_{x \in R} [G : G_x],$$

donde $R \subseteq X$ es un conjunto que contiene exactamente un punto de cada órbita.

Demostración. — Sabemos que X es la unión disjunta de órbitas y, en virtud de (1), cada órbita está en biyección con G/G_x donde x es un elemento de la órbita correspondiente. □

Un punto $x \in X$ es un **punto fijo de la acción** de G si $g \cdot x = x$ para todo $g \in G$, es decir, si la órbita de x se reduce a $\{x\}$. Denotamos por X^G el **conjunto de puntos fijos** de X bajo la acción de G.

Ejemplo 2.2.11. — Sea k un cuerpo. El grupo $k^\times$ actúa sobre el espacio afín k^n por multiplicación. El origen 0 es el único punto fijo; los otros puntos tienen un estabilizador trivial. Si k es un cuerpo finito $\mathbb{F}_q$ de q elementos, el cardinal de k^n es q^n y la fórmula de clases se reduce a escribir (c.f. Ejemplo 2.2.2 (4))

$$q^n = 1 + (q-1)\,\mathrm{card}(\mathbb{P}^{n-1}(\mathbb{F}_q)).$$

Así, $\mathrm{card}(\mathbb{P}^n(\mathbb{F}_q)) = 1 + q + q^2 + \ldots + q^n$.

***Definición 2.2.12* (p-grupo).** — Sea p un número primo. Un grupo finito G es llamado un **p-grupo** si $|G| = p^n$ para cierto entero positivo $n \in \mathbb{N}^{\geq 1}$.

Proposición 2.2.13. — *Sea G un grupo finito.*

1. *Si un p-grupo G actúa sobre X, entonces*
$$\operatorname{card}(X^G) \equiv \operatorname{card}(X) \mod p.$$
En particular, si p no divide a $\operatorname{card}(X)$ entonces $X^G \neq \emptyset$.
2. *Si G es un p-grupo, el centro $Z(G)$ de G no se reduce al singleton $\{e\}$.*

Demostración. — Si $x \in X^G$ es un punto fijo, entonces la órbita $Gx = \{x\}$ está reducida a un único elemento y luego $[G : G_x] = 1$. Así, la fórmula de clases se reescribe como
$$\operatorname{card}(X) = \sum_{x \in R} [G : G_x] = \operatorname{card}(X^G) + \sum_{x \in R \setminus X^G} [G : G_x].$$
Por otro lado, el teorema de Lagrange implica que $[G : G_x]$ divide a $|G| = p^n$. En particular, si $x \notin X^G$ entonces $[G : G_x] > 1$ y luego p divide a $[G : G_x]$. De lo anterior se concluye que $\operatorname{card}(X) \equiv \operatorname{card}(X^G) \mod p$, y por ende (1).

Para probar (2), consideramos la acción de G sobre sí mismo por conjugación $g \cdot x := gxg^{-1}$. En este caso $X = G$ y se tiene que el conjunto de puntos fijos $X^G = Z(G)$ es el centro del grupo. En particular, el punto (1) implica que $|Z(G)| \equiv |G| \equiv 0 \mod p$, puesto que $|G| = p^n$. Dado que $e \in Z(G)$ se tiene que $|Z(G)| \geq 1$ y luego necesariamente $|Z(G)| \geq p \geq 2$. □

Ejercicio 2.2.14 **(Lema de Cauchy).** — Sea G un grupo finito y p un número primo tal que p divide $|G|$. Considerar la acción de $\mathbb{Z}/p\mathbb{Z}$ sobre el conjunto
$$X = \{(g_1, \ldots, g_p) \in G^p \mid g_1 \cdots g_p = 1\}$$
dado por $k \cdot (g_1, \ldots, g_p) := (g_{1+k}, \ldots, g_{p+k})$, donde los índices pertenecen a $\mathbb{Z}/p\mathbb{Z}$. Usar la fórmula de clases para probar que G posee un elemento de orden p.

Corolario 2.2.15. — *Sea p un número primo y sea G un grupo finito.*

1. *Si $|G| = p^2$ entonces G es abeliano.*
2. *Si G es un p-grupo simple entonces $G \cong \mathbb{Z}/p\mathbb{Z}$.*

Demostración. — Para probar (1) notamos que la Proposición 2.2.13 implica que el orden $|Z(G)|$ es p o p^2. Observemos que para todo $x \in G$ el centralizador $C(x) = \{g \in G \mid gx = xg\}$ contiene $Z(G)$ y $\{x\}$.

Si $x \notin Z(G)$ entonces $|C(x)| \geq |Z(G)| + 1 \geq p + 1$ y luego $|C(x)| = p^2$, pues $|C(x)|$ divide $|G| = p^2$. Luego $C(x) = G$, lo cual equivale a que $x \in Z(G)$, una contradicción.

Así, se tiene que $x \in Z(G)$ para todo $x \in G$. En otras palabras $Z(G) = G$ y luego G es un grupo abeliano.

Para probar (2) notamos que $\{e\} \lneq Z(G) \trianglelefteq G$. Dado que G es simple, se tiene en este caso que $Z(G) = G$ y luego G es un grupo abeliano. Finalmente, sabemos que si G es un grupo abeliano simple entonces $G \cong \mathbb{Z}/p\mathbb{Z}$ (c.f. Ejemplo 2.1.20 (1) y Ejemplo 2.1.24). □

Observación 2.2.16. — Sea p un número primo y sea G un grupo finito. Vimos que si $|G| = p$ entonces $G \cong \mathbb{Z}/p\mathbb{Z}$ (ver Corolario 2.1.27). Veremos más adelante que $|G| = p^2$ implica que $G \cong \mathbb{Z}/p^2\mathbb{Z}$ o bien $G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ (ver Teorema 2.4.9).

2.3. Teoremas de Sylow

Sea G un grupo y sea p un número primo tal que p divide $|G|$. En toda esta sección escribiremos $|G| = p^\alpha m$ con $p \nmid m$, i.e. α es maximal.

***Definición 2.3.1* (p-sub-grupo de Sylow).** — Un **p-sub-grupo de Sylow** de G es un sub-grupo $H \leq G$ de orden maximal $|H| = p^\alpha$.

Ejercicio 2.3.2. — Probar que el sub-grupo $T_n(\mathbb{F}_p)$ de matrices **unipotentes** de la forma

$$\begin{pmatrix} 1 & * & \cdots & \cdots & * \\ 0 & 1 & * & \cdots & * \\ 0 & 0 & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & * \\ 0 & \cdots & 0 & 0 & 1 \end{pmatrix}$$

es un p-sub-grupo de Sylow de $\mathrm{GL}_n(\mathbb{F}_p)$.

El siguiente lema prueba que si un grupo finito contiene un p-sub-grupo de Sylow entonces todos sus sub-grupos también.

Lema 2.3.3. — *Si S es un p-sub-grupo de Sylow de G y $H \leq G$ es un sub-grupo arbitrario, entonces existe $g \in G$ tal que $gSg^{-1} \cap H$ es un p-sub-grupo de Sylow de H.*

Demostración. — El grupo H actúa sobre el conjunto de clases laterales $X = G/S$ mediante $h \cdot (gS) := hgS$. El estabilizador de la clase gS está dado

por

$$H_{gS} = \{h \in H \mid hgS = gS\} = \{h \in H \mid g^{-1}hg \in S\} = gSg^{-1} \cap H.$$

Nótese que $|G/S| = \frac{|G|}{|S|} = \frac{p^\alpha m}{p^\alpha} = m$, por el teorema de Lagrange. Como p no divide a $m = |G/S| = \text{card}(X)$, la fórmula de clases $|G/S| = \sum_{gS \in R}[H : H_{gS}]$ implica que existe una clase gS tal que $p \nmid [H : H_{gS}]$.

Por otro lado, $H_{gS} = gSg^{-1} \cap H \leq gSg^{-1}$ y gSg^{-1} es un p-grupo. Luego, H_{gS} es un p-grupo también. Finalmente, dado que $p \nmid [H : H_{gS}] = \frac{|H|}{|H_{gS}|}$ se tiene que H_{gS} es un p-sub-grupo de Sylow de H. □

Una noción esencial para la demostración del Teorema de Sylow es la de normalizador.

***Definición 2.3.4* (normalizador).** — Sea G un grupo y sea $H \leq G$ un sub-grupo. Definimos el **normalizador** de H en G como

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

Observamos que $H \trianglelefteq G$ si y sólo si $N_G(H) = G$. Más aún, si consideramos la acción de G sobre el conjunto $X = \{H \mid H \leq G\}$ de sub-grupos de G por conjugación $g \cdot H := gHg^{-1}$, entonces $N_G(H)$ coincide con el estabilizador de H respecto a esta acción.

***Teorema 2.3.5* (Sylow, 1872).** — *Sea G un grupo y sea p un número primo tal que p divide $|G|$. Escribamos $|G| = p^\alpha m$ con $p \nmid m$. Entonces*

1. *G contiene un p-sub-grupo de Sylow.*
2. *Todo p-sub-grupo de G está contenido en algún p-sub-grupo de Sylow.*
3. *Todos los p-sub-grupos de Sylow son conjugados en G.*
4. *Sea n_p el número de p-sub-grupos de Sylow de G. Entonces $n_p \mid m$ y $n_p \equiv 1 \mod p$.*

Demostración. — Sea $n := |G|$ el orden de G. Entonces, el teorema de Cayley (Ejemplo 2.2.3) implica que hay un morfismo inyectivo $G \hookrightarrow \mathfrak{S}_n$. Más aún, tenemos un morfismo inyectivo $\mathfrak{S}_n \hookrightarrow \mathrm{GL}_n(\mathbb{F}_p)$, $\sigma \mapsto u_\sigma$ donde u_σ es la matriz de permutación asociada a σ (c.f. Ejercicio 2.2.4 (b)).

Así, G puede ser visto como un sub-grupo de $\mathrm{GL}_n(\mathbb{F}_p)$. Por un lado, el Ejercicio 2.3.2 implica que $\mathrm{GL}_n(\mathbb{F}_p)$ admite un p-sub-grupo de Sylow. Por otro lado, el Lema 2.3.3 implica que G contiene un p-sub-grupo de Sylow, de donde se obtiene (1).

Para probar (2) y (3) consideremos $H \leq G$ un p-sub-grupo y $S \leq G$ un p-sub-grupo de Sylow. El Lema 2.3.3 implica que existe $g \in G$ tal que $gSg^{-1} \cap H$

es un p-sub-grupo de Sylow de H. Dado que H es también un p-grupo, se tiene que $gSg^{-1} \cap H = H$, es decir, $H \leq gSg^{-1}$.

Notar que gSg^{-1} tiene el mismo orden que S y luego gSg^{-1} es un p-sub-grupo de Sylow, de donde se obtiene (2). Si además H es un p-sub-grupo de Sylow, tenemos que $|H| = |gSg^{-1}|$ y $H \leq gSg^{-1}$, de donde se concluye que $H = gSg^{-1}$ y por lo tanto (3).

Para probar (4) consideramos la acción de G en el conjunto

$$X = \{S \mid S \leq G \text{ } p\text{-sub-grupo de Sylow}\}$$

por conjugación $g \cdot S := gSg^{-1}$. Notar que gracias al punto (3) dicha acción es transitiva, y por ende $n_p = \text{card}(X)$ divide $|G|$.

Sea $S \in X$ un p-sub-grupo de Sylow fijo, y restringamos la acción de G en X a una acción de S en X: $s \cdot S' := sS's^{-1}$ para $s \in S$ y $S' \in X$.

Supongamos que $S' \in X^S$, es decir, $sS's^{-1} = S'$ para todo $s \in S$. Entonces $S \leq N_G(S')$ es sub-grupo del normalizador de S' en G. Luego, S y S' son p-sub-grupos de Sylow de $N_G(S')$, los cuales deben ser conjugados en $N_G(S')$ por (3). En otras palabras, existe $g \in N_G(S')$ tal que $gS'g^{-1} = S$. Por otra parte, sabemos que $gS'g^{-1} = S'$ por definición de $N_G(S')$, de donde se concluye que $S = S'$.

En conclusión, $S \in X$ es el único púnto fijo de la acción de S sobre X (i.e, $X^S = \{S\}$). Dado que $\text{card}(X) \equiv \text{card}(X^S) \mod p$ y $\text{card}(X) = n_p$ y $\text{card}(X^S) = 1$, se concluye que $n_p \equiv 1 \mod p$. Finalmente, sabemos que n_p divide $|G| = p^\alpha m$ por lo que se tiene necesariamente que n_p divide m. □

Corolario 2.3.6. — *Un p-sub-grupo de Sylow H de G es normal en G si y sólo si es el único p-sub-grupo de Sylow de G. En otras palabras, $H \trianglelefteq G$ si y sólo si $n_p = 1$.*

Ejemplo 2.3.7. —

1. La demostración del punto (4) muestra que $n_p = [G : N_G(S)]$, donde S es cualquier p-sub-grupo de Sylow de G.
2. El punto (3) junto con el Ejercicio 2.3.2 muestra que todo p-sub-grupo de Sylow de $\text{GL}_n(\mathbb{F}_p)$ está dado, en una base conveniente, por matrices unipotentes.
3. Determinemos el número de p-sub-grupos de Sylow de $\mathfrak{S}_p$. Notar que $|\mathfrak{S}_p| = p! = p(p-1)\cdots 2 \cdot 1$ y luego $S \leq \mathfrak{S}_p$ es un p-sub-grupo de Sylow si y sólo si $|S| = p$. Esto último es a su vez equivalente a que $S = \langle (a_1, \ldots, a_p) \rangle \cong \mathbb{Z}/p\mathbb{Z}$ es un grupo cíclico.

Observar que $a_1 \neq 1$, por lo que hay $p-1$ posibles elecciones para dicho elemento. Una vez escogido a_1, tenemos que $a_2 \neq 2$ y $a_2 \neq a_1$, por lo que hay $p-2$ posibles elecciones para a_2. Continuando de este modo notamos que existen $(p-1)!$ ciclos de largo p en $\mathfrak{S}_p$, los cuales denotamos por $\sigma_1, \sigma_1^2, \ldots, \sigma_1^{p-1}, \sigma_2, \ldots, \sigma_2^{p-1}, \ldots, \sigma_r, \ldots, \sigma_r^{p-1}$.

Finalmente, notamos que $\langle \sigma_i \rangle = \langle \sigma_i^j \rangle$ para todo $j \in \{1, \ldots, p-1\}$ y luego $r = n_p$, por definición. Así $(p-1)n_p = (p-1)!$, de donde se concluye que $n_p = (p-2)!$. Más áun, el Teorema de Sylow implica que $(p-2)! \equiv 1 \mod p$.

Corolario 2.3.8. — *Sea G un grupo y sea p un número primo tal que p divide $|G|$. Escribamos $|G| = p^\alpha m$ con $p \nmid m$. Entonces, para todo $\beta \leq \alpha$ existe $H \leq G$ con $|H| = p^\beta$. En particular, si p divide $|G|$ entonces existe un elemento $g \in G$ con $\mathrm{ord}(g) = p$.*

Demostración. — Sea S un p-sub-grupo de Sylow de G, es decir, $|S| = p^\alpha$. La Proposición 2.2.13 (2) implica que el centro $Z(S)$ es un p-grupo no trivial. Sea $g \in Z(S) \setminus \{e\}$ elemento de orden $\mathrm{ord}(g) = p^\gamma$, para cierto $\gamma \in \mathbb{N}^{\geq 1}$.

Consideremos $H := \langle g^{p^{\gamma-1}} \rangle \cong \mathbb{Z}/p\mathbb{Z}$. Dado que $g \in Z(S)$ se tiene que $H \trianglelefteq S$, además se tiene $|S/H| = p^{\alpha-1}$. Razonando por inducción en α, se tiene que S/H posee sub-grupos de orden p, p^2, $\ldots, p^{\alpha-2}$. Al considerar sus pre-imagenes vía la proyección canónica $S \to S/H$ obtenemos sub-grupos de órdenes $p^2, p^3, \ldots, p^{\alpha-1}$. □

***Ejemplo 2.3.9* (grupos abelianos finitos).** — Sea G un grupo abeliano finito. Entonces todo p-sub-grupo de Sylow es normal y por ende es único (ver Corolario 2.3.6). Para p número primo, consideremos

$$T_p(G) := \{g \in G \mid \exists\, n \in \mathbb{N}^{\geq 1} \text{ tal que } p^n g = 0\}.$$

No es díficil verificar, usando el hecho que G es abeliano, que $T_p(G) \leq G$ sub-grupo. Dicho sub-grupo es llamado el **sub-grupo de p-torsión** de G.

Notar que si S es el único p-sub-grupo de Sylow de G y $g \in S$, entonces g es un elemento de orden $\mathrm{ord}(g) = p^m$ para cierto $m \in \mathbb{N}^{\geq 1}$, y luego $g \in T_p(G)$. En otras palabras, $S \leq T_p(G)$ es un sub-grupo.

Por otro lado, todo elemento $g \in T_p(G)$ verifica $\mathrm{ord}(g) = p^n$ para cierto $n \in \mathbb{N}^{\geq 1}$. Así, el Corolario 2.3.8 implica que $|T_p(G)| = p^\alpha$ para cierto $\alpha \in \mathbb{N}$. Dado que S es un p-sub-grupo de Sylow se concluye que $S = T_p(G)$.

Ejemplo 2.3.10. — Veamos algunos ejemplos concretos de aplicaciones del Teorema de Sylow. Sea G un grupo finito.

1. Veamos que si $|G| = 42$, entonces G no es un grupo simple. En efecto, notamos que $42 = 2 \cdot 3 \cdot 7$ y luego el Teorema de Sylow implica que $n_7 \equiv 1 \mod 7$ y $n_7 \mid 6$, lo cual implica necesariamente que $n_7 = 1$. Así, se tiene que G admite un único 7-sub-grupo de Sylow S, el cual es necesariamente normal $S \trianglelefteq G$ (ver Corolario 2.3.6).
2. Veamos que si G es simple, entonces necesariamente $|G|$ divide $n_p!$. En efecto, vimos en la demostración del Teorema de Sylow que G actúa transitivamente sobre $X = \{S \mid S \leq G \text{ } p\text{-sub-grupo de Sylow}\}$ por conjugación $g \cdot S := gSg^{-1}$. Dado que G es un grupo simple, entonces necesariamente $n_p > 1$ (ver Corolario 2.3.6). La acción de G en X se traduce en la existencia de un morfismo de grupos $\Phi : G \to \mathrm{Biy}(X) \cong \mathfrak{S}_{n_p}$. Dado que la acción de G es transitiva, tenemos que $\ker(\Phi) \neq G$ y luego tenemos necesariamente que $\ker(\Phi) = \{e\}$, ya que G es un grupo simple. Así, $\Phi : G \hookrightarrow \mathfrak{S}_{n_p}$ es un morfismo inyectivo el cual nos permite pensar G como un sub-grupo de $\mathfrak{S}_{n_p}$. Finalmente, el Teorema de Lagrange nos permite concluir que en este caso se tiene que $|G|$ divide $|\mathfrak{S}_{n_p}| = n_p!$.
3. Veamos que si $|G| = 48$ entonces G no es un gruo simple. En efecto, notamos que $48 = 2^4 \cdot 3$ y luego el Teorema de Sylow implica que $n_2 \equiv 1 \mod 2$ y $n_2 \mid 3$, lo cual implica que $n_2 \in \{1, 3\}$. Si G es un grupo simple entonces necesariamente $n_2 = 3$ (ver Corolario 2.3.6). Por otra parte, en tal caso tendríamos gracias al ejemplo anterior que $|G| = 48$ divide $n_2! = 3! = 6$, una contradicción.

2.4. Grupos abelianos finitamente generados

2.4.1. Teorema chino del resto y grupos abelianos de tipo finito. —

Recuerdo 2.4.1. — Recordemos que un **grupo cíclico** es un grupo isomorfo a $\mathbb{Z}/n\mathbb{Z}$ para cierto $n \in \mathbb{N}^{\geq 1}$.

***Teorema 2.4.2* (Teorema chino del resto).** — *Sea $n \in \mathbb{N}^{\geq 1}$ con $n = \Pi_{i=1}^{r} p_i^{\alpha_i}$ descomposición en números primos. Entonces,*

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_r^{\alpha_r}\mathbb{Z}.$$

Demostración. — La prueba consiste en inducción en el número de factores r. Basta probar que si $\mathrm{mcd}(d, e) = 1$ entonces

$$\mathbb{Z}/de\mathbb{Z} \cong \mathbb{Z}/d\mathbb{Z} \times \mathbb{Z}/e\mathbb{Z}.$$

El morfismo

$$f : \mathbb{Z} \longrightarrow \mathbb{Z}/d\mathbb{Z} \times \mathbb{Z}/e\mathbb{Z}$$
$$x \longmapsto ([x]_d, [x]_e)$$

verifica $\ker(f) = de\mathbb{Z}$. La propiedad universal del cociente implica que existe un único morfismo $\widehat{f} : \mathbb{Z}/de\mathbb{Z} \to \mathbb{Z}/d\mathbb{Z} \times \mathbb{Z}/e\mathbb{Z}$ inyectivo. Dado que $|\mathbb{Z}/de\mathbb{Z}| = |\mathbb{Z}/d\mathbb{Z} \times \mathbb{Z}/e\mathbb{Z}| = de$, se concluye que $\widehat{f}$ es un isomorfismo. □

¡Atención! — Es importante notar que $\widehat{f}$ es en realidad un *isomorfismo de anillos*. En particular, hay un isomorfismo entre los grupos de unidades

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_r^{\alpha_r}\mathbb{Z})^\times.$$

Recuerdo 2.4.3. — Sea G un grupo. Recordemos que G es **finitamente generado** si existe un conjunto finito $A \subseteq G$ tal que $G = \langle A \rangle$. En particular, si G es un grupo abeliano finitamente generado existen $x_1, \ldots, x_r \in G$ tal que

$$p : \mathbb{Z}^r \longrightarrow G$$
$$(a_1, \ldots, a_r) \longmapsto \sum_{i=1}^{r} a_i x_i$$

es un morfismo sobreyectivo.

Proposición 2.4.4. — *Sea G un grupo abeliano finitamente generado y sea $H \leq G$ un sub-grupo. Entonces H es finitamente generado.*

Demostración. — La prueba es por inducción en el número de generadores r. Si $p : \mathbb{Z}^r \twoheadrightarrow G$ morfismo sobreyectivo, denotamos por $K = p(\mathbb{Z}^{r-1} \times \{0\})$ la imagen del sub-grupo $\mathbb{Z}^{r-1} \times \{0\} \leq \mathbb{Z}^r$, el cual está generado por $r-1$ elementos. Si $f : G \to G/K$ es la proyección canónica, entonces la composición

$$f \circ p : \mathbb{Z}^r \twoheadrightarrow G \twoheadrightarrow G/K$$
$$(a_1, \ldots, a_r) \mapsto \sum a_i x_i \mapsto \left[\sum a_i x_i\right] \mod K = [a_r x_r] \mod K$$

se factoriza en

$$\mathbb{Z}^r \twoheadrightarrow \mathbb{Z}^r/(\mathbb{Z}^{r-1} \times \{0\}) \xrightarrow{\widehat{f \circ p}} G/K.$$

Dado que $\mathbb{Z}^r/(\mathbb{Z}^{r-1} \times \{0\}) \cong \mathbb{Z}$, se tiene que $G/K \cong \mathbb{Z}/d\mathbb{Z}$ para cierto $d \in \mathbb{N}^{\geq 1}$.

Sea $H \leq G$ un sub-grupo, y sea $\varphi : H \hookrightarrow G \xrightarrow{f} G/K$ la composición de la inclusión y la proyección al cociente. Entonces, $\ker(\varphi) = H \cap K$ es finitamente generado, por hipótesis de inducción. Por otro lado, $\mathrm{Im}(\varphi) \cong H/(H \cap K)$ es un sub-grupo de $G/K \cong \mathbb{Z}/d\mathbb{Z}$, y luego $\mathrm{Im}(\varphi) \cong \mathbb{Z}/e\mathbb{Z}$ para cierto $e \mid d$. En particular, $H/(H \cap K)$ es un grupo generado por un elemento.

Finalmente, dado que $H \cap K$ es finitamente generado y $H/(H \cap K)$ es finitamente generado, se concluye que H es finitamente generado. □

2.4.2. Grupos abelianos libres finitamente generados. —

***Definición 2.4.5* (grupo abeliano libre).** — Un grupo abeliano G es **libre finitamente generado** si $G \cong \mathbb{Z}^r$ para cierto $r \in \mathbb{N}^{\geq 1}$.

Se sigue a partir de la definición anterior que un grupo abeliano G es libre finitamente generado si existen $x_1, \ldots, x_r \in G$ tales que

$$p : \mathbb{Z}^r \to G,\ (a_1, \ldots, a_r) \mapsto \sum_{i=1}^{r} a_i x_i$$

es un isomorfismo. Diremos en tal caso que $\{x_1, \ldots, x_r\}$ es una **base** de G.

De manera similar, diremos que $\{x_1, \ldots, x_m\} \subseteq G$ es **linealmente independiente** si el morfismo asociado $p : \mathbb{Z}^m \to G$ es inyectivo.

El siguiente lema (sin demostración) relacionado con la estructura de matrices con coeficientes enteros es súmamente importante.

Lema 2.4.6. — *Sea $A \in M_{m\times n}(\mathbb{Z})$. Entonces, existen $P \in \mathrm{GL}_m(\mathbb{Z})$, $Q \in \mathrm{GL}_n(\mathbb{Z})$ tales que*

$$PAQ = \begin{pmatrix} d_1 & & & & & & \\ & \ddots & & & & & \\ & & d_s & & & & \\ & & & 0 & & & \\ & & & & \ddots & & \\ & & & & & 0 & \cdots & 0 \end{pmatrix}$$

donde $d_1, ..., d_s \in \mathbb{N}^{\geq 1}$ con $d_1 \mid d_1 \mid \cdots \mid d_s$ son llamados **factores invariantes** *de A, los cuales están completamente determinados por A.*

Teorema 2.4.7. — *Todas las bases de un grupo abeliano libre finitamente generado G tienen el mismo cardinal, llamado el* **rango** *de G.*

Demostración. — Basta probar que si $\{x_1, \ldots, x_r\}$ es una base de G y $\{y_1, \ldots, y_n\} \subseteq G$ es una familia linealmente independiente, entonces $n \leq r$.

Dado que $\{x_1, \ldots, x_r\}$ es una base, existe $A = (a_{ij}) \in M_{r\times n}(\mathbb{Z})$ tal que

$$y_j = \sum_{i=1}^{r} a_{ij} x_i.$$

En otras palabras, A es la matriz asociada al morfismo $\mathbb{Z}^n \to G,\ e_i \mapsto y_i$, donde $\{e_1, \ldots, e_n\}$ es la base canónica de $\mathbb{Z}^n$.

El lema anterior implica que existen P, Q matrices invertibles con coeficientes enteros tales que PAQ se escribe de la forma

$$PAQ = \begin{pmatrix} D & \\ & 0_{(r-s)\times(n-s)} \end{pmatrix},$$

donde D es la matriz diagonal formada por los factores invariantes de A.

Si $n > r$ entonces $PAQe_n = 0$. Dado que P es invertible, esto implica que $AQe_n = 0$. Si escribimos $Qe_n = (q_1, \ldots, q_n) \neq 0$ entonces obtenemos que

$$q_1 \underbrace{Ae_1}_{y_1} + \ldots + q_n \underbrace{Ae_n}_{y_n} = 0,$$

de donde obtenemos una relación entre los $\{y_1, \ldots, y_n\}$, una contradicción. □

***Teorema 2.4.8* (de la base adaptada).** — *Sea G un grupo abeliano libre de rango r y sea $H \leq G$ un sub-grupo. Entonces H es un grupo abeliano libre de rango $s \leq r$. Más aún, existe $\{e_1, \ldots, e_r\}$ base de G y $d_1, \ldots, d_s \in \mathbb{N}^{\geq 1}$ tales que*

1. *$\{d_1 e_1, \ldots, d_s e_s\}$ es una base de H.*
2. *$d_1 \mid d_2 \mid \cdots \mid d_s$.*

Demostración. — Sea $\{x_1, \ldots, x_r\}$ una base de G y sea $\Phi : \mathbb{Z}^r \xrightarrow{\sim} G$ el isomorfismo inducido. La Proposición 2.4.4 implica que H es finitamente generado, es decir, existe $\{y_1, \ldots, y_n\}$ conjunto finito de generadores de H. Si escribimos

$$y_j = \sum_{i=1}^{r} a_{ij} x_i$$

obtenemos una matriz $A = (a_{ij}) \in M_{r\times n}(\mathbb{Z})$. Sea $\{\varepsilon_1, \ldots, \varepsilon_n\}$ la base canónica de $\mathbb{Z}^n$ y consideremos el morfismo $f = \Phi \circ A$ dado por $f(\varepsilon_j) = y_j$

$$\mathbb{Z}^n \xrightarrow{A} \mathbb{Z}^r \xrightarrow[\sim]{\Phi} G \qquad (f : \mathbb{Z}^n \to G)$$

cuya imagen está dada precisamente por $\mathrm{Im}(f) = H$.

El lema anterior implica que existe una factorización (i.e., cambio de base) de $f \circ Q = \Phi \circ A \circ Q = (\Phi \circ P^{-1}) \circ (P \circ A \circ Q)$ como sigue

$$\mathbb{Z}^n \xrightarrow[\sim]{Q} \mathbb{Z}^n \xrightarrow{A} \mathbb{Z}^r \xrightarrow[\sim]{P} \mathbb{Z}^r \xrightarrow[\sim]{P^{-1}} \mathbb{Z}^r \xrightarrow[\sim]{\Phi} G,$$

en donde el isomorfismo $\Phi \circ P^{-1} : \mathbb{Z}^r \to G$ corresponde a darse una nueva base $\{e_1, \ldots, e_n\}$ de G. Dado que Q es invertible, tenemos que $H = \mathrm{Im}(f) = \mathrm{Im}(f \circ Q)$ y por ende H está generado por $\{d_1 e_1, \ldots, d_s e_s\}$.

Finalmente, dado que $\{d_1 e_1, \ldots, d_s e_s\}$ es una familia linealmente independiente y generadora, es una base de H y $H \cong \mathbb{Z}^s$. □

El siguiente resultado permite clasificar completamente los grupos abelianos finitamente generado en términos del rango de la parte libre y de los factores invariantes de la parte finita.

Teorema 2.4.9 **(de estructura de grupos abelianos de tipo finito)**

Sea G un grupo abeliano finitamente generado. Entonces existen naturales $r, s \in \mathbb{N}$ y enteros $1 < d_1 \mid \cdots \mid d_s$, únicamente determinados por G, tales que

$$G \cong \mathbb{Z}^r \times \prod_{i=1}^{s} \mathbb{Z}/d_i\mathbb{Z}.$$

En particular, se tiene que G es finito si y sólo si $r = 0$, y que G es abeliano libre si y sólo si $s = 0$.

Demostración. — Dado que G es finitamente generado, existe un morfismo $f : \mathbb{Z}^n \twoheadrightarrow G$ sobreyectivo. El teorema de la base adaptada implica que $H = \ker(f)$ es un grupo abeliano libre de rango $s \leq r$ y que existe una base $\{e_1, \ldots, e_n\}$ de $\mathbb{Z}^n$ tal que $\{d_1 e_1, \ldots, d_s e_s\}$ es base de H, donde $d_1 \mid \cdots \mid d_s$. En otras palabras, $H \cong d_1\mathbb{Z} \times \cdots \times d_s\mathbb{Z} \leq \mathbb{Z}^n$. Luego,

$$G \cong \mathbb{Z}^n/H \cong \mathbb{Z}^{n-s} \times \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_s\mathbb{Z}$$

donde, sin pérdida de generalidad, podemos retirar de dicho producto los factores con coeficiente $d_i = 1$, de donde obtenemos la descomposición deseada.

Resta verificar la unicidad de r, s y los d_i. Para ello consideremos el subgrupo de torsión

$$T(G) := \{x \in G \mid \exists m \in \mathbb{N}^{\geq 1} \text{ tal que } mx = 0\},$$

que corresponde al factor $\prod_{i=1}^{s} \mathbb{Z}/d_i\mathbb{Z}$. Así, $G/T(G) \cong \mathbb{Z}^r$ es un grupo abeliano libre, cuyo rango r es único.

Veamos ahora que, para el grupo finito $T(G)$, los d_i están únicamente determinados. Para ello notemos que, por el teorema chino del resto, tenemos que

$$T(G) \cong \prod_{j \in J} \mathbb{Z}/p_j^{\alpha_j}\mathbb{Z},$$

donde los p_j son números primos, eventualmente repetidos.

Por otro lado, notamos que podemos recuperar de manera única los factores invariantes d_i a partir de los $p_j^{\alpha_j}$. Por ejemplo, el factor más grande d_s está dado por el mínimo común múltiplo entre los $p_j^{\alpha_j}$ y por ende se escribe como $d_s = \prod_{j' \in J'} p_{j'}^{\alpha_{j'}}$ para cierto $J' \subseteq J$. De manera similar, d_{s-1} es el mínimo común múltiplo entre los $p_j^{\alpha_j}$ donde $j \in J \setminus J'$, y así sucesivamente. En otras palabras, basta probar que los factores $p_j^{\alpha_j}$ están únicamente determinados.

Sea p un número primo y consideremos el sub-grupo $T_p(G)$ de elementos de p-torsión, i.e., elementos de orden p^α para cierto $\alpha \in \mathbb{N}^{\geq 1}$. Queremos probar que en la escritura

$$T_p(G) = \mathbb{Z}/p^{\alpha_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{\alpha_s}\mathbb{Z},\ \alpha_1 \leq \ldots \leq \alpha_s,$$

los exponentes α_j están únicamente determinados por G. Para esto último, consideremos para todo entero $i > 0$ el subgrupo

$$T_{p,i} := \{x \in G \mid p^i x = 0\} \leq T_p(G),$$

el cual está únicamente determinado por G. Notar que $T_{p,i} \leq T_{p,i+1}$, que $|T_{p,i}| = \prod_{\alpha_j \leq i} p^{\alpha_j} \prod_{\alpha_j > i} p^j$ y en particular $|T_{p,i+1}/T_{p,i}| = p^{\mathrm{card}\{j \mid \alpha_j > i\}}$. Así, los exponentes α_j están completamente determinados por los sub-grupos $T_{p,i}$. □

¡Atención! — Concretamente, la prueba del teorema de estructuras de grupos abelianos finitamente generados nos dice que para determinar los factores invariantes d_i debemos escribir los factores $p_j^{\alpha_j}$ en una tabla con una línea para cada número primo, en orden creciente, y alinear cada línea a la última columna. Luego, los d_i se obtienen al tomar los productos de cada columna.

Ejemplo 2.4.10. —

1. Sea

$$G = (\mathbb{Z}/2\mathbb{Z})^2 \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z} \times (\mathbb{Z}/3\mathbb{Z})^3 \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z}$$

y consideremos la tabla

$$\begin{array}{cccc} 2 & 2 & 2^2 & 2^3 \\ & 3 & 3 & 3 \\ & & 5 & 5^2 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ d_1 = 2 & d_2 = 6 & d_3 = 60 & d_4 = 600 \end{array}$$

Notamos que $2 \mid 6 \mid 60 \mid 600$ y luego

$$G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/60\mathbb{Z} \times \mathbb{Z}/600\mathbb{Z}.$$

2. Todos los grupos abelianos de orden 18 están determinados por las secuencias $1 < d_1 \mid \cdots \mid d_s$ tales que $d_1 \cdots d_s = 18 = 2 \cdot 3^2$. Así, los únicos grupos de orden 18 (módulo isomorfismo) son $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ y $\mathbb{Z}/18\mathbb{Z}$.

Ejercicio 2.4.11. — Verificar que

$$\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/18\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/72\mathbb{Z}.$$

***Observación 2.4.12* (curvas elípticas).** — Sea k un cuerpo y recordemos que el plano proyectivo $\mathbb{P}^2(k)$ es el conjunto de rectas vectoriales en k^3 o, equivalentemente, el cociente $k^\times \backslash (k^3 \setminus \{0\})$ donde $k^\times$ actúa mediante $\lambda \cdot (x, y, z) = (\lambda x, \lambda y, \lambda z)$ y donde denotamos por $[x : y : z] \in \mathbb{P}^2(k)$ a la clase de equivalencia de (x, y, z). Dados $a, b \in k$ consideramos el conjunto

$$E = E_{a,b} = \left\{ [x : y : z] \in \mathbb{P}^2(k) \mid y^2 z = x^3 + axz^2 + bz^3 \right\}$$

de ceros del polinomio cúbico asociado, donde $\Delta = -16(4a^3 + 27b^2) \neq 0$. Dicho sub-conjunto del plano proyectivo es llamado una **curva elíptica** y es posible probar que puede ser dotado de estructura de grupo abeliano $(E, +)$.

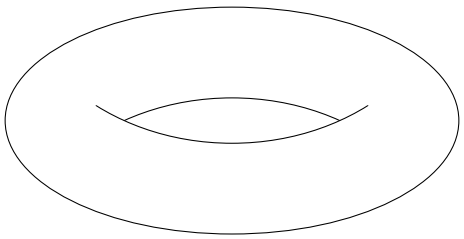


IMAGEN 1. Curva elíptica sobre $k = \mathbb{C}$

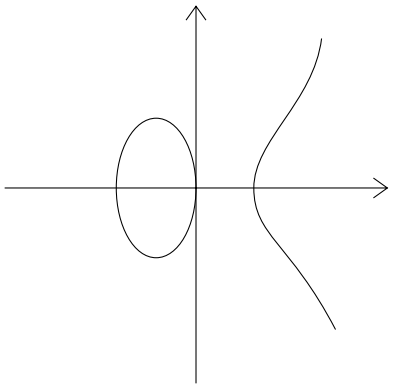


IMAGEN 2. Curva elíptica sobre $k = \mathbb{R}$

El Teorema de Mordell (1922) afirma que si $k = \mathbb{Q}$ entonces $(E, +)$ es un grupo abeliano finitamente generado. Más aún, el Teorema de Mazur (1977) clasifica todos los posibles grupos de torsión $T(E)$, los cuales son de la forma $T(E) \cong \mathbb{Z}/d\mathbb{Z}$ con $d \in \{0, 1, \ldots, 10, 12\}$ o bien $T(E) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/d\mathbb{Z}$ con $d \in \{2, 4, 6, 8\}$. La parte libre de torsión $E/T(E) \cong \mathbb{Z}^r$ es más complicada. Se conjetura que rangos r arbitrariamente grandes deberían poder alcanzarse, sin embargo el ejemplo con rango más grande que se ha calculado hasta la fecha verifica $E/T(E) \cong \mathbb{Z}^{28}$ (Elkies, 2006).

2.5. Grupos simples y series de composición

Recuerdo 2.5.1. — Recordemos que un grupo G es **simple** si $G \neq \{e\}$ es no trivial, y si $\{e\}$ y G son sus únicos sub-grupos normales.

En esta sección discutiremos sobre cómo los grupos simples pueden ser pensados como los bloques estructurales de la teoría de grupos.

Ejemplo 2.5.2. —

1. Sea $n \geq 3$. El grupo simétrico $\mathfrak{S}_n$ **no** es simple, pues el grupo alternante $\mathfrak{A}_n \trianglelefteq \mathfrak{S}_n$ es normal de índice 2.
2. El grupo alternante $\mathfrak{A}_3$ es simple. En efecto, $|\mathfrak{S}_3| = 3! = 6$ y luego $|\mathfrak{A}_3| = 3$, lo cual implica que $\mathfrak{A}_3 \cong \mathbb{Z}/3\mathbb{Z}$.
3. El grupo alternante $\mathfrak{A}_4$ **no** es simple. En efecto, dado que $2 + 2 = 4$, las dobles transposiciones $(a, b)(c, d)$ son conjugadas (ver Proposición 2.2.8). Así, el sub-grupo
$$K = \{\mathrm{id}; (1,2)(3,4); (1,3)(2,4); (1,4)(2,3)\} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$
es normal en $\mathfrak{A}_4$, y es usualmente conocido como **grupo de Klein**.

Ejercicio 2.5.3. — Probar que un grupo abeliano finitamente generado G es simple si y sólo si $G \cong \mathbb{Z}/p\mathbb{Z}$ para cierto p primo.

Ejercicio 2.5.4. — Probar que el grupo alternante $\mathfrak{A}_5$ consiste exactamente en la identidad, las dobles transposiciones, los 3-ciclos y los 5-ciclos.

Teorema 2.5.5. — *El grupo alternante $\mathfrak{A}_n$ es simple para todo $n \geq 5$.*

Corolario 2.5.6. — *Sea $n \geq 2$. Si $n \neq 4$, entonces los únicos sub-grupos normales de $\mathfrak{S}_n$ son $\{e\}$, $\mathfrak{A}_n$ y $\mathfrak{S}_n$.*

Demostración. — El caso $n = 2$ es trivial. Supongamos que $n = 3$ o $n \geq 5$. En tal caso se tiene que $\mathfrak{A}_n$ es un grupo simple. Así, si $H \trianglelefteq \mathfrak{S}_n$ se tiene que $H \cap \mathfrak{A}_n \trianglelefteq \mathfrak{A}_n$ (c.f. Ejercicio 2.1.22), de donde se deduce que la intersección $H \cap \mathfrak{A}_n$ es $\mathfrak{A}_n$ o bien $\{e\}$.

En caso que $H \cap \mathfrak{A}_n = \mathfrak{A}_n$, se tiene que $\mathfrak{A}_n \leq H$ y luego $[H : \mathfrak{A}_n]$ divide $[\mathfrak{S}_n : \mathfrak{A}_n] = 2$, por el Teorema de Lagrange. Si $[H : \mathfrak{A}_n] = 1$ entonces $H = \mathfrak{A}_n$, mientras que si $[H : \mathfrak{A}_n] = 2$ entonces $H = \mathfrak{S}_n$.

En caso que $H \cap \mathfrak{A}_n = \{e\}$ tendríamos que la composición

$$H \hookrightarrow \mathfrak{S}_n \twoheadrightarrow \mathfrak{S}_n/\mathfrak{A}_n \cong \mathbb{Z}/2\mathbb{Z}$$

es un morfismo inyectivo. En particular, $H = \{e\}$ o bien $|H| = 2$. Por otra parte, si $|H| = 2$ y $\sigma \in H$ es el elemento no-trivial de orden 2, entonces podemos escribir $\sigma = (a, b)(c, d) \cdots$ como producto de transposiciones con soportes disjuntos. Dado que $n \geq 3$, existe $c \notin \{a, b\}$. Así, el elemento $\widetilde{\sigma} := (a, c)\sigma(a, c)^{-1}$ pertenece a H (pues $H \trianglelefteq \mathfrak{S}_n$) y envía $c \mapsto b$. En otras palabras, $\widetilde{\sigma} \notin \{\mathrm{id}, \sigma\} = H$, una contradicción. □

Demostración del Teorema 2.5.5. — Sea $H \neq \{e\}$ sub-grupo normal de $\mathfrak{A}_n$, i.e., tal que para todo $\sigma \in \mathfrak{A}_n$ y para todo $\tau \in H$ se verifica $\sigma\tau\sigma^{-1} \in H$.

Para facilitar la lectura, dividiremos la demostración en cuatro etapas.

Paso 1. *$\mathfrak{A}_n$ está generado por 3-ciclos.*

Por definición $\mathfrak{A}_n$ está generado por permutaciones pares, es decir, producto par de transposiciones. Notar que $(a, b)(c, d) = (a, c, b)(a, c, d)$ y que $(a, b)(a, c) = (a, c, b)$. Así, todo producto par de transposiciones es un producto de 3-ciclos.

Paso 2. *Todos los 3-ciclos (a, b, c) son conjugados en $\mathfrak{A}_n$. Todas las dobles transposiciones $(a, b)(c, d)$ son conjugadas en $\mathfrak{A}_n$.*

Vimos en la Proposición 2.2.8 que todos los 3-ciclos son conjugados en $\mathfrak{S}_n$. Por ejemplo, $(2, 3, 1) = \sigma\tau\sigma^{-1}$, donde $\sigma \in \mathfrak{S}_n$ y τ un 3-ciclo. Dado que $n \geq 5$, podemos escribir

$$(2, 3, 1) = (4, 5)(2, 3, 1)(4, 5)^{-1} = (4, 5)\sigma\tau\sigma^{-1}(4, 5)^{-1} = \widetilde{\sigma}\tau\widetilde{\sigma}^{-1},$$

donde $\widetilde{\sigma} := (4, 5)\sigma$. Por un lado, si σ es una permutación par (i.e., $\sigma \in \mathfrak{A}_n$) entonces $(2, 3, 1)$ y τ son conjugados en $\mathfrak{A}_n$ por σ. Por otro lado, si σ es una permutación impar, entonces $\widetilde{\sigma}$ es una permutación par y luego $(2, 3, 1)$ y τ son conjugados en $\mathfrak{A}_n$ por $\widetilde{\sigma}$.

De manera completamente análoga, si por ejemplo $(1, 2)(3, 4) = \sigma\tau\sigma^{-1}$ entonces $(1, 2)(3, 4) = \widetilde{\sigma}\tau\widetilde{\sigma}^{-1}$, donde $\widetilde{\sigma} := (1, 2)\sigma$. De donde se concluye el resultado.

Observación: El Paso 2 implica que si H contiene un 3-ciclo entonces contiene todos los 3-ciclos, pues $H \trianglelefteq \mathfrak{A}_n$. En este caso, el Paso 1 implica que $H = \mathfrak{A}_n$. Así, basta probar que H contiene al menos un 3-ciclo para concluir.

Paso 3. *Si H contiene una (luego todas) doble transposición $(a,b)(c,d)$ o si H contiene un 5-ciclo (a,b,c,d,e), entonces H contiene un 3-ciclo.*

Dado que $n \geq 5$, existen a, b, c, d, e diferentes. Calculamos

$$(a,b,c) = \underbrace{(a,e)(c,d)}_{\in H}\underbrace{(a,d)(c,e)}_{\in H}\underbrace{(a,b)(d,e)}_{\in H}$$

y

$$(a,b,d) = \underbrace{(a,b,c)(a,b,c,d,e)(a,b,c)^{-1}}_{\in H}\underbrace{(a,b,c,d,e)^{-1}}_{\in H},$$

de donde se concluye.

Observación: Notar que el Paso 1, Paso 2 y Paso 3 implican, junto con el Ejercicio 2.5.4, que el grupo $\mathfrak{A}_5$ es simple.

Paso 4. *Sea $n \geq 6$. Si $\mathfrak{A}_{n-1}$ es simple, entonces $\mathfrak{A}_n$ es simple.*

Veamos que $H \trianglelefteq \mathfrak{A}_n$ contiene necesariamente un elemento $\sigma \neq \mathrm{id}$ tal que $\sigma(1) = 1$. En efecto, sea $\sigma \in H$ tal que $\sigma(1) = i \neq 1$ y consideremos $j \notin \{1, i\}$ tal que $\sigma(j) \neq j$, siendo esto último posible gracias a que $\sigma \neq (1,i) \notin \mathfrak{A}_n$. Dado que $n \geq 6$, existen l, m con $l \neq m$ y $l, m \notin \{1, i, j, \sigma(j)\}$. Luego, el elemento

$$\widetilde{\sigma} := (j,l,m)\sigma^{-1}(j,l,m)^{-1}\sigma \in H$$

satisface $\widetilde{\sigma}(1) = 1$ y $\widetilde{\sigma}(j) = l \neq j$.

Así, $\widetilde{\sigma} \neq \mathrm{id}$ y $\widetilde{\sigma} \in K \cap H$, donde

$$K := \{\sigma \in \mathfrak{A}_n \mid \sigma(1) = 1\} \cong \mathfrak{A}_{n-1}.$$

En particular, $H \cap K \neq \{e\}$. Dado que $H \cap K \trianglelefteq K$ y este último es simple, se tiene que necesariamente $K = H \cap K$. Finalmente, $K \leq H$ y luego H contiene un 3-ciclo, de donde se concluye que $H = \mathfrak{A}_n$. □

***Definición 2.5.7* (serie de composición).** — Una **serie de composición** de un grupo G es una serie finita

$$G =: G_0 \rhd G_1 \rhd G_2 \rhd \cdots \rhd G_r = \{e\}$$

tal que cada cociente G_i/G_{i+1} es un grupo simple.

Ejemplo 2.5.8. — Veamos algunos ejemplos concretos.

1. El grupo $\mathbb{Z}/6\mathbb{Z}$ admite la serie de composición
$$\mathbb{Z}/6\mathbb{Z} \rhd \mathbb{Z}/3\mathbb{Z} \rhd \{0\}$$
con cocientes $G_0/G_1 \cong \mathbb{Z}/2\mathbb{Z}$ y $G_1/G_2 \cong \mathbb{Z}/3\mathbb{Z}$. De manera similar, el grupo $\mathbb{Z}/6\mathbb{Z}$ admite la serie de composición
$$\mathbb{Z}/6\mathbb{Z} \rhd \mathbb{Z}/2\mathbb{Z} \rhd \{0\}$$
con cocientes $G_0/G_1 \cong \mathbb{Z}/3\mathbb{Z}$ y $G_1/G_2 \cong \mathbb{Z}/2\mathbb{Z}$.
2. El grupo simétrico $\mathfrak{S}_4$ admite la serie de composición
$$G_0 = \mathfrak{S}_4 \rhd G_1 = \mathfrak{A}_4 \rhd G_2 = K \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \rhd G_3 \cong \mathbb{Z}/2\mathbb{Z} \rhd G_4 = \{e\}$$
con cocientes $G_0/G_1 \cong \mathbb{Z}/2\mathbb{Z}$, $G_1/G_2 \cong \mathbb{Z}/3\mathbb{Z}$, $G_2/G_3 \cong \mathbb{Z}/2\mathbb{Z}$ y $G_3/G_4 \cong \mathbb{Z}/2\mathbb{Z}$.
3. Si $n = 3$ o $n \geq 5$, el grupo simétrico $\mathfrak{S}_n$ admite la serie de composición
$$\mathfrak{S}_n \rhd \mathfrak{A}_n \rhd \{e\}$$
con cocientes simples $\mathbb{Z}/2\mathbb{Z}$ y $\mathfrak{A}_n$.

Ejercicio 2.5.9. — Probar que $\mathbb{Z}$ **no** admite una serie de composición.

***Definición 2.5.10* (series equivalentes).** — Dos series de composición
$$G = G_0 \rhd G_1 \rhd G_2 \rhd \cdots \rhd G_r = \{e\}$$
y
$$G = G'_0 \rhd G'_1 \rhd G'_2 \rhd \cdots \rhd G'_s = \{e\}$$
de un grupo G son **equivalentes** si $r = s$ y si existe una permutación $\sigma \in \mathfrak{S}_r$ tal que $G_{\sigma(i)}/G_{\sigma(i)+1} \cong G'_i/G'_{i+1}$ para todo i. En tal caso, escribiremos $(G_1, \ldots, G_r) \sim (G'_1, \ldots, G'_s)$.

***Teorema 2.5.11* (Jordan-Hölder).** — *Todo grupo finito admite una serie de composición, y todas sus series de composición son equivalentes.*

Observación 2.5.12. —

1. Los cocientes G_i/G_{i+1} son llamados **factores simples** del grupo G.
2. Es importante notar que los factores simples **no** determinan al grupo G. Por ejemplo, los grupos $\mathfrak{S}_4$, $(\mathbb{Z}/2\mathbb{Z})^3 \times \mathbb{Z}/3\mathbb{Z}$ y $\mathbb{Z}/24\mathbb{Z}$ tienen los mismos factores simples, pero no son isomorfos.

El siguiente lema será de utilidad en la prueba del Teorema de Jordan-Hölder.

Lema 2.5.13. — *Sea G un grupo. Sean $H \trianglelefteq G$ y $K \trianglelefteq G$ sub-grupos normales tales que $H \neq K$ y tales que los cocientes G/H y G/K son grupos simples. Entonces, $H \cap K \trianglelefteq H$ y $H \cap K \trianglelefteq K$ son sub-grupos normales. Más aún, $G/H \cong K/(H \cap K)$ y $G/K \cong H/(H \cap K)$.*

Demostración. — El kernel de la composición $K \hookrightarrow G \twoheadrightarrow G/H$ está dado por $H \cap K \trianglelefteq K$, de donde obtenemos un morfismo inyectivo $K/(H \cap K) \hookrightarrow G/H$.

Dejamos como ejercicio al lector verificar que si $K \trianglelefteq G$ sub-grupo normal, entonces $K/(H \cap K) \trianglelefteq G/H$ también es un sub-grupo normal.

Dado que el grupo G/H es simple, tenemos que $K/(H \cap K) \cong G/H$ o bien $K/(H \cap K)$ es trivial.

Supongamos por contradicción que $K/(H \cap K)$ es trivial, entonces $H \cap K = K$, i.e., $K \trianglelefteq H$ (c.f. Ejercicio 2.1.22). Por un lado, en este caso tendríamos que $H/K \trianglelefteq G/K$ es un sub-grupo normal, que además es no-trivial pues $H \neq K$. Notar por otro lado que $(G/K)/(H/K) \cong G/H$, y que este último grupo es no-trivial por definición de grupo simple. Así, la simplicidad de G/K implicaría que H/K es el grupo trivial, una contradicción.

Concluimos finalmente que $G/H \cong K/(H \cap K)$. De manera completamente análoga se deduce que $G/K \cong H/(H \cap K)$. □

Demostración del Teorema 2.5.11. — Sea G un grupo finito. Comencemos por probar la existencia de una serie de composición de G.

Si G es un grupo simple, basta considerar la serie $G = G_0 \rhd G_1 = \{e\}$. Si G no es simple, consideramos G_1 un sub-grupo normal de orden maximal tal que $G_1 \neq G$.

Notemos que el cociente G/G_1 es un grupo simple. En efecto, todo sub-grupo normal $\widetilde{H}$ de G/G_1 corresponde, vía la proyección canónica $G \twoheadrightarrow G/G_1$, a un sub-grupo normal H de G tal que $G_1 \leq H$. Dado que G_1 es de orden maximal necesariamente $H = G_1$, en cuyo caso $\widetilde{H}$ es trivial, o bien $H = G$, en cuyo caso $\widetilde{H} = G/G_1$.

Recomenzamos el proceso a partir de G_1 y construimos G_2, y así sucesivamente. Dicha construcción tiene que detenerse puesto que por un lado $|G| > |G_1| > |G_2| > \ldots$, y por otro lado G es un grupo finito.

Para probar la unicidad, módulo equivalencia, procedemos por inducción en el largo de la serie. En otras palabras, supongamos que el resultado es cierto para grupos que admiten una serie de composición de largo a lo más $r - 1$.

Sean $G \rhd H_1 \rhd \cdots \rhd H_r$ y $G \rhd K_1 \rhd \cdots \rhd K_s$ dos series de composición de G, donde $r \leq s$. Observamos que si $H_1 = K_1$, entonces podemos

aplicar la hipótesis de inducción al grupo $H_1 = K_1$ y así obtener que $(H_1, \ldots, H_r) \sim (K_1, \ldots, K_s)$ son equivalentes y, en particular, $r = s$.

Supongamos que $H_1 \neq K_1$ y consideremos el diagrama

$$\begin{array}{ccccccccccc} & & H_1 & \rhd & H_2 & & \rhd & \cdots & \rhd & H_r = \{e\} & \\ & \triangleleft & & \triangleleft & & & & & & & \\ G & & & & L_2 := H_1 \cap K_1 & \rhd & \cdots & \cdots & \rhd & L_t = \{e\} & \\ & \triangleleft & & \triangleleft & & & & & & & \\ & & K_1 & \rhd & K_2 & & \rhd & \cdots & \cdots & \cdots \quad \rhd & K_s = \{e\} \end{array}$$

El lema anterior implica que los grupos H_1/L_2 y K_1/L_2 son simples. Así, $(H_2, \ldots, H_r)$ y $(L_2, \ldots, L_t)$ son series de composición de H_1. La hipótesis de inducción implica que las series $(H_2, \ldots, H_r) \sim (L_2, \ldots, L_t)$ son equivalentes y, en particular, $r = t$.

Más aún, los cocientes $\{H_1/H_2, \ldots, H_{r-1}/H_r\}$ son isomorfos a los cocientes $\{H_1/L_2 \cong G/K_1, L_2/L_3, \ldots, L_{r-1}/L_r\}$, donde el isomorfismo $H_1/L_2 \cong G/K_1$ se obtiene gracias al lema anterior. Dado que $t = r$, K_1 admite una serie $(L_2, \ldots, L_r)$ de largo $r-1$ y una serie $(K_2, \ldots, K_s)$ de largo $s-1$. Por hipótesis de inducción concluimos entonces que $s = r$ y que las series $(L_2, \ldots, L_r) \sim (K_2, \ldots, K_s)$ son equivalentes. En particular, los cocientes $\{K_1/K_2, \ldots, K_{r-1}/K_r\}$ son isomorfos a los cocientes $\{K_1/L_2 \cong G/H_1, L_2/L_3, \ldots, L_{r-1}/L_r\}$, donde el isomorfismo $K_1/L_2 \cong G/H_1$ se obtiene gracias al lema anterior. En conclusión, las series $(H_1, \ldots, H_r)$ y $(K_1, \ldots, K_s)$ son equivalentes. □

Ejercicio 2.5.14. — Sea $n \in \mathbb{N}^{\geq 2}$ y sea $n = \prod p_i^{\alpha_i}$ una descomposición en producto de factores primos.

a) Probar, usando el teorema chino del resto, que el grupo $\mathbb{Z}/n\mathbb{Z}$ admite una serie de composición donde los factores simples son los $\mathbb{Z}/p_i\mathbb{Z}$, cada uno repetido α_i veces.
b) Utilizar el Teorema de Jordan-Hölder para concluir que la descomposición $n = \prod p_i^{\alpha_i}$ en factores primos es única, módulo permutación de los factores.

Observación 2.5.15. — El llamado **programa de Gorenstein**, iniciado por Galois en 1832 y completado por varios autores en 2012, tiene por objetivo la clasificación de todos los grupos finitos simples. Hoy en día, sabemos que todo grupo finito simple es isomorfo a uno de los siguientes grupos:

1. El grupo cíclico $\mathbb{Z}/p\mathbb{Z}$, donde p es un número primo.

2. El grupo alternante $\mathfrak{A}_n$, donde $n \geq 5$.
3. Grupos de tipo Lie, los cuales están íntimamente relacionados a grupos de matrices con coeficientes en un cuerpo finito.
4. 27 grupos esporádicos, entre los cuales se encuentra el "monstruo" de Fischer-Griess de orden

$$2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71 \approx 8 \cdot 10^{53}.$$

CAPÍTULO 3

REPRESENTACIONES DE GRUPOS FINITOS

En todo este capítulo G será un grupo finito y V un espacio vectorial complejo de dimensión finita, es decir, $V \cong \mathbb{C}^n$ para cierto $n \in \mathbb{N}$. Recordemos que

$$\mathrm{GL}(V) = \{T : V \to V \text{ transformación lineal invertible}\}.$$

3.1. Representaciones lineales

Definición 3.1.1 **(representación).** — Sea G un grupo finito. Una **representación** (lineal) de G en V es un morfismo de grupos

$$\rho : G \longrightarrow \mathrm{GL}(V)$$
$$g \longmapsto \rho(g) = \rho_g,$$

es decir, $\rho_{gh} = \rho_g \rho_h$ para todos $g, h \in G$. En particular, $\rho_e = \mathrm{id}_V$ y $\rho_{g^{-1}} = (\rho_g)^{-1}$. En ocasiones escribiremos que (V, ρ) es una representación de G.

Concretamente, si fijamos una base $\{e_1, \ldots, e_n\}$ de V, entonces hay un isomorfismo inducido $\mathrm{GL}(V) \cong \mathrm{GL}_n(\mathbb{C})$. Si R_g es la matriz de ρ_g respecto a dicha base, entonces tenemos que $\det(R_g) \neq 0$ y además

$$R_{gh} = R_g \cdot R_h$$

para todos $g, h \in G$.

Definición 3.1.2 **(grado).** — Sea (V, ρ) una representación de un grupo G. Definimos el **grado** de la representación como $\dim_{\mathbb{C}}(V)$.

Definición 3.1.3 **(equivalencia).** — Sean (V, ρ) y (V, ρ') dos representaciones de un grupo G. Decimos que estas representaciones son **equivalentes**,

en cuyo caso escribimos $(V,\rho) \cong (V',\rho')$, si existe $\tau : V \to V'$ isomorfismo lineal tal que

$$\tau \circ \rho_g = \rho'_g \circ \tau$$

para todo $g \in G$.

Matricialmente, y conservando la notación anterior, dos representaciones son equivalentes si existe una matríz $T \in \mathrm{GL}_n(\mathbb{C})$ tal que $TR_g = R'_g T$, es decir, si $R'_g = TR_gT^{-1}$ para todo $g \in G$. En otras palabras, las matrices R_g y R'_g son las mismas, módulo un cambio de base dado por T.

Ejemplo 3.1.4. —

1. Una representación de grado 1 de un grupo finito G es un morfismo de grupos
$$\rho : G \longrightarrow \mathrm{GL}_1(\mathbb{C}) = \mathbb{C}^*.$$
Dado que G es un grupo finito, los valores $\rho_g \in \mathbb{C}$ son raíces de la únidad, es decir, existe $n \in \mathbb{N}^{\geq 1}$ tal que $\rho_g^n = 1$. Así, la imagen $\rho(G) \subseteq \mathbb{S}^1 = \{z \in \mathbb{C} \mid |z| = 1\}$ está contenida en el círculo unitario. Más aún, se puede probar que $\rho(G)$ es necesariamente un grupo cíclico (ver Ejercicio 2.1.36).
2. Sea $\rho : G \to \mathbb{C}^*$ una representación de grado 1. Si $\rho_g = 1$ para todo $g \in G$ decimos que ρ es la **representación trivial** de G.
3. Si $G \subseteq \mathrm{GL}_n(\mathbb{C})$ es un sub-grupo finito de matrices, la inclusión
$$\rho : G \hookrightarrow \mathrm{GL}_n(\mathbb{C})$$
es la **representación estándar** de G. En el caso del grupo simétrico $\mathfrak{S}_n$, la inclusión $\rho : \mathfrak{S}_n \hookrightarrow \mathrm{GL}_n(\mathbb{C})$ que asocia una permutación $\sigma \mapsto P_\sigma$ a su matriz de permutación respecto a la base canónica de $\mathbb{C}^n$, es llamada la **representación de permutación**.
4. Sea $|G| = N$ y sea $V \cong \mathbb{C}^N$ con base $\{e_g\}_{g\in G}$ indexada por los elementos de G. Si definimos $\rho_g : V \to V$ mediante $e_h \mapsto e_{gh}$, entonces
$$\rho : G \longrightarrow \mathrm{GL}(V) \cong \mathrm{GL}_N(\mathbb{C})$$
es llamada la **representación regular** de G. Notar que, si denotamos por $1 \in G$ a la identidad del grupo, entonces en este caso se tiene que la imagen $\rho_g(e_1) = e_g$ es un elemento de la base para todo $g \in G$. Recíprocamente, si una representación $\rho : G \to \mathrm{GL}(W)$ es tal que existe un vector $w \in W$ de tal suerte que el conjunto de imagenes $\{\rho_g(w)\}_{g\in G}$ sea una base de W, entonces W es equivalente a la representación regular. En efecto, basta considerar $\tau : \mathbb{C}^N \xrightarrow{\sim} W$ dada por $\tau(e_g) = \rho_g(w)$.

5. Supongamos que G actúa sobre un conjunto finito X, y sea $V \cong \mathbb{C}^{\mathrm{card}(X)}$ con base $\{e_x\}_{x\in X}$ indexada por los elementos de X. Si definimos $\rho_g : V \to V$ mediante $e_x \mapsto e_{g\cdot x}$, entonces $\rho : G \longrightarrow \mathrm{GL}(V) \cong \mathrm{GL}_{\mathrm{card}(X)}(\mathbb{C})$ es la **representación de permutación** asociada a X.

3.2. Sub-representaciones y morfismos

***Definición 3.2.1* (sub-representación).** — Sea $\rho : G \to \mathrm{GL}(V)$ una representación y sea $W \subseteq V$ un sub-espacio vectorial. Decimos que W es **G-estable** o **G-invariante** si para todo $w \in W$ y todo $g \in G$ se tiene que $\rho_g(w) \in W$. Notar que en este caso la restricción $\rho_g^W := \rho_g|_W : W \to W$ es un isomorfismo que verifica $\rho_{gh}^W = \rho_g^W \rho_h^W$ y por ende $\rho^W : G \to \mathrm{GL}(W)$ es también una representación de G. Diremos que W es una **sub-representación** de V.

Ejemplo 3.2.2. — Sea V la representación regular de G y sea

$$W = \mathrm{Vect}_{\mathbb{C}} \left\langle x = \sum_{g\in G} e_g \right\rangle = \mathrm{Vect}_{\mathbb{C}}\langle (1,\ldots,1)\rangle \cong \mathbb{C}.$$

Dado que $\rho_g(x) = x$ para todo $g \in G$, se tiene que W es G-invariante. Más aún, $\rho^W : G \to \mathrm{GL}(W)$ es la representación trivial.

Ejercicio 3.2.3. — Sea $\rho : G \to \mathrm{GL}(V)$ una representación. Probar que el sub-espacio de vectores invariantes

$$V^G = \{v \in V \mid \rho_g(v) = v \text{ para todo } g \in G\}$$

es G-invariante.

De manera análoga a la equivalencia de representaciones (ver Definición 3.1.3), podemos definir la noción de morfismo de representaciones.

***Definición 3.2.4* (morfismo).** — Un **morfismo** entre representaciones (V, ρ_V) y (W, ρ_W) de un grupo G es una aplicación lineal $u : V \to W$ tal que

$$u \circ \rho_{V,g} = \rho_{W,g} \circ u$$

para todo $g \in G$.

Observación 3.2.5. — Notar que si $u : V \to W$ es un morfismo de representaciones, entonces $\ker(u)$ (resp. $\mathrm{Im}(u)$) es una sub-representación de V (resp. W). Además, u induce una equivalencia

$$V/\ker(u) \xrightarrow{\sim} \mathrm{Im}(u)$$

de representaciones.

Recuerdo 3.2.6. — Sea V un espacio vectorial sobre $\mathbb{C}$ y sean W, W' sub-espacios vectoriales. Recordemos que V es **suma directa** de W y W', en cuyo caso escribimos $V = W \oplus W'$, si todo vector $v \in V$ se escribe de manera única como $v = w + w'$, donde $w \in W$ y $w' \in W$. De manera equivalente, $V = W \oplus W'$ si y sólo si $W \cap W' = \{0\}$ y $\dim_{\mathbb{C}}(V) = \dim_{\mathbb{C}}(W) + \dim_{\mathbb{C}}(W')$.

Si $V = W \oplus W'$, entonces decimos que W' es un sub-espacio **complementario** de W en V. Recordemos que todo sub-espacio vectorial no-nulo W de V admite un sub-espacio complementario W', pero este no es único (ver §2.1.7).

Recordemos que un **operador de proyección** en un espacio vectorial V es una transformación lineal $p : V \to V$ idempotente, es decir, que satisface $p^2 = p$.

Por ejemplo, si $V = W \oplus W'$ y $p : V \to V$ está dada por $v = w + w' \mapsto w$, entonces $\mathrm{Im}(p) = W$, $\ker(p) = W'$ y $p(w) = w$ para todo $w \in W$. En particular, p es el operador de proyección de V sobre W. Recíprocamente, si $p : V \to V$ es un operador de proyección con $W := \mathrm{Im}(p)$ y $W' := \ker(p)$, entonces $V = W \oplus W'$. Así, existe una correspondencia biyectiva

$$\begin{array}{rcl} \{p : V \to V \text{ proyección}\} & \longleftrightarrow & \{V = W \oplus W' \text{ suma directa}\} \\ p & \longmapsto & W := \mathrm{Im}(p),\ W' := \ker(p) \\ p(v) = p(w + w') := w & \longleftarrow & V = W \oplus W' \end{array}$$

***Teorema 3.2.7* (Maschke, 1899).** — *Sea $\rho : G \to \mathrm{GL}(V)$ una representación y sea $W \subseteq V$ un sub-espacio G-invariante. Entonces, existe un sub-espacio $W' \subseteq V$ que es G-invariante y que es complementario de W en V, es decir, tal que $V = W \oplus W'$.*

Demostración. — El producto interno hermitiano en $\mathbb{C}^n$ dado por

$$\langle x, y \rangle_{\mathbb{C}^n} := x_1 \overline{y}_1 + \ldots + x_n \overline{y}_n$$

induce, luego de escoger una base, un producto interno hermitiano $\langle u, v \rangle_0$ en V. Definimos el nuevo producto

$$\langle u, v \rangle := \frac{1}{|G|} \sum_{g \in G} \langle \rho_g(u), \rho_g(v) \rangle_0$$

para todos $u, v \in V$. Notemos que dicho producto es G-invariante, es decir, para todo $g \in G$ tenemos que

$$\langle \rho_g(u), \rho_g(v) \rangle = \langle u, v \rangle$$

para todos $u, v \in V$.[1]

En particular, si W es G-invariante, entonces el complemento ortogonal

$$W^{\perp} = \{v \in V \mid \langle v, w\rangle = 0 \text{ para todo } w \in W\}$$

es un complemento G-invariante de W en V. □

Observación 3.2.8. — Si $V = W \oplus W'$ como en el Teorema de Maschke y escribimos $v = w + w'$, donde $w \in W$ y $w' \in W'$, entonces

$$\rho_g(v) = \rho_g(w) + \rho_g(w').$$

Luego, las sub-representaciones ρ^W y $\rho^{W'}$ determinan ρ. Matricialmente, si R_g y R'_g son las matrices asociadas a ρ_g^W y $\rho_g^{W'}$ respectivamente, entonces la matriz de ρ_g está dada por

$$\begin{pmatrix} R_g & 0 \\ 0 & R'_g \end{pmatrix}.$$

3.3. Representaciones irreducibles

Definición 3.3.1. — Una representación (V, ρ) es **irreducible** si $V \neq \{0\}$, y si $\{0\}$ y V son sus únicas sub-representaciones. En otras palabras, V es irreducible si y sólo si todo sub-espacio G-invariante $W \subseteq V$ satisface $W = \{0\}$ o bien $W = V$.

Ejemplo 3.3.2. —

1. Toda representación de grado 1 es irreducible.
2. El grupo cíclico $\mathbb{Z}/n\mathbb{Z}$ tiene n representaciones irreducibles de grado 1. En efecto, una representación $\rho : \mathbb{Z}/n\mathbb{Z} \to \mathbb{C}^{\times}$ está determinada por la imagen de un generador $\rho([1]) \in \mathbb{C}^{\times}$. Además, $\rho([k])^n = 1$ para todo $[k] \in \mathbb{Z}/n\mathbb{Z}$. Obtenemos así representaciones $\rho_0, \ldots, \rho_{n-1}$ dadas por

   $$\rho_j([k]) = \exp\left(j\frac{2\pi k i}{n}\right)$$

   para todo $[k] \in \mathbb{Z}/n\mathbb{Z}$.

[1] En particular, si $\{e_1, \ldots, e_n\}$ es una base ortonormal respecto al nuevo producto $\langle \cdot, \cdot \rangle$, entonces la G-invarianza del producto interno se traduce en el hecho que las matrices asociadas a ρ_g respecto a dicha base son unitarias. En otras palabras,

$$R_g \in U_n(\mathbb{C}) = \{U \in \mathrm{GL}_n(\mathbb{C}) \mid U^*U = UU^* = \mathrm{I}_n\}$$

para todo $g \in G$, donde $U^* = \overline{{}^tU}$ es la matriz adjunta de U.

3. Si $\dim_{\mathbb{C}}(V) \geq 2$, las representaciones estándar (de los grupos infinitos) $\mathrm{SL}(V)$ y $\mathrm{GL}(V)$ son irreducibles, pues estos grupos actúan transitivamente en $V \setminus \{0\}$.

Ejercicio 3.3.3. — Probar que toda representación irreducible de un grupo finito G es grado $\leq |G|$.

Teorema 3.3.4. — *Toda representación es suma directa de representaciones irreducibles.*

Demostración. — Sea (V, ρ) una representación de un grupo finito G. Procedemos por inducción en la dimensión $\dim_{\mathbb{C}}(V)$.

Si V es irreducible entonces no hay nada que probar. Si por el contrario V no es irreducible y $W \subseteq V$ es una sub-representación no-nula, entonces el teorema de Maschke implica que existe una sub-representación complementaria $W' \subseteq V$ tal que $V = W \oplus W'$. Dado que $\dim_{\mathbb{C}}(W), \dim_{\mathbb{C}}(W') < \dim_{\mathbb{C}}(V)$ tenemos por hipótesis de inducción que W y W' son sumas directas de representaciones irreducibles, de donde se deduce el resultado. □

¡Atención! — Sea (V, ρ) una representación de un grupo finito G. La descomposición

$$V = W_1 \oplus W_2 \oplus \cdots \oplus W_k$$

en representaciones irreducibles **no es única**. Por ejemplo, la representación $\rho : G \to \mathrm{GL}(V),\ g \mapsto \mathrm{id}_V$ para todo $g \in G$ no es irreducible si $\dim_{\mathbb{C}}(V) \geq 2$. Por otra parte, si $\{e_1, \ldots, e_n\}$ es una base de V y si $W_i := \mathrm{Vect}_{\mathbb{C}}\langle e_i \rangle$ es la recta vectorial asociada a e_i, entonces $V = W_1 \oplus \cdots \oplus W_n$ es una descomposición en representaciones irreducibles, la cual claramente no es única.

Observación 3.3.5. — Sea W una representación irreducible de un grupo G. Dada V una representación arbitraria de G, veremos más adelante (ver Teorema 3.7.5) que dada cualquier descomposición

$$V = W_1 \oplus W_2 \oplus \cdots \oplus W_k$$

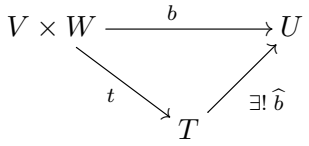
en representaciones irreducibles, el número de factores W_i tales que $W_i \cong W$ **no depende** de la descomposición.

3.4. Producto tensorial de espacios vectoriales

En esta sección, independiente del resto del capítulo, discutiremos generalidades sobre el producto tensorial (o producto de Kronecker) de dos espacios vectoriales.

Durante esta sección, denotaremos por k un cuerpo cualquiera.

***Definición 3.4.1* (producto tensorial).** — Sean V y W dos k-espacios vectoriales. Un **producto tensorial** de V y W es un k-espacio vectorial T junto con una aplicación **bilineal** $t : V \times W \to T$ verificando la siguiente propiedad universal: si $b : V \times W \to U$ es una aplicación bilineal, entonces existe una única aplicación lineal $\widehat{b} : T \to U$ tal que $b = \widehat{b} \circ t$. En otras palabras, tal que el siguiente diagrama es conmutativo



Teorema 3.4.2. — *Sean V y W dos k-espacios vectoriales. Existe un producto tensorial de V y W, denotado $V \otimes W$, el cual es único módulo un único isomorfismo.*

Demostración. — Comencemos por probar la existencia de un producto tensorial. Sea $k^{V\times W}$ el k-espacio vectorial de base $\{e_{(v,w)}\}_{(v,w)\in V\times W}$. En otras palabras, un elemento de $k^{V\times W}$ es una suma finita de la forma

$$\sum_{\text{finita}} \lambda_{(v,w)} e_{(v,w)}, .$$

donde $\lambda_{(v,w)} \in k$.

Es importante notar que la aplicación $V \times W \to k^{V\times W}$, $(v, w) \mapsto e_{(v,w)}$ no es bilineal. Sin embargo, si denotamos por S al k-sub-espacio vectorial de $k^{V\times W}$ generado por los elementos de la forma

$$e_{(v+v',w)} - e_{(v,w)} - e_{(v',w)},\ e_{(v,w+w')} - e_{(v,w)} - e_{(v,w')},$$
$$e_{(\lambda v,w)} - \lambda e_{(v,w)},\ e_{(v,\lambda w)} - \lambda e_{(v,w)},$$

donde $v, v' \in V$, $w, w' \in W$ y $\lambda \in k$, entonces el espacio vectorial cociente $T := k^{V\times W}/S$ dotado de la aplicación bilineal

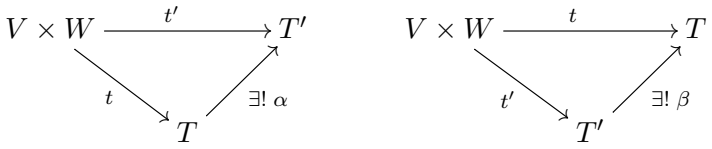
$$t : V \times W \longrightarrow k^{V\times W}/S$$
$$(v, w) \longmapsto [e_{(v,w)}]$$

es un producto tensorial de V y W. En lo que sigue denotaremos $V \otimes W := T$ y $v \otimes w := t((v, w)) = [e_{(v,w)}]$, donde $v \in V$ y $w \in W$.

No es difícil notar que si $b : V \times W \to U$ es una aplicación bilineal, entonces la aplicación inducida $B : k^{V\times W} \to U$, $e_{(v,w)} \mapsto b(v, w)$ es lineal y se anula en $S \subseteq k^{V\times W}$. Luego, la propiedad universal del cociente implica que existe

una única aplicación lineal $\widehat{b} : V \otimes W \mapsto U,\ v \otimes w \mapsto b(v,w)$, la cual verifica $b = \widehat{b} \circ t$.

La únicidad de $T = V \otimes W$ módulo un único isomorfismo es consecuencia de la propiedad universal. En efecto, si (T', t') es otro producto tensorial de V y W entonces los diagramas conmutativos



donde $t' = \alpha \circ t$ y $t = \beta \circ t'$. Luego, $t' = \alpha \circ t = \alpha \circ (\beta \circ t') = (\alpha \circ \beta) \circ t' = \mathrm{id}_{T'} \circ t'$ y $t = \beta \circ t' = \beta \circ (\alpha \circ t) = (\beta \circ \alpha) \circ t = \mathrm{id}_T \circ t$. Finalmente, la unicidad de α y β implica que $\beta \circ \alpha = \mathrm{id}_T$ y $\alpha \circ \beta = \mathrm{id}_{T'}$, es decir, α y β son isomorfismos. □

Recuerdo 3.4.3. — Sean V y W dos k-espacios vectoriales. Recordemos que $\mathrm{Hom}(V,W) = \{f : V \to W \text{ lineal}\}$, y que $V^* = \mathrm{Hom}(V,k)$ es el espacio dual de V.

Corolario 3.4.4. — *Hay un isomorfismo entre k-espacios vectoriales*

$$\{b : V \times W \to U \text{ bilineal}\} \cong \mathrm{Hom}(V \otimes W, U).$$

En particular, $\{b : V \times W \to k \text{ forma bilineal}\} \cong (V \otimes W)^*$.

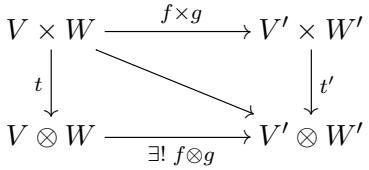
Demostración. — La aplicación $b \mapsto \widehat{b}$ es un isomorfismo. □

***Proposición 3.4.5* (functorialidad).** — *Sean $f : V \to V'$ y $g : W \to W'$ son aplicaciones lineales. Entonces existe una única aplicación lineal*

$$f \otimes g : V \otimes W \to V' \otimes W'$$

tal que $(f \otimes g)(v \otimes w) = f(v) \otimes g(w)$ para todos $v \in V$, $w \in W$. Más aún, $(f' \otimes g') \circ (f \otimes g) = (f' \circ f) \otimes (g' \circ g)$.

Demostración. — Basta completar el diagrama conmutativo



donde el morfismo $f \otimes g$ se obtiene al aplicar la propiedad universal a la aplicación bilineal $t' \circ (f \times g)$. La última parte del enunciado se deduce del mismo modo, y se deja como ejercicio para el lector. □

Ejercicio 3.4.6. — Sea $\{v_i\}_{i\in I}$ una base de V y sea $\{w_j\}_{j\in J}$ una base de W. Probar que $\{v_i \otimes w_j\}_{(i,j)\in I\times J}$ es una base de $V \otimes W$. En particular, $\dim_k(V \otimes W) = \dim_k(V)\dim_k(W)$.

Usando el ejercicio anterior, o bien usando la propiedad universal del producto tensorial, es posible probar el siguiente resultado (cuya demostración dejamos como ejercicio).

Proposición 3.4.7. — *Sean U, V y W tres k-espacios vectoriales. Hay isomorfismos canónicos:*

1. $k \otimes V \xrightarrow{\sim} V$, $\lambda \otimes v \mapsto \lambda v$.
2. $(U \oplus V) \otimes W \xrightarrow{\sim} (U \otimes W) \oplus (V \otimes W)$, $(u+v)\otimes w \mapsto u\otimes w + v \otimes w$.
3. $U \otimes V \xrightarrow{\sim} V \otimes U$, $u \otimes v \mapsto v \otimes u$.
4. $U \otimes (V \otimes W) \xrightarrow{\sim} (U \otimes V) \otimes W$, $u \otimes (v \otimes w) \mapsto (u \otimes v) \otimes w$.

Ejemplo 3.4.8. — Supongamos que $\{v_{1,j}\}_{j\in I_1}$ es una base de V_1, que $\{v_{2,i}\}_{i\in I_2}$ es una base de V_2, que $\{w_{1,l}\}_{l\in J_1}$ es una base de W_1, y que $\{w_{2,k}\}_{k\in J_2}$ es una base de W_2. Si $f : V_1 \to V_2$ y $g : W_1 \to W_2$ son aplicaciones lineales dadas por matrices $A = (a_{ij})_{i\in I_2,\, j\in I_1}$ y $B = (b_{kl})_{k\in J_2,\, l\in J_1}$ respecto a las bases anteriores, entonces obtenemos por bilinealidad del producto tensorial que

$$(f \otimes g)(v_{1,j} \otimes w_{1,l}) = \sum_{\substack{i\in I_2\\ k\in J_2}} a_{ij}b_{kl}v_{2,i} \otimes w_{2,k},$$

de tal suerte que la matriz de $f \otimes g$ en las bases $\{v_{1,j} \otimes w_{1,l}\}_{(j,l)\in I_1\times J_1}$ de $V_1 \otimes W_1$ y $\{v_{2,i} \otimes w_{2,k}\}_{(i,k)\in I_2\times J_2}$ de $V_2 \otimes W_2$ está dada por

$$A \otimes B := (a_{ij}b_{kl})_{(i,k)\in I_2\times J_2,\,(j,l)\in I_1\times J_1}.$$

Por ejemplo, si todos los espacios vectoriales involucrados son de dimensión 2, entonces tenemos que $A \otimes B$ está dada por

$$\begin{pmatrix} a_{11} & a_{12}\\ a_{21} & a_{22}\end{pmatrix} \otimes \begin{pmatrix} b_{11} & b_{12}\\ b_{21} & b_{22}\end{pmatrix} = \begin{pmatrix} a_{11}B & a_{12}B\\ a_{21}B & a_{22}B\end{pmatrix} = \begin{pmatrix} a_{11}b_{11} & a_{11}b_{12} & a_{12}b_{11} & a_{12}b_{12}\\ a_{11}b_{21} & a_{11}b_{22} & a_{12}b_{21} & a_{12}b_{22}\\ a_{21}b_{11} & a_{21}b_{12} & a_{22}b_{11} & a_{22}b_{12}\\ a_{21}b_{21} & a_{21}b_{22} & a_{22}b_{21} & a_{22}b_{22}\end{pmatrix}.$$

Ejercicio 3.4.9. —

a) Probar que $\operatorname{tr}(A \otimes B) = \operatorname{tr}(A)\operatorname{tr}(B)$.
b) Probar que $\operatorname{rango}(A \otimes B) = \operatorname{rango}(A)\operatorname{rango}(B)$.
c) Si $A \in M_{a\times a}(k)$ y $B \in M_{b\times b}(k)$, probar que $\det(A\otimes B) = \det(A)^b \det(B)^a$.

En lo que sigue, supondremos que $k = \mathbb{C}$. Supongamos que $\{e_1, \ldots, e_n\}$ es una base de $V \cong \mathbb{C}^n$ y consideremos el automorfismo

$$\Theta : V \otimes V \xrightarrow{\sim} V \otimes V$$
$$e_i \otimes e_j \mapsto e_j \otimes e_i$$

Notar que para todos $v, w \in V$ se tiene que $\Theta(v \otimes w) = w \otimes v$ y luego Θ es independiente de la base escogida.

Si denotamos $T^2V := V \otimes V$, entonces T^2V se descompone en suma directa

$$T^2V = S^2V \oplus \bigwedge^2 V,$$

donde

1. $S^2V = \mathrm{Sym}^2(V) = \{z \in V \otimes V \mid \Theta(z) = z\}$ es el llamado **cuadrado simétrico** de V. Notar que $\{e_i \otimes e_j + e_j \otimes e_i\}_{i \leq j}$ es una base de S^2V y luego $\dim_{\mathbb{C}} S^2V = \frac{n(n+1)}{2}$.
2. $\bigwedge^2 V = \mathrm{Alt}^2(V) = \{z \in V \otimes V \mid \Theta(z) = -z\}$ es el llamado **cuadrado alternado** de V. Notar que $\{e_i \otimes e_j - e_j \otimes e_i\}_{i < j}$ es una base de $\bigwedge^2 V$ y luego $\dim_{\mathbb{C}} \bigwedge^2 V = \frac{n(n-1)}{2}$.

Observamos que todo elemento $v \otimes w \in T^2V$ se escribe de la forma

$$v \otimes w = \underbrace{\frac{1}{2}(v \otimes w + w \otimes v)}_{\text{en } S^2V} + \underbrace{\frac{1}{2}(v \otimes w - w \otimes v)}_{\text{en } \bigwedge^2 V}.$$

Por lo anterior, definimos para $v, w \in V$ los vectores

$$vw := \frac{1}{2}(v \otimes w + w \otimes v) \in S^2V,$$
$$v \wedge w := \frac{1}{2}(v \otimes w - w \otimes v) \in \bigwedge^2 V.$$

En particular, con la notación anterior, tenemos que $\{e_i e_j\}_{i \leq j}$ es una base de S^2V, y que $\{e_i \wedge e_j\}_{i<j}$ es una base de $\bigwedge^2 V$.

Definición 3.4.10. — Sean $\rho_1 : G \to \mathrm{GL}(V_1)$ y $\rho_2 : G \to \mathrm{GL}(V_2)$ representaciones de un grupo G. Definimos su **producto tensorial**

$$\rho_1 \otimes \rho_2 : G \to \mathrm{GL}(V_1 \otimes V_2)$$

mediante $\rho_g(v_1 \otimes v_2) := \rho_{1,g}(v_1) \otimes \rho_{2,g}(v_2)$ para todo $g \in G$, $v_1 \in V_1$ y $v_2 \in V_2$.

Matricialmente, si $R_{1,g}$ y $R_{2,g}$ son las matrices asociadas a $\rho_{1,g}$ y $\rho_{2,g}$ respectivamente, entonces la matriz asociada a $(\rho_1 \otimes \rho_2)_g$ es $R_{1,g} \otimes R_{2,g}$.

Ejercicio 3.4.11. — Probar que si V y W son representaciones de grado 1, entonces $V \otimes W$ es una representación de grado 1. Describir esta situación matricialmente.[(2)]

Un caso particular importante es el siguiente. Sea $\rho : G \to \mathrm{GL}(V)$ una representación de un grupo G. Entonces, obtenemos una representación inducida $\rho_{T^2V} : G \to \mathrm{GL}(T^2V)$ dada por $\rho_{T^2V}(v_1 \otimes v_2) = \rho_g(v_1) \otimes \rho_g(v_2)$. En particular, observamos que S^2V y $\bigwedge^2 V$ son G-invariantes, y luego inducen sub-representaciones ρ_{S^2V} y $\rho_{\bigwedge^2 V}$ de G.

3.5. Caracteres

Recuerdo 3.5.1. — Recordemos que si $A \in M_{n\times n}(\mathbb{C})$ y $P \in \mathrm{GL}_n(\mathbb{C})$, entonces la traza verifica $\mathrm{tr}(A) = \mathrm{tr}(PAP^{-1})$. En otras palabras, la traza de una transformación lineal es independiente de la base. Más aún, si $\lambda_1, \ldots, \lambda_n \in \mathbb{C}$ son los valores propios de A, entonces se tiene que $\mathrm{tr}(A) = \lambda_1 + \ldots + \lambda_n$.

***Definición 3.5.2* (carácter).** — Sea $\rho : G \to \mathrm{GL}(V)$ una representación de un grupo G. El **carácter** de $\rho = \rho_V$ es la función χ_V (o χ_ρ) dada por

$$\begin{aligned} \chi_V : G &\longrightarrow \mathbb{C} \\ g &\longmapsto \mathrm{tr}(\rho_g). \end{aligned}$$

A partir de las propiedades de la traza se deducen las siguientes propiedades de los caracteres.

Proposición 3.5.3. — *Sea $\chi : G \to \mathbb{C}$ el carácter de una representación $\rho : G \to \mathrm{GL}_n(\mathbb{C})$ de grado n. Entonces:*

1. $\chi(e) = n$.
2. $\chi(g^{-1}) = \overline{\chi(g)}$ *para todo* $g \in G$.
3. $\chi(hgh^{-1}) = \chi(g)$ *para todos* $g, h \in G$. *En particular,* $\chi(g_1g_2) = \chi(g_2g_1)$ *para todos* $g_1, g_2 \in G$.

Demostración. — El punto (1) se obtiene de $\mathrm{tr}(\rho_e) = \mathrm{tr}(\mathrm{id}_V) = \dim_{\mathbb{C}}(V)$. Para probar (2), notamos que el hecho que G sea un grupo finito implica que cada transformación lineal ρ_g es de orden finito. Luego, todos los valores propios $\lambda_1, \ldots, \lambda_n$ de ρ_g son raíces de la unidad. En efecto, si $\rho_g^m = \mathrm{id}_V$ para cierto

[(2)] Mas adelante veremos que, en general, el producto tensorial de dos representaciones irreducibles puede no ser irreducible.

m y v_i es un vector propio asociado al valor propio λ_i, entonces tenemos que $\rho_g^m v_i = \lambda_i^m v_i = v_i$, de donde se concluye que $\lambda_i^m = 1$.

Por otra parte, si $\lambda = e^{i\theta}$ donde $\theta \in \mathbb{R}$ entonces $\overline{\lambda} = e^{-i\theta} = \lambda^{-1}$. Luego,[3]

$$\overline{\chi(g)} = \overline{\mathrm{tr}(\rho_g)} = \sum_{i=1}^{n} \overline{\lambda_i} = \sum_{i=1}^{n} \frac{1}{\lambda_i} = \mathrm{tr}(\rho_g^{-1}) = \mathrm{tr}(\rho_{g^{-1}}) = \chi(g^{-1}).$$

Finalmente, el punto (3) sigue de la igualdad $\mathrm{tr}(AB) = \mathrm{tr}(BA)$. □

***Definición 3.5.4* (función central).** — Una función $f : G \to \mathbb{C}$ es llamada una **función central** si es constante en cada clase de conjugación de G, es decir, si $f(hgh^{-1}) = f(g)$ para todos $g, h \in G$. Si C es una clase de conjugación de G, denotamos por $f(C)$ el valor de f en C. El $\mathbb{C}$-espacio vectorial

$$\mathscr{C}(G) := \{f : G \to \mathbb{C} \text{ función central}\}$$

tiene dimensión $\dim_{\mathbb{C}} \mathscr{C}(G) = \mathrm{card}(\{\text{clases de conjugación de } G\})$.

Observación 3.5.5. — Veremos más adelante (ver Teorema 3.8.3) que los caracteres forman una base del espacio de funciones centrales $\mathscr{C}(G)$.

Ejemplo 3.5.6. —

1. El carácter de la representación regular $\rho_R : G \to \mathrm{GL}_{|G|}(\mathbb{C})$ de G está dado por
$$\chi_R(g) = \begin{cases} |G| & \text{si } g = e \\ 0 & \text{si } g \neq e \end{cases},$$
es decir, $\chi_R = |G| \mathbb{1}_{C_e}$, donde $\mathbb{1}_{C_e}$ denota la función característica de la clase de conjugación $C_e = \{e\}$.
2. Recordemos que las clases de conjugación de $\mathfrak{S}_3$ están en biyección con las particiones de $n = 3$ (ver Proposicipon 2.2.8). Las particiones de $n = 3$ son $1+1+1$, $1+2$ y 3, y las clases de conjugación correspondientes en $\mathfrak{S}_3$ son $C_e = \{\mathrm{id}\}$, $C_t = \{(1,2),(1,3),(2,3)\}$ y $C_c = \{(2,3,1),(1,3,2)\}$. Sea $\rho : \mathfrak{S}_3 \to \mathrm{GL}_3(\mathbb{C})$ la representación de permutación, entonces[4] $\chi_\rho(C_e) = 3$, $\chi_\rho(C_t) = 1$ y $\chi_\rho(C_c) = 0$.

[3] Si $A \in \mathrm{GL}_n(\mathbb{C})$ y $A = PJP^{-1}$ es la forma canónica de Jordan, entonces $A^{-1} = PJ^{-1}P^{-1}$. En particular, si $\lambda_1, \ldots, \lambda_n$ son los valores propios de A, entonces $\mathrm{tr}(A) = \lambda_1 + \ldots + \lambda_n$ y $\mathrm{tr}(A^{-1}) = \frac{1}{\lambda_1} + \ldots + \frac{1}{\lambda_n}$.

[4] Notar que el valor del carácter de la representación de permutación en cada clase de conjugación es exactamente la cantidad de 1 que aparecen en la respectiva partición, es decir, la cantidad de elementos fijos por la acción de una permutación cualquiera en dicha clase de conjugación. Esta observación se generaliza a $\mathfrak{S}_n$.

3. Sea $\rho = \rho_V : G \to \mathrm{GL}(V)$ una representación de un grupo G. Definimos su **representación dual** mediante

$$\rho^* := \rho_{V^*} : G \to \mathrm{GL}(V^*)$$
$$g \mapsto \rho_g^* := {}^{\mathrm{t}}\rho_{g^{-1}} = {}^{\mathrm{t}}\rho_g^{-1}$$

Equivalentemente, ρ_g^* se define mediante la relación $\langle x^*, x\rangle = \langle \rho_g^*(x^*), \rho_g(x)\rangle$ para todos $x \in V$ y $x^* \in V^* = \mathrm{Hom}(V, \mathbb{C})$. Calculamos

$$\chi_{V^*}(g) = \chi_{\rho^*}(g) = \mathrm{tr}({}^{\mathrm{t}}\rho_g^{-1}) = \mathrm{tr}(\rho_g^{-1}) = \chi_V(g^{-1}) = \overline{\chi_V(g)},$$

gracias a la Proposición 3.5.3.

***Recuerdo 3.5.7* (Cayley-Hamilton).** — Recordemos que si $A \in M_{n\times n}(\mathbb{C})$ es una matriz con coeficientes complejos, su **polinomio característico** está dado por

$$p_A(\lambda) = \det(\lambda\,\mathrm{I}_n - A).$$

Por otra parte, su **polinomio minimal** es por definición el polinomio complejo $m_A(\lambda)$ con coeficiente principal 1 y de grado minimal de tal suerte que $m_A(A) = 0$. En otras palabras, cualquier otro polinomio $Q(\lambda)$ verificando $Q(A) = 0$ es un múltiplo (polinomial) de $m_A(\lambda)$.

Un resultado importante de álgebra lineal es que la matriz A es diagonalizable si y sólo su el polinomio minimal $m_A(\lambda)$ se factoriza sobre $\mathbb{C}$ en factores lineales *distintos*. Por ejemplo, si $m_A(\lambda) = \lambda^m - 1$ o bien $m_A(\lambda) = \lambda(\lambda - 1)$ entonces A es diagonalizable.

El teorema de Cayley-Hamilton (c.f. Teorema 4.2.37), demostrado en ciertos casos particulares por Cayley (1853) y por Hamilton (1858), y finalmente probado por Frobenius (1878), afirma que el polinomio minimal $m_A(\lambda)$ de una matriz A divide al polinomio característico $p_A(\lambda)$. Equivalentemente, $p_A(A) = 0$.

Observación 3.5.8. — Una aplicación importante del teorema de Cayley-Hamilton es probar que toda matriz $A \in M_{n\times n}(\mathbb{C})$ de orden finito es diagonalizable sobre $\mathbb{C}$. En efecto, si $A^m = \mathrm{I}_n$ para cierto $m \in \mathbb{N}^{\geq 1}$ entonces $m_A(\lambda)$ divide al polinomio $\lambda^m - 1$, por minimalidad de m_A. Dado que este último se factoriza en factores lineales distintos, $m_A(\lambda)$ también y luego A es diagonalizable[(5)].

[(5)] De manera completamente análoga, utilizando que $m_A(\lambda)$ divide $\lambda^2 - \lambda$, se prueba que todo operador de proyección es diagonalizable.

Proposición 3.5.9. — *Sean $\rho_V : G \to \mathrm{GL}(V)$ y $\rho_W : G \to \mathrm{GL}(W)$ dos representaciones de un grupo G. Entonces:*

1. $\chi_{V^*} = \overline{\chi_V}$.
2. $\chi_{V\oplus W} = \chi_V + \chi_W$.
3. $\chi_{V\otimes W} = \chi_V \cdot \chi_W$.
4. *Si $W \subseteq V$ es una sub-representación, entonces* $\chi_V = \chi_W + \chi_{V/W}$.
5. $\chi_{S^2V}(g) = \frac{1}{2}(\chi_V(g)^2 + \chi_V(g^2))$.
6. $\chi_{\bigwedge^2 V} = \frac{1}{2}(\chi_V(g)^2 - \chi_V(g^2))$.

En particular, $\chi_{V\otimes V} = \chi_V^2 = \chi_{S^2V} + \chi_{\bigwedge^2 V}$.

Demostración. — Ya hemos demostrado (1), (2), (3) y (4).

Veamos (5) y (6). Sea $g \in G$ y notemos que ρ_g es de orden finito, puesto que G es un grupo finito. En particular ρ_g es diagonalizable, gracias a la Observación 3.5.8.

Sea $\{e_1, \dots, e_n\}$ una base de V formada por los vectores propios de ρ_g, i.e., $\rho_g(e_i) = \lambda_i e_i$ con $\lambda_i \in \mathbb{C}$. En particular, $\rho_{g^2}(e_i) = (\rho_g \circ \rho_g)(e_i) = \rho_g(\lambda_i e_i) = \lambda_i^2 e_i$, y luego $\chi_V(g) = \sum_{i=1}^n \lambda_i$ y $\chi_V(g^2) = \sum_{i=1}^n \lambda_i^2$.

Recordemos que $\{e_i \wedge e_j\}_{1\le i<j\le n}$ es una base de $\bigwedge^2 V$. Notamos que los $\{e_i \wedge e_j\}_{1\le i<j\le n}$ son además vectores propios de $\rho_{\bigwedge^2 V, g}$ con valores propios $\{\lambda_i\lambda_j\}_{1\le i<j\le n}$. Luego,

$$\chi_{\bigwedge^2 V}(g) = \sum_{1\le i<j\le n} \lambda_i\lambda_j = \frac{1}{2}\left(\sum_{1\le i\le n} \lambda_i\right)^2 - \frac{1}{2}\sum_{1\le i\le n} \lambda_i^2 = \frac{1}{2}(\chi_V(g)^2 - \chi_V(g^2)).$$

De manera similar, los vectores $\{e_ie_j\}_{1\le i\le j\le n}$ forman una base de S^2V, y además son vectores propios de $\rho_{S^2V,\rho}$ con valores propios $\{\lambda_i\lambda_j\}_{1\le i\le j\le n}$. Luego,

$$\chi_{S^2V}(g) = \sum_{1\le i\le j\le n} \lambda_i\lambda_j = \frac{1}{2}\left(\sum_{1\le i\le n} \lambda_i\right)^2 + \frac{1}{2}\sum_{1\le i\le n} \lambda_i^2 = \frac{1}{2}(\chi_V(g)^2 + \chi_V(g^2)),$$

de donde se concluye el resultado. □

Ejercicio 3.5.10. — Si $\chi = \chi_V : G \to \mathbb{C}$ es un carácter, denotamos

$$\chi_\sigma^2 := \chi_{S^2V} \text{ y } \chi_\alpha^2 := \chi_{\bigwedge^2 V}.$$

En particular, $\chi^2 = \chi_\sigma^2 + \chi_\alpha^2$. Sean χ y χ' dos caracteres. Probar que

$$(\chi+\chi')_\sigma^2 = \chi_\sigma^2 + \chi'^2_\sigma + \chi\chi' \text{ y } (\chi+\chi')_\alpha^2 = \chi_\alpha^2 + \chi'^2_\alpha + \chi\chi'.$$

3.6. Lema de Schur

El siguiente resultado de Schur probado en 1905 es una observación simple sobre morfismos entre representaciones irreducibles, y que tiene importantes consecuencias en la teoría de representaciones.

***Proposición 3.6.1* (Lema de Schur).** — *Sean* $\rho_V : G \to \mathrm{GL}(V)$ *y* $\rho_W : G \to \mathrm{GL}(W)$ *dos representaciones* irreducibles *de un grupo* G*, y sea* $u : V \to W$ *un morfismo de representaciones. Entonces:*

1. u *es un isomorfismo o bien* $u = 0$.
2. *Si* $\rho_V = \rho_W$ *entonces* u *es una* homotecia*, i.e.,* $u = \lambda \mathrm{Id}_V$ *con* $\lambda \in \mathbb{C}$.

Demostración. — Para probar (1) notamos que tanto $\ker(u)$ como $\mathrm{Im}(u)$ son G-invariantes. Si u no es inyectivo entonces $\ker(u) \neq \{0_V\}$ y luego $\ker(u) = V$, pues V es una representación irreducible. En otras palabras, si u no es inyectivo entonces $u = 0$. Por otra parte, si u no es sobreyectivo entonces $\mathrm{Im}(u) \neq W$ y luego $\mathrm{Im}(u) = \{0_W\}$, pues W es una representación irreducible. En otras palabras, si u no es sobreyectivo entonces $u = 0$.

Para probar (2) notamos que si $\lambda \in \mathbb{C}$ es un valor propio de u, entonces el sub-espacio $\ker(u - \lambda \mathrm{Id}_V)$ es G-invariante, pues por definición de morfismo de representaciones u conmuta con la acción de G. Dicho sub-espacio es no-nulo pues contiene al menos un vector propio $v \neq 0$, de donde se concluye que $\ker(u - \lambda \mathrm{Id}_V) = V$, gracias a que V es una representación irreducible. En otras palabras, $u = \lambda \mathrm{Id}_V$. □

Corolario 3.6.2. — *Sean* $\rho_V : G \to \mathrm{GL}(V)$ *y* $\rho_W : G \to \mathrm{GL}(W)$ *dos representaciones* irreducibles *de un grupo* G*, y sea* $u : V \to W$ *una* aplicación lineal *arbitraria. Consideremos la aplicación*

$$u^0 := \frac{1}{|G|} \sum_{g \in G} \rho_{W,g}^{-1} \circ u \circ \rho_{V,g},$$

la cual define un morfismo de representaciones $u^0 : V \to W$*. Más aún,*

1. *Si* ρ_V *y* ρ_W *no son isomorfas, entonces* $u = 0$.
2. *Si* $\rho_V = \rho_W$*, entonces* u^0 *es una homotecia de factor* $\frac{\mathrm{tr}(u)}{\dim_{\mathbb{C}}(V)}$.

Demostración. — Veamos que $u^0 : V \to W$ define efectivamente un morfismo de representaciones, es decir, $\rho_{W,g} \circ u^0 = u^0 \circ \rho_{V,g}$ para todo $g \in G$. Calculamos

$$\begin{aligned}\rho_{W,g}^{-1} \circ u^0 \circ \rho_{V,g} &= \frac{1}{|G|} \sum_{h \in G} \rho_{W,g}^{-1} \circ \rho_{W,h}^{-1} \circ u \circ \rho_{V,h} \circ \rho_{V,g} \\ &= \frac{1}{|G|} \sum_{h \in G} \rho_{W,hg}^{-1} \circ u \circ \rho_{V,hg} \\ &\underbrace{=}_{k=hg} \frac{1}{|G|} \sum_{k \in G} \rho_{W,k}^{-1} \circ u \circ \rho_{V,k} = u^0.\end{aligned}$$

Luego, el Lema de Schur aplicado al morfismo de representaciones u^0 implica (1). Del mismo modo, el Lema de Schur implica que si $\rho_V = \rho_W$ entonces $u^0 = \lambda \operatorname{Id}_V$. En particular, $\operatorname{tr}(u^0) = \lambda \dim_{\mathbb{C}}(V)$. Basta notar que en este caso

$$\operatorname{tr}(u^0) = \frac{1}{|G|} \sum_{g \in G} \operatorname{tr}(\rho_{V,g}^{-1} \circ u \circ \rho_{V,g}) = \frac{1}{|G|} \sum_{g \in G} \operatorname{tr}(u) = \operatorname{tr}(u),$$

de donde se obtiene (2). □

Observación 3.6.3. — Matricialmente, si $R_{V,g} = (a_{i_1 j_1}(g))$, $R_{W,g} = (a_{i_2 j_2}(g))$, $u = (u_{i_2 i_1})$ y $u^0 = (u^0_{i_2 i_1})$ entonces:

$$u^0_{i_2 i_1} = \frac{1}{|G|} \sum_{\substack{g \in G \\ j_1, j_2}} a_{i_2 j_2}(g^{-1}) u_{j_2 j_1} a_{j_1 i_1}(g),$$

la cual es una forma lineal en $u_{j_2 j_1}$. Luego (1) en el Corolorio 3.6.2 se traduce en que si $\rho_V \ncong \rho_W$ entonces

$$\sum_{g \in G} a_{i_2 j_2}(g^{-1}) a_{j_1 i_1}(g) = 0$$

para todos i_1, i_2, j_1, j_2. Por otra parte, si denotamos por

$$\delta_{i_2 i_1} = \begin{cases} 0 & \text{si } i_1 \neq i_2 \\ 1 & \text{si } i_1 = i_2 \end{cases}$$

la función delta de Kronecker, entonces (2) en el Corolorio 3.6.2 se traduce en que

$$u^0_{i_2 i_1} = \frac{\operatorname{tr}(u)}{\dim_{\mathbb{C}}(V)} \delta_{i_2 i_1} = \frac{1}{\dim_{\mathbb{C}}(V)} \sum_{j_1, j_2} \delta_{i_2 i_1} \delta_{j_2 j_1} u_{j_2 j_1},$$

de donde se deduce que

$$\frac{1}{|G|}\sum_{\substack{g\in G\\ j_1,j_2}} a_{i_2j_2}(g^{-1})u_{j_2j_1}a_{j_1i_1}(g) = \frac{1}{\dim_{\mathbb{C}}(V)}\sum_{j_1,j_2}\delta_{i_2i_1}\delta_{j_2j_1}u_{j_2j_1}.$$

Igualando los coeficientes que acompañan a $u_{j_2j_1}$ obtenemos la relación

$$\frac{1}{|G|}\sum_{g\in G} a_{i_2j_2}(g^{-1})a_{j_1i_1}(g) = \frac{1}{\dim_{\mathbb{C}}(V)}\delta_{i_2i_1}\delta_{j_2j_1} = \begin{cases} \frac{1}{\dim_{\mathbb{C}}(V)} & \text{si } i_1 = i_2 \text{ y } j_1 = j_2 \\ 0 & \text{sino} \end{cases}$$

para todos i_1, i_2, j_1, j_2.

3.7. Ortogonalidad de caracteres

***Definición 3.7.1* (producto bilineal).** — Sean $\varphi : G \to \mathbb{C}$ y $\psi : G \to \mathbb{C}$ dos funciones a valores complejos, donde G es un grupo finito. Definimos el producto bilineal

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

Observación 3.7.2. — Utilizando el producto bilineal anterior, podemos reescribir la interpretación matricial del Lema de Schur obtenida en la Observación 3.6.3 de la manera siguiente:

1. Si ρ_V y ρ_W no son isomorfas, entonces $\langle a_{i_2j_2}, a_{j_1i_1}\rangle = 0$ para todos i_1, i_2, j_1, j_2.
2. Si $\rho_V = \rho_W$ entonces $\langle a_{i_2j_2}, a_{j_1i_1}\rangle = \frac{1}{\dim_{\mathbb{C}}(V)}\delta_{i_2i_1}\delta_{j_2j_1}$ para todos i_1, i_2, j_1, j_2.

En particular, si las matrices $(a_{ij}(g))$ son *unitarias* entonces $(a_{ij}(g^{-1})) = (\overline{a_{ji}(g)})$ y luego (1) y (2) se interpretan como **relaciones de ortogonalidad**.

***Definición 3.7.3* (producto hermitiano).** — Sean $\varphi : G \to \mathbb{C}$ y $\psi : G \to \mathbb{C}$ dos funciones a valores complejos, donde G es un grupo finito. Definimos el producto hermitiano

$$(\varphi|\psi) := \frac{1}{|G|}\sum_{g\in G}\varphi(g)\overline{\psi(g)}.$$

En particular, si definimos $\psi^*(g) := \overline{\psi(g^{-1})}$ entonces $(\varphi \mid \psi) = \langle \varphi, \psi^*\rangle$, donde $\langle\cdot,\cdot\rangle$ es el producto bilineal de la Definición 3.7.1.

Un caso particular importante son los caracteres $\chi_V : G \to \mathbb{C}$. Sabemos gracias a la Proposición 3.5.3 que $\chi_V(g^{-1}) = \overline{\chi_V(g)}$ y luego $\chi_V^* = \chi_V$, es decir, los caracteres son *autoadjuntos*. En particular, $(\varphi \mid \chi_V) = \langle \varphi, \chi_V \rangle$ para toda función $\varphi : G \to \mathbb{C}$.

***Teorema 3.7.4* (Teorema de Frobenius).** — *Sean* $\rho_V : G \to \mathrm{GL}(V)$ *y* $\rho_W : G \to \mathrm{GL}(W)$ *dos representaciones* irreducibles *de un grupo* G. *Entonces:*

1. *Si* ρ_V *y* ρ_W *no son isomorfas, entonces* $\langle \chi_V, \chi_W \rangle = 0$.
2. *Si* $\rho_V = \rho_W$, *entonces* $\langle \chi_V, \chi_V \rangle = 1$.

Demostración. — Si $\rho_{V,g}$ corresponde a la matriz $R_{V,g} = (a_{i_1 j_1}(g))$, entonces $\chi_V(g) = \sum a_{i_1 i_1}(g)$. Del mismo modo, si $\rho_{W,g}$ corresponde a la matriz $R_{W,g} = (a_{i_2 j_2}(g))$, entonces $\chi_W(g) = \sum a_{i_2 i_2}(g)$. Luego, tenemos que si ρ_V y ρ_W no son isomorfas entonces

$$\langle \chi_V, \chi_W \rangle = \sum_{i_1, i_2} \langle a_{i_1 i_1}, a_{i_2 i_2} \rangle = 0,$$

donde la última igualdad se obtuvo en la Observación 3.7.2. Del mismo modo, la Observación 3.7.2 permite calcular

$$\langle \chi_V, \chi_V \rangle = \sum_{i_1, i_2} \langle a_{i_1 i_1}, a_{i_2 i_2} \rangle = \sum_{i_1, i_2} \frac{1}{\dim_{\mathbb{C}}(V)} \delta_{i_1 i_2} = \frac{\dim_{\mathbb{C}}(V)}{\dim_{\mathbb{C}}(V)} = 1,$$

de donde se concluye el resultado. □

Veamos ahora algunas consecuencias del Teorema de Frobenius.

Teorema 3.7.5. — *Sea* $\rho : G \to \mathrm{GL}(V)$ *una representación de un grupo finito* G *y sea*

$$V = W_1 \oplus \cdots \oplus W_k$$

una descomposición en representaciones irreducibles. Sea W *una representación* irreducible *arbitraria. Entonces, el número de representaciones* W_i *tales que* $W_i \cong W$ *está dado por* $\langle \chi_V, \chi_W \rangle$. *En particular, dicho número es independiente de la descomposición dada.*

Demostración. — Tenemos que $\chi_V = \chi_{W_1} + \ldots + \chi_{W_k}$. Entonces,

$$\langle \chi_V, \chi_W \rangle = \langle \chi_{W_1}, \chi_W \rangle + \ldots + \langle \chi_{W_k}, \chi_W \rangle.$$

Por otra parte, dado que W_i y W son irreducibles, el Teorema de Frobenius implica que

$$\langle \chi_{W_i}, \chi_W \rangle = \begin{cases} 1 & \text{si } \rho_{W_i} \cong \rho_W \\ 0 & \text{sino} \end{cases}$$

de donde se concluye el resultado. □

Corolario 3.7.6. — *Sean $\rho_V : G \to \mathrm{GL}(V)$ y $\rho_W : G \to \mathrm{GL}(W)$ dos representaciones de un grupo G. Entonces $\rho_V \cong \rho_W$ si y sólo si $\chi_V = \chi_W$.*

Demostración. — Si $\chi_V = \chi_W$ entonces el Teorema 3.7.5 implica que V y W contienen el mismo número de veces cualquier representación irreducible dada. □

Observación 3.7.7. — Notar que el Ejercicio 3.3.3 implica que para todo grupo finito G, existen sólo un número finito $W_1, \ldots, W_h$ de representaciones irreducibles de G, módulo isomorfismo. En efecto, dado que toda representación V está determinada por su carácter χ_V, basta notar que $\chi_V(g)$ es la suma de $\dim_{\mathbb{C}}(V) \leq |G|$ raíces de la unidad cuyo orden divide $\mathrm{ord}(g)$. Más adelante (ver Teorema 3.8.4) probaremos que hay tantas representaciones irreducibles como clases de conjugación de G.

En conclusión, podemos reducir el estudio de representaciones de un grupo finito G al estudio de todos los posibles caracteres $\chi_1, \ldots, \chi_h$ de las (finitas) representaciones irreducibles $W_1, \ldots, W_h$. Luego, toda representación V es isomorfa a la suma directa

$$V \cong W_1^{\oplus m_1} \oplus \cdots \oplus W_h^{\oplus m_h},$$

para ciertos enteros $m_i \in \mathbb{N}$. Más aún, el Teorema de Frobenius y el hecho que $\chi_V = m_1\chi_1 + \ldots + m_h\chi_h$ implican que $m_i = \langle \chi_V, \chi_i \rangle$ y que

$$\langle \chi_V, \chi_V \rangle = m_1^2 + \ldots + m_h^2.$$

Una consecuencia de la discusión anterior es el siguiente criterio de irreducibilidad.

Teorema 3.7.8. — *Sea $\rho_V : G \to \mathrm{GL}(V)$ representación de un grupo G. Entonces V es irreducible si y sólo si $\langle \chi_V, \chi_V \rangle = 1$.*

Demostración. — La representación V es irreducible si y sólo si $V \cong W_i$ para cierto $i \in \{1, \ldots, h\}$. Esto último equivale a que $m_i = 1$ y $m_j = 0$ si $j \neq i$, que a su vez equivale a que $\langle \chi_V, \chi_V \rangle = 1$, puesto que $\langle \chi_V, \chi_V \rangle = m_1^2 + \ldots + m_h^2$. □

Recuerdo 3.7.9 **(representación regular).** — Sea

$$R : G \longrightarrow \mathrm{GL}_{|G|}(\mathbb{C})$$
$$g \longmapsto \rho_g$$

la representación regular de G, es decir, en $\mathbb{C}^{|G|}$ con base $\{e_g\}_{g\in G}$ definimos $\rho_g(e_h) = e_{gh}$. Notar que si $g \neq 1$ es no-trivial, entonces $gh \neq h$ para todo $h \in G$ y luego $\mathrm{tr}(\rho_g) = 0$. En otras palabras,

$$\chi_R(g) = \begin{cases} |G| & \text{si } g = 1 \\ 0 & \text{si } g \neq 1 \end{cases}$$

es el carácter de la representación regular.

Corolario 3.7.10. — *Sean $W_1, \ldots, W_h$ las representaciones irreducibles de un grupo finito G, y sea $n_i := \dim_{\mathbb{C}}(W_i)$. Entonces, cada W_i está contenida n_i veces en la representación regular de G. En particular,*

1. $|G| = n_1^2 + \ldots + n_h^2$.
2. *Si $g \neq 1$ entonces $\sum_{i=1}^{h} n_i\chi_i(g) = 0$.*

Demostración. — La representación W_i está contenida $\langle \chi_R, \chi_i\rangle$ veces en la representación regular. Calculamos

$$\begin{aligned}\langle \chi_R, \chi_i\rangle &= \frac{1}{|G|}\sum_{g\in G} \chi_R(g^{-1})\chi_i(g) \\ &= \frac{1}{|G|}\chi_R(1)\chi_i(1) = \frac{1}{|G|}|G|\dim_{\mathbb{C}}(W_i) = \dim_{\mathbb{C}}(W_i) = n_i.\end{aligned}$$

Luego, $\mathbb{C}^{|G|} \cong W_1^{\oplus n_1} \oplus \cdots \oplus W_h^{\oplus n_h}$ y así $\chi_R(g) = n_1\chi_1(g) + \ldots + n_h\chi_h(g)$. En particular, $|G| = \chi_R(1) = n_1\chi_1(1) + \ldots + n_h\chi_h(1) = n_1^2 + \ldots + n_h^2$ de donde se deduce (1). Similar, si $g \neq 1$ entonces $0 = n_1\chi_1(g) + \ldots + n_h\chi_h(g)$ de donde se deduce (2). □

Observación 3.7.11. —

1. El resultado anterior implica que el grado de una representación irreducible es menor o igual que $\sqrt{|G|}$.
2. La fórmula $|G| = n_1^2 + \ldots + n_h^2$ implica que si construimos h representaciones irreducibles $V_1, \ldots, V_h$ **no isomorfas** (i.e., ortogonales) de grados $n_1, \ldots, n_h$ tales que $|G| = n_1^2 + \ldots + n_h^2$, entonces necesariamente son **todas** las representaciones irreducibles de G.

3.8. Caracteres y funciones centrales

Recuerdo 3.8.1. — Sea G un grupo finito. Recordemos que $f : G \to \mathbb{C}$ es una **función central** si $f(hgh^{-1}) = f(g)$ para todos $h, g \in G$, i.e., si el valor de

$f(g)$ sólo depende de la clase de conjugación de g. El $\mathbb{C}$-espacio vectorial $\mathscr{C}(G)$ de funciones centrales es de $\dim_{\mathbb{C}} \mathscr{C}(G) = \mathrm{card}(\{\text{clases de conjugación de } G\})$.

Proposición 3.8.2. — *Sea $f : G \to \mathbb{C}$ una función central y sea $\rho : G \to \mathrm{GL}(V)$ una representación. Consideremos la aplicación lineal $\rho_f : V \to V$ definida por*

$$\rho_f := \sum_{g \in G} f(g)\rho_g.$$

Si V es una representación irreducible, entonces $\rho_f = \lambda \,\mathrm{Id}_V$ f es una homotecia de factor

$$\lambda = \frac{1}{\dim_{\mathbb{C}}(V)} \sum_{g \in G} f(g)\chi_V(g) = \frac{|G|}{\dim_{\mathbb{C}}(V)} \langle f, \overline{\chi_V} \rangle.$$

Demostración. — Veamos que $\rho_f : V \to V$ es un morfismo de representaciones, es decir, que $\rho_f \circ \rho_g = \rho_g \circ \rho_f$ para todo $g \in G$. En efecto, calculamos para $h \in G$

$$\begin{aligned} \rho_h^{-1} \circ \rho_f \circ \rho_h = \sum_{g \in G} f(g)\rho_h^{-1} \circ \rho_g \circ \rho_h = \sum_{g \in G} f(g)\rho_{h^{-1}gh} \\ \underbrace{=}_{k = h^{-1}gh} \sum_{k \in G} f(hkh^{-1})\rho_k = \sum_{k \in G} f(k)\rho_k = \rho_f. \end{aligned}$$

Luego, el Lema de Schur implica que $\rho_f = \lambda \,\mathrm{Id}_V$ para cierto $\lambda \in \mathbb{C}$. Finalmente, se tiene que

$$\begin{aligned} \mathrm{tr}(\lambda \,\mathrm{Id}_V) &= \lambda \dim_{\mathbb{C}}(V) = \mathrm{tr}(\rho_f) \\ &= \sum_{g \in G} f(g) \,\mathrm{tr}(\rho_g) = \sum_{g \in G} f(g)\chi_V(g) \\ &= |G| \cdot \frac{1}{|G|} \sum_{g \in G} f(g)\overline{\chi_V(g^{-1})} = |G| \langle f, \overline{\chi_V} \rangle, \end{aligned}$$

de donde se obtiene el resultado. □

Teorema 3.8.3. — *Los caracteres $\chi_1, \ldots, \chi_h$ de las representaciones irreducibles del grupo G forman una base ortonormal de $\mathscr{C}(G)$.*

Demostración. — El Teorema de Frobenius implica que $\{\chi_1, \ldots, \chi_h\}$ es un sistema ortonormal respecto al producto hermitiano definido anteriormente.

Por otra parte, $\{\chi_1, \ldots, \chi_h\}$ es una base de $\mathscr{C}(G)$ si y sólo si para toda función $f \in \mathscr{C}(G)$ se tiene que si $(f \mid \chi_i) = 0$ para todo $i \in \{1, \ldots, h\}$ entonces

necesariamente $f = 0$. Además, esto último equivale[6] a que si $\langle f, \overline{\chi_i}\rangle = 0$ para todo $i \in \{1, \ldots, h\}$ entonces necesariamente $f = 0$.

Por otra parte, la Proposición anterior implica que si $\rho : G \to \mathrm{GL}(V)$ es una representación irreducible entonces $\rho_f = 0$. Más aún, si $\rho : G \to \mathrm{GL}(V)$ es una representación arbitraria entonces, al considerar la descomposición en sub-representaciones irreducibles, notamos que también se tiene $\rho_f = 0$.

En particular, si $\rho = R : G \to \mathrm{GL}_{|G|}(\mathbb{C})$ es la representación regular de G, entonces calculamos $\rho_f(e_1) = \sum_{g\in G} f(g)\rho_g(e_1) = \sum_{g\in G} f(g)e_g = 0$. Dado que $\{e_g\}_{g\in G}$ es una base, concluimos que $f(g) = 0$ para todo $g \in G$, i.e., $f = 0$. □

Teorema 3.8.4. — *El número de representaciones irreducibles de G (módulo isomorfismo) es igual al número de clases de conjugación de G.*

Demostración. — Por definición tenemos que

$$\dim_{\mathbb{C}} \mathscr{C}(G) = \mathrm{card}(\{\text{clases de conjugación de } G\}).$$

Por otra parte, el Teorema anterior implica que $\dim_{\mathbb{C}} \mathscr{C}(G) = h$, donde h es el número de representaciones irreducibles de G, módulo isomorfismo. □

Veamos algunas consecuencias de los resultados anteriores.

Proposición 3.8.5. — *Sean $\chi_1, \ldots, \chi_h$ los caracteres de las representaciones irreducibles del grupo G, y definamos*

$$c(g) := \mathrm{card}\{hgh^{-1},\ h \in G\},$$

donde $g \in G$. Entonces:

1. $\sum_{i=1}^{h} |\chi_i(g)|^2 = \frac{|G|}{c(g)}$.
2. *Si h no es conjugado a g, entonces* $\sum_{i=1}^{h} \overline{\chi_i(g)}\chi_i(h) = 0$.

En particular, si $g = 1$ obtenemos el Corolario 3.7.10.

Demostración. — Dado $g \in G$ consideramos la función $f_g \in \mathscr{C}(G)$ igual a 1 en la clase de conjugación C_g de g y 0 afuera. Dado que $f_g \in \mathscr{C}(G)$ podemos escribir

$$f_g = \sum_{i=1}^{h} \lambda_i \chi_i,$$

[6] Observamos que $\overline{(\chi_i \mid f)} = (f \mid \chi_i) = \langle f, \chi_i\rangle$ implica $(\chi_i \mid f) = \langle \overline{\chi_i}, \overline{f}\rangle$ y luego $(\chi_i \mid \overline{f}) = \langle f, \overline{\chi_i}\rangle$.

donde $\lambda_i = \langle f_g, \chi_i \rangle = (f_g \mid \chi_i) = \frac{c(g)}{|G|}\overline{\chi_i(g)}$. En otras palabras,

$$f_g(h) = \frac{c(g)}{|G|}\sum_{i=1}^{h} \overline{\chi_i(g)}\chi_i(h).$$

Si consideramos $h = g$ obtenemos directamente (1), mientras que (2) se deduce al considerar h fuera de la clase de conjugación de g. □

Teorema 3.8.6. — *Sea G un grupo finito. Entonces G es abeliano si y sólo si toda representación irreducible de G es de grado 1.*

Demostración. — El grupo G es abeliano si y sólo si

$$c(g) = \text{card}\{hgh^{-1},\ h \in G\} = 1$$

para todo $g \in G$. Esto último equivale a

$$|G| = \text{card}(\{\text{clases de conjugación de } G\}).$$

Por otra parte, sabemos que el número h de representaciones irreducibles de G (módulo isomorfismo) es igual al número de clases de conjugación de G. Luego, esta última igual se traduce en que $|G| = h$, lo cual equivale gracias al Corolario 3.7.10 a la igualdad

$$|G| = n_1^2 + \ldots + n_{|G|}^2 \Leftrightarrow n_1 = \ldots = n_{|G|} = 1,$$

que es lo que queríamos probar. □

Corolario 3.8.7. — *Sea $A \leq G$ sub-grupo abeliano. Entonces toda representación irreducible de G es de grado a lo más $[G : A] = \frac{|G|}{|A|}$.*

Demostración. — Sea $\rho : G \to \text{GL}(V)$ una representación irreducible. Consideremos la restricción

$$\rho_A := \rho|_A : A \to \text{GL}(V),$$

la cual a priori no tiene porqué ser irreducible. Sea $W \subseteq V$ una sub-representación irreducible de ρ_A. Luego, $\dim_{\mathbb{C}}(W) = 1$ gracias al Teorema anterior.

Por otra parte, si consideramos el sub-espacio

$$V' := \text{Vect}_{\mathbb{C}}\langle\{\rho_g(W)\}_{g\in G}\}\rangle \subseteq V,$$

entonces tenemos que V' es G-invariante no-nulo y luego, dado que V es una representación irreducible, tenemos necesariamente que $V' = V$.

Finalmente, notamos que si $g \in G$ y $h \in A$ entonces se tiene que $\rho_h(W) = W$ y luego $\rho_{gh}(W) = \rho_g(\rho_h(W)) = \rho_g(W)$. De donde se deduce que $\rho_g(W)$ sólo

depende de la clase lateral gA. Así, la cantidad de $\rho_g(W)$ diferentes es a lo más $[G : A]$ y por ende $\dim_{\mathbb{C}}(V) \leq [G : A]$. □

Ejemplo 3.8.8. — El grupo diedral D_n contiene $\langle r \rangle \cong \mathbb{Z}/n\mathbb{Z}$ grupo cíclico de índice 2. Luego, todas las representaciones irreducibles de D_n son de grado ≤ 2. Más aún, si $n \geq 3$ entonces D_n no es abeliano, y luego D_n admite necesariamente una representación irreducible de grado 2.

Ejercicio 3.8.9. — Demostrar que un grupo no abeliano de orden 8 posee exactamente 5 clases de conjugación.

3.9. Tablas de caracteres

Una **tabla de caracteres** de G da el valor de cada carácter irreducible (i.e., carácter de una representación irreducible) sobre cada clase de conjugación. Las líneas corresponden a los caracteres y las columnas a las clases de conjugación.

Consideremos por ejemplo el grupo simétrico $G = \mathfrak{S}_3$. Las clases de conjugación de $\mathfrak{S}_3$ son $C_e = \{\mathrm{id}\}$, $C_t = \{(1,2),(1,3),(2,3)\}$ y $C_c = \{(2,3,1),(1,3,2)\}$, por lo que tenemos que hay 3 representaciones irreducibles de $\mathfrak{S}_3$ módulo isomorfismo.

Hay dos representaciones de grado 1 (y por lo tanto irreducibles) fáciles de ver. La primera es la representación trivial

$$\rho_1 = \rho_{\text{trivial}} : \mathfrak{S}_3 \to \mathbb{C}^\times,\ \sigma \mapsto 1$$

para todo $\sigma \in \mathfrak{S}_3$. La segunda es la representación signo

$$\rho_2 = \rho_{\text{signo}} : \mathfrak{S}_3 \to \{\pm 1\} \subseteq \mathbb{C}^\times,\ \sigma \mapsto \varepsilon(\sigma).$$

Luego, obtenemos la siguiente tabla de caracteres de $\mathfrak{S}_3$.

$\mathfrak{S}_3$	C_e	C_t	C_c
χ_{trivial}	1	1	1
χ_{signo}	1	-1	1
χ_3	?	?	?

Donde $\chi_3 : \mathfrak{S}_3 \to \mathbb{C}$ es el carácter de una representación irreducible $\rho_3 : \mathfrak{S}_3 \to \mathrm{GL}(V)$ de grado n, no isomorfa a ρ_1 ni a ρ_2. Notamos que $n \geq 2$ dado que $\mathfrak{S}_3$ no es abeliano.

Hay varias formas de deducir que necesariamente $n = 2$. Por ejemplo, notamos que $\mathfrak{S}_3$ contiene un grupo cíclico $\langle (2,3,1) \rangle \cong \mathbb{Z}/3\mathbb{Z}$ de índice 2 y

luego $n \leq 2$. De manera similar, calculamos $|\mathfrak{S}_3| = 6 = 1^2 + 1^2 + n^2$ de donde se concluye igualmente que $n = 2$. En particular, $\chi_3(C_e) = \dim_{\mathbb{C}}(V) = n = 2$.

Podemos usar los resultados anteriores para calcular los valores de χ_3 sin conocer explícitamente la representación ρ_3. Por ejemplo, tenemos que

$$\chi_{\text{regular}} = \chi_{\text{trivial}} + \chi_{\text{signo}} + n\chi_3 = \chi_1 + \chi_2 + 2\chi_3.$$

En particular, $0 = \chi_1(C_t) + \chi_2(C_t) + 2\chi_3(C_t) = 1 + (-1) + 2\chi_3(C_t)$ implica que $\chi_3(C_t) = 0$. Del mismo modo se deduce que $\chi_3(C_c) = -1$, de donde se obtiene finalmente la tabla de caracteres de $\mathfrak{S}_3$.

$\mathfrak{S}_3$	C_e	C_t	C_c
χ_1	1	1	1
χ_2	1	-1	1
χ_3	2	0	-1

Ejercicio 3.9.1. — Verificar que la representación $\rho_3 : \mathfrak{S}_3 \to \mathrm{GL}(V)$ se obtiene a partir de la representación de permutación $\rho_{\text{perm}} : \mathfrak{S}_3 \to \mathrm{GL}_3(\mathbb{C})$ al restringirse al sub-espacio invariante

$$V = \{(x_1, x_2, x_3) \in \mathbb{C}^3 \mid x_1 + x_2 + x_3 = 0\} \cong \mathbb{C}^2.$$

Ejercicio 3.9.2. — Calcular la tabla de caracteres del grupo D_4.
Indicación: Además de la representación trivial, considerar ρ_{det} al ver D_4 como sub-grupo de $\mathrm{GL}_2(\mathbb{C})$, ρ_{signo} al ver D_4 como sub-grupo de $\mathfrak{S}_4$, $\rho_{\text{det}} \otimes \rho_{\text{signo}}$, y determinar el carácter de la representación restante (c.f. Ejercicio 3.8.9).

CAPÍTULO 4

ANILLOS Y MÓDULOS

4.1. Anillos e ideales

4.1.1. Primeras definiciones. —

Recuerdo 4.1.1. — Sea $(A, +, \cdot)$ un conjunto no-vacío con dos leyes de composición interna. Se dice que A es un **anillo** si:

1. $(A, +)$ es un grupo abeliano.
2. $(A, \cdot)$ es un semi-grupo.
3. Para todos $a, b, c \in A$ se tiene que $a(b+c) = ab+ac$ y $(b+c)a = ba+ca$.

Además, se dice que A es un **anillo abeliano** si $ab = ba$ para todos $a, b \in A$. Finalmente, diremos que un anillo abeliano k es un **cuerpo** si $k \neq \{0\}$ y si $(k \setminus \{0\}, \cdot)$ es un grupo.

Ejemplo 4.1.2. — 1. $(\mathbb{Z}, +, \cdot)$ y $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ son anillos abelianos.
2. $M_{n\times n}(\mathbb{C})$ es un anillo (no abeliano si $n \geq 2$).
3. $\mathbb{F}_p$, $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ son cuerpos.

¡Atención! — Todos los anillos que consideraremos en este texto serán abelianos, salvo $M_{n\times n}(A)$.

Recordemos la noción de unidades en un anillo abeliano.

Recuerdo 4.1.3. — Se dice que $A^\times = \{a \in A \mid \exists b \in A \text{ tal que } ab = 1\}$ es el grupo de **unidades** de A. En particular, si k es un cuerpo entonces $k^\times = k \setminus \{0\}$.

Del mismo modo que para grupos tenemos una noción asociada de morfismo de grupos, existe una noción natural de morfismo asociada al concepto de anillo.

***Definición 4.1.4* (morfismo de anillos).** — Sean A y B anillos. Un **morfismo de anillos** $\varphi : A \to B$ es una aplicación que preserva sumas, productos, y tal que $\varphi(1_A) = 1_B$. En particular, $\varphi(A^\times) \subseteq B^\times$. Se dice que φ es un:

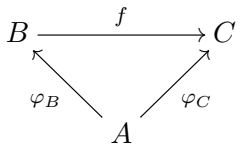
1. **isomorfismo** si es biyectivo, y escribimos $\varphi : A \xrightarrow{\sim} B$.
2. **endomorfismo** si $A = B$.
3. **automorfismo** si es un isomorfismo y un endomorfismo.

***Definición 4.1.5* (A-álgebra).** — Sea A un anillo. Una **A–álgebra** es un anillo B y un morfismo $\varphi : A \to B$ llamado **morfismo estructural**.

Notación 4.1.6. — Si $a \in A$ y $b \in B$, escribimos $ab := \varphi(a)b$.

Observación 4.1.7. — Si k es un cuerpo, una k-álgebra es un k-espacio vectorial con estructura de anillo.

***Definición 4.1.8* (morfismo de A–álgebras).** — Sea A un anillo. Un **morfismo de A–álgebras** es un morfismo de anillos $f : B \to C$ entre A–álgebras, compatible con sus morfismos estructurales. Es decir, tal que el diagrama



es conmutativo.

***Ejemplo 4.1.9* (anillo de polinomios).** — Sea A un anillo. Denotamos por $A[X_1, \ldots, X_n]$ al anillo de polinomios con coeficientes en A en n variables $X_1, \ldots, X_n$.

El siguiente resultado, cuya demostración se deja como ejercicio, permite pensar a $A[X_1, \ldots, X_n]$ como la A–álgebra más pequeña equipada con una lista de n elementos.

***Teorema 4.1.10* (propiedad universal).** — *Sea B un anillo. Sea $\varphi : A \to B$ un morfismo y sean $x_1, \ldots, x_n \in B$. Entonces, existe un único morfismo $\pi : A[X_1, \ldots, X_n] \to B$ tal que $\pi|_A = \varphi$ y $\pi(X_i) = x_i$ para todo $i \in \{1, \ldots, n\}$. Explícitamente,*

$$\pi\left(\sum a_{(i_1,\ldots,i_n)} X_1^{i_1} \cdots X_n^{i_n}\right) = \sum \varphi(a_{(i_1,\ldots,i_n)}) x_1^{i_1} \cdots x_n^{i_n}.$$

Una de las definiciones fundamentales en la teoría de anillos es la de dominio de integridad.

***Definición 4.1.11* (dominio de integridad).** — Sea A un anillo tal que $A \neq \{0\}$. Decimos que A es un **dominio de integridad** (ó **dominio**) si para todos $a, b \in A$ tales que $ab = 0$ se tiene que $a = 0$ ó $b = 0$.

Ejemplo 4.1.12. —

1. $\mathbb{Z}$ es un dominio.
2. Todo cuerpo es un dominio.
3. $\mathbb{Z}/n\mathbb{Z}$ es un dominio si y sólo si n es primo.

***Definición 4.1.13* (cuerpo de fracciones).** — Sea A un dominio. Definimos su **cuerpo de fracciones** K_A ó $\mathrm{Fr}(A)$ como el conjunto de "fracciones" $\frac{a}{b}$ (es decir, de clases de equivalencia $[(a, b)]$) donde $a \in A$, $b \in A \setminus \{0\}$, en donde definimos

$$\frac{a}{b} = \frac{a'}{b'} \iff ab' = a'b.$$

Ejercicio 4.1.14. —

a) Demostrar que K_A es un cuerpo, y que $A \overset{\iota}{\hookrightarrow} K_A$ (es decir, la aplicación natural $\iota : A \to K_A$, $a \mapsto \frac{a}{1}$ es un morfismo inyectivo).

b) Demostrar que si A es un dominio, entonces $A[X]$ también.

c) Haciendo uso del ítem anterior, demostrar (por inducción) que si A es un dominio, entonces $A[X_1, ..., X_n]$ también. Esto nos permite definir el **cuerpo de funciones racionales**

$$A(X_1, \ldots, X_n) := \mathrm{Fr}(A[X_1, \ldots, X_n]) = \left\{ \frac{f(X_1, \ldots, X_n)}{g(X_1, \ldots, X_n)} \;\middle|\; f, g \in A[X_1, \ldots, X_n],\ g \neq 0 \right\}.$$

d) Sea A un dominio. Calcular $(A[X])^\times$.
Notar que en general, si A no es un dominio, esto es más difícil. Por ejemplo, $(2X + 1)^2 = 1$ en $(\mathbb{Z}/4\mathbb{Z})[X]$.

4.1.2. Ideales. —

***Definición 4.1.15* (ideal).** — Sea A un anillo. Un sub-conjunto $I \subseteq A$ es un **ideal** de A si

1. $(I, +)$ es un sub-grupo de $(A, +)$; y
2. para todo $a \in A$ y todo $b \in I$ se tiene que $ab \in I$.

Observación 4.1.16. — Sea A un anillo, sea $I \subseteq A$ un ideal, y sean $a, b \in A$. Consideremos el grupo abeliano cociente $(A/I, +)$. Es claro que la clase $(a + I) + (b + I) = (a + b)I$ (es decir, que la clase $(a + b)I$ está

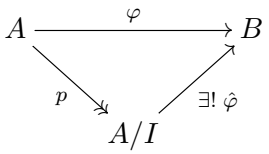
bien definida). Observemos que $(a+I)(b+I) = ab+I$ (es decir, que la clase $ab+I$ está bien definida). En efecto, si $a' \in a+I$ y $b' \in b+I$, existen $i_1, i_2 \in I$ tales que $a' = a+i_1$ y $b' = b+i_2$. Por lo tanto, $a'b' = (a+i_1)(b+i_2) = ab + ai_2 + bi_1 + i_1 i_2 \in ab+I$.

El análisis anterior se traduce en el hecho que la proyección

$$\begin{aligned} p : A &\to A/I \\ a &\mapsto a+I \end{aligned}$$

es un morfismo de anillos. Notar que p es sobreyectivo y que $\ker(p) = I$. Recíprocamente, dado $(I,+)$ un sub-grupo de $(A,+)$, es posible demostrar que si $p : A \to A/I$ es un morfismo de anillos entonces I es un ideal.

***Teorema 4.1.17* (propiedad universal).** — *Sean A, B anillos, sea $I \subseteq A$ un ideal, y sea $\varphi : A \to B$ un morfismo tal que $\varphi(I) = \{0_B\}$. Entonces, existe un único morfismo $\widehat{\varphi} : A/I \to B$ tal que $\varphi = \widehat{\varphi} \circ p$. Es decir, tal que el siguiente diagrama es conmutativo*



Proposición 4.1.18. — *Sean A, B anillos, sea $\varphi : A \to B$ un morfismo, y sea $J \subseteq B$ un ideal. Entonces, $\varphi^{-1}(J) \subseteq A$ es un ideal. En particular,* $\ker(\varphi)$ *es un ideal de A.*

Demostración. — Sean $a \in A$ y $b \in \varphi^{-1}(J)$ (i.e., $\varphi(b) \in J$). Notar que $\varphi(ab) = \varphi(a)\varphi(b) \in J$, pues $\varphi(b) \in J$ y J es un ideal. Así, $ab \in \varphi^{-1}(J)$. □

El siguiente resultado permite caracterizar a los cuerpos a traves de sus ideales.

Proposición 4.1.19. — *Sea A un anillo tal que $A \neq \{0\}$. Entonces, A es un cuerpo si y sólo si $\{0\}$ y A son sus únicos ideales.*

Demostración. — Supongamos que A es un cuerpo. Si $\{0\} \neq I$ es un ideal y $a \in I \setminus \{0\}$, entonces $a^{-1}a = 1 \in I$. Luego, para todo $b \in A$, se tiene que $b = b \cdot 1 \in I$, lo que implica que $I = \langle 1 \rangle = A$.

Supongamos ahora que los únicos ideales del anillo A son $\{0\}$ y A. Dado un elemento arbitrario $0 \neq a \in A$, consideremos $\langle a \rangle := \{ab,\ b \in A\}$, el **ideal generado** por a. Como $a \in \langle a \rangle$, se tiene que $\langle a \rangle \neq \{0\}$ y luego $\langle a \rangle = A = \langle 1 \rangle$.

En particular, existe $b \in A$ tal que $ab = 1$. Como $a \neq 0$ es fue escogido de manera arbitraria, esto implica que A es un cuerpo. □

Ejemplo 4.1.20. —

1. Los ideales de $\mathbb{Z}$ son de la forma $I_n := n\mathbb{Z}$, $n \in \mathbb{N}$.
2. La inclusión $\iota : \mathbb{Z} \hookrightarrow \mathbb{R}$ es un morfismo de anillos. Si $n \geq 1$, entonces $\varphi(I_n)$ **no** es un ideal de $\mathbb{R}$. En particular, la imagen de un ideal via un morfismo de anillos no es necesariamente un ideal.
3. Sea A un anillo. Si $\{I_j\}_{j\in J}$ es una familia de ideales de A, entonces $\cap_{j\in J} I_j$ es un ideal de A.
4. Sea A un anillo. Si $S \subseteq A$ es un sub-conjunto, entonces
$$\langle S\rangle := \bigcap_{\substack{S\subseteq I \\ I \text{ ideal}}} I = \left\{ \sum_{\text{finita}} a_i s_i,\ a_i \in A, s_i \in S \right\}$$
es el **ideal generado** por S. En particular, si $S = \{a\}$ denotamos por $\langle S\rangle = \langle a\rangle$ al ideal generado por $a \in A$.
5. Sean A, B anillos. Si $\varphi : A \to B$ es un morfismo, entonces la propiedad universal del cociente implica (al igual que en el caso de grupos) que el morfismo inducido $\widehat{\varphi} : A/\ker(\varphi) \xrightarrow{\sim} \mathrm{Im}(\varphi)$ es un isomorfismo.
6. Sea A un anillo. Sean $a \in A$ y $\pi : A[X] \to A$ un morfismo de A-álgebras tal que $\pi(X) = a$. El algoritmo de la división implica que si $f(X) \in A[X]$, entonces $f(X) = g(X)(X - a) + b$, para ciertos $g(X) \in A[X]$ y $b \in A$. Luego, $\pi(f(X)) = b$. Esto basta para concluir que $\ker(\pi) = \langle X - a\rangle$ y que $\mathrm{Im}(\pi) = A$. Por lo tanto, el ejemplo anterior implica que existe un isomorfismo $A[X]/\langle X - a\rangle \xrightarrow{\sim} A$.

Definición 4.1.21 **(conjunto multiplicativo).** — Sea A un anillo y sea $S \subseteq A$ un sub-conjunto. Diremos que que S es un **conjunto multiplicativo** si $1 \in S$, y si para todos $a, b \in S$ se tiene que $ab \in S$.

Uno de los conceptos fundamentales en la teoría de anillos es la de ideal primo, generalizando la idea de número primo.

Definición 4.1.22 **(ideal primo).** — Sea A un anillo y sea $\mathfrak{p} \subseteq A$ un ideal. Diremos que $\mathfrak{p}$ es **primo** si $A \setminus \mathfrak{p}$ es un conjunto multiplicativo, es decir, si $1 \notin \mathfrak{p}$, y si para todos $a, b \in A$ tales que $ab \in \mathfrak{p}$ se tiene que $a \in \mathfrak{p}$ ó bien $b \in \mathfrak{p}$.

Lema 4.1.23. — *Sea $\varphi : A \to B$ un morfismo de anillos y sea $T \subseteq B$ un sub-conjunto. Entonces,*

1. *Si T es multiplicativo, $\varphi^{-1}(T)$ es multiplicativo.*

2. *Si φ es sobreyectivo y $\varphi^{-1}(T)$ es multiplicativo, T es multiplicativo.*

Demostración. — Definamos $S := \varphi^{-1}(T) \subseteq A$. Para probar (1) notamos que $1 \in S$, pues $\varphi(1) = 1 \in T$. Además, para todos $a, b \in S$ se tiene que $\varphi(ab) = \varphi(a)\varphi(b) \in T$, pues $\varphi(a) \in T$ y $\varphi(b) \in T$. Por lo tanto, S es multiplicativo.

Para probar (2), notamos que $\varphi(1) = 1 \in T$, pues $1 \in S$. Además, para todos $a, b \in S$ se tiene que $\varphi(a), \varphi(b), \varphi(ab) \in T$. Como φ es sobreyectivo, para todo $t \in T$ existe un $s \in S$ tal que $t = \varphi(s)$. □

Proposición 4.1.24. — *Sea $\varphi : A \to B$ un morfismo de anillos y sea $\mathfrak{q} \subseteq B$ un ideal. Entonces,*

1. *Si $\mathfrak{q}$ es primo, $\varphi^{-1}(\mathfrak{q})$ es primo.*
2. *Si φ es sobreyectivo y $\varphi^{-1}(\mathfrak{q})$ es primo, $\mathfrak{q}$ es primo.*

Demostración. — Aplicar el lema anterior al conjunto $T = B \setminus \mathfrak{q}$. □

Corolario 4.1.25. — *Sean A un anillo y $\mathfrak{p} \subseteq A$ un ideal. Entonces, $\mathfrak{p}$ es un ideal primo si y sólo si $A/\mathfrak{p}$ es un dominio.*

Demostración. — Consideramos la proyección canónica $\pi : A \to A/\mathfrak{p}$, la cual es sobreyectiva. Luego, la Proposición anterior implica que $\mathfrak{p} = \pi^{-1}(\langle 0 \rangle)$ es un ideal primo si y sólo si $\langle 0 \rangle \subseteq A/\mathfrak{p}$ es un ideal primo. Esto último, por definición, equivale a decir que $\overline{1} \notin \langle 0 \rangle$ (i.e., $A/\mathfrak{p} \neq \{0\}$) y que si $\overline{ab} \in \langle 0 \rangle$ entonces $\overline{a} \in \langle 0 \rangle$ ó bien $\overline{b} \in \langle 0 \rangle$. Siendo esto último precisamente la definición de dominio. □

Ejemplo 4.1.26. —

1. El ideal $I_n = n\mathbb{Z} \subseteq \mathbb{Z}$ es primo si y sólo si n es primo.
2. Sea A un dominio y sea $a \in A$. Como $A[X]/\langle X - a \rangle \cong A$, se tiene que $\langle X - a \rangle \subseteq A[X]$ es un ideal primo.

Otro concepto fundamental es el de ideal maximal.

***Definición 4.1.27* (ideal maximal).** — Sean A un anillo y $\mathfrak{m} \subseteq A$ un ideal. Diremos que $\mathfrak{m}$ es un **ideal maximal** si $\mathfrak{m} \neq A$, y si para todo ideal $I \subseteq A$ tal que $\mathfrak{m} \subsetneq I$ se tiene que $I = A$, es decir, $\mathfrak{m}$ es maximal respecto a la inclusión.

Ejemplo 4.1.28. — Si A es un dominio, entonces $\langle X \rangle \subseteq A[X, Y]$ es un ideal primo pues $A[X, Y]/\langle X \rangle \cong A[Y]$, y este último es un dominio. Sin embargo, $\langle X \rangle \subsetneq \langle X, Y \rangle$, y como $\langle X, Y \rangle \subseteq A[X, Y]$ es un ideal propio, se tiene que $\langle X \rangle \subseteq A[X, Y]$ **no** es maximal.

Proposición 4.1.29. — *Sea A un anillo. Entonces, A es un cuerpo si y sólo si $\langle 0\rangle$ es un ideal maximal.*

Demostración. — Supongamos que A es un cuerpo y sea $\langle 0\rangle \neq I \subseteq A$ un ideal. Sea $a \in I \setminus \{0\}$. Dado que A es un cuerpo, se tiene que $a^{-1}a = 1 \in I$, y luego $I = A$.

Por otro lado, si suponemos que $\langle 0\rangle$ es un ideal maximal de A y $a \in A \setminus \{0\}$ es un elemento arbitrario no-nulo, entonces $\langle 0\rangle \subsetneq \langle a\rangle$ y luego $\langle a\rangle = A$, por maximalidad. En particular, existe $a^{-1} \in A$ tal que $a^{-1}a = 1$. □

Ejercicio 4.1.30. — Sea k un cuerpo y sea $A \neq \{0\}$ un anillo. Demostrar que todo morfismo de anillos $\varphi : k \to A$ es inyectivo.

Corolario 4.1.31. — *Sean A un anillo y $\mathfrak{m} \subseteq A$ un ideal. Entonces, $\mathfrak{m}$ es maximal si y sólo si $A/\mathfrak{m}$ es un cuerpo.*

Demostración. — Sea $I \subseteq A$ un ideal y $p : A \to A/I$ la proyección canónica. Hay una correspondencia biyectiva

$$\begin{aligned}\{\text{ideales } J \subseteq A \text{ tal que } I \subseteq J\} &\overset{1:1}{\longleftrightarrow} \{\text{ideales } K \subseteq A/I\}\\ J &\longmapsto J/I := \{b + I,\ b \in J\} = p(J)\\ p^{-1}(K) &\longmapsfrom K\end{aligned}$$

la cual preserva inclusiones. Luego, dado que $\mathfrak{m}$ es enviado a $\langle 0\rangle \subseteq A/\mathfrak{m}$ vía la proyección canónica, tenemos que $\mathfrak{m} \subseteq A$ es maximal si y sólo si $\langle 0\rangle \subseteq A/\mathfrak{m}$ es maximal, siendo esto último equivalente a que $A/\mathfrak{m}$ sea un cuerpo, gracias a la Proposición 4.1.29. □

Ejemplo 4.1.32. — Sea k un cuerpo, sea $n \in \mathbb{N}^{\geq 1}$, y sean $a_1, \ldots, a_n \in k$. Entonces, el ideal $\mathfrak{m} := \langle X_1 - a_1, \ldots, X_n - a_n\rangle \subseteq k[X_1, \ldots, X_n]$ es maximal, pues $k[X_1, \ldots, X_n]/\mathfrak{m} \cong k$.

Recuerdo 4.1.33 **(Lema de Zorn).** — Sea P un conjunto y sea $\mathscr{R}$ una relación en P. Si para todo $(a, b) \in P \times P$ tal que $(a, b) \in \mathscr{R}$ escribimos $a \preccurlyeq b$, entonces decimos que $\mathscr{R}$ es un **orden parcial** si es:

1. **reflexiva:** $a \preccurlyeq a$ para todo $a \in P$,
2. **anti-simétrica:** si $a \preccurlyeq b$ y $b \preccurlyeq a$ entonces $a = b$, para todos $a, b \in P$,
3. **transitiva:** si $a \preccurlyeq b$ y $b \preccurlyeq c$ entonces $a \preccurlyeq c$, para todos $a, b, c \in P$.

El par $(P, \preccurlyeq)$ es llamado un **conjunto parcialmente ordenado**.

Sea $(P, \preccurlyeq)$ un conjunto parcialmente ordenado y sea $T \subseteq A$ un sub-conjunto. Decimos que T es **totalmente ordenado** o una **cadena** si para todos $a, b \in T$ se tiene que $a \preccurlyeq b$ o bien $b \preccurlyeq a$.

Sea $T \subseteq P$ una cadena y sea $s \in P$. Decimos que s es una **cota superior** de T si $t \preccurlyeq s$ para todo $t \in T$. Un conjunto parcialmente ordenado no vacío tal que toda cadena posee una cota superior es llamado un **conjunto inductivo**.

Sea $m \in P$. Decimos que m es un **elemento maximal** si para todo $a \in P$ se tiene que $m \preccurlyeq a$ implica que $m = a$.

Finalmente, el **lema de Zorn** afirma que todo conjunto inductivo posee al menos un elemento maximal.

Proposición 4.1.34. — *Todo anillo A posee un ideal maximal, y todo ideal $I \subsetneq A$ está contenido en un ideal maximal.*

Demostración. — Sea $I \subsetneq A$ un ideal. Consideremos el conjunto P de los ideales $J \subsetneq A$ tales que $I \subseteq J$. El conjunto P es no vacío, pues $I \in P$, y es un conjunto parcialmente ordenado respecto a la inclusión $\preccurlyeq := \subseteq$. Sea $J_0 \subseteq J_1 \subseteq \ldots \subseteq J_n \subseteq \ldots$ una cadena en P. Notar que $S := \cup_{i \geq 0} J_i \in P$, pues $1 \notin J_i$ para todo $i \geq 0$, y que S es una cota superior de la cadena. Luego, el lema de Zorn implica que P posee un elemento maximal $\mathfrak{m}$. Más aún, se tiene que $\mathfrak{m}$ es un ideal maximal, de donde se concluye la demostración. □

4.1.3. Anillos reducidos y anillos noetherianos. —

***Definición 4.1.35* (radical de un ideal).** — Sea A un anillo y sea $I \subseteq A$ un ideal. El **radical** de I es el ideal

$$\sqrt{I} := \left\{ a \in A \mid \exists n \in \mathbb{N}^{\geq 1} \text{ tal que } a^n \in I \right\}.$$

En particular, $I \subseteq \sqrt{I}$. Decimos que I es un **ideal radical** si $I = \sqrt{I}$.

***Ejemplo 4.1.36* (nilradical).** — El **nilradical** de un anillo A está dado por

$$\mathrm{Nil}(A) := \sqrt{\langle 0 \rangle} = \{ a \in A \mid \exists n \in \mathbb{N}^{\geq 1} \text{ tal que } a^n = 0 \}.$$

Decimos que A es un **anillo reducido** si $\mathrm{Nil}(A) = \langle 0 \rangle$. En otras palabras, A es reducido si y sólo si $0 \in A$ es el único elemento nilpotente de A.

Ejercicio 4.1.37. — Sean $A = \mathbb{Z}$ y $I_n = n\mathbb{Z}$. Calcular $\sqrt{I_n}$.

Ejemplo 4.1.38. — Sea A un anillo, y sea $\mathfrak{p} \subseteq A$ un ideal primo. Entonces $\mathfrak{p}$ es un ideal radical.

En efecto, si $a \in \sqrt{\mathfrak{p}}$ entonces existe $n \in \mathbb{N}^{\geq 1}$ tal que $a^n \in \mathfrak{p}$. Si $n = 1$, entonces $a \in \mathfrak{p}$. Si $n \geq 2$, entonces $a \cdot a^{n-1} \in \mathfrak{p}$, lo que implica que $a \in \mathfrak{p}$ ó bien

$a^{n-1} \in \mathfrak{p}$, pues $\mathfrak{p}$ es un ideal primo. Por inducción, obtenemos que $a \in \mathfrak{p}$ y así $\sqrt{\mathfrak{p}} \subseteq \mathfrak{p}$. Dado que para todo ideal se tiene $\mathfrak{p} \subseteq \sqrt{\mathfrak{p}}$, se concluye que $\sqrt{\mathfrak{p}} = \mathfrak{p}$. En particular, si $I \subseteq A$ es un ideal entonces

$$I \text{ maximal} \implies I \text{ primo} \implies I \text{ radical.}$$

Proposición 4.1.39. — *Sea A un anillo, y sea $I \subseteq A$ un ideal. Entonces, I es radical si y sólo si A/I es reducido.*

Demostración. — El ideal I es radical si y sólo si $\sqrt{I} \subseteq I$, es decir, si $a^n \in I$ para cierto $n \in \mathbb{N}^{\geq 1}$ implica que $a \in I$. Dado que I corresponde al ideal nulo $\langle 0 \rangle \subseteq A/I$ vía la proyección canónica $p : A \to A/I$, esto último equivale a que $\overline{a}^n = 0$ en A/I implica que $\overline{a} = 0$ en A/I, que es precisamente la definición de que A/I sea un anillo reducido. □

Proposición 4.1.40. — *Sea A un anillo y sea $I \subseteq A$ un ideal. Entonces,*

$$\sqrt{I} = \bigcap_{\substack{I \subseteq \mathfrak{p} \\ \text{primo}}} \mathfrak{p},$$

es la intersección de todos los ideales primos que contienen a I.

Demostración. — Sea $\mathfrak{p}$ un ideal primo que contiene a I, entonces $I \subseteq \mathfrak{p}$ implica que $\sqrt{I} \subseteq \sqrt{\mathfrak{p}} = \mathfrak{p}$. Luego, $\sqrt{I} \subseteq \bigcap_{\mathfrak{p} \subseteq A} \mathfrak{p}$.

Recíprocamente, supongamos que $a \notin \sqrt{I}$ y sea P el conjunto ordenado (por inclusión) de todos los ideales de A que contienen a I pero que no contienen ninguna potencia a^m para $m \geq 1$. El conjunto P es no-vacío pues $I \in P$, y todo sub-conjunto totalmente ordenado de elementos de P admite una cota superior (su unión). Luego, el lema de Zorn implica que existe un elemento maximal $J \in P$. Veamos que J es un ideal primo: si x e y no pertenecen a J, entonces $\langle x, J \rangle \notin P$ y luego existe $m \geq 1$ tal que $a^m \in \langle x, J \rangle$. Del mismo modo, existe $n \geq 1$ tal que $a^n \in \langle y, J \rangle$. Deducimos que $a^{n+m} \in \langle xy, J \rangle$, de donde se tiene que $\langle xy, J \rangle \notin P$ y $xy \notin J$. Finalmente, como $a \notin J$ tenemos que $a \notin \bigcap_{\mathfrak{p} \subseteq A} \mathfrak{p}$, de donde se concluye la demostración. □

Ejercicio 4.1.41. — Sea A un anillo y sean $I, J \subseteq A$ ideales.

a) Probar que $\sqrt{IJ} = \sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$. En particular, para todo $n \in \mathbb{N}^{\geq 1}$ se tiene que $\sqrt{I^n} = \sqrt{I}$.

b) Probar que $\sqrt{I + J} = \sqrt{\sqrt{I} + \sqrt{J}}$.

***Definición 4.1.42* (anillo noetheriano).** — Sea A un anillo. Se dice que A es un **anillo noetheriano** si para toda cadena creciente

$$I_1 \subseteq I_2 \subseteq \ldots \subseteq I_k \subseteq I_{k+1} \subseteq \ldots$$

de ideales en A, existe $n \in \mathbb{N}^{\geq 1}$ tal que $I_n = I_{n+k}$ para todo $k \in \mathbb{N}^{\geq 1}$. Esta condición se denomina **Ascending Chain Condition (ACC)**.

Ejemplo 4.1.43. — Si k es un cuerpo, entonces k es noetheriano.

Ejercicio 4.1.44. —

a) Demostrar que $\mathbb{Z}$ es noetheriano.
b) Sea A un anillo, y sea $I \subseteq A$ un ideal. Demostrar que si A es noetheriano, entonces A/I también lo es.

4.1.4. Algunos teoremas de Hilbert. — El siguiente resultado probado por Hilbert en 1890 es uno de los primeros resultados centrales en la geometría algebraica.

***Teorema 4.1.45* (de la base de Hilbert).** — *Sea A un anillo. Si A es noetheriano, entonces $A[X]$ también lo es.*

Demostración. — Observemos que si $I_1 \subseteq I_2 \subseteq \ldots \subseteq I_k \subseteq I_{k+1} \subseteq \ldots$ es una cadena ascendente de ideales de $A[X]$, entonces $I = \cup_{i \geq 1} I_i$ es un ideal de $A[X]$. Luego, basta demostrar que todo ideal $I \subseteq A[X]$ es finitamente generado.

Supongamos que existe un ideal $J \subseteq A[X]$ que no finitamente generado. En particular, $J \neq \langle 0 \rangle$.

Sea $J_0 := \langle 0 \rangle$. Para todo $i \geq 1$ consideremos $f_i \in J \setminus J_{i-1}$ de grado d_i minimal, y sea $J_i := \langle f_1, \ldots, f_i \rangle$. Sea c_i el coeficiente principal de f_i y definamos el ideal $\mathfrak{a} := \langle \{c_i\}_{i \geq 1} \rangle \subseteq A$. Dado que A es noetheriano, se tiene que $\mathfrak{a} = \langle c_1, \ldots, c_n \rangle$ para cierto $n \in \mathbb{N}^{\geq 1}$. Luego, $c_{n+1} = a_1 c_1 + \ldots + a_n c_n$ para ciertos $a_i \in A$. Además, notemos que $d_i \leq d_{i+1}$.

Consideremos el elemento

$$\begin{aligned} f &:= f_{n+1} - (a_1 f_1 x^{d_{n+1}-d_1} + \ldots + a_n f_n x^{d_{n+1}-d_n}) \in J \\ &= (c_{n+1} x^{d_{n+1}} + \ldots) - ((a_1 c_1 + \ldots + a_n c_n) x^{d_{n+1}} + \ldots) \\ &= (c_{n+1} x^{d_{n+1}} + \ldots) - (c_{n+1} x^{d_{n+1}} + \ldots). \end{aligned}$$

Se sigue que $\deg(f) < d_{n+1}$ y luego $f \in J_n$. Por otra parte, tenemos que $(a_1 f_1 x^{d_{n+1}-d_1} + \ldots + a_n f_n x^{d_{n+1}-d_n}) \in J_n$, de donde se deduce que $f_{n+1} \in J_n$, una contradicción. □

Corolario 4.1.46. — *Sea k un cuerpo. Entonces, $k[X_1, \ldots, X_n]$ es un anillo noetheriano. En particular, todo ideal $I = \langle f_1, \ldots, f_r \rangle$ es finitamente generado.*

La motivación de lo que sigue proviene de la geometría algebraica clásica, iniciada por Hilbert.

Sea $n \in \mathbb{N}^{\geq 1}$. Si $S \subseteq \mathbb{C}[X_1, \ldots, X_n]$ es un conjunto de polinomios, el teorema de la base de Hilbert implica que $I := \langle S \rangle = \langle f_1, \ldots, f_r \rangle$ es finitamente generado.

***Definición 4.1.47* (variedad algebraica afín).** — El conjunto

$$V(S) := \{(a_1, \ldots, a_n) \in \mathbb{C}^n \mid f(a_1, \ldots, a_n) = 0 \text{ para todo } f \in S\}$$

es llamado un **conjunto algebraico**, ó bien una **variedad algebraica afín**, ó bien un **cerrado de Zariski**. El uso de este último término será justificado en la siguiente subsección.

¡Atención! — Sea k un cuerpo y $n \in \mathbb{N}$. El **espacio afín** $\mathbb{A}^n(k)$ sobre el cuerpo k es el conjunto $\mathbb{A}^n(k) = k^n$, el cual se denota usualmente por $\mathbb{A}^n$ si el cuerpo k se sobreentiende. La principal distinción entre el espacio afín $\mathbb{A}^n$ y el espacio vectorial k^n es que el origen no juega ningún rol especial en el espacio afín. En estricto rigor, las variedades afines se definen como $V(S) \subseteq \mathbb{A}^n$. Sin embargo, en esta introducción a la geometría algebraica afín sólo consideraremos $k = \mathbb{C}$ y escribiremos $\mathbb{A}^n(\mathbb{C}) = \mathbb{C}^n$, por simplicidad.

Ejemplo 4.1.48. —

1. Tenemos que $V(1) = \emptyset$, y que $V(\emptyset) = V(0) = \mathbb{C}^n$.
2. Las intersecciones arbitrarias de conjuntos algebraicos son conjuntos algebraicos. Más precisamente,
$$\bigcap_{i \in I} V(S_i) = V\left(\bigcup_{i \in I} S_i\right).$$
3. Las uniones finitas de conjuntos algebraicos son conjuntos algebraicos.

   En efecto, basta probar que $V(S_1) \cup V(S_2) = V(S_1 S_2)$, donde $S_1 S_2 := \{f_1 f_2,\ f_1 \in S_1 \text{ y } f_2 \in S_2\}$.

   Para la inclusión $V(S_1) \cup V(S_2) \subseteq V(S_1 S_2)$ notamos que si $a \in V(S_1) \cup V(S_2)$ entonces $f_1(a) = 0$ para todo $f_1 \in S_1$ ó bien $f_2(a) = 0$ para todo $f_2 \in S_2$. En cualquier caso, se tiene que $(f_1 f_2)(a) = f_1(a) f_2(a) = 0$ y luego $a \in V(S_1 S_2)$.

Para la otra inclusión, basta notar (por contrapositivo) que si $a \notin V(S_1) \cup V(S_2)$ entonces existen $f_1 \in S_1$ y $f_2 \in S_2$ tales que $f_1(a) \neq 0$ y $f_2(a) \neq 0$. En particular, $(f_1 f_2)(a) \neq 0$ y luego $a \notin V(S_1 S_2)$.

4. Consideremos el ideal maximal $\langle X_1 - a_1, \ldots, X_n - a_n \rangle \subseteq \mathbb{C}[X_1, \ldots, X_n]$. Entonces $V(\langle X_1 - a_1, \ldots, X_n - a_n \rangle) = \{(a_1, \ldots, a_n)\}$ consiste en un punto, gracias al algoritmo de la división.
5. Si $S' \subseteq S$, entonces $V(S) \subseteq V(S')$. En otras palabras, mientras más ecuaciones, menos puntos.

El siguiente resultado de Hilbert (sin demostración) caracteriza los ideales maximales de $\mathbb{C}[X_1, \ldots, X_n]$.

***Proposición 4.1.49* (Hilbert).** — *Sea $\mathfrak{m} \subseteq \mathbb{C}[X_1, \ldots, X_n]$ un ideal maximal. Entonces, $\mathfrak{m} = \langle X_1 - a_1, \ldots, X_n - a_n \rangle$ para ciertos $a_1, \ldots, a_n \in \mathbb{C}$.*

Corolario 4.1.50. — *Si $\{f_i\}_{i \in I}$ es una familia de polinomios sin ceros comunes en $\mathbb{C}^n$, entonces $\langle \{f_i\}_{i \in I} \rangle = \mathbb{C}[X_1, \ldots, X_n]$.*

Demostración. — Sea $I = \langle \{f_i\}_{i \in I} \rangle$ como en el enunciado. Si $I \subsetneq A$ es un ideal propio, entonces existe un ideal maximal $\mathfrak{m}$ tal que $I \subseteq \mathfrak{m}$. La Proposición anterior implica que $\mathfrak{m} = \langle X_1 - a_1, \ldots, X_n - a_n \rangle$ para ciertos $a_1, \ldots, a_n \in \mathbb{C}$ y por lo tanto $I \subseteq \langle X_1 - a_1, \ldots, X_n - a_n \rangle$. En particular, $\{(a_1, \ldots, a_n)\} = V(\langle X_1 - a_1, \ldots, X_n - a_n \rangle) \subseteq V(I)$. Así, todos los elementos $f \in I$ se anulan en el punto $(a_1, \ldots, a_n) \in \mathbb{C}^n$, una contradicción. □

Ejemplo 4.1.51. — En $\mathbb{C}^2$ tenemos los siguientes ejemplos de variedades algebraicas afines.

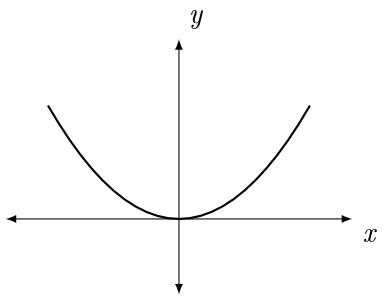


IMAGEN 1. La parábola $V(Y - X^2)$.

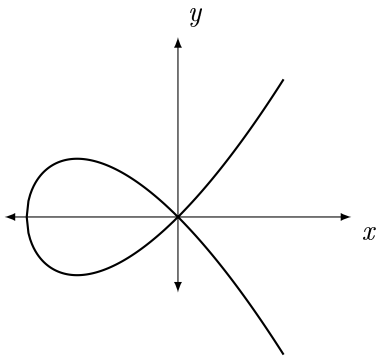


IMAGEN 2. La cúbica nodal $V(Y^2 - X^2 - X^3)$.

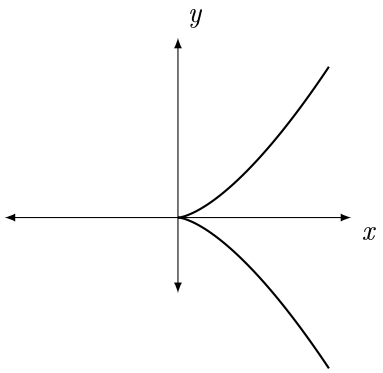


IMAGEN 3. La cúbica cuspidal $V(Y^2 - X^3)$.

El siguiente resultado, llamado comunmente el **Teorema de los ceros de Hilbert** o **Hilbert Nullstellensatz** (en alemán), data de 1893 y es un resultado fundamental en geometría algebraica.

***Teorema 4.1.52* (Hilbert Nullstellensatz).** — *Sea $g \in \mathbb{C}[X_1, \ldots, X_n]$, y sea $I \subseteq \mathbb{C}[X_1, \ldots, X_n]$ un ideal. Si para todo $(a_1, \ldots, a_n) \in V(I) \subseteq \mathbb{C}^n$ se tiene que $g(a_1, \ldots, a_n) = 0$, entonces existe $N \in \mathbb{N}^{\geq 1}$ tal que $g^N \in I$, i.e., $g \in \sqrt{I}$.*

Demostración. — El teorema de la base de Hilbert implica que el ideal $I = \langle f_1, \ldots, f_r \rangle \subseteq \mathbb{C}[X_1, \ldots, X_n]$ es finitamente generado.

El truco de Rabinowitch consiste en introducir una nueva variable X_{n+1}. Notemos que los polinomios $f_1, \ldots, f_r$ y $X_{n+1}g - 1$ no tienen ceros comunes

en $\mathbb{C}^{n+1}$. Luego, por el Corolario anterior, tenemos que

$$\langle f_1, \ldots, f_r, X_{n+1}g - 1\rangle = \mathbb{C}[X_1, \ldots, X_{n+1}].$$

Así, existen $p_1, \ldots, p_{r+1} \in \mathbb{C}[X_1, \ldots, X_{n+1}]$ tales que

$$1 = p_1 f_1 + \ldots + p_r f_r + p_{r+1}(X_{n+1}g - 1)$$

Si tomamos la imagen de esta expresión a través del morfismo

$$\begin{aligned} \mathbb{C}[X_1, \ldots, X_{n+1}] &\to \mathbb{C}(X_1, \ldots, X_n) \\ X_i &\mapsto X_i,\ i = 1, \ldots, n \\ X_{n+1} &\mapsto \frac{1}{g} \end{aligned}$$

obtenemos

$$1 = p_1\left(X_1, \ldots, X_n, \frac{1}{g}\right) f_1 + \ldots + p_n\left(X_1, \ldots, X_n, \frac{1}{g}\right) f_n.$$

Finalmente, multiplicamos por el denominador común g^N, y obtenemos $g^N \in \langle f_1, \ldots, f_r\rangle = I$. □

Definición 4.1.53 **(ideal de un subconjunto).** — Sea $X \subseteq \mathbb{C}^n$ un subconjunto. Definimos el **ideal de** X en $\mathbb{C}[X_1, \ldots, X_n]$ como

$$\mathfrak{I}(X) := \{f \in \mathbb{C}[X_1, \ldots, X_n] \mid f(a) = 0 \text{ para todo } a \in X\}.$$

Ejemplo 4.1.54. —

1. Si $X_1 \subseteq X_2 \subseteq \mathbb{C}^n$, entonces $\mathfrak{I}(X_1) \supseteq \mathfrak{I}(X_2)$.
2. Si $X_1, X_2 \subseteq \mathbb{C}^n$, entonces $\mathfrak{I}(X_1 \cup X_2) = \mathfrak{I}(X_1) \cap \mathfrak{I}(X_2)$.
3. Una formulación alternativa del Hilbert Nullstellensatz es la siguiente: Sea $I \subseteq \mathbb{C}[X_1, \ldots, X_n]$ un ideal. Entonces,
$$\mathfrak{I}(V(I)) = \sqrt{I}$$
En particular, si I es radical, entonces $\mathfrak{I}(V(I)) = I$.

4.1.5. Topología de Zariski y geometría. —

En primer lugar, recordaremos el concepto de topología, e introduciremos una topología muy útil en geometría algebraica.

Definición 4.1.55 **(topología).** — Sea X un conjunto, y sea $\tau = \{U_i\}_{i\in I}$ una familia de subconjuntos de X. Se dice que τ es una **topología** si:

1. $\emptyset \in \tau$ y $X \in \tau$.
2. **unión arbitraria**: para todo $J \subseteq I$ se tiene que $\cup_{j\in J} U_j \in \tau$.

3. **intersección finita**: si $U_1, U_2 \in \tau$, entonces $U_1 \cap U_2 \in \tau$.

Los elementos de τ son llamados **abiertos**, ó **conjuntos abiertos**, y los complementos de elementos de τ son llamados **cerrados**, ó **conjuntos cerrados**.

Observación 4.1.56. — Equivalentemente, una topología τ se define a partir de sus cerrados $\{F_i\}_{i\in I}$ de la siguiente manera:

1. X y $\emptyset$ son conjuntos cerrados.
2. **intersección arbitraria**: para todo $J \subseteq I$ se tiene que $\cap_{j\in J} F_j$ es un conjunto cerrado.
3. **unión finita**: si F_1, F_2 son conjuntos cerrados, entonces $F_1 \cup F_2$ es un conjunto cerrado.

Definición 4.1.57 **(topología de Zariski).** — La **topología de Zariski** en $\mathbb{C}^n$ es la topología cuyos cerrados son los conjuntos algebraicos $V(S)$. Un conjunto $U \subseteq \mathbb{C}^n$ es un **abierto Zariski** si $U = \mathbb{C}^n \setminus V(S)$ para algún $S \subseteq \mathbb{C}[X_1, \ldots, X_n]$. Más informalmente, en la topología de Zariski los cerrados son ceros comunes de polinomios, y los abiertos sus complementos.

¡Atención! — Si U, V son abiertos Zariski no vacíos, entonces $U \cap V \neq \emptyset$. En otras palabras, la topología de Zariski **no** es Hausdorff.

Ejemplo 4.1.58. —

1. En $\mathbb{C}$ los cerrados (Zariski) son $\emptyset$, $\mathbb{C}$ y conjuntos finitos.
2. Sea $X \subseteq \mathbb{C}^n$, y consideremos la notación de la subsección anterior. Se tiene que
$$V(I(X)) =: \overline{X}^{\,\mathrm{Zar}}$$
es la **adherencia de Zariski** de X en $\mathbb{C}^n$.
3. Notar que $\overline{\{z \in \mathbb{C} \mid \sin(z) = 0\}}^{\,\mathrm{Zar}} = \mathbb{C}$.

Ahora discutiremos sobre anillos de funciones en geometría.

Definición 4.1.59 **(morfismo regular).** — Sean $X \subseteq \mathbb{C}^n$ e $Y \subseteq \mathbb{C}^m$ variedades algebraicas afines. Un **morfismo regular** $\varphi : X \to Y$ es la restricción de una función polinomial $\Phi : \mathbb{C}^n \to \mathbb{C}^m$ tal que $\Phi(X) \subseteq Y$, es decir, una función de la forma

$$(X_1, \ldots, X_n) \mapsto (f_1(X_1, \ldots, X_n), \ldots, f_m(X_1, \ldots, X_n))$$

donde $f_i \in \mathbb{C}[X_1, \ldots X_n]$ para todo $i \in \{1, \ldots, m\}$. En particular, una **función regular** en X es un morfismo regular $\varphi : X \to \mathbb{C}$.

***Notación 4.1.60* (funciones regulares).** — Sea $X \subseteq \mathbb{C}^n$ una variedad algebraica afín. Denotamos por

$$\mathscr{O}(X) := \{f : X \to \mathbb{C} \text{ función regular}\}$$

a la $\mathbb{C}$–**álgebra de funciones regulares** de X.

***Proposición 4.1.61* (functorialidad).** — *Sean $X \subseteq \mathbb{C}^n$ e $Y \subseteq \mathbb{C}^m$ dos variedades algebraicas afines. Si $\varphi : X \to Y$ es un morfismo regular, entonces*

$$\begin{aligned} \varphi^* : \mathscr{O}(Y) &\to \mathscr{O}(X) \\ f &\mapsto f \circ \varphi \end{aligned}$$

es un morfismo de $\mathbb{C}$–álgebras. Este morfismo es denominado **pullback**.

Un hecho importante (que no probaremos) es que las variedades algebraicas afines están completamente determinadas por su álgebra de funciones regulares.

Proposición 4.1.62. — *Sean $X \subseteq \mathbb{C}^n$ e $Y \subseteq \mathbb{C}^m$ variedades algebraicas afines. Existe una correspondencia*

$$\begin{Bmatrix} \text{morfismos regulares} \\ \varphi : X \to Y \end{Bmatrix} \xrightarrow{\sim} \begin{Bmatrix} \text{morfismos de } \mathbb{C}\text{–álgebras} \\ \mathscr{O}(Y) \to \mathscr{O}(X) \end{Bmatrix}$$
$$\varphi \longmapsto \varphi^*$$

En particular, $X \cong Y$ si y sólo si $\mathscr{O}(X) \cong \mathscr{O}(Y)$.

De la Proposición anterior concluimos que basta estudiar $\mathbb{C}$–álgebras para comprender la teoría de variedades algebraicas afines.

Luego, una cuestión fundamental es saber qué anillos aparecen como álgebras de funciones regulares. Por definición,

$$\mathscr{O}(\mathbb{C}^n) = \mathbb{C}[X_1, \ldots, X_n],$$

donde las X_i son funciones coordenadas. Además, si $X \subseteq \mathbb{C}^n$ es una variedad algebraica afín, entonces el morfismo de restricción

$$\begin{aligned} \mathscr{O}(\mathbb{C}^n) &\xrightarrow{\text{res}} \mathscr{O}(X) \\ f &\mapsto f|_X \end{aligned}$$

es sobreyectivo. Notamos que por definición

$$\ker(\text{res}) = \mathfrak{I}(X) = \{f \in \mathbb{C}[X_1, \ldots, X_n] \mid f(a) = 0 \text{ para todo } a \in X\}.$$

Esto implica que $\mathscr{O}(X) \cong \mathbb{C}[X_1, \ldots, X_n]/\mathfrak{I}(X)$. Por lo tanto, $\mathscr{O}(X)$ es una $\mathbb{C}$–álgebra finitamente generada (por las clases $[X_1], \ldots, [X_n]$). Más aún, si

$f \in \mathscr{O}(X)$ y $n \in \mathbb{N}^{\geq 1}$ son tales que $f^n = 0$, entonces $f = 0$. En otras palabras, $\mathscr{O}(X)$ es un anillo reducido (su único elemento nilpotente es el 0).

Recíprocamente, dada A una $\mathbb{C}$–álgebra finitamente generada y reducida, si escribimos $A = \langle b_1, \ldots, b_n \rangle_{\mathbb{C}\text{–álg}}$ entonces el morfismo

$$\begin{aligned} \mathbb{C}[X_1, \ldots, X_n] &\xrightarrow{\varphi} A \\ X_i &\mapsto b_i \end{aligned}$$

es sobreyectivo. Si $I = \ker(\varphi)$, entonces $A \cong \mathbb{C}[X_1, \ldots, X_n]/I$. Por otra parte, el teorema de la base de Hilbert implica que $I = \langle f_1, \ldots, f_r \rangle$ es finitamente generado. Así, $X = V(I) \subseteq \mathbb{C}^n$ y $\mathscr{O}(X) \cong A$. Más aún, $\mathbb{C}[X_1, \ldots, X_n]/I$ es reducido si y sólo si I es radical.

Concluimos de este modo que existe una correspondencia

$$\left\{ \begin{array}{c} \text{variedades algebraicas} \\ \text{afines } X \subseteq \mathbb{C}^n \end{array} \right\} \overset{1:1}{\longleftrightarrow} \left\{ \begin{array}{c} \text{ideales radicales} \\ I \subseteq \mathbb{C}[x_1, \ldots, x_n] \end{array} \right\}$$

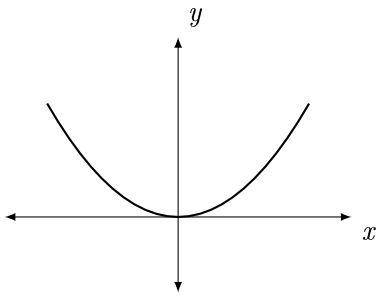
$$\begin{aligned} X &\longmapsto \mathfrak{I}(X) \\ V(I) &\longmapsfrom I \end{aligned}$$

En otras palabras, y más informalmente, las propiedades geométricas de X se traducen en propiedades algebraicas de $\mathscr{O}(X)$.

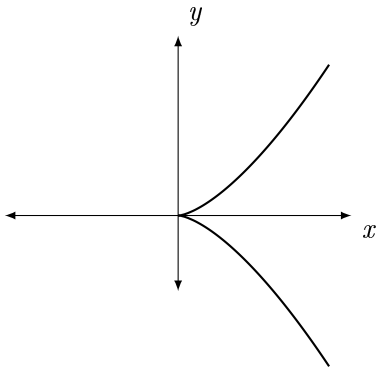
Observación 4.1.63. — La biyección en la conclusión anterior se tiene ya que $\mathfrak{I}(V(I)) = \sqrt{I} = I$, donde la primera igualdad es implicada por el Hilbert Nullstellensatz, y la segunda igualdad se tiene pues I es radical.

Ejemplo 4.1.64. —

1. Si consideramos la variedad algebraica afín dada por
$$X = \{(x, y) \in \mathbb{C}^2 \mid y = x^2\},$$
entonces tenemos que $\mathfrak{I}(X) = \langle y - x^2 \rangle \subseteq \mathbb{C}[x, y]$. Luego,
$$\mathscr{O}(X) = \mathbb{C}[x, y]/\langle y - x^2 \rangle \cong \mathbb{C}[x] = \mathscr{O}(\mathbb{C}).$$
Así, $X \cong \mathbb{C}$ son isomorfas como variedades algebraicas afines.



2. Si consideramos la variedad algebraica afín dada por
$$X = \{(x, y) \in \mathbb{C}^2 \mid y^2 = x^3\},$$
entonces tenemos que $\mathfrak{I}(X) = \langle y^2 - x^3 \rangle \subseteq \mathbb{C}[x, y]$. Luego,
$$\mathscr{O}(X) = \mathbb{C}[x, y]/\langle y^2 - x^3 \rangle.$$
Es posible probar que $X \ncong \mathbb{C}$ como variedades algebraicas afines.



Ejercicio 4.1.65. — Sea $X \subseteq \mathbb{C}^n$ es una variedad algebraica afín. Probar que existe una correspondencia
$$\left\{ \begin{array}{c} \text{puntos } a = (a_1, \ldots, a_n) \\ \text{en la variedad } X \end{array} \right\} \overset{1:1}{\longleftrightarrow} \left\{ \begin{array}{c} \text{ideales maximales} \\ \mathfrak{m}_a \subseteq \mathscr{O}(X) \end{array} \right\}$$

El ejercicio anterior motiva a considerar el conjunto de todos los ideales maximales de un anillo dado.[(1)]

[(1)] El término **espectro** proviene de la analogía con el espectro de Gelfand de una álgebra de Banach conmutativa.

***Definición 4.1.66* (espectro maximal).** — Sea A un anillo. Definimos su **espectro maximal** mediante

$$\mathrm{Specm}(A) := \{\mathfrak{m} \subseteq A \text{ ideal maximal}\},$$

el conjunto cuyos elementos son los ideales maximales de A.

Ejemplo 4.1.67. —

1. El conjunto $\mathrm{Specm}(\mathbb{Z}) = \{\langle p\rangle,\ p \text{ primo}\}$ está en biyección con el conjunto de números primos.
2. El ejercicio anterior implica que si $X \subseteq \mathbb{C}^n$ es una variedad algebraica afín, entonces $\mathrm{Specm}(\mathscr{O}(X))$ está en biyección con los puntos de X. En particular, $\mathrm{Specm}(\mathbb{C}[X_1, \ldots, X_n])$ está en biyección con $\mathbb{C}^n$.

4.1.6. Geometría de ideales. — En esta subsección discutiremos sobre la geometría de los ideales primos, asi como de operaciones entre ideales y su correspondiente interpretación geométrica.

***Definición 4.1.68* (variedad irreducible).** — Sea $X \subseteq \mathbb{C}^n$ una variedad algebraica afín. Decimos que X es **irreducible** si no puede ser escrita de la forma $X = X_1 \cup X_2$, donde $X_1, X_2 \subseteq X$ son variedades algebraicas afines no vacías y distintas de X. En caso contrario, diremos que X es **reducible**.

Ejemplo 4.1.69. — La variedad algebraica afín

$$X = \{(x, y) \in \mathbb{C}^2 :\ xy = 0\} = \{x = 0\} \cup \{y = 0\}$$

no es irreducible. Notar que $\mathfrak{I}(X) = \langle xy\rangle$ **no** es un ideal primo pues $xy \in \mathfrak{I}(X)$ pero $x \notin \mathfrak{I}(X)$ y $y \notin \mathfrak{I}(X)$.

Proposición 4.1.70. — *Sea $X \subseteq \mathbb{C}^n$ una variedad algebraica afín. Entonces,*

$$X \text{ irreducible} \iff \mathscr{O}(X) \text{ dominio entero} \iff \mathfrak{I}(X) \text{ ideal primo.}$$

Demostración. — Como $\mathscr{O}(X) \cong \mathbb{C}[X_1, \ldots, X_n]/\mathfrak{I}(X)$, se tiene que $\mathscr{O}(X)$ es un dominio si y sólo si $\mathfrak{I}(X)$ es primo. Luego, basta probar que X es irreducible si y sólo si $\mathscr{O}(X)$ es un dominio entero.

Supongamos que X es irreducible, y sean $f, g \in \mathscr{O}(X)$ funciones regulares tales que $fg = 0$. Igual que antes, si $S \subseteq \mathscr{O}(X)$ es un subconjunto, definimos

$$V(S) := \{a \in X \mid f(a) = 0\ \forall f \in S\},$$

y luego

$$\begin{aligned} V(0) = X = V(fg) &= V(f) \cup V(g) \\ &= \{a \in X \mid f(a) = 0\} \cup \{a \in X \mid g(a) = 0\}, \end{aligned}$$

donde los últimos dos subconjuntos son variedades algebraicas afines no-vacías. Como X es irreducible, se tiene que $V(f) = X$ ó $V(g) = X$ si y sólo si $f = 0$ ó $g = 0$. Así, $fg = 0$ implica que $f = 0$ ó $g = 0$, es decir, que $\mathscr{O}(X)$ es un dominio entero.

Recíprocamente, si $X = X_1 \cup X_2$, donde $X_1, X_2 \subsetneq X$ son subvariedades algebraicas afines no-vacías, escribimos $X_1 = V(S_1)$ y $X_2 = V(S_2)$, donde $S_1, S_2 \subseteq \mathscr{O}(X)$ son subconjuntos. Luego, $X = V(S_1) \cup V(S_2) = V(S_1 S_2)$. Dado que $X_1 \subsetneq X$, existe $a \in V(S_1) \setminus V(S_2)$. En otras palabras, existe $f_2 \in S_2$ tal que $f_2(a) \neq 0$, y en particular $f_2 \neq 0$ en $\mathscr{O}(X)$. Análogamente, existen $b \in V(S_2) \setminus V(S_1)$ y $f_1 \in S_1$ tales que $f_1(a) \neq 0$, y en particular $f_1 \neq 0$ en $\mathscr{O}(X)$. Sin embargo $f_1 f_2 \in S_1 S_2$ es 0, pues $X = V(S_1 S_2)$. Concluimos que $\mathscr{O}(X)$ no es un dominio entero. □

***Definición 4.1.71* (operaciones sobre ideales).** — Sea A un anillo, y sean $I, J \subseteq A$ ideales. Definimos:

1. La **suma** de I y J mediante
$$I + J := \{a + b \mid a \in I, b \in J\} = \langle I \cup J \rangle.$$
2. El **producto** de I y J mediante
$$IJ := \langle \{ab : \ a \in I, b \in J\} \rangle = \left\{ \sum_{\text{finita}} a_i b_i : \ a_i \in I, b_i \in J \right\}.$$

Notación 4.1.72. — Sea A un anillo. Si $\{I_k\}_{k \in K}$ es una colección de ideales en A, entonces escribimos
$$\sum_{k \in K} I_k = \langle \{I_k\}_{k \in K} \rangle = \left\{ \sum_{\text{finita}} a_k, \ a_k \in I_k \right\}.$$

Observación 4.1.73. — Si los ideales $I, J \subseteq A$ son finitamente generados, entonces la suma $I + J$ y producto IJ pueden ser descritos explícitamente en término de los generadores. Concretamente, si $I = \langle a_1, \dots a_r \rangle$ y $J = \langle b_1, \dots, b_s \rangle$, entonces
$$I + J = \langle a_1, \dots, a_r, b_1, \dots, b_s \rangle$$
y
$$IJ = \langle a_1 b_1, \dots, a_r b_1, a_1 b_2, \dots, a_r b_2, \dots, a_r b_s \rangle.$$

Ejercicio 4.1.74. — Sean $n, m \in \mathbb{N}^{\geq 1}$, y sean $I_n = n\mathbb{Z} \subseteq \mathbb{Z}$ y $I_m = m\mathbb{Z} \subseteq \mathbb{Z}$ ideales. Demostrar que $I_n I_m = nm\mathbb{Z}$, que $I_n \cap I_m = \text{mcm}(n, m)\mathbb{Z}$, y que $I_n + I_m = \text{mcd}(n, m)\mathbb{Z}$.

Interpretación geométrica 4.1.75. — Si $I, J \subseteq \mathbb{C}[X_1, \ldots, X_n]$ son ideales, entonces $V(IJ) = V(I) \cup V(J)$ y $V(\sum_{k\in K} I_k) = \cap_{k\in K} V(I_k)$.

Observación 4.1.76. — En general, siempre se cumple que $IJ \subseteq I \cap J$. Sin embargo, esta inclusión puede ser estricta. Por ejemplo, en el ejercicio anterior, $I_n I_m = I_n \cap I_m$ si y sólo si n y m son primos relativos.

¡Atención! — Recordemos que si A es un anillo, entonces su espectro maximal está dado por

$$\mathrm{Specm}(A) = \{\mathfrak{m} \subseteq A \text{ ideal maximal}\}.$$

En general, si $\varphi : A \to B$ es un morfismo de anillos, y $\mathfrak{m}_B \subseteq B$ es un ideal maximal (y, por lo tanto, primo), entonces $\varphi^{-1}(\mathfrak{m}_B)$ es un ideal primo pero **no** necesariamente es maximal. Por ejemplo, si $A = \mathbb{Z}$, $B = \mathbb{Q}$, y $\varphi = \iota : \mathbb{Z} \hookrightarrow \mathbb{Q}$ es la inclusión, entonces $\langle 0\rangle \subseteq \mathbb{Q}$ es maximal, pero $\langle 0\rangle \subseteq \mathbb{Z}$ **no** es maximal.

***Observación 4.1.77* (geometría algebraica moderna)**

En 1960, Alexander Grothendieck (1928–2014) introdujo la noción de esquema afín, que generaliza la noción de variedad algebraica afín en geometría algebraica clásica. Explícitamente, si A es un anillo, definimos su **espectro** como

$$\mathrm{Spec}(A) = \{\mathfrak{p} \subseteq A \text{ ideal primo}\}$$

Podemos dotar a $\mathrm{Spec}(A)$ de la **topología de Zariski**, cuyos cerrados son

$$V(S) := \{\mathfrak{p} \in \mathrm{Spec}(A) \mid \mathfrak{p} \supseteq S\}$$

donde $S \subseteq A$ es un subconjunto arbitrario. Esta es una *mejor* definición que la que presentamos al inicio de la subsección, pues si B es otro anillo, y $\varphi : A \to B$ es un morfismo, la aplicación

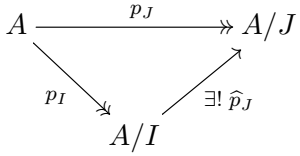
$$\begin{aligned} \varphi^{\#} : \mathrm{Spec}(B) &\to \mathrm{Spec}(A) \\ \mathfrak{p} &\mapsto \varphi^{-1}(\mathfrak{p}) \end{aligned}$$

está bien definida, y es continua respecto a la topología de Zariski.

4.1.7. Morfismos entre cocientes y teorema chino del resto. —

Sea A un anillo, y sean $I, J \subseteq A$ ideales tales que $I \subseteq J$. Denotemos por $p_I : A \to A/I$ y $p_J : A \to A/J$ las proyecciones canónicas asociadas a los cocientes respectivos. Como $p_J(I) = \langle 0\rangle$ en A/J, por propiedad universal del

cociente asegura la existencia de un único morfismo $\widehat{p}_J$ tal que el siguiente diagrama conmuta:



Proposición 4.1.78. — *La imagen $J/I := p_I(J)$ de J es A/I es un ideal, y $\widehat{p}_J$ induce un isomorfismo*

$$(A/I)/(J/I) \cong A/J.$$

Demostración. — Notemos que $\ker(\widehat{p}_J) = \ker(p_J)/I = J/I$ es un ideal. Como p_J es sobreyectivo, $\widehat{p}_J$ es sobreyectivo también. Luego,

$$(A/I)/\ker(\widehat{p}_J) = (A/I)/(J/I) \cong \mathrm{Im}(\widehat{p}_J) = A/J,$$

de donde se concluye el resultado. □

Interpretación geométrica 4.1.79. — Si $Y \subseteq X \subseteq \mathbb{C}^n$ son variedades algebraicas afines, se tiene que $\mathscr{O}(X) \cong \mathscr{O}(\mathbb{C}^n)/\mathfrak{I}(X)$, y que $\mathscr{O}(Y) \cong \mathscr{O}(\mathbb{C}^n)/\mathfrak{I}(Y)$. La Proposición anterior implica que $\mathscr{O}(Y) \cong \mathscr{O}(X)/(\mathfrak{I}(Y)/\mathfrak{I}(X))$.

Ejemplo 4.1.80. — Un caso particular importante donde se aplica lo anterior es el de dos ideales $I, J \subseteq A$ (no necesariamente incluidos uno en el otro), y donde se considera la inclusión $I \subseteq I + J$. La Proposición anterior implica que

$$(A/I)/((I+J)/I) \cong A/(I+J).$$

Observación 4.1.81. — Sea A un anillo, y sean $I, J \subseteq A$ ideales. Definimos el morfismo

$$\begin{aligned} \varphi : A &\to A/I \times A/J \\ a &\mapsto (a \mod I, a \mod J) \end{aligned}$$

y notamos que $\ker(\varphi) = I \cap J$. La propiedad universal del cociente implica que el morfismo

$$A/(I \cap J) \xrightarrow{\widehat{\varphi}=(p_I,p_J)} A/I \times A/J$$

es inyectivo. El siguiente resultado permite determinar cuándo $\widehat{\varphi}$ es un isomorfismo.

***Teorema 4.1.82* (chino del resto).** — *Sea A un anillo, y sean $I, J \subseteq A$ ideales. Sea*

$$\varphi : A/(I \cap J) \hookrightarrow A/I \times A/J$$

el morfismo inyectivo natural. Entonces, φ es un isomorfismo si y sólo si $I + J = A$. Más aún, en tal caso se tiene que $IJ = I \cap J$, y luego

$$A/(IJ) \cong A/(I \cap J) \cong A/I \times A/J.$$

Demostración. — Supongamos que $I + J = A$. Luego, existen $a \in I$ y $b \in J$ tales que $a + b = 1$. Dados $x, y \in A$, buscamos hallar $\overline{c} \in A/(I \cap J)$ tal que $c \equiv x \mod I$ y $c \equiv y \mod J$. Definamos $c := ay + bx \in A$. Entonces,

$$c - x = ay + bx - x = ay + x(b-1) = ay + x(-a) = a(y - x).$$

Como $a(y - x) \in I$ pues $a \in I$, se tiene que $c \equiv x \mod I$. Análogamente, $c \equiv y \mod J$. Por lo tanto, φ es sobreyectivo.

Supongamos que φ es sobreyectivo. Entonces, existe $b \in A$ tal que $\varphi(b) = (\overline{1}, \overline{0}) \in A/I \times A/J$. Esto último es equivalente a que $b \in 1 + I$ y $b \in J$. Definamos $a = 1 - b \in I$, y notemos que como $a \in I$, $b \in J$ y $a + b = 1$, tenemos que $I + J = A$.

Finalmente, notemos que siempre se tiene que $IJ \subseteq I \cap J$. Por lo tanto, basta demostrar que $I \cap J \subseteq IJ$. Para ello, escribamos $a + b = 1$, donde $a \in I$ y $b \in J$. Dado $x \in I \cap J$, tenemos que $ax \in IJ$ y $bx \in IJ$, de donde concluimos que $x = ax + bx \in IJ$. □

Ejemplo 4.1.83. — Sean $n, m \in \mathbb{N}^{\geq 1}$, y sean $I_n = n\mathbb{Z} \subseteq \mathbb{Z}$ e $I_m = m\mathbb{Z} \subseteq \mathbb{Z}$ ideales. Entonces, por el lema de Bézout, $I_n + I_m = \mathbb{Z}$ si y sólo si n y m son primos relativos. En este caso, $I_n I_m = I_n \cap I_m = nm\mathbb{Z}$, y luego

$$\mathbb{Z}/(nm\mathbb{Z}) \cong \mathbb{Z}/(n\mathbb{Z}) \times \mathbb{Z}/(m\mathbb{Z}),$$

que es precisamente la versión del teorema chino del resto que hemos estudiado anteriormente en el contexto de grupos (ver Teorema 2.4.2).

4.2. Módulos sobre un anillo

4.2.1. Primeras definiciones. —

***Definición 4.2.1* (módulo).** — Sea A un anillo. Un **A-módulo** M es un grupo abeliano dotado de una "acción" de A

$$A \times M \to M$$
$$(a, m) \mapsto am$$

tal que para todos $a, b \in A$ y $m, n \in M$ se tiene:

1. $a(m + n) = am + an$
2. $(a + b)m = am + bm$, y también $(ab)m = a(bm)$

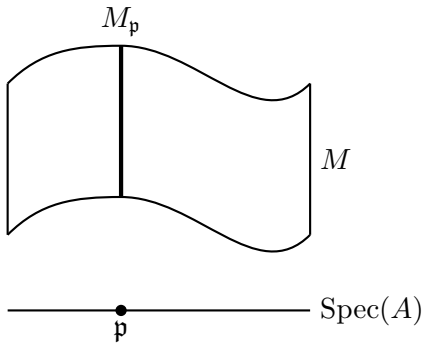
3. $1 \cdot m = m$

Ejemplo 4.2.2. —

1. Un ideal I de A es un A-módulo. En particular, A es un A-módulo.
2. Si $A = k$ cuerpo, un A-módulo es un k-espacio vectorial.
3. Si $A = \mathbb{Z}$, un $\mathbb{Z}$-módulo es un grupo abeliano (definiendo $nx := \overbrace{x + \ldots + x}^{n \text{ veces}}$).
4. $A[x]$ es un A-módulo.
5. A/I es un A-módulo (definiendo $a \cdot (b + I) = ab + I$).

¡Atención! — Los módulos generalizan muchos conceptos conocidos (cf. Teorema de Freyd–Mitchell (1965))

Interpretación geométrica 4.2.3. — Si $A = k$ es un cuerpo, un k-módulo es un k-espacio vectorial. En general, si A es un anillo (conmutativo con unidad) arbitrario, la forma intuitiva de pensar un A-módulo es como una colección de espacios vectoriales, uno sobre cada punto de $\operatorname{Spec}(A)$ (c.f. espacio tangente).



Definición 4.2.4 **(morfismo de módulos).** — Un **morfismo** $\varphi : M \to M'$ de A-módulos es un morfismo de grupos abelianos que es A-lineal, es decir,

$$\varphi(am) = a\varphi(m)$$

para todos $a \in A$ y $m \in M$.

Notación 4.2.5. — Sean M, M' dos A-módulos. Denotamos

$$\begin{aligned} \operatorname{Hom}_{A-\mathrm{mod}}(M, M') &:= \operatorname{Hom}_A(M, M') \\ &= \{\varphi : M \to M' \text{ morfismo de } A\text{-módulos}\} \end{aligned}$$

Además, $\operatorname{End}_A(M) := \operatorname{Hom}_A(M, M)$.

Ejemplo 4.2.6. — Sean $A = k$ un cuerpo, $M \cong k^n$ y $M' \cong k^m$ espacios vectoriales. Entonces $\mathrm{End}_A(M) \cong M_{n\times n}(k)$ y $\mathrm{Hom}_A(M, M') \cong M_{m\times n}(k)$

Observación 4.2.7. — $\mathrm{Hom}_A(M, M')$ puede ser dotado de una estructura natural de A-módulo definiendo

$$(a \cdot \varphi)(m) := a\varphi(m) \text{ y } (\varphi_1 + \varphi_2)(m) := \varphi_1(m) + \varphi_2(m).$$

Como siempre, un isomorfismo de A-módulos es un morfismo biyectivo.

Ejemplo 4.2.8. — Si $f \in \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z})$ entonces $f(1) = n$ para cierto $n \in \mathbb{Z}$. Luego $f(m) = f(m\cdot 1) = mf(1) = mn$, donde la penúltima igualdad se obtiene al ver m como un escalar. En particular, $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}) \cong \mathbb{Z}$

Ejemplo 4.2.9. — $A = \mathbb{R}$, $M = \mathscr{C}^1(\mathbb{R})$, $M' = \mathscr{C}^0(\mathbb{R})$, entonces

$$\begin{aligned} \varphi : M &\to M' \\ f &\mapsto \varphi(f) = f' \end{aligned}$$

es un morfismo de A-módulos.

Ejercicio 4.2.10. — Sea A un anillo y M un A-módulo. Determinar $\mathrm{Hom}_A(A, M)$ (cf. Ejemplo 4.2.8).

Definición 4.2.11 **(sub-módulo).** — Sea M un A-módulo. Un **sub-módulo** N de M es un subgrupo $N \subseteq M$ estable por la acción de A sobre M, i.e., $an \in N$ para todos $a \in A$ y $n \in N$. En otras palabras, la inclusión $N \hookrightarrow M$ es un morfismo de A-módulos.

Ejemplo 4.2.12. —

1. Si $A = k$ cuerpo. Un sub-módulo es un sub-espacio vectorial.
2. Si consideremos A como un A-módulo via la multiplicación, un sub-módulo de A es un ideal de A
3. Sea $\varphi : M \to M'$ morfismo de A-módulos.
   a) Si $N \subseteq M$ es un sub-módulo, entonces $\varphi(N) \subseteq M'$ es un sub-módulo.
   b) Si $N' \subseteq M'$ es un sub-módulo, entonces $\varphi^{-1}(N') \subseteq M$ es un sub-módulo.

   En particular, $\ker(\varphi)$ e $\mathrm{Im}(\varphi)$ son sub-módulos.

El siguiente resultado, cuya demostración se deja como ejercicio, describe cómo un morfismo de módulos induce naturalmente morfismos llamados comunmente como *pullback* y *pushforward*.

***Teorema 4.2.13* (functorialidad).** — *Sea $\varphi : M \to M'$ un morfismo de A-módulos y sea N un A-módulo cualquiera. Entonces, el* **pullback**

$$\begin{aligned} \varphi^* : \mathrm{Hom}_A(M', N) &\to \mathrm{Hom}_A(M, N) \\ f &\mapsto f \circ \varphi \end{aligned}$$

es un morfismo de A-módulos. Similarmente, el **pushforward**

$$\begin{aligned} \varphi_* : \mathrm{Hom}_A(N, M) &\to \mathrm{Hom}_A(N, M') \\ f &\mapsto \varphi \circ f \end{aligned}$$

es un morfismo de A-módulos.

4.2.2. Módulos cocientes. — Del mismo modo que para grupos, espacios vectoriales y anillos, podemos considerar cocientes de módulos. Concretamente, si M es un A-módulo y $N \subseteq M$ un sub-módulo, definimos el conjunto cociente M/N de M por la relación de equivalencia

$$m \sim m' \Leftrightarrow m - m' \in N,$$

y denotamos por

$$\begin{aligned} \pi : M &\to M/N \\ m &\mapsto [m] \end{aligned}$$

la proyección canónica. Del mismo modo que para los casos anteriormente discutidos, denotaremos también la clase $[m]$ de $m \in M$ en M/N mediante los símbolos $\overline{m}$, $m + N$ o $m \mod N$, de acuerdo al contexto.

Dejamos como ejercicio para el lector verificar que las propiedades análogas a los cocientes estudiados anteriormente también se verifican en el contexto de módulos:

Ejercicio 4.2.14. — Sea A un anillo, y sean M, M', N tres A-módulos.

a) Probar que existe una única estructura de A-módulo sobre el conjunto cociente M/N de tal suerte que $\pi : M \to M/N$ sea un morfismo de A-módulos.

b) Probar que π^{-1} induce una biyección

$$\left\{ \begin{array}{c} \text{sub-módulos} \\ \text{de } M/N \end{array} \right\} \xrightarrow{\sim} \left\{ \begin{array}{c} \text{sub-módulos de } M \\ \text{que contienen } N \end{array} \right\},$$

cuya inversa está dada por $P \mapsto \pi(P) = P/N$.

c) Probar la siguiente **propiedad universal** del cociente: Sea $\varphi : M \to M'$ morfismo de A-módulos tal que $\varphi(N) = \{0\}$. Entonces, existe un único morfismo de A-módules $\widehat{\varphi} : M/N \to M'$ tal que $\varphi = \widehat{\varphi} \circ \pi$. Escribir el correspondiente diagrama conmutativo.

En particular, si $\varphi : M \to M'$ es cualquier morfismo de A-módulos y aplicamos el Ejercicio 4.2.14(c) al sub-módulo $N = \ker(\varphi) \subseteq M$, obtenemos el resultado siguiente.

Proposición 4.2.15. — *Todo morfismo $\varphi : M \to M'$ de A-módulos admite una factorización única*

$$M \twoheadrightarrow M/\ker(\varphi) \xrightarrow{\sim} \mathrm{Im}(\varphi) \hookrightarrow M',$$

donde el primer morfismo es la proyección canónica al cociente, el segundo es inducido por la propiedad universal del cociente, y el tercero es la inclusión.

Además del kernel y de la imagen del morfismo, uno de los principales objectos asociados a un morfismo es el *cokernel*.

***Definición 4.2.16* (cokernel).** — Sea $\varphi : M \to M'$ morfismo de A-módulos. Definimos el **cokernel** del morfismo como

$$\mathrm{coker}(\varphi) := M'/\mathrm{Im}(\varphi).$$

Observación 4.2.17. — Sea $\varphi : M \to M'$ morfismo de A-módulos. Por la definición de kernel y cokernel tenemos las siguientes equivalencias.

1. φ es inyectivo si y sólo si $\ker(\varphi) = \{0\}$.
2. φ es sobreyectivo si y sólo si $\mathrm{coker}(\varphi) = \{0\}$.

4.2.3. Operaciones sobre sub-módulos. — A partir de una familia de sub-módulos de M, podemos formar los siguientes nuevos sub-módulos de M.

***Definición 4.2.18* (suma e intersección).** — Sea M un A-módulo y sea $\{M_i\}_{i\in I} \subseteq M$ una familia de sub-módulos.

1. La **suma** $\sum_{i\in I} M_i$ es el conjunto de todas las sumas finitas
$$\sum_{\text{finita}} x_i,$$
con $x_i \in M_i$. En otras palabras, $\sum_{i\in I} M_i$ es el sub-módulo más pequeño de M que contiene todos los M_i.
2. La **intersección** $\bigcap_{i\in I} M_i$ es también un sub-módulo de M.

Ejercicio 4.2.19. — Dar un ejemplo donde la suma $\sum_{i\in I} M_i$ y la intersección $\bigcap_{i\in I} M_i$ sean diferentes.

Del mismo modo que para grupos y anillos, podemos considerar cocientes sucesivos de módulos.

Proposición 4.2.20. — *Sea A un anillo.*

1. *Si $N \subseteq P \subseteq M$ son A-módulos, entonces*
$$(M/N)/(P/N) \cong M/P.$$
2. *Si $N_1,\ N_2 \subseteq M$ son A-módulos, entonces*
$$(N_1 + N_2)/N_1 \cong N_2/(N_1 \cap N_2).$$

Demostración. — Para probar (1) consideramos el morfismo $\varphi : M/N \to M/P$ definido por $\varphi(m+N) = m+P$. Notar que φ está bien definido y es sobreyectivo. Además,
$$\ker(\varphi) = \{\overline{m} \in M/N \text{ tales que } \overline{m} = 0 \bmod P\} = P/N.$$
De esto, se tiene que
$$(M/N)/\ker(\varphi) = (M/N)/(P/N) \xrightarrow{\sim} \mathrm{Im}(\varphi) = M/P.$$
Para probar (2) basta notar que la composición
$$N_2 \hookrightarrow N_1 + N_2 \twoheadrightarrow (N_1 + N_2)/N_1$$
es sobreyectiva y su kernel es $N_1 \cap N_2$. □

No podemos definir en general el producto de sub-módulos de M, pero podemos definir el producto de sub-módulos e ideales.

Definición 4.2.21. — Sea $I \subseteq A$ un ideal y sea M un A-módulo. Definimos el sub-módulo
$$IM := \left\{ \sum_{\text{finita}} a_i m_i \;\middle|\; a_i \in I, m_i \in M \right\}.$$

Ejercicio 4.2.22. — Sea $I \subseteq A$ un ideal y sea M un A-módulo. Probar que M/IM puede ser dotado de una estructura de A/I-módulo. En particular, si $\mathfrak{m} \subseteq A$ es un ideal maximal y $\kappa = A/\mathfrak{m}$ es el cuerpo cociente, entonces $M/\mathfrak{m}M$ es un κ-espacio vectorial.

Del mismo modo que para grupos y anillos, dada una familia de módulos podemos formar un nuevo módulo *producto*.

***Definición 4.2.23* (producto y suma directa).** — Sea A un anillo y sea $\{M_i\}_{i\in I}$ una familia de A-módulos. El **producto** de los M_i se define como el producto cartesiano $\prod_{i\in I} M_i$ cuyos elementos son los $(m_i)_{i\in I}$ con $m_i \in M_i$, y cuya estructura de A-módulo está dada por

$$(m_i)_{i\in I} + (m_i')_{i\in I} := (m_i + m_i')_{i\in I}$$

y

$$a \cdot (m_i)_{i\in I} := (am_i)_{i\in I}.$$

La **suma directa** de los M_i es el sub-módulo de $\prod_{i\in I} M_i$ dado por

$$\bigoplus_{i\in I} M_i := \left\{ (m_i)_{i\in I} \in \prod_{i\in I} M_i \text{ tales que } m_i = 0 \text{ salvo finitos } i \in I \right\}.$$

Observación 4.2.24. — Si el conjunto de índices $I = \{1, \ldots, r\}$ es finito, entonces $\bigoplus_{i\in I} M_i = \prod_{i\in I} M_i$. En tal caso, dicho módulo es denotado $M_1 \times \cdots \times M_r$ o bien $M_1 \oplus \cdots \oplus M_r$.

4.2.4. Módulos finitamente generados y módulos libres. — El objetivo de esta sub-sección es extender algunas de las nociones de álgebra lineal al contexto de módulos.

Definición 4.2.25. — Sea M un A-módulo y sea $S \subseteq M$ un subconjunto cualquiera. Definimos el **submódulo generado por** S mediante

$$\langle S\rangle_{A-\text{mód}} = \langle S\rangle_A := \left\{ \sum_{\text{finita}} a_i s_i \;\middle|\; a_i \in A, s_i \in S \right\} = \bigcap_{\substack{S\subseteq N \\ N \text{ sub-módulo}}} N,$$

es decir, es el sub-módulo más pequeño de M que contiene a S.

Ejemplo 4.2.26. — Sea $\{M_i\}_{i\in I} \subseteq M$ familia de sub-módulos, entonces

$$\langle \{M_i\}_{i\in I}\rangle_A = \sum_{i\in I} M_i.$$

De manera equivalente, consideremos el morfismo

$$\begin{aligned} \psi : \bigoplus_{i\in I} M_i &\to M \\ (m_i)_{i\in I} &\mapsto \sum_{i\in I} m_i \end{aligned}$$

siendo esta última suma finita, por la definición de suma directa. Entonces, $\sum_{i\in I} M_i = \operatorname{Im}(\psi)$.

Definición 4.2.27. — Sea M un A-módulo y sea $\{M_i\}_{i\in I} \subseteq M$ familia de sub-módulos. Diremos que la familia $\{M_i\}_{i\in I}$ **está en suma directa** si el morfismo

$$\begin{aligned} \psi : \bigoplus_{i\in I} M_i &\to M \\ (m_i)_{i\in I} &\mapsto \sum_{i\in I} m_i \end{aligned}$$

es inyectivo. En otras palabras, si para toda colección finita de $m_i \in M_i$ se tiene que

$$\sum_{\text{finita}} m_i = 0 \text{ implica que } m_i = 0 \text{ para todo } i.$$

En este caso, ψ induce un isomorfismo $\bigoplus_{i\in I} M_i \xrightarrow{\sim} \sum_{i\in I} M_i$.

Observación 4.2.28. — Sea $A = k$ es un cuerpo y $M = V$ un k-espacio vectorial. Entonces, todo sub-espacio no trivial $W \subseteq V$ admite un sub-espacio complementario, es decir, existe un sub-espacio $W' \subseteq V$ tal que $V = W \oplus W'$. Sin embargo, si $A = \mathbb{Z}$, el sub-módulo $N = 2\mathbb{Z}$ de $M = \mathbb{Z}$ **no** posee un suplementario, pues todo $N' \neq \{0\}$ sub-módulo de $\mathbb{Z}$ tiene intersección no nula con $2\mathbb{Z}$.

Notación 4.2.29. — Un caso particular importante del producto y la suma directa de módulos $\{M_i\}_{i\in I}$ es el caso cuando $M_i = A$ para todo $i \in I$. En tal caso, denotamos $A^I := \prod_{i\in I} A$ y $A^{(I)} := \bigoplus_{i\in I} A$. En particular, si $I = \{1, \ldots, r\}$ finito, entonces escribimos A^r o $A^{\oplus r}$.

En general, si $i \in I$, denotamos por e_i al elemento de $A^{(I)}$ con i-ésima coordenada 1 y 0 en todas las otras coordenadas.

Proposición 4.2.30. — *Sea A un anillo e I un conjunto. Entonces,*

1. *Todo elemento de $A^{(I)}$ se escribe de manera única como $\sum_{i\in I} a_i e_i$ para cierta familia $(a_i)_{i\in I}$* casi nula *(i.e., a lo más finitos elementos $\neq 0$) de elementos de A.*
2. Propiedad universal de $A^{(I)}$: *Para todo A-módulo M y toda familia $(m_i)_{i\in I}$ de elementos de M, existe un único morfismo de A-módulos $\psi : A^{(I)} \to M$ tal que $\psi(e_i) = m_i$ para todo $i \in I$.*

Demostración. — La prueba de (1) sigue directamente de la definición de $A^{(I)}$ y los detalles se dejan como ejercicio al lector. La prueba de (2) se obtiene al considerar de manera explícita $\psi(\sum_{i\in I} a_i e_i) := \sum_{i\in I} a_i m_i$. □

La propiedad universal de la suma directa $A^{(I)}$ permite definir en el contexto de módulos las siguientes nociones clásicas de álgebra lineal.

Definición 4.2.31. — Sea $(m_i)_{i\in I} \subseteq M$ una familia de elementos de M y sea $\psi : A^{(I)} \to M$ definido como $e_i \mapsto m_i$ el morfismo asociado. Decimos que la familia es:

1. **linealmente independiente** (o **libre**) si ψ es inyectivo, es decir, si $\sum_{\text{finita}} a_i m_i = 0$ implica que $a_i = 0$ para todo i.
2. **generadora** si ψ es sobreyectivo, es decir, si todo $m \in M$ puede ser escrito como $m = \sum_{\text{finita}} a_i m_i$ para ciertos $a_i \in A$.
3. una **base** si ψ es un isomorfismo, es decir, si todo $m \in M$ se escribe de manera única como $m = \sum_{\text{finita}} a_i m_i$ para únicos $a_i \in A$.

Ejemplo 4.2.32. — Sea $A = \mathbb{Z}$ y $M = \mathbb{Z}$, entonces:

1. La familia $\{2, 3\}$ es generadora (cf. lema de Bézout), pero no es una base, pues $0 = 2 \cdot 3 - 3 \cdot 2$.
2. La familia $\{2\}$ es libre, pero no es generadora.
3. Las únicas bases de M son $\{1\}$ y $\{-1\}$, cuya prueba se deja como ejercicio.

Definición 4.2.33. — Sea M un A-módulo. Diremos que M es un módulo:

1. **finitamente generado** (o **de tipo finito**) si existe una familia generadora finita.
2. **libre** si posee una base. En otras palabras, si $M \cong A^{(I)}$ para cierto conjunto I.

Un resultado fundamental de álgebra lineal es el hecho que todo espacio vectorial sobre un cuerpo posee una base. El siguiente ejemplo ilustra que esto último no es necesariamente cierto en el contexto de módulos.

Ejemplo 4.2.34. — Sea A un anillo.

1. Si $\langle 0\rangle \neq I \subsetneq A$ es un ideal propio, entonces el A-módulo $M := A/I$ **no** es libre. En efecto, si $a \in I \setminus \{0\}$ y $m \in M$, entonces $am = 0$. Esto último implica que no existen familias libres.
2. Sea M es un A-módulo libre finitamente generado de base $\{e_i\}_{i=1,\dots,n}$, y N un A-módulo libre finitamente generado de base $\{f_j\}_{j=1,\dots,m}$. Entonces, para todo $\varphi \in \mathrm{Hom}_A(N, M)$ podemos escribir $\varphi(f_j) = \sum_{i=1}^{n} a_{ij} e_i$ para ciertos $a_{ij} \in A$. Luego $\mathrm{Hom}_A(N, M) \cong M_{n\times m}(A)$.

3. Un endomorfismo inyectivo de un módulo libre finitamente generado **no** es necesariamente sobreyectivo: considerar por ejemplo $A = M = \mathbb{Z}$ y $\varphi(m) = 2m$.
4. No se puede (en general) extraer una base de una familia generadora: considerar por ejemplo $A = M = \mathbb{Z}$ y la familia $\{2, 3\}$.
5. Una familia linealmente independiente no se puede (en general) completar en una base: considerar por ejemplo $A = M = \mathbb{Z}$ y la familia $\{2\}$.

El Teorema 2.4.7 afirma que toda base de un grupo abeliano libre finitamente generado (i.e., $\mathbb{Z}$-módulo libre finitamente generado) posee el mismo cardinal, llamado el rango. El siguiente resultado (que no demostraremos) extiende dicho al contexto de módulos sobre cualquier anillo A.

Teorema 4.2.35. — *Sea M un A-módulo libre finitamente generado. Entonces, todas sus bases son finitas y del mismo cardinal, llamado el* **rango** *de M y denotado* $\mathrm{rg}(M)$. *Más aún, el cardinal de una familia linealmente independiente (resp., generadora) es $\leq$ (resp., $\geq$)* $\mathrm{rg}(M)$.

Ejercicio 4.2.36. — Sean M y N dos A-módulos tales que $N \subseteq M$.

1. Probar que si M es finitamente generado y $N \subseteq M$, entonces M/N es finitamente generado.
2. Probar que si N y M/N son finitamente generados, entonces M es finitamente generado.
3. Sea $A = \mathbb{Z}[x_1, x_2, \ldots] = \mathbb{Z}[x_i, i \in \mathbb{N}^{\geq 1}]$ y $M = A$ (finitamente generado por $\{1\}$). Probar que $N = \{\text{polinomios de término constante nulo}\} \subseteq M$ **no** es finitamente generado.

4.2.5. Teorema de Cayley-Hamilton y Lema de Nakayama. — Recordemos que si $R \in M_{n\times n}(A)$ es una matriz cuadrada, entonces

$$R \cdot {}^{\mathrm{t}}\mathrm{com}(R) = \det(R) \cdot I_n$$

En particular, $R \in \mathrm{GL}_n(A)$ si y sólo si $\det(R) \in A^\times$.

***Teorema 4.2.37* (Cayley-Hamilton).** — *Sea M un A-módulo finitamente generado, y sea $u : M \to M$ un endomorfismo. Sean $m_1, \ldots, m_n$ generadores de M y escribamos $u(m_i) = \sum_{j=1}^n a_{ij} m_j$, donde $R = (a_{ij})_{1\leq i,j\leq n} \in M_{n\times n}(A)$. Sea $P(X) = \det(XI_n - R) \in A[X]$, entonces $P(u) = 0$ en $\mathrm{End}_A(M)$.*

Observación 4.2.38. — Sea M un A-módulo y $u : M \to M$ un endomorfismo. Si $I \subseteq A$ es un ideal tal que $u(M) \subseteq IM$, entonces podemos suponer que $a_{ij} \in I$. En tal caso, si escribimos $P(X) = X^n + c_1 X^{n-1} + \cdots + c_{n-1}X + c_n$,

entonces se tiene que $c_j \in I^j$ para todo $j \in \{1, \ldots, n\}$. Esto último se deja como ejercicio para el lector.

Demostración del Teorema 4.2.37. — El principal ingrediente de la prueba es dotar a M de estructura de $A[X]$-módulo. En efecto, para todo polinomio $Q \in A[X]$ y todo $m \in M$ definimos

$$Q \cdot m := Q(u)(m).$$

En particular, si $Q(X) = X$ entonces $Q \cdot m_i = u(m_i) = \sum_{j=1}^{n} a_{ij} m_j$ para todo $i \in \{1, \ldots, n\}$. Luego, tenemos que

$$(XI_n - R) \cdot \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = 0,$$

donde $(XI_n - R) \in M_{n \times n}(A[X])$ es una matriz con coefientes en $A[X]$. Al multiplicar a la izquierda por ${}^{\mathrm{t}}\mathrm{com}(XI_n - R)$ obtenemos

$$\det(XI_n - R) \cdot \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = 0,$$

donde $\det(XI_n - R) \in A[X]$. Dado que $M = \langle m_1, \ldots, m_n \rangle_{A\text{-mod}}$, tenemos que el polinomio $P(X) = \det(XI_n - R)$ anula todo elemento del $A[X]$-módulo M. En particular, $P(u)$ es nulo sobre M. □

¡Atención! — Si $A = k$ es un cuerpo, el Teorema de Cayley-Hamilton dice que toda matriz cuadrada A, de polinomio característico P_A, verifica $P_A(A) = 0$.

Corolario 4.2.39. — *Sea M un A-módulo finitamente generado. Entonces, todo endomorfismo sobreyectivo de M es biyectivo.*

Demostración. — Sea $f : M \to M$ un endomorfismo sobreyectivo. Tal como en la demostración del teorema de Cayley-Hamilton, dotamos a M de estructura de $A[X]$-módulo al definir $X \cdot m := f(m)$.

Como f es sobreyectivo tenemos que $M = IM$, donde $I = \langle X \rangle$. En efecto, esto último equivale a decir que $M = f(M)$.

Aplicamos Cayley-Hamilton al endomorfismo $u = \mathrm{id}_M$, de donde deducimos

$$0 = P(u) = u^n + c_1 u^{n-1} + \cdots + c_{n-1} u + c_n \mathrm{id}_M$$

en $\mathrm{End}_A(M)$. La Observación 4.2.38 implica que $c_j \in I^j = \langle X^j \rangle$ y en particular para todo c_j existe $d_j \in A[X]$ tal que $c_j = Xd_j$. Luego, para todo $m \in M$ se tiene que

$$\begin{aligned} 0 &= (u^n + c_1 u^{n-1} + \cdots + c_n \mathrm{id}_M)(m) \\ &= m + c_1 \cdot m + \cdots + c_{n-1} \cdot m + c_n \cdot m \\ &= m + c_1(f)(m) + \cdots + c_n(f)(m) \\ &= m + f(d_1(f) + \cdots + d_n(f))(m), \end{aligned}$$

donde la última igualdad se obtiene del hecho que $c_j = Xd_j$. Así, tenemos que $\mathrm{id}_M + f \circ Q(f) = 0$ para cierto $Q \in A[X]$. Finalmente, el endomorfismo $-Q(f) \in \mathrm{End}_A(M)$ es la inversa de f. □

Ejercicio 4.2.40. — Sea M un A-módulo libre de rango n. Demostrar que toda familia generadora de n elementos es una base de M.

Corolario 4.2.41. — *Sea M un A-módulo finitamente generado y sea $I \subseteq A$ un ideal tal que $IM = M$. Entonces, existe $a \in I$ tal que $(1+a)M = 0$.*

Demostración. — La Observación 4.2.38 junto con el teorema de Cayley-Hamilton aplicado al endomorfismo $u = \mathrm{id}_M$ implican que existen $c_j \in I^j$ tales que

$$u^n + c_1 u^{n-1} + \cdots + c_{n-1} u + c_n \mathrm{id}_M = 0.$$

Basta entonces considerar $a := c_1 + \ldots + c_n \in I$. □

Definición 4.2.42 **(radical de Jacobson).** — Sea $A \neq \{0\}$ un anillo. Definimos el **radical de Jacobson** de A como

$$\mathrm{rad}(A) = \bigcap_{\substack{\mathfrak{m} \subseteq A \\ \text{maximal}}} \mathfrak{m},$$

la intersección de todos los ideales maximales de A.

Lema 4.2.43. — *Sea A un anillo no nulo. Entonces*

$$\mathrm{rad}(A) = \{a \in A \mid 1 + ax \text{ es invertible para todo } x \in A\}.$$

Demostración. — Supongamos que $a \notin \mathrm{rad}(A)$. Luego, existe un ideal maximal $\mathfrak{m} \subseteq A$ tal que $a \notin \mathfrak{m}$. En particular, tenemos que $\mathfrak{m} + \langle a \rangle = A$, por lo que existe $m \in \mathfrak{m}$ y $x \in A$ tales que $1 = m + ax$. Dado que $\mathfrak{m} \cap A^\times = \emptyset$, concluimos que $1 + a(-x) \notin A^\times$.

Recíprocamente, si $1+ax$ no es invertible para cierto $x \in A$, entonces $\langle 1+ax\rangle \subsetneq A$ es un ideal propio, y luego está contenido en algún ideal maximal $\mathfrak{m}$ de A. Dado que $1 \notin \mathfrak{m}$, concluimos que $a \notin \mathfrak{m}$. □

Teorema 4.2.44 **(Lema de Nakayama, 1951).** — *Sea A un anillo no nulo y sea $I \subseteq \mathrm{rad}(A)$ un ideal. Para todo A-módulo M finitamente generado se tiene que:*

1. *Si $IM = M$, entonces $M = 0$.*
2. *Sean $m_1 \dots m_n \in M$. Si las imagenes de $m_1, \dots, m_n$ en el cociente M/IM generan dicho A-módulo, entonces $m_1, \dots, m_n$ generan M.*

Demostración. — Para probar (1) observamos que la condición $IM = M$ implica que existe $a \in I$ tal que $(1+a)M = 0$. Dado que $I \subseteq \mathrm{rad}(A)$, el Lema anterior implica que $1+a \in A^\times$ y luego la igualdad $(1+a)M = 0$ implica que $M = 0$.

Para probar (2) consideramos el A-módulo $N := M/(Am_1 \cdots + Am_n)$. Sea $m \in M$. Dado que las imagenes de $m_1, \dots, m_n$ en el cociente M/IM generan dicho A-módulo, podemos escribir

$$m = \sum_{j=1}^{n} a_j m_j \pmod{IM},$$

con $a_j \in A$, es decir, $m \in IM \mod (Am_1 \cdots + Am_n)$. De esto último deducimos que $IN = N$. Dado que N es finitamente generado, el punto (1) aplicado a N implica que $N = 0$ o, equivalentemente, que $M = \langle Am_1 \cdots + Am_n\rangle$. □

Un caso particular muy importante en geometría algebraica donde el Lema de Nakayama adopta una forma particularmente simple es el caso de anillos que poseen un único ideal maximal.

Definición 4.2.45 **(anillo local).** — Un anillo A no nulo es un **anillo local** si existe un único ideal maximal $\mathfrak{m} \subseteq A$. El cuerpo $\kappa = A/\mathfrak{m}$ se llama **cuerpo residual** del anillo local $(A, \mathfrak{m})$.

Corolario 4.2.46 **(Nakayama).** — *Sea $(A, \mathfrak{m})$ un anillo local con cuerpo residual $\kappa = A/\mathfrak{m}$. Sea M un A-módulo finitamente generado, entonces:*

1. *Si $\mathfrak{m}M = M$ entonces $M = 0$.*
2. *Si las imagenes de $m_1, \dots, m_n$ generan el κ-espacio vectorial $M/\mathfrak{m}M$, entonces $M = \langle m_1, \dots, m_n\rangle_{A-\mathrm{mod}}$.*

El siguiente ejemplo, que es la versión topológica de construcciones análogas en geometría algebraica, explica el porqué del adjetivo *local*.

***Ejemplo 4.2.47* (de anillo local).** — Sea $\mathscr{C} = C^0([0,1])$ el anillo de funciones continuas $f : [0,1] \to \mathbb{R}$. Sea $p \in]0,1[$ un punto arbitrario que fijaremos, y consideremos el ideal $I \subseteq \mathscr{C}$ de funciones continuas que se anulan en una vecindad de p.

El cociente $A := \mathscr{C}/I$ es el **anillo de gérmenes** de funciones continuas en p, i.e., identificamos dos funciones si coinciden en una vecindad de p.

Los ideales (resp. ideales maximales) de A corresponden a ideales (resp. ideales maximales) de $\mathscr{C}$ que contienen I. Más aún, si $x \in [0,1]$, entonces

$$\mathfrak{m}_x := \{f \in \mathscr{C} \mid f(x) = 0\}$$

es un ideal maximal. En efecto, si definimos el *morfismo evaluación* $\mathrm{ev}_x : \mathscr{C} \to \mathbb{R}$ mediante $f \mapsto f(x)$, entonces ev_x es un morfismo sobreyectivo y $\mathfrak{m}_x = \ker(\mathrm{ev}_x)$. Luego, el cociente

$$\mathscr{C}/\mathfrak{m}_x \cong \mathbb{R}$$

es un cuerpo, por lo que tenemos que $\mathfrak{m}_x$ es maximal. El Ejercicio 4.2.48 implica que $m_{\mathfrak{p}}$ es el único ideal maximal que contiene a I. En conclusión, el anillo A de gérmenes de funciones continuas en p es un anillo local con ideal maximal $\mathfrak{m}_A := \mathfrak{m}_p/I$ dado por gérmenes de funciones continuas que se anulan en p, y cuyo cuerpo residual está dado por $\kappa = A/\mathfrak{m}_A \cong \mathbb{R}$.

Ejercicio 4.2.48. — Con la notación del ejemplo anterior, probar que todo ideal maximal de $\mathscr{C}$ es de la forma $\mathfrak{m}_x$ para cierto $x \in [0,1]$.

Interpretación geométrica 4.2.49. — El Lema de Nakayama puede ser pensado como un análogo algebraico del teorema de la función inversa. En efecto, con la notación del ejemplo anterior, considerar $A = \mathscr{C}/I$, $M = \mathfrak{m}_A$ y $\mathfrak{m} = \mathfrak{m}_A$. La versión del Lema de Nakayama para anillos locales se dice entonces que si la imagen de ciertas funciones en $M/\mathfrak{m}M = \mathfrak{m}/\mathfrak{m}^2$ generan dicho $\mathbb{R}$-espacio vectorial, entonces generan M. Si $f(t) = \sum_{n\geq 0} a_n(t-p)^n$ es la expansión en serie de Taylor de una función analítica $f \in A$ en torno a p, entonces $f \in \mathfrak{m}$ si y sólo si $a_0 = 0$ y la imagen de f en cociente $\mathfrak{m}/\mathfrak{m}^2$ está dada por $f'(p)$.

4.2.6. Sucesiones exactas y complejos. — Hemos discutido anteriormente que el kernel (resp. el cokernel) de un morfismo de módulos permite medir *que tan lejos* está dicho morfismo de ser inyectivo (resp. sobreyectivo). El área de las matemáticas llamada **álgebra homológica** busca generalizar dichas ideas.

Definición 4.2.50 **(sucesión exacta y complejo)**

Sea $\{M^i\}_{i\in\mathbb{Z}}$ una familia de A-módulos indexada por los enteros, y sea $\{d^i : M^i \to M^{i+1}\}_{i\in\mathbb{Z}}$ una familia de morfismos de A-módulos, estos últimos llamados usualmente *diferenciales*. Diremos que la colección

$$M^\bullet : \cdots \xrightarrow{d^{i-2}} M^{i-1} \xrightarrow{d^{i-1}} M^i \xrightarrow{d^i} M^{i+1} \xrightarrow{d^{i+1}} \cdots$$

es

1. un **complejo** si $d^{i+1} \circ d^i = 0$ para todo $i \in \mathbb{Z}$. En otras palabras, si $\operatorname{Im}(d^i) \subseteq \ker(d^{i+1})$ para todo $i \in \mathbb{Z}$.
2. una **sucesión exacta** si $\operatorname{Im}(d^i) = \ker(d^{i+1})$ para todo $i \in \mathbb{Z}$.

Las sucesiones exactas permites escribir de manera compacta propiedades de morfismos, tal como lo ejemplificamos a continuación.

Ejemplo 4.2.51. — Sean $f : M \to M'$ y $g : M' \to M''$ dos morfismos de A-módulos. Entonces,

1. La sucesión
$$0 \to M' \xrightarrow{f} M$$
es exacta si y sólo si f es inyectivo.
2. La sucesión
$$M' \xrightarrow{f} M \to 0$$
es exacta f es sobreyectiva.
3. La sucesión
$$0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$$
es exacta si y sólo si
   a) f es inyectivo,
   b) g es sobreyectivo, y
   c) $\operatorname{Im}(f) = \ker(g)$.

   En particular, $\operatorname{coker}(f) = M/\operatorname{Im}(f) \cong M''$. Este último tipo de sucesión exacta es sumamente importante, y es llamada una **sucesión exacta corta**.

Ejercicio 4.2.52. — Sea $f : M \to N$ un morfismo de A-módulos. Probar que la sucesión

$$0 \to \ker(f) \to M \xrightarrow{f} N \to \operatorname{coker}(f) \to 0$$

es exacta.

Como es de esperar, no todo complejo define una sucesión exacta. Los grupos de cohomología, permiten medir qué tan lejos está un complejo de ser una sucesión exacta.

Definición 4.2.53 **(cohomología).** — Sea $(M^\bullet, d^\bullet)$ un complejo de A-módulos dado por

$$M^\bullet : \cdots \xrightarrow{d^{i-2}} M^{i-1} \xrightarrow{d^{i-1}} M^i \xrightarrow{d^i} M^{i+1} \xrightarrow{d^{i+1}} \cdots$$

El A-módulo cociente

$$\mathrm{H}^i(M^\bullet) := \frac{\ker(d^i)}{\mathrm{Im}(d^{i-1})}$$

es llamado el i**-ésimo grupo de cohomología** del complejo $(M^\bullet, d^\bullet)$

Observación 4.2.54 **(homología).** — Si en lugar de considerar morfismos $d^i : M^i \to M^{i+1}$ crecientes en los índices, consideramos una familia $\{M_i\}_{i\in\mathbb{Z}}$ de A-módulos junto con una familia de morfismos $\{\partial_i : M_i \to M_{i-1}\}_{i\in\mathbb{Z}}$, entonces la colección

$$M_\bullet : \cdots \xrightarrow{\partial_{i+2}} M^{i+1} \xrightarrow{\partial_{i+1}} M_i \xrightarrow{\partial_i} M_{i-1} \xrightarrow{\partial_{i-1}} \cdots$$

es un **complejo** si $\partial_i \circ \partial_{i+1} = 0$ para todo $i \in \mathbb{Z}$ o, equivalentemente, si $\mathrm{Im}(\partial_{i+1}) \subseteq \ker(\partial_i)$ para todo $i \in \mathbb{Z}$. El A-módulo cociente

$$\mathrm{H}_i(M_\bullet) := \ker(\partial_i)/\,\mathrm{Im}(\partial_{i+1})$$

es llamado el i**-ésimo grupo de homología** del complejo $(M_\bullet, d_\bullet)$.

Así, intuitivamente, las nociones de homología y cohomología son duales una de la otra. Uno de los ejemplos más importantes de homología es la **homología singular** asociada a un espacio topológico X: informalmente, M_i es el A-módulo generado por sub-variedades X_i de dimensión real $i \geq 0$, y el morfismo $\partial_i : M_i \to M_{i-1}$ se obtiene geométricamente al considerar la frontera topológica $\partial_i(X_i) = \partial X_i$.

Definición 4.2.55 **(morfismo de complejos).** — Un morfismo

$$\varphi^\bullet : (M^\bullet, d_M^\bullet) \to (N^\bullet, d_N^\bullet)$$

entre dos complejos $(M^\bullet, d_M^\bullet)$ y $(N^\bullet, d_N^\bullet)$ es una familia de morfismos $\{\varphi^i : M^i \to N^i\}_{i\in\mathbb{Z}}$ compatible con los diferenciales: $\varphi^{i+1} \circ d_M^i = d_N^i \circ \varphi^i$ para

todo $i \in \mathbb{Z}$. En otras palabras, el diagrama

$$\begin{array}{ccccccccccc} M^\bullet: & \cdots & \xrightarrow{d_M^{i-2}} & M^{i-1} & \xrightarrow{d_M^{i-1}} & M^i & \xrightarrow{d_M^i} & M^{i+1} & \xrightarrow{d_M^{i+1}} & \cdots \\ \downarrow{\scriptstyle \varphi^\bullet} & & & \downarrow{\scriptstyle \varphi^{i-1}} & & \downarrow{\scriptstyle \varphi^i} & & \downarrow{\scriptstyle \varphi^{i+1}} & & \\ N^\bullet: & \cdots & \xrightarrow{d_N^{i-2}} & N^{i-1} & \xrightarrow{d_N^{i-1}} & N^i & \xrightarrow{d_N^i} & N^{i+1} & \xrightarrow{d_N^{i+1}} & \cdots \end{array}$$

es conmutativo.

Ejercicio 4.2.56. — Demostrar que un morfismo de complejos $\varphi^\bullet : M^\bullet \to N^\bullet$ induce morfismos

$$\mathrm{H}^i(\varphi^\bullet) : \mathrm{H}^i(M^\bullet) \to \mathrm{H}^i(N^\bullet)$$

entre los respectivos grupos de cohomología, para todo $i \in \mathbb{Z}$.

Complejo de de Rham. — A continuación daremos uno de los ejemplos fundamentales de complejos y de cohomología, el llamado **complejo de de Rham**. Tal como hemos mencionado en la Observación 4.2.54, la cohomología de este complejo debería ser dual a cierta homología. Dicha homología resulta ser precisamente la homología singular, y la relación precisa entre ellas es lo que conocemos como el **teorema de dualidad de Poincaré** (que se escapa de los contenidos tratados en este texto).

***Definición 4.2.57* (formas diferenciales).** — Sea $V \cong \mathbb{R}^n$ un $\mathbb{R}$-espacio vectorial de dimensión n y sea $r \in \mathbb{N}^{\geq 1}$. Denotamos por $\bigwedge^r V^*$ al espacio vectorial de r-formas multilineales alternadas sobre V. Típicamente, si $\ell_1, \ldots, \ell_r$ son formas lineales en V (i.e., elementos de V^*) entonces la r-forma multilineal

$$(x_1, \ldots, x_r) \mapsto \sum_{\sigma \in \mathfrak{S}_r} \varepsilon(\sigma) \ell_1(x_{\sigma(1)}) \ldots \ell_r(x_{\sigma(r)})$$

es alternada, y la denotamos $\ell_1 \wedge \cdots \wedge \ell_r$. Por ejemplo, si $r = 2$ entonces

$$(\ell_1 \wedge \ell_2)(x, y) = \ell_1(x)\ell_2(y) - \ell_1(y)\ell_2(x).$$

Si $(e_1, \ldots, e_n)$ es una base de V y $(e_1^*, \ldots, e_n^*)$ base dual de V^*, entonces los $\{e_{j_1}^* \wedge \cdots \wedge e_{j_r}^*\}_{1 \leq j_1 < \cdots < jr \leq n}$ forman una base de $\bigwedge^r V^*$. En particular, $\dim_{\mathbb{R}} \bigwedge^r V^* = \binom{n}{r}$ y todo elemento $\omega \in \bigwedge^r V^*$ se escribe como

$$\omega = \sum_{1 \leq j_1 < \cdots < j_r \leq n} \omega(e_{j_1}, \ldots, e_{j_r})\, e_{j_1}^* \wedge \cdots \wedge e_{j_r}^*.$$

Si elegimos coordenadas[2] $x_1, \ldots, x_n$ de V y denotamos por $\mathrm{d}x_1, \ldots, \mathrm{d}x_n \in V^*$ sus diferenciales[3], entonces para cada abierto $U \subseteq V$ denotamos por $\Omega^r(U)$ al espacio vectorial de funciones $\omega : U \to \bigwedge^r V^*$ de clase $\mathscr{C}^\infty$. Explícitamente,

$$\Omega^0(U) = \mathscr{C}^\infty(U) = \{f : U \to \mathbb{R} \text{ de clase } \mathscr{C}^\infty\},$$

y todo $\omega \in \Omega^r(U)$ se escribe de la forma

$$\omega(x) = \sum_{1 \leq j_1 < \cdots < j_r \leq n} \omega_{j_1,\ldots,j_r}(x)\, \mathrm{d}x_{j_1} \wedge \cdots \wedge \mathrm{d}x_{j_r},$$

donde $w_{j_1,\ldots,j_r} \in \mathscr{C}^\infty(U)$. Si $A = \mathscr{C}^\infty(U)$ es el $\mathbb{R}$-álgebra de funciones $\mathscr{C}^\infty$ en el abierto U, entonces $\Omega^r(U)$ es un A-módulo cuyos elementos son llamados **r-formas diferenciales** en U.

Así como podemos derivar funciones, podemos definir la derivada *exterior* de una r-forma diferencial.

Definición 4.2.58. — Sea $f \in \mathscr{C}^\infty(U)$. Su **diferencial** $\mathrm{d}f \in \Omega^1(U)$ está dada por

$$\mathrm{d}f(x) = \sum_{j=1}^{n} \frac{\partial f}{\partial x_j}(x)\, \mathrm{d}x_j$$

Más generalmente, si $\omega = \sum \omega_{j_1}, \ldots, \omega_{j_r}\, \mathrm{d}x_{j_1} \wedge \cdots \wedge \mathrm{d}x_{j_r} \in \Omega^r(U)$, entonces definimos su **diferencial exterior** por

$$\mathrm{d}\omega := \sum \mathrm{d}\omega_{j_1,\ldots,j_r} \wedge \mathrm{d}x_{j_1} \wedge \cdots \wedge \mathrm{d}x_{j_r} \in \Omega^{r+1}(U)$$

Diremos que $\omega \in \Omega^r(U)$ es una **forma cerrada** si $\mathrm{d}\omega = 0$, y diremos que es una **forma exacta** si existe $\eta \in \Omega^{r-1}(U)$ tal que $\omega = \mathrm{d}\eta$.

Ejercicio 4.2.59. — Probar que $\mathrm{d}^2 = 0$. En otras palabras, toda forma exacta es una forma cerrada.

Si $A = \mathscr{C}^\infty(U)$ y $\iota : \mathbb{R} \hookrightarrow \mathscr{C}^\infty(U)$ es la inclusión natural de $\mathbb{R}$ en A a través de las funciones constantes, el ejercicio anterior implica que tenemos el siguiente complejo de A-módulos (resp. $\mathbb{R}$-módulos):

$$(\text{resp. } 0 \to \mathbb{R} \xrightarrow{\iota}) \; \Omega^0(U) \xrightarrow{d} \Omega^1(U) \xrightarrow{d} \Omega^2(U) \xrightarrow{d} \ldots \xrightarrow{d} \Omega^n(U) \xrightarrow{d} 0,$$

llamado el **complejo de de Rham**.

---

[2] i.e., una base del espacio dual V^*.

[3] Por definición, $\mathrm{d}x_i(x_1 e_1 + \ldots + x_n e_n) = x_i$.

Definición 4.2.60. — El $\mathbb{R}$-espacio vectorial definido como

$$\mathrm{H}^r_{\mathrm{dR}}(U) := \frac{\ker\{d : \Omega^r(U) \to \Omega^{r+1}(U)\}}{\mathrm{Im}\{d : \Omega^{r-1}(U) \to \Omega^r(U)\}} = \frac{\{r\text{-formas cerradas en } U\}}{\{r\text{-formas exactas en } U\}}$$

es llamado el **r-ésimo grupo de cohomología de de Rham** de U.

Ejemplo 4.2.61. — Veamos algunos ejemplos concretos en dimensión pequeña. Sea $U = \mathbb{R}^n$.

1. Si $n = 1$ y x es una coordenada en $\mathbb{R}$, entonces

$$\Omega^0(\mathbb{R}) = \mathscr{C}^\infty(\mathbb{R}) = \{f : \mathbb{R} \to \mathbb{R} \text{ de clase } \mathscr{C}^\infty\},$$
$$\Omega^1(\mathbb{R}) = \{\omega(x) = g(x)\,\mathrm{d}x,\ g \in \mathscr{C}^\infty(\mathbb{R})\}.$$

   Dado que $\mathrm{d}x \wedge \mathrm{d}x = -\mathrm{d}x \wedge \mathrm{d}x = 0$, tenemos que $\Omega^r(\mathbb{R}) = \{0\}$ para $r > 1$. En general, $\Omega^r(\mathbb{R}^n) = \{0\}$ si $r > n$. En el caso $n = 1$, el complejo de de Rham está dado por

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{R} & \xrightarrow{\iota} & \Omega^0(\mathbb{R}) & \xrightarrow{\mathrm{d}} & \Omega^1(\mathbb{R}) & \longrightarrow & 0 \\ & & & & f & \longmapsto & f'(x)\,\mathrm{d}x & & \end{array}$$

2. Si $n = 2$ y (x, y) son coordenadas en $\mathbb{R}^2$, entonces

$$\Omega^0(\mathbb{R}^2) = \mathscr{C}^\infty(\mathbb{R}^2) = \{f : \mathbb{R}^2 \to \mathbb{R} \text{ de clase } \mathscr{C}^\infty\},$$
$$\Omega^1(\mathbb{R}^2) = \{\omega(x,y) = P(x,y)\,\mathrm{d}x + Q(x,y)\,\mathrm{d}y,\ P, Q \in \mathscr{C}^\infty(\mathbb{R}^2)\},$$
$$\Omega^2(\mathbb{R}^2) = \{\omega(x,y) = g(x,y)\,\mathrm{d}x \wedge \mathrm{d}y,\ g \in \mathscr{C}^\infty(\mathbb{R}^2)\}.$$

   Dado que $\mathrm{d}x \wedge \mathrm{d}y = -\mathrm{d}y \wedge \mathrm{d}x$ y $\mathrm{d}x \wedge \mathrm{d}x = \mathrm{d}y \wedge \mathrm{d}y = 0$, el complejo de de Rham está dado por

$$\begin{array}{ccccccccccc} 0 & \longrightarrow & \mathbb{R} & \xrightarrow{\iota} & \Omega^0(\mathbb{R}^2) & \xrightarrow{\mathrm{d}} & \Omega^1(\mathbb{R}^2) & \xrightarrow{\mathrm{d}} & \Omega^2(\mathbb{R}^2) & \longrightarrow & 0 \\ & & & & f & \longmapsto & \frac{\partial f}{\partial x}\,\mathrm{d}x + \frac{\partial f}{\partial y}\,\mathrm{d}y & & & & \\ & & & & & & P\,\mathrm{d}x + Q\,\mathrm{d}y & \longmapsto & \left(\frac{\partial Q}{\partial y} - \frac{\partial P}{\partial x}\right)\mathrm{d}x \wedge \mathrm{d}y & & \end{array}$$

   donde este último cálculo proviene de

$$\begin{aligned} \mathrm{d}(P\,\mathrm{d}x + Q\,\mathrm{d}y) &= \left(\frac{\partial P}{\partial x}\,\mathrm{d}x + \frac{\partial P}{\partial y}\,\mathrm{d}y\right) \wedge \mathrm{d}x + \left(\frac{\partial Q}{\partial x}\,\mathrm{d}x + \frac{\partial Q}{\partial y}\,\mathrm{d}y\right) \wedge \mathrm{d}y \\ &= \left(\frac{\partial Q}{\partial y} - \frac{\partial P}{\partial x}\right)\mathrm{d}x \wedge \mathrm{d}y. \end{aligned}$$

   Cabe destacar que en este caso, si $f \in \mathscr{C}^\infty(\mathbb{R}^2)$ entonces $\mathrm{d}f$ permite determinar el *rotor* de f dado por $\nabla f = (\frac{\partial f}{\partial x}, \frac{\partial f}{\partial y})$. Del mismo modo, si

asociamos a la 1-forma diferencial $\omega = P\,\mathrm{d}x + Q\,\mathrm{d}y$ el campo vectorial $F = (P, Q)$, entonces $\mathrm{d}\omega$ permite determinar el *rotor* de F dado por $\mathrm{rot}(F) = \frac{\partial Q}{\partial y} - \frac{\partial P}{\partial x}$. Más aún, el hecho que $\mathrm{d}^2 = 0$ se traduce en el conocido hecho de cálculo vectorial que dice que *todo campo gradiente es irrotacional*: $\mathrm{rot}(\nabla f) = 0$.

Luego, el primer grupo de cohomología de de Rham $\mathrm{H}^1_{\mathrm{dR}}(U)$ de un abierto $U \subseteq \mathbb{R}^2$ mide cuántos campos irrotacionales no son gradientes.[4]

Ejercicio 4.2.62. —

1. Describir explícitamente el complejo de de Rham de $\mathbb{R}^3$ y verificar que el diferencial
$$\mathrm{d} : \Omega^2(\mathbb{R}^3) \to \Omega^3(\mathbb{R}^3)$$
permite determinar la *divergencia* del campo vectorial $F = (u, v, w)$ asociado a la 2-forma diferencial $\omega = u\,\mathrm{d}y \wedge \mathrm{d}z + v\,\mathrm{d}z \wedge \mathrm{d}x + w\,\mathrm{d}x \wedge \mathrm{d}y$, la cual está dada por
$$\mathrm{div}(F) = \frac{\partial u}{\partial x} + \frac{\partial v}{\partial y} + \frac{\partial w}{\partial z}.$$
2. El **teorema de Stokes** afirma que si $K \subseteq \mathbb{R}^n$ es una sub-variedad compacta y orientable de $\dim_{\mathbb{R}}(K) = r$ y $\omega \in \Omega^{r-1}(\mathbb{R}^n)$ es una $(r-1)$-forma diferencial, entonces
$$\int_K \mathrm{d}\omega = \int_{\partial K} \omega.$$
Describir explícitamente el enunciado del teorema de Stokes en dimension $n \in \{1, 2, 3\}$ y comparar con los enunciados del teorema fundamental del cálculo ($n = 1$), teorema de Green ($n = 2$) y teorema de Gauss ($n = 3$).

4.2.7. Módulos proyectivos e inyectivos. — Recordemos que si $\varphi : M \to M'$ es un morfismo de A-módulos y N un A-módulo cualquiera. Entonces, el **pullback**
$$\varphi^* : \mathrm{Hom}_A(M', N) \to \mathrm{Hom}_A(M, N)$$
$$f \mapsto f \circ \varphi$$
es un morfismo de A-módulos. Dado que $\mathrm{Hom}_A(\cdot, N)$ *invierte el orden*, decimos que $\mathrm{Hom}(\cdot, N)$ es **contravariante**.

[4] Un resultado clásico de cálculo vectorial señala que todo campo irrotacional es gradiente cuando U es símplemente conexo. De manera mucho más general, el lema de Poincaré afirma que si $U \subseteq \mathbb{R}^n$ es símplemente conexo, entonces $\mathrm{H}^r_{\mathrm{dR}}(U) = \{0\}$ para todo $r > 0$.

Similarmente, el **pushforward**

$$\varphi_* : \mathrm{Hom}_A(N, M) \to \mathrm{Hom}_A(N, M')$$
$$f \mapsto \varphi \circ f$$

es un morfismo de A-módulos. Dado que $\mathrm{Hom}_A(N, \cdot)$ *preserva el orden*, decimos que $\mathrm{Hom}(N, \cdot)$ es **covariante**.

La siguiente proposición detalla cómo se comportan $\mathrm{Hom}_A(\cdot, N)$ y $\mathrm{Hom}_A(N, \cdot)$ respecto a las sucesiones exactas.[5]

Proposición 4.2.63. — *Sea* $0 \to N_1 \xrightarrow{\alpha} N_2 \xrightarrow{\beta} N_3$ *una sucesión exacta y sea* M *un* A*-módulo. Entonces,*

$$0 \to \mathrm{Hom}_A(M, N_1) \xrightarrow{\alpha_*} \mathrm{Hom}_A(M, N_2) \xrightarrow{\beta_*} \mathrm{Hom}_A(M, N_3)$$

es exacta.

Sea $M_1 \xrightarrow{\gamma} M_2 \xrightarrow{\delta} M_3 \to 0$ *una sucesión exacta y sea* N *un* A*-módulo. Entonces,*

$$0 \to \mathrm{Hom}_A(M_3, N) \xrightarrow{\delta^*} \mathrm{Hom}_A(M_2, N) \xrightarrow{\gamma^*} \mathrm{Hom}_A(M_1, N)$$

es exacta.

Demostración. — Probaremos la primera parte de la proposición que concierne a $\mathrm{Hom}_A(M, \cdot)$, pues la demostración para $\mathrm{Hom}_A(\cdot, N)$ es completamente análoga.

Notar que por definición $\beta_* \circ \alpha_* = (\beta \circ \alpha)_* = 0_* = 0$, donde la igualdad $\beta \circ \alpha = 0$ se deduce gracias a la exactitud de la sucesión original. Luego, $\mathrm{Im}(\alpha_*) \subseteq \ker(\beta_*)$.

Veamos que $\ker(\beta_*) \subseteq \mathrm{Im}(\alpha_*)$. Para esto, consideremos $\varphi : M \to N_2$ tal que $\beta \circ \varphi = 0$ (i.e. $\varphi \in \ker(\beta_*)$). Por exactitud de la sucesión original, tenemos

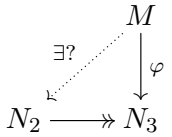
$$\varphi(m) \in \ker(\beta) = \mathrm{Im}(\alpha) \text{ para todo } m \in M.$$

En particular, existe $n = n(m) \in N_1$ tal que $\varphi(m) = \alpha(n)$. Más aún, dicho n es único pues α es inyectivo. Si definimos $\psi : M \to N_1$ como $m \mapsto n = n(m)$ entonces ψ es morfismo de A-módulos, y por definición tenemos que $\alpha(\psi(m)) = \varphi(m)$ para todo $m \in M$. En otras palabras, $\varphi = \alpha_*(\psi)$, de donde se concluye que $\ker(\beta_*) \subseteq \mathrm{Im}(\alpha_*)$.

[5] El método de la prueba de dicha proposición, es lo que se cónoce en álgebra homológica como **cacería de diagramas** (o *diagram chasing*): dado un diagrama conmutativo, una demostración mediante cacería de diagramas implica el uso formal de las propiedades del diagrama, tales como los mapas inyectivos o sobreyectivos, o sucesiones exactas.

Finalmente, $\alpha \circ \psi = 0$ implica que $\psi = 0$, pues α es inyectivo. Luego, $\ker(\alpha_*) = 0$. □

¡Atención! — Si $N_2 \to N_3 \to 0$ es sobreyectivo, **no** necesariamente el morfismo $\mathrm{Hom}_A(M, N_2) \to \mathrm{Hom}_A(M, N_3)$ es sobreyectivo. En efecto, dado $N_2 \twoheadrightarrow N_3$ morfismo sobreyectivo, y $\varphi : M \to N_3$ morfismo de A-módulos, nos gustaría completar el diagrama siguiente



No es difícil notar que esto es imposible para $N_2 = \mathbb{Z} \twoheadrightarrow N_3 = \mathbb{Z}/2\mathbb{Z}$, $M = \mathbb{Z}/2\mathbb{Z}$ y $\varphi : \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ es la identidad, ya que $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}) = \{0\}$.

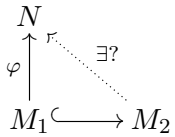
Definición 4.2.64 **(módulo proyectivo).** — Un A-módulo P es **proyectivo** si para todo morfismo sobreyectivo $f : N_2 \twoheadrightarrow N_3$, el pushforward

$$f_* : \mathrm{Hom}_A(P, N_2) \to \mathrm{Hom}_A(P, N_3)$$

es sobreyectivo.

Ejercicio 4.2.65. — Probar que un módulo libre es proyectivo.

¡Atención! — Si $0 \to M_1 \to M_2$ inyectivo, **no** necesariamente el morfismo $\mathrm{Hom}_A(M_2, N) \to \mathrm{Hom}_A(M_1, N)$ es sobreyectivo. En efecto, dado $M_1 \hookrightarrow M_2$ morfismo inyectivo, y $\varphi : M_1 \to N$ morfismo de A-módulos, nos gustaría completar el diagrama siguiente



Es decir, extender el morfismo φ de M_1 a M_2. Sin embargo, esto es imposible para $\iota : M_1 = 2\mathbb{Z} \hookrightarrow M_2 = \mathbb{Z}$ dado por la inclusión, $N = \mathbb{Z}$ y $\varphi : 2\mathbb{Z} \to \mathbb{Z}$ dado por $\varphi(n) = \frac{n}{2}$, puesto que si existiera $\psi : \mathbb{Z} \to \mathbb{Z}$ de tal suerte que el diagrama conmute entonces tendríamos que $2 \mapsto \iota(2) = 2 \mapsto \psi(2) = 2\psi(1) \neq \varphi(2) = 1$.

Definición 4.2.66 **(módulo inyectivo).** — Un A-módulo I es **inyectivo** si para todo morfismo inyectivo $f : M_1 \hookrightarrow M_2$, el pullback

$$f^* : \mathrm{Hom}_A(M_2, I) \to \mathrm{Hom}_A(M_1, I)$$

es sobreyectivo.

Ejercicio 4.2.67. — La noción de módulo inyectivo es muy importante en álgebra homológica, y fue introducida por Baer en 1940. El **criterio de Baer** señala que un A-módulo M es inyectivo si y sólo si todo morfismo de A-módulos $\varphi : I \to M$ desde un ideal $I \subseteq A$ se extiende a un morfismo $\Phi : A \to M$.

Demostrar, usando el criterio de Baer, que $\mathbb{Q}$ es un $\mathbb{Z}$-módulo inyectivo.

4.2.8. Lema de la serpiente. —

Recuerdo 4.2.68. — Sea $f : M \to N$ un morfismo de A-módulos, entonces

$$0 \to \ker(f) \xrightarrow{\iota} M \xrightarrow{f} N \xrightarrow{p} \operatorname{coker}(f) \to 0$$

es una sucesión exacta, donde $\iota : \ker(f) \hookrightarrow M$ es el morfismo de inclusión y $p : N \twoheadrightarrow \operatorname{coker}(f) := N/\operatorname{Im}(f)$ es la proyección canónica al cociente.

El resultado siguiente, conocido comunmente como *lema de la serpiente*, prueba la existencia del llamado *morfismo de conexión*. Esto último es un paso crucial para el estudio de grupos de cohomología en álgebra homológica.

***Lema 4.2.69* (de la serpiente).** — *Sea*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M_1 & \xrightarrow{f} & M_2 & \xrightarrow{g} & M_3 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \\ 0 & \longrightarrow & N_1 & \xrightarrow{f'} & N_2 & \xrightarrow{g'} & N_3 & \longrightarrow & 0 \end{array}$$

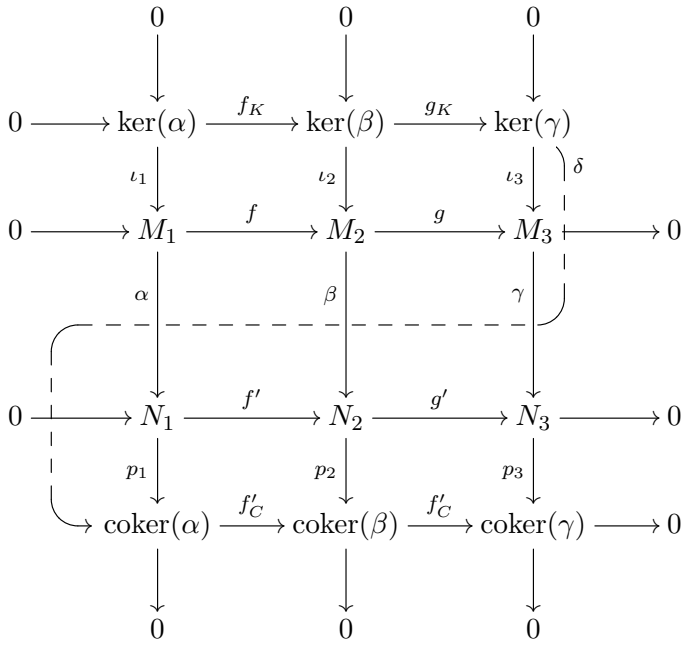
un diagrama conmutativo *de A-módulos , donde las filas son sucesiones exactas cortas. Entonces existe una sucesión exacta*[(6)]

$$0 \to \ker(\alpha) \to \ker(\beta) \to \ker(\gamma) \xrightarrow{\delta} \operatorname{coker}(\alpha) \to \operatorname{coker}(\beta) \to \operatorname{coker}(\gamma) \to 0,$$

donde δ es llamado el morfismo de conexión.

Idea de la demostración. — Como es de esperar, la demostración es mediante cacería de diagramas. Más precisamente, consideramos el diagrama siguiente

(6) Comunmente, una sucesión exacta que no es corta es llamada una *sucesión exacta larga*. Así, el lema de la serpiente puede resumirse en: dado un morfismo entre dos sucesiones exactas cortas, existe una sucesión exacta larga de kernels y cokernels asociada.



donde f_K y g_K (resp. f'_C y g'_C) son morfismos inducidos por f y g a nivel de kernels (resp. inducidos por f' y g' a nivel de cokernels). Por ejemplo, si $m \in \ker(\alpha) \subseteq M_1$ entonces $f(m) \in M_2$ verifica $\beta(f(m)) = f'(\alpha(m)) = 0$, y luego $f(m) \in \ker(\beta)$. Así, el morfismo $f_K(m) := f(m)$ está bien definido.

El *morfismo de conexión*

$$\delta : \ker(\gamma) \to \operatorname{coker}(\alpha)$$

se define a través de la siguiente cacería de diagramas: Sea $m_3 \in \ker(\gamma)$. Dado que g es sobreyectivo, existe $m_2 \in M_2$ tal que $m_3 = g(m_2)$. Más aún,

$$g'(\beta(m_2)) = \gamma(g(m_2)) = \gamma(m_3) = 0,$$

y luego $\beta(m_2) \in \ker(g') = \operatorname{Im}(f')$. En particular, existe $n_1 \in N_1$ tal que $\beta(m_2) = f'(n_1)$. Definimos $\delta(m_3)$ como la imagen de $n_1 \in N_1$ en el cociente $\operatorname{coker}(\alpha) = N_1/\operatorname{Im}(\alpha)$. □

Ejercicio 4.2.70. — Verificar que δ está bien definido y que la sucesión de kernels y cokernels es exacta.

***Observación 4.2.71* (cohomología).** — Si $\varphi^\bullet : M^\bullet \to N^\bullet$ es un morfismo de complejos de A-módulos (ver Definición 4.2.55), entonces el *kernel* $K^\bullet := \{\ker(\varphi^i)\}_{i\in\mathbb{Z}}$ y el *cokernel* $C^\bullet := \{\operatorname{coker}(\varphi^i)\}_{i\in\mathbb{Z}}$ son complejos con

diferenciales inducidos por $M^\bullet$ y $N^\bullet$, respectivamente. Por consiguiente, tiene sentido hablar de *sucesiones exactas* de complejos.

Como mencionamos anteriormente, la principal aplicación del lema de la serpiente es el estudio de grupos de cohomología. Más precisamente, si

$$0 \to L^\bullet \xrightarrow{\alpha^\bullet} M^\bullet \xrightarrow{\beta^\bullet} N^\bullet \to 0$$

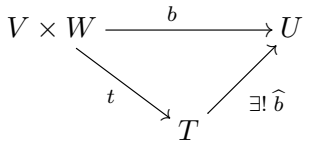
es una sucesión exacta de complejos de A-módulos, entonces el lema de la serpiente implica que existe una sucesión exacta larga

$$\cdots \xrightarrow{\delta^{i-1}} \mathrm{H}^i(L^\bullet) \xrightarrow{\mathrm{H}^i(\alpha^\bullet)} \mathrm{H}^i(M^\bullet) \xrightarrow{\mathrm{H}^i(\beta^\bullet)} \mathrm{H}^i(N^\bullet) \xrightarrow{\delta^i} \mathrm{H}^{i+1}(L^\bullet) \xrightarrow{\mathrm{H}^{i+1}(\alpha^\bullet)} \cdots$$

a nivel de grupos de cohomología, donde los $\{\delta^i\}_{i\in\mathbb{Z}}$ son los *morfismos de conexión* asociados y los $\mathrm{H}^i(\alpha^\bullet), \mathrm{H}^i(\beta^\bullet)$ son los morfismos asociados a α y β (ver Ejercicio 4.2.56).

4.2.9. Producto tensorial de módulos. —

Recuerdo 4.2.72. — Sean V y W dos k-espacios vectoriales. Existe un espacio vectorial $T := V \otimes W$, el cual es único módulo un único isomorfismo, junto con una aplicación bilineal $t : V \times W \to T$ verificando la propiedad universal siguiente: para todo k-espacio vectorial U y toda aplicación *bilineal* $b : V \times W \to U$, existe una única aplicación *lineal* $\widehat{b} : T \to U$ tal que $b = \widehat{b} \circ t$.



En otras palabras,

$$\{b : V \times W \to U \text{ bilineal}\} \cong \mathrm{Hom}_{k\text{-e.v.}}(V \otimes W, U).$$

Esta construcción se extiende *verbatim* al contexto de A-módulos.

***Definición 4.2.73* (forma bilineal).** — Sean M, N, P tres A-módulos. Una aplicación

$$b : M \times N \to P$$

es **A-bilineal** si para todo $m \in M$ (resp. $n \in N$) la aplicación

$$b(m, \cdot) : N \to P \text{ (resp. } b(\cdot, n) : M \to P)$$

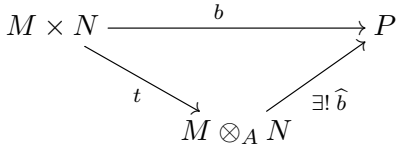
es un morfismo de A-módulos.

Ejemplo 4.2.74. — Sea A un anillo.

1. Si B es un A-álgebra, el producto
$$\begin{aligned} B \times B &\longrightarrow B \\ (b_1, b_2) &\longmapsto b_1 b_2 \end{aligned}$$
es A-bilineal.
2. Si M, N son A-módulos, la aplicación
$$\begin{aligned} M \times \mathrm{Hom}_A(M,N) &\longrightarrow N \\ (m, \varphi) &\longmapsto \varphi(m) \end{aligned}$$
es A-bilineal.

Notación 4.2.75. — Sea A un anillo y sean M, N, P tres A-módulos. Denotaremos por
$$\mathrm{Bil}_A(M \times N, P) := \{b : M \times N \to P \text{ aplicación } A\text{-bilineal}\}$$
al A-módulo de aplicaciones A-bilineales de $M \times N$ en P.

Teorema 4.2.76. — *Sean M, N dos A-módulos. Entonces existe un A-módulo $M \otimes_A N$ dotado de una aplicación A-bilineal*
$$\begin{aligned} t : M \times N &\longrightarrow M \otimes_A N \\ (m,n) &\longmapsto t(m,n) := m \otimes n \end{aligned}$$
verificando que para todo A-módulo P y toda aplicación A-bilineal $b : M \times N \to P$, existe un único morfismo de A-módulos $\widehat{b} : M \otimes_A N \to P$ tal que $b = \widehat{b} \circ t$.



En otras palabras, $\mathrm{Hom}_A(M \otimes_A N, P) \cong \mathrm{Bil}_A(M \times N, P)$. *Más aún, el par $(M \otimes_A N, t)$ es único módulo un único isomorfismo.*

Idea de la demostración. — Considerar el A-módulo libre $A^{(M \times N)}$ con base canónica $\{e_{(m,n)}\}_{(m,n) \in M \times N}$ y cocientar por el sub-módulo
$$\begin{aligned} K = \langle & e_{(m+m',n)} - e_{(m,n)} - e_{(m',n)},\ e_{(m,n+n')} - e_{(m,n)} - e_{(m,n')}, \\ & e_{(am,n)} - a e_{(m,n)} (a \in A),\ e_{(m,an)} - a e_{(m,n)} (a \in A) \rangle_A. \end{aligned}$$
Definimos $M \otimes_A N := A^{(M \times N)}/K$ y $m \otimes n := e_{(m,n)} \mod K$. La aplicación $t : M \times N \to M \otimes_A N$, $(m,n) \mapsto m \times n$ es bilineal por construcción, y verifica la propiedad universal deseada. □

Del mismo modo que para espacios vectoriales, las siguientes propiedades son consecuencia de la construcción anterior y de la propiedad universal del producto tensorial.

Proposición 4.2.77. — *Si M, M', N, N' son A-módulos, entonces:*

1. **Functorialidad:** *Si $\varphi : M \to N$ y $\psi : M' \to N'$ son morfismos de A-módulos, entonces existe un único morfismo de A-módulos*
$$\varphi \otimes \psi : M \otimes_A M' \to N \otimes_A N'$$
tal que $(\varphi \otimes \psi)(m \otimes m') = \varphi(m) \otimes \psi(m')$ para todos $m \in M$, $m' \in M'$.
2. **Propiedades monoidales:** *Hay isomorfismos canónicos*
   a) $A \otimes_A M \xrightarrow{\sim} M,\ a \otimes m \mapsto am$[7].
   b) $(M \oplus M') \otimes_A N \xrightarrow{\sim} (M \otimes_A N) \oplus (M' \otimes_A N),\ (m, m') \otimes n \mapsto (m \otimes n, m' \otimes n)$.
   c) $M \otimes_A N \xrightarrow{\sim} N \otimes_A M,\ m \otimes n \mapsto n \otimes m$.
   d) $M \otimes_A (M' \otimes_A N) \xrightarrow{\sim} (M \otimes_A M') \otimes N,\ m \otimes (m' \otimes n) \mapsto (m \otimes m') \otimes n$.

Ejercicio 4.2.78. —

a) Sea A un anillo y M un A-módulo. Probar que para todo $n \in \mathbb{N}^{\geq 1}$ se tiene que
$$A^n \otimes_A M \cong M^n.$$

b) Sea G un grupo abeliano (i.e., un $\mathbb{Z}$-módulo) finito. Probar que
$$G \otimes_{\mathbb{Z}} \mathbb{Q} = 0.$$

c) Probar que si $m, n \in \mathbb{N}^{\geq 1}$ son coprimos, entonces
$$(\mathbb{Z}/m\mathbb{Z}) \otimes_{\mathbb{Z}} (\mathbb{Z}/n\mathbb{Z}) = 0.$$

d) Sean V_1 y V_2 dos $\mathbb{C}$-espacios vectoriales de dimension > 0. Verificar que los espacios $V_1 \otimes_{\mathbb{C}} V_2$ y $V_1 \otimes_{\mathbb{R}} V_2$ **no** son isomorfos como $\mathbb{R}$-espacios vectoriales.

[7] Con inversa dada por $M \to A \otimes_A M,\ m \mapsto 1 \otimes m$.

COMENTARIOS FINALES

Para finalizar, quisiera señalar algunas referencias que me agradan y que recomiendo a quienes deseen complementar los contenidos desarollados en el presente texto.

1. **Teoría de Categorías**: Ver [**ML98**].
2. **Teoría de Grupos**: Ver [**Suz82, Suz86**], así como el Capítulo II del apunte [**Deb13**].
3. **Teoría de Representaciones**: El Capítulo 2 de este texto está basado en [**Ser77**]. Otra excelente referencia es [**FH91**].
4. **Álgebra conmutativa**: La teoría de anillos conmutativos (i.e., aquella que consideramos principalmente en el Capítulo 3) es llamada también álgebra conmutativa. Recomiendo los textos [**AM69, Rei95**], así como el Capítulo III del apunte [**Deb10**].
5. **Álgebra homológica:** Recomiendo leer [**Eis95, Lan02**] para seguir profundizando en aspectos algebraicos, y [**BT82, Hat02**] para aprender la motivación topológica y geométrica.
6. **Teoría de Galois:** Ver [**Art98**], así como el Capítulo I del apunte [**Deb10**].
7. **Teoría algebraica de números**: Ver [**Sam70**] para una introducción, y [**Neu99**] para profundizar.
8. **Geometría aritmética**: Ver [**Liu02**].
9. **Geometría algebraica**: Una sugerencia (voluntariamente muy acotada) es leer [**Rei88, Har95, Mum95, Per08, Sha13**], así como los apuntes [**Deb99, LP01**].

Espero complementar versiones futuras de este texto con capítulos introductorios a algunos de estos tópicos.

ÍNDICE

A-álgebra, 82
abierto, 95
  Zariski, 95
acción
  cociente por, 31
  de grupo, 30
  fiel, 32
  orbita de, 31
  por conjugación, 34
  punto fijo de, 35
  transitiva, 31
adherencia
  de Zariski, 95
anillo, 18, 81
  de gérmenes, 116
  abeliano, 18, 81
  de polinomios, 82
  local, 115
  noetheriano, 90
  reducido, 88
  unidades $A^\times$, 18, 81
Ascending Chain Condition (ACC), 90
automorfismo, 82
automorfismo exterior, 27
automorfismo interno, 22
centralizador, 34
cerrado, 95
  de Zariski $V(S)$, 91
clase lateral, 22
clases de conjugación, 34
cokernel, 107
congruencia módulo n, 10
conjunto
  generador, 21
  abierto, 95
  algebraico $V(S)$, 91
  cerrado, 95
  de puntos fijos X^G, 35
  parcialmente ordenado, 87
  totalmente ordenado, 88
cuadrado alternado $\bigwedge^2 V$, 64
cuadrado simétrico S^2V, 64
cuerpo, 18, 81
  de p elementos $\mathbb{F}_p$, 12
  de fracciones, 83
  de funciones racionales, 83
  residual, 115
curva elíptica, 47
dominio, 83
endomorfismo, 82
equivalencia
  clase de, 10
  cociente por una relación de, 10
  relación de, 9
espacio proyectivo $\mathbb{P}^{n-1}(k)$, 32
espectro
  de un anillo, 101
  maximal, 99
estabilizador G_x, 31
factores invariantes, 43
factores simples, 51
familia
  base, 111
  generadora, 111

libre, 111
función
regular, 95
función central, 66
functorialidad, 106
fórmula
de clases, 35
Grothendieck, Alexander, 101
grupo
p-grupo, 35
libre finitamente generado, 43
alternante $\mathfrak{A}_n$, 22
cociente, 25
cíclico, 18
de cohomología, 118
de homología, 118
de Klein, 48
de tipo finito, 21
diedral D_n, 20
especial lineal $\mathrm{SL}_n(k)$, 22
finitamente generado, 21
finito, 18
general afín $\mathrm{GA}(V)$, 19
general lineal $\mathrm{GL}_n(k)$, 19
grupo, 17
grupo abeliano, 18
ortogonal $O_n(\mathbb{R})$, 20
simple, 23
simétrico $\mathfrak{S}_n$, 19
grupo de isotropía G_x, 31
Hilbert Nullstellensatz, 93
homomorfismo, 21
ideal, 83
de un subconjunto $\mathfrak{I}(X)$, 94
generado por un elemento, 84
generado por un subconjunto, 85
maximal, 86
primo, 85
producto, 100
radical, 88
suma, 100
imagen, 21
indice de un sub-grupo, 23
intersección
de sub-módulos, 107
inversión, 13
isomorfismo, 82
kernel, 21
lema
de Cauchy, 36
de Bézout, 11
de Schur, 69
de Zorn, 87
monoide, 17
morfismo
automorfismo, 21
de A-álgebras, 82
de anillos, 82
de complejos, 118
de conexión, 125
de grupos, 21
de módulos, 104
endomorfismo, 21
estructural, 82
isomorfismo, 21
pullback, 106, 122
pushforward, 106, 123
regular, 95
módulo, 103
finitamente generado, 111
inyectivo, 124
libre, 111
proyectivo, 124
sub-módulo, 105
generado por un subconjunto, 109
nilradical, 88
orden
relación de, 87
orden de un elemento, 26
permutación, 12
producto
de sub módulos, 109
producto directo, 18
producto tensorial
espacios vectoriales, 61
módulos, 128
programa de Gorenstein, 53
propiedad universal
de A-módulos, 107
de $A^{(I)}$, 110
de los ideales, 84
de un anillo de polinomios, 82
del cociente, 25
proyección canónica, 25
pullback, 96
radical
de Jacobson, 114
radical de un ideal, 88

rango, 43
de un módulo libre, 112
representación
carácter χ_V, 65
de permutación, 56
dual, 67
equivalencia, 55
estándar, 56
grado, 55
irreducible, 59
lineal, 55
morfismo, 57
regular, 56
sub-representación, 57
tabla de caracteres, 78
trivial, 56
semi-grupo, 17
semi-plano de Poincaré, 30
serie de composición, 50
equivalencia, 51
signatura de una permutación $\varepsilon(\sigma)$, 14
sub-espacio
G-estable, 57
G-invariante, 57
sub-grupo
de p-torsión, 40
de Sylow, 37
centro, 20
generado, 20
normal, 23
normalizador de, 38
sub-grupo, 19
subconjunto
multiplicativo, 85
sucesión
complejo, 117
exacta, 117
corta, 117
suma
de sub-módulos, 107
suma directa
de módulos, 109
de módulos
estar en suma directa, 110
teorema
de Sylow, 38
chino del resto, 41, 102
de Cayley, 33
de Cayley-Hamilton, 67, 112
de estructura de grupos abelianos, 45
de Frobenius, 72
de Jordan-Hölder, 51
de la base adaptada, 44
de la base de Hilbert, 90
de Lagrange, 23
de los ceros de Hilbert, 93
de Maschke, 58
de Stokes, 122
topología, 94
de Zariski, 95, 101
transposición, 13
variedad
algebraica
afín, 91
álgebra
de funciones regulares, 96

BIBLIOGRAFIA

[AM69] M. F. Atiyah and I. G. Macdonald. *Introduction to commutative algebra*. Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969.

[Art98] Emil Artin. *Galois theory*. Dover Publications, Inc., Mineola, NY, second edition, 1998. Edited and with a supplemental chapter by Arthur N. Milgram.

[BT82] Raoul Bott and Loring W. Tu. *Differential forms in algebraic topology*, volume 82 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Berlin, 1982.

[Deb99] Olivier Debarre. *Introduction à la géométrie algébrique*. Cours de DEA, `https://www.math.ens.fr/~debarre/DEA99.pdf`, 1999.

[Deb10] Olivier Debarre. *Algèbre 2*. Cours de M1, `https://www.math.ens.fr/~debarre/Algebre1.pdf`, 2010.

[Deb13] Olivier Debarre. *Algèbre 1*. Cours de L3, `https://www.math.ens.fr/~debarre/Algebre2.pdf`, 2013.

[Eis95] David Eisenbud. *Commutative algebra*, volume 150 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995. With a view toward algebraic geometry.

[FH91] William Fulton and Joe Harris. *Representation theory*, volume 129 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1991. A first course, Readings in Mathematics.

[Har95] Joe Harris. *Algebraic geometry*, volume 133 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995. A first course, Corrected reprint of the 1992 original.

[Hat02] Allen Hatcher. *Algebraic topology*. Cambridge University Press, Cambridge, 2002.

[Lan02] Serge Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2002.

[Liu02] Qing Liu. *Algebraic geometry and arithmetic curves*, volume 6 of *Oxford Graduate Texts in Mathematics*. Oxford University Press, Oxford, 2002. Translated from the French by Reinie Erné, Oxford Science Publications.

[LP01] Joseph Le Potier. *Géométrie Algébrique*. Cours de DEA, `https://www.imj-prg.fr/tga/jlp/coursM2_le_potier.pdf`, 2001.

[ML98] Saunders Mac Lane. *Categories for the working mathematician*, volume 5 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1998.

[Mum95] David Mumford. *Algebraic geometry. I*. Classics in Mathematics. Springer-Verlag, Berlin, 1995. Complex projective varieties, Reprint of the 1976 edition.

[Neu99] Jürgen Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[Per08] Daniel Perrin. *Algebraic geometry*. Universitext. Springer-Verlag London, Ltd., London; EDP Sciences, Les Ulis, 2008. An introduction, Translated from the 1995 French original by Catriona Maclean.

[Rei88] Miles Reid. *Undergraduate algebraic geometry*, volume 12 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 1988.

[Rei95] Miles Reid. *Undergraduate commutative algebra*, volume 29 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 1995.

[Sam70] Pierre Samuel. *Algebraic theory of numbers*. Translated from the French by Allan J. Silberger. Houghton Mifflin Co., Boston, Mass., 1970.

[Ser77] Jean-Pierre Serre. *Linear representations of finite groups*. Springer-Verlag, New York-Heidelberg, 1977. Translated from the second

French edition by Leonard L. Scott, Graduate Texts in Mathematics, Vol. 42.

[Sha13] Igor R. Shafarevich. *Basic algebraic geometry. 1.* Springer, Heidelberg, third edition, 2013. Varieties in projective space.

[Suz82] Michio Suzuki. *Group theory. I*, volume 247 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin-New York, 1982. Translated from the Japanese by the author.

[Suz86] Michio Suzuki. *Group theory. II*, volume 248 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, New York, 1986. Translated from the Japanese.